

**From:** [Phuong Fromm](#)  
**To:** [Craig Anderson](#); [Hyun Jim Choi](#)  
**Subject:** FW: California Public Records Act Request: BlueLeaks (Department of Public Safety)  
**Date:** Monday, June 29, 2020 7:23:35 AM

---

Another PRA Request – FYI Only

---

**From:** 96980-16753617@requests.muckrock.com <96980-16753617@requests.muckrock.com>  
**Sent:** Saturday, June 27, 2020 7:49 PM  
**To:** Phuong Fromm <PFromm@sunnyvale.ca.gov>  
**Subject:** California Public Records Act Request: BlueLeaks (Department of Public Safety)

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Department of Public Safety  
PRA Office  
700 All America Way  
Sunnyvale, CA 94086

June 27, 2020

To Whom It May Concern:

Pursuant to the California Public Records Act, I hereby request the following records:

1. Documents mentioning, describing or generated in response to the BlueLeaks release, the preceding hack or subsequent fallout, including but not limited to:

- \* Damage assessments
- \* Emails
- \* Interagency communications (local, state, or federal)
- \* Communications with the press about BlueLeaks
- \* Communications with Twitter or other social media or sharing platforms

2. Documents mentioning or describing Distributed Denial of Secrets (DDoSecrets)

You may limit this request to records generated between November 1, 2018 and the present.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): [96980-16753617@requests.muckrock.com](mailto:96980-16753617@requests.muckrock.com)

Upload documents directly: [https://accounts.muckrock.com/accounts/login/?url\\_auth\\_token=AAAtUTCtQdXLyracyEt6LwWlsc%3A1jpNNh%3AqGkytMsG\\_B35HlxKewQzqc-3vrg&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency\\_login%252Fpolice-department-9569%252Fblueleaks-department-of-public-safety-96980%252F%253Femail%253DPFromm%252540sunnyvale.ca.gov](https://accounts.muckrock.com/accounts/login/?url_auth_token=AAAtUTCtQdXLyracyEt6LwWlsc%3A1jpNNh%3AqGkytMsG_B35HlxKewQzqc-3vrg&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fpolice-department-9569%252Fblueleaks-department-of-public-safety-96980%252F%253Femail%253DPFromm%252540sunnyvale.ca.gov)

[https://accounts.muckrock.com/accounts/login/?url\\_auth\\_token=AAAtUTCtQdXLyracyEt6LwWlsc%3A1jpNNh%3AqGkytMsG\\_B35HlxKewQzqc-3vrg&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency\\_login%252Fpolice-department-9569%252Fblueleaks-department-of-public-safety-96980%252F%253Femail%253DPFromm%252540sunnyvale.ca.gov](https://accounts.muckrock.com/accounts/login/?url_auth_token=AAAtUTCtQdXLyracyEt6LwWlsc%3A1jpNNh%3AqGkytMsG_B35HlxKewQzqc-3vrg&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fpolice-department-9569%252Fblueleaks-department-of-public-safety-96980%252F%253Femail%253DPFromm%252540sunnyvale.ca.gov)

[https://accounts.muckrock.com/accounts/login/?url\\_auth\\_token=AAAtUTCtQdXLyracyEt6LwWlsc%3A1jpNNh%3AqGkytMsG\\_B35HlxKewQzqc-3vrg&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency\\_login%252Fpolice-department-9569%252Fblueleaks-department-of-public-safety-96980%252F%253Femail%253DPFromm%252540sunnyvale.ca.gov](https://accounts.muckrock.com/accounts/login/?url_auth_token=AAAtUTCtQdXLyracyEt6LwWlsc%3A1jpNNh%3AqGkytMsG_B35HlxKewQzqc-3vrg&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fpolice-department-9569%252Fblueleaks-department-of-public-safety-96980%252F%253Femail%253DPFromm%252540sunnyvale.ca.gov)

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News  
DEPT MR 96980  
411A Highland Ave  
Somerville, MA 02144-2516



PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



**From:** [P1 Weekend Rewind](#)  
**To:** [klemos@sunnyvale.ca.gov](mailto:klemos@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:51:01 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [sgorshe@sunnyvale.ca.gov](mailto:sgorshe@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:50:38 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [dklein@sunnyvale.ca.gov](mailto:dklein@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:50:11 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 Why You Should Ditch Your

 World Class Performance Has



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [elarkin@sunnyvale.ca.gov](mailto:elarkin@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:50:06 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices




### Police: Missing girls were never at Milwaukee home set afire


☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 **Why You Should Ditch Your**

 **World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [jdoss@sunnyvale.ca.gov](mailto:jdoss@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:50:01 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices




### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 Why You Should Ditch Your

 World Class Performance Has



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [cabernathy@ci.sunnyvale.ca.us](mailto:cabernathy@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:50:00 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [tgibo@sunnyvale.ca.gov](mailto:tgibo@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:49:55 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [bwilkes@ci.sunnyvale.ca.us](mailto:bwilkes@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:49:22 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou



☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [tfoley@ci.sunnyvale.ca.us](mailto:tfoley@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:54 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [them@ci.sunnyvale.ca.us](mailto:them@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:52 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [aserrano@sunnyvale.ca.gov](mailto:aserrano@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:37 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [tsprayberry@sunnyvale.ca.gov](mailto:tsprayberry@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [cketchum@sunnyvale.ca.gov](mailto:cketchum@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:33 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices




### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 **Why You Should Ditch Your**

 **World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou



☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [skotani@sunnyvale.ca.gov](mailto:skotani@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:28 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [jlockwood@sunnyvale.ca.gov](mailto:jlockwood@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:25 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [Jasselin@sunnyvale.ca.gov](mailto:Jasselin@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:21 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [dodischer@ci.sunnyvale.ca.us](mailto:dodischer@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:13 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [mplonka@ci.sunnyvale.ca.us](mailto:mplonka@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:13 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [joramirez@ci.sunnyvale.ca.us](mailto:joramirez@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:48:11 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices




### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 Why You Should Ditch Your

 World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [mpeel@sunnyvale.ca.gov](mailto:mpeel@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:55 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou



☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [dapang@sunnyvale.ca.gov](mailto:dapang@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:54 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [janton@ci.sunnyvale.ca.us](mailto:janton@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:50 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 Why You Should Ditch Your

 World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [srocheville@sunnyvale.ca.gov](mailto:srocheville@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:45 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

 **Why You Should Ditch Your**

 **World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [ramirez@ci.sunnyvale.ca.us](mailto:ramirez@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:44 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [ssewart@sunnyvale.ca.gov](mailto:ssewart@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [maguirre@ci.sunnyvale.ca.us](mailto:maguirre@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:32 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [bmcmoore@sunnyvale.ca.gov](mailto:bmcmoore@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:30 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou



☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [msmith@sunnyvale.ca.gov](mailto:msmith@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:29 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [aherbert@sunnyvale.ca.gov](mailto:aherbert@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:28 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [kjenks@ci.sunnyvale.ca.us](mailto:kjenks@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:25 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [fmonge@ci.sunnyvale.ca.us](mailto:fmonge@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:24 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [jkirk@ci.sunnyvale.ca.us](mailto:jkirk@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:23 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [schen@ci.sunnyvale.ca.us](mailto:schen@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:23 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices




### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

 Why You Should Ditch Your

 World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [jgalazzo@sunnyvale.ca.gov](mailto:jgalazzo@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:22 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou



☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [atani@ci.sunnyvale.ca.us](mailto:atani@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:21 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [Kdedely@sunnyvale.ca.gov](mailto:Kdedely@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:18 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [rhuihui@ci.sunnyvale.ca.us](mailto:rhuihui@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:16 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [bgantt@sunnyvale.ca.gov](mailto:bgantt@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:09 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [Skuhlmann@sunnyvale.ca.gov](mailto:Skuhlmann@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:47:08 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [dsakurai@ci.sunnyvale.ca.us](mailto:dsakurai@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:46:47 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [sgorshe@ci.sunnyvale.ca.us](mailto:sgorshe@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:46:33 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou



☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [srocheville@ci.sunnyvale.ca.us](mailto:srocheville@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:46:21 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [dchong@ci.sunnyvale.ca.us](mailto:dchong@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:46:16 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [ssimpson@sunnyvale.ca.gov](mailto:ssimpson@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:45 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [cabernathy@sunnyvale.ca.gov](mailto:cabernathy@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:41 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [bmilitano@ci.sunnyvale.ca.us](mailto:bmilitano@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:39 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [jboone@ci.sunnyvale.ca.us](mailto:jboone@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:36 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices




### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 **Why You Should Ditch Your**

 **World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [mirose@sunnyvale.ca.gov](mailto:mirose@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:21 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has



## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou



☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [rcortez@sunnyvale.ca.gov](mailto:rcortez@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:20 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [dswanger@ci.sunnyvale.ca.us](mailto:dswanger@ci.sunnyvale.ca.us)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:13 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to  
☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

Authorities have not yet  
☐ determined the San Jose man's cause of death

 **Why You Should Ditch Your**

 **World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



**From:** [P1 Weekend Rewind](#)  
**To:** [gvierra@sunnyvale.ca.gov](mailto:gvierra@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:12 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

**Why You Should Ditch Your**

**World Class Performance Has**

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [P1 Weekend Rewind](#)  
**To:** [sdrewniany@sunnyvale.ca.gov](mailto:sdrewniany@sunnyvale.ca.gov)  
**Subject:** Cadet death, "BlueLeaks" hack & other top stories  
**Date:** Sunday, June 28, 2020 5:45:04 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 28, 2020 | [View as webpage](#)

## FEATURED CONTENT



### Ga. House passes bill that could dissolve county PDs

The House voted 152-3 to

- ☐ allow voters to decide to eliminate their county police departments, moving authority to county sheriff's offices



### Police: Missing girls were never at Milwaukee home set afire

- ☐ The house was set on fire during unrest that saw three people shot and 10 police officers and a firefighter injured



### Academy cadet dies after training exercise

- ☐ Authorities have not yet determined the San Jose man's cause of death

Why You Should Ditch Your

World Class Performance Has

## Clunky 'Throw' Phones



Read how Sacramento crisis negotiators ditched their clunky 'throw' phones, and why you should too, in this exclusive article. This crisis negotiation

app replaces traditional and expensive communications tools from the past.

[Read the article](#)

## Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

[Learn more](#)



## 'BlueLeaks' exposes files from hundreds of US police departments

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs



## Analysis: What cops need to know about the changes to qualified immunity in Colorado

By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



## My five sense worth on police reform

By Lt. Dan Marcou

☐ We must address some critical issues of grave importance to the survival of our honorable profession



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe](#). Visit our [Customer Support](#) page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** 96980-16753617@requests.muckrock.com  
**To:** PFromm@sunnyvale.ca.gov  
**Subject:** California Public Records Act Request: BlueLeaks (Department of Public Safety)  
**Date:** Saturday, June 27, 2020 7:49:49 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Department of Public Safety  
PRA Office  
700 All America Way  
Sunnyvale, CA 94086

June 27, 2020

To Whom It May Concern:

Pursuant to the California Public Records Act, I hereby request the following records:

1. Documents mentioning, describing or generated in response to the BlueLeaks release, the preceding hack or subsequent fallout, including but not limited to:

- \* Damage assessments
- \* Emails
- \* Interagency communications (local, state, or federal)
- \* Communications with the press about BlueLeaks
- \* Communications with Twitter or other social media or sharing platforms

2. Documents mentioning or describing Distributed Denial of Secrets (DDoSecrets)

You may limit this request to records generated between November 1, 2018 and the present.

I am a member of the news media and request classification as such. I have previously written about the government and its activities, with some reaching over 100,000 readers in outlets such as Gizmodo, MuckRock, Motherboard, Property of the People, Unicorn Riot, and The Outline, among others. As such, as I have a reasonable expectation of publication and my editorial and writing skills are well established. In addition, I discuss and comment on the files online and make them available through non-profits such as the library Internet Archive and the journalist non-profit MuckRock, disseminating them to a large audience. While my research is not limited to this, a great deal of it, including this, focuses on the activities and attitudes of the government itself. As such, it is not necessary for me to demonstrate the relevance of this particular subject in advance.

As my primary purpose is to inform about government activities by reporting on it and making the raw data available, I request that fees be waived.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Emma Best

Filed via MuckRock.com

E-mail (Preferred): 96980-16753617@requests.muckrock.com

Upload documents directly: <https://accounts.muckrock.com/accounts/login/>?

url\_auth\_token=AAAtUTCtQdXLyracyEt6LwW1sc%3A1jpNNh%3AqGkytMsG\_B35HlxKewQzqc-3vrg&next=https%3A%2F%2Fwww.muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency\_login%252Fpolice-department-9569%252Fblueleaks-department-of-public-safety-96980%252F%253Femail%253DPFromm%252540sunnyvale.ca.gov

Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):

MuckRock News  
DEPT MR 96980  
411A Highland Ave  
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.



From: [Homeland Security News Wire](#)  
To: [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)  
Subject: Week in Review  
Date: Saturday, June 27, 2020 9:22 52 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



## Week in Review

BIOMETRICS BORDER/IMMIG. BUSINESS CYBERSECURITY DETECTION DISASTERS GOVERNMENT INFRASTRUCTURE  
PUBLIC HEALTH PUBLIC SAFETY REGIONAL SCI-TECH SURVEILLANCE TERRORISM TRANSPORTATION WATER

Saturday 27 June 2020 vol. 14 no. 126

### Terrorism

#### Growing Terrorism Threats: Iran-backed groups, IS in Africa, and White Supremacists: State Dept. Report

The Trump administration, noting significant victories against global terrorism, says Iran continues to increase its support for extremists, while IS is increasing its presence in Africa and Southeast Asia. Attacks by white supremacists are on the rise, and the terrorism threat posed by white nationalists is of particular concern.

[Read more](#)

#### Terrorism in Europe is Geographically Widespread and Multifaceted

Europol's just-published report shows that in 2019, there were 119 foiled, failed, and completed terrorist attacks in 13 EU member states, and that 1,004 individuals were arrested on suspicion of terrorism-related offenses in 19 EU member states. Nearly all of deaths and 26 injuries were the result of jihadist attacks.

[Read more](#)

### Extremism

#### U.S. Army Soldier Charged with Plotting "Mass Casualty" Attack on His Own Unit

A U.S. Army soldier, 22, has been charged with plotting a mass attack on his unit by sending sensitive military information to the Order of Nine Angles (O9A), a U.K.-based occult-obsessed, neo-Nazi, white supremacist group, the Justice Department announced Monday. O9A has affiliates around the world, including the United States, where they are associated with the neo-Nazi Atomwaffen Division.

[Read more](#)

#### DHS Warns Boogaloo Bois May Be Targeting Washington, D.C.

On Monday, DHS has circulated intelligence memos to law enforcement agencies around the country, warning public safety officials that Boogaloo Bois, an extremist anti-government movement, may be targeting Washington, D.C. for violent attacks. The intelligence assessment stated that "the District is likely an attractive target for violent adherents of the boogaloo ideology due to the significant presence of U.S. law enforcement entities, and the wide range of First Amendment-Protected events hosted here."

[Read more](#)

#### Viruses and Violence: How COVID-19 Has Impacted Extremism

By Stevie Kiesel

In April 2020, the Tony Blair Institute acknowledged that "extremist

groups are beginning to recognize the scale of the COVID-19 pandemic, seeing opportunities to exploit fears, exacerbate tensions and mobilize supporters while government are occupied with trying to address COVID-19.” Extremists across the ideological spectrum have incorporated the pandemic into their messaging and their operations, though groups have differed on just what COVID-19 means and how to best exploit the pandemic and its resultant unrest.

[Read more](#)

#### **Lone wolves**

### **Profiling of Lone-Wolf Terrorists Is Flawed**

Terrorism has typically been considered an organized activity undertaken by networks of individuals who share a collective identity and purpose. However, in recent years, media, law enforcement and scholarly attention has increasingly focused on the construct of the lone terrorist. Researchers say that this approach may be flawed.

[Read more](#)

#### **The Russia connection**

### **Russian Info Ops Putting U.S. Police in Their Crosshairs**

By Jeff Seldin

Russia appears to be intensifying its focus on police enforcement issues in the United States, using popular reactions to protests that have gripped the nation as part of a larger propaganda campaign to divide Americans ahead of the U.S. presidential election in November. For weeks Russia has used state-controlled RT and Sputnik, and social media posts, to spread disinformation about the protests. Only now, it seems that Russia, through the English-language RT in particular, is reaching out to U.S. police officers and union officials, in what some U.S. officials and lawmakers say is an effort to further inflame tensions.

[Read more](#)

#### **China syndrome**

### **Analysts See Shift in EU’s Approach Toward Dealing with China**

By Liyuan Lu

Following a videoconference summit this week between leaders from China and the European Union, European officials released a statement that analysts say is the clearest sign yet that the relationship between the two massive economies is entering a new phase.

[Read more](#)

### **A Selective Retreat from Trade with China Makes Sense for the United States**

By Amitrajeet A. Batabyal

Behind the headlines and politics, a basic question remains: How much benefit is the U.S. getting out of its trade relationship with China? As a scholar in international trade theory and policy, I believe that answer must be looked at through a wider lens than just economics – one that includes national security.

[Read more](#)

#### **Cyberbiosecurity**

### **Preventing Cyberbiosecurity Threats and Protecting Vulnerable Countries**

AI can automate the manipulation of medical datasets, expanding a cyberattack's impact through health and biotech industries. Cyber- and biosecurity threats can erode trust in technology. Eroded trust in technology is dangerous at any time but especially during a global pandemic such as COVID-19.

[Read more](#)

#### **Privacy**

### **How Much Control Would People Be Willing to Grant to a Personal Privacy Assistant?**

CyLab’s Jessica Colnago believes that in the future, the simple act of walking down the street is going to be a little weird. “You know how

every time you enter a website, and it says: ‘We use cookies. Do you consent?’ Imagine that same thing walking down the street, but for a light pole, or a surveillance camera, or an energy sensor on a house,” Colnago says.

[Read more](#)

## **Protecting Children's Online Privacy**

A University of Texas at Dallas study of 100 mobile apps for kids found that 72 violated a federal law aimed at protecting children’s online privacy. Researchers developed a tool that can determine whether an Android game or other mobile app complies with the federal Children’s Online Privacy Protection Act (COPPA).

[Read more](#)

**Truth decay**

## **How Conspiracy Theories Emerge – and How Their Storylines Fall Apart**

New research offers a new way to understand how unfounded conspiracy theories emerge online. The research, which combines sophisticated artificial intelligence and a deep knowledge of how folklore is structured, explains how unrelated facts and false information can connect into a narrative framework that would quickly fall apart if some of those elements are taken out of the mix.

[Read more](#)

## **Who Shares the Most Fake News?**

Facebook is a more fertile breeding ground for fake news than Twitter, and those on the far ends of the liberal-conservative spectrum are most likely to share it, according to new research. “We found that certain types of people are disproportionately responsible for sharing the false, misleading, and hyper-partisan information on social media,” said the lead researcher. “If we can identify those types of users, maybe we can get a better grasp of why people do this and design interventions to stem the transfer of this harmful information.”

[Read more](#)

**First responders**

## **Gear Treated with “Forever Chemicals” Poses Risk to Firefighters**

Firefighters face occupational hazards on a daily basis. Now, new research shows they face additional risk just by gearing up. Fabric used for firefighter turnout gear tested positive for the presence of per- and polyfluorinated alkyl substances (PFAS), according to a new study.

[Read more](#)

**Tunnel evacuation**

## **Sound Beacons Support Safer Tunnel Evacuation**

By Christina Benjaminsen

Research conducted as part of the project EvacSound demonstrates that auditory guidance using sound beacons is an effective aid during the evacuation of smoke-filled road tunnels. This is good news. It is a fact that vehicle drivers and passengers cannot normally expect to be rescued by the emergency services during such accidents.

[Read more](#)

**Flu vaccine**

## **Universal Flu Vaccine May Be More Challenging than Expected**

Some common strains of influenza have the potential to mutate to evade broad-acting antibodies that could be elicited by a universal flu vaccine, according to a study led by scientists at Scripps Research. The findings highlight the challenges involved in designing such a vaccine, and should be useful in guiding its development.

[Read more](#)

**Food security**

## **Coronavirus: A Wake-Up Call to Strengthen the Global Food System**

A new commentary in the journal *One Earth* highlights not only climate-related risks to the global food system, such as drought and floods, but also exposes the coronavirus pandemic as a shock to the system that has led to food crises in many parts of the world. To address the challenges of a globally interconnected food system, a systems approach is required.

[Read more](#)

#### Argument

### Crisis Response When the Status Quo Is a Crisis

As the world experiences a global pandemic in the form of the novel coronavirus, the focus of most governments has understandably been on the health implications of this virus, and on the economic fallout of the lockdowns and other mitigation measures taken to stop its spread. Tellis Bethel and Ian Ralby write that there are two major issues whose careful consideration becomes more necessary by the day: security matters and natural disasters. “If the status quo is a pervasive disaster, how can we cope with incidental or episodic emergencies? Few states, if any, are ready for the challenge,” they write.

[Read more](#)

### Nuclear Alarmism: Proliferation and Terrorism

Alarmism about nuclear weapons is common coin in the foreign policy establishment, John Mueller writes. He notes that during the course of the Cold War, for example, the chief concern was that the weapons would somehow go off, by accident or by intention, devastating the planet in the process. More recently, the worry has been that terrorists would get their hands on nuclear weapons. Concerns about the dangers inherent in nuclear proliferation and in nuclear terrorism certainly seem overwrought, Mueller writes, concluding: “There may be reason for concern, or at least for interest and watchfulness. But alarm and hysteria (not to mention sleeplessness) are hardly called for.”

[Read more](#)

#### Perspective

### Northern Ireland’s Lessons for American Policing

Not that long ago, Americans would regularly go to Northern Ireland to offer advice on reforming the region’s notoriously repressive policing. Martin S. Flaherty writes that happily for Northern Ireland, and tragically for the United States, the lessons now run in the other direction. The 1998 Good Friday Agreement changed Northern Ireland, and one of the major changes was a profound reform of policing methods – and of the police itself: The Royal Ulster Constabulary (RUC), Northern Ireland’s police force, which reflected the Protestant majority almost exclusively, was replaced with the Police Service of Northern Ireland (PSNI), which was much more reflective of Northern Ireland’s society and sensibilities. “None of this is to say that policing in Northern Ireland today lacks problems or critics. But the PSNI is nonetheless widely regarded as a substantial step in the right direction,” Flaherty writes. “Those seeking a hopeful model for change would do well to look to a land where change once seemed hopeless.”

[Read more](#)

#### Our picks this week

### Extremists in the U.S. Military | Russia Targets U.S. Critical Infrastructure | DHS Insider Threat Program, and more

- Soldiers’ Cases Highlight Reach of White Supremacy in U.S. Military
- Far-Right Groups Like the “Boogaloo” and “O9A” Continue to Attract Troops and Veterans
- Facebook Tries to Contain Damage as Verizon Joins Ad Boycott
- “Facebook’s Business Model Is Poison & Its Algorithms Amplify Misinformation”: Digital Forensics Expert Testifies
- White Supremacists Openly Organize Racist Violence on Telegram, Report Finds
- In 2016, Putin Didn’t Expect Trump to Win. Now, He Needs Him

to

- Answer to Energy Storage Problem Could Be Hydrogen
- “Digital Twins” Can Help Monitor Infrastructure and Save Us Billions
- “Sorry, We’re Closed”: Applying Business Models to Failed Terrorist Organizations
- Information Warfare: Iran Receives A Warning Shot
- Far-Right Obsession with Bioterror Could Lead to Work with al-Qaeda, Iran
- Sahara Dust Cloud Looms Over Cuba, Caribbean and Florida
- China is Retooling, and Russia Seeks Harm to Critical Infrastructure
- U.S. Soldier’s Alleged Connection to Satanic Nazi Extremist Group Renews Calls to Ban It
- Neo-Nazi Memoir Describes Terror Group’s Acid-Soaked Ram Sacrifice
- Lawsuit Alleges Scientific Misconduct at U.S. Nuclear Weapons Lab
- How the U.S. military has failed to address white supremacy in its ranks
- Rise in Far-Right and Islamic Extremism Activity in Ireland Last Year, Says Europol
- China Has “First-Strike” Capability to Melt U.S. Power Grid with Electromagnetic Pulse Weapon
- What Are the Key Tenets of China’s Propaganda Regime? – Analysis
- Reading Is Latest in Seven Years of Terrorist Knife Attacks in U.K.
- DHS Insider Threat Program Expanding to Anyone Who Accesses Agency Info
- The Meme-Fueled Rise of a Dangerous, Far-Right Militia
- As Protests Spread to Small-Town America, Militia Groups Respond with Armed Intimidation and Online Threats
- Black Hat Research Predicts Significant Changes to Security Operations Post COVID-19 and Exploit Concerns for 2020 U.S. Election
- What Antifa Is, what It Isn’t, and Why It Matters
- As More Violence Links to Boogaloo Bois, This Is What the Extremist Movement Believes
- Trump Wants to Label Antifa a Terrorist Organization. What About the KKK?
- The Iconoclast Unmasked: The Man Behind Far-Right YouTube Channel
- How to Prepare for the Coronavirus’s Impact on Terrorism
- Reading Fatal Stabbing Suspect Khairi Saadallah Was Known to MI5
- Terror Groups “Exploiting Coronavirus Pandemic to Radicalize New Recruits,” QC Warns
- Team Trump Pushes Antifa Panic Hard on Facebook
- Vehicle Attacks Rise as Extremists Target Protesters
- Black Lives Matter Unrest in U.S. Makes It Easy for Vladimir Putin’s Election Trolls to Spread Fake News
- Russian Operatives Behind Fake Claim that Real IRA Was Recruiting Jihadists
- Russia report: U.K. MPs Condemn “Utterly Reprehensible” delay
- Fighting the Dark Art of Russian Disinformation This Election Season
- The Lapses That Let a Saudi Extremist Shoot Up a U.S. Navy Base

[Read more](#)

## Also noted this week

- The ‘triple dividend’ of early warning systems: evidence from Tanzania’s coastal areas
- How to fight China’s cyber-warriors
- Could Obama have stopped Putin’s election interference? A new

book argues he didn't think he needed to.

- US Cybercom virtual war game girds against increased threats
- New wave of ransomware from Russian-led hackers
- Local de-radicalization programs effectively combat extremism: study
- U.S. Economic Losses from Severe Weather During May Topped \$4 Billion: Aon
- Securing voter registration databases takes on added importance in pandemic, DHS official says
- DDoSecrets' mission is 'unchanged' in wake of 'Blue Leaks' Twitter ban
- Senate Republicans target encryption with bill aimed at Apple, Facebook, other tech giants
- How to fight election cyber attacks while protecting the health of voters during a pandemic
- Trump to suspend foreign work visas for rest of year with some exceptions
- House subpanel offers mixed bag to Solarium Commission
- Dept. of Homeland Security Spied on Protesters in 15+ U.S. Cities
- 5G-Focused Legislation Aims to Improve Security in Military Telecom Infrastructure
- They Were Watching: Homeland Security Reportedly Used Surveillance Aircraft to Monitor George Floyd Protests
- TSA insider faults agency's response to coronavirus
- Trump expected to extend limits on foreign workers
- Al-Qaeda North Africa confirms chief is dead
- Twitter, Facebook see new tactics in foreign disinformation efforts

[Read more](#)

---

BIOMETRICS | BORDER/IMMIG. | BUSINESS | CYBERSECURITY | DETECTION | DISASTERS | GOVERNMENT | INFRASTRUCTURE  
PUBLIC HEALTH | PUBLIC SAFETY | REGIONAL | SCI-TECH | SURVEILLANCE | TERRORISM | TRANSPORTATION | WATER

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



Advertising & Marketing [advertise@newswirepubs.com](mailto:advertise@newswirepubs.com)

Editorial [editor@newswirepubs.com](mailto:editor@newswirepubs.com)

General [info@newswirepubs.com](mailto:info@newswirepubs.com)

2010-2011 © News Wire Publications, LLC News Wire Publications, LLC

220 Old Country Road | Suite 200 | Mineola | New York | 11501

[Permissions and Policies](#)

Homeland Security News Wire, 220 Old Country Road, Suite 200, Mineola, NY 11501

SafeUnsubscribe™ [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)

[Forward email](#) | [Update Profile](#) | [About our service provider](#)

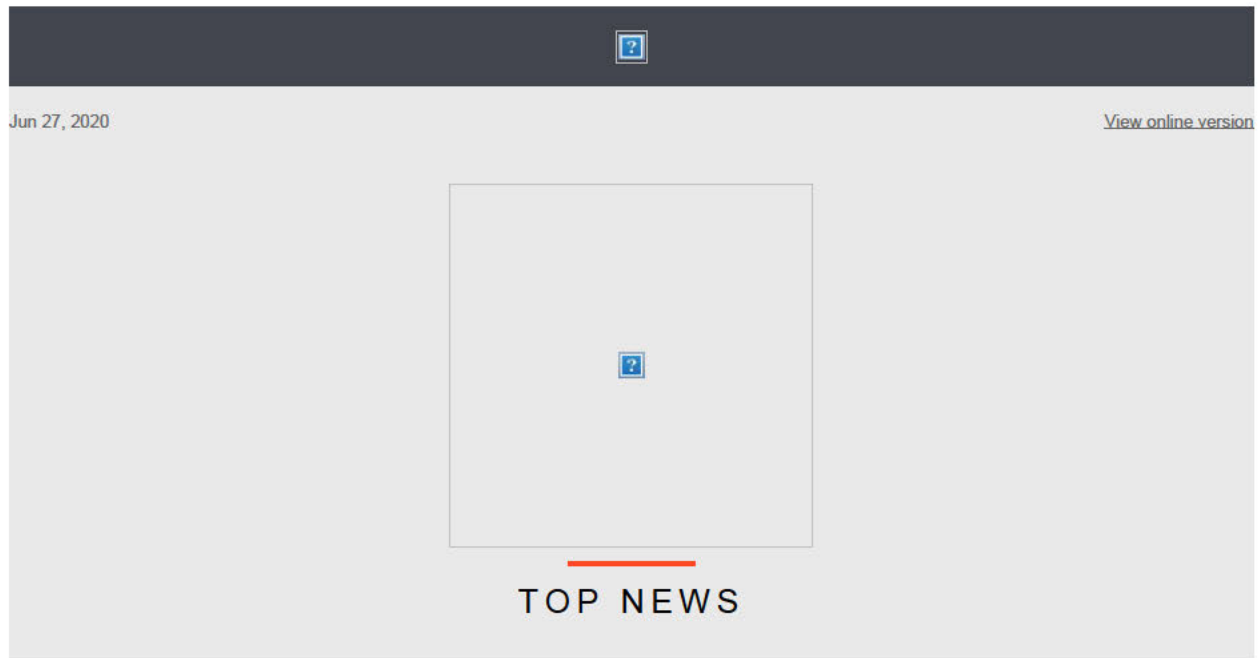
Sent by [hsnewswire@newswirepubs.com](mailto:hsnewswire@newswirepubs.com)



**From:** [Police Top Stories](#)  
**To:** [mirose@sunnyvale.ca.gov](mailto:mirose@sunnyvale.ca.gov)  
**Subject:** Top 5 News & Articles of the Week  
**Date:** Saturday, June 27, 2020 8:05:11 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



### Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

[READ MORE](#)



### Three North Carolina Officers Fired Over Hate Speech

Piner reportedly said he is "ready" for the civil war and martial law he believes is coming, saying, "we are just gonna go out and start slaughtering them..."

[READ MORE](#)



### Minneapolis Takes First Steps Toward Disbanding Police



## Department

The head of the new department would be somebody with "non-law-enforcement experience in community safety services, including but not limited to public health and/or restorative justice approaches."

[READ MORE](#)

---

## NYPD Officers May be Planning July 4 Strike, NY Post Reports

The paper says a pair of flyers making the rounds among NYPD officers are encouraging them to call out sick July 4. "NYPD cops will strike on July 4th to let the city have their independence without cops," the message, which is being passed among cops via text, according to Post sources.

[READ MORE](#)

---



## New Jersey Trooper Thrown from Patrol Vehicle in Horrific Crash

A trooper with the New Jersey State Police trooper was thrown 30 feet from his patrol vehicle in a vehicle collision with a dump truck Monday on the New Jersey Turnpike.

[READ MORE](#)

---

## Rasmussen Poll: Majority of Americans Want to Keep Police

A recent poll conducted by Rasmussen indicates that Americans value the role of the police and worry that increasing criticism of cops will make their communities less safe.

[READ MORE](#)

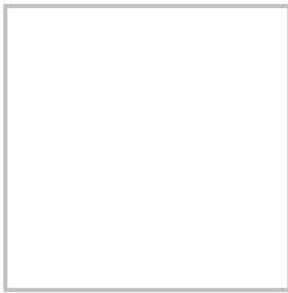
---



## Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

[READ MORE](#)



## Senate Democrats Torpedo GOP's Police Reform Bill

On one major point of dissension between the parties, the Republican bill leaves intact the "qualified immunity" standard that Democrats want to erode, to make it easier for law enforcement officials to be sued for misconduct.

[READ MORE](#)



## Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

[READ MORE](#)



## Mock Lynching of Mannequin in Police Uniform Found in Florida

A mock lynching of a mannequin wearing a police uniform was found hanging over an interstate highway in Florida over the weekend.

[READ MORE](#)





## FREE WHITEPAPERS

---

- ☐ SPECIAL REPORT: Drug Enforcement, Protection & Testing
- ☐ Police and the Coronavirus Pandemic
- ☐ SPECIAL REPORT: Fleet Management & Upfitting
- ☐ Special Report: Preventing & Preparing for Workplace Attacks
- ☐ Best Practices for Setting Up and Implementing a First Responder Network
- ☐ Special Report: Software & Mobile Apps
- ☐ Special Report: Ballistic Protection
- ☐ The Top 5 Emerging Technologies Police Agencies Can't Do Without
- ☐ How Technology Mitigates Threats at Large-Scale Events
- ☐ Special Report: Critical Incident Response
- ☐ Special Report: Upfitting & Fleet Management



## POLICE MAGAZINE

You are currently subscribed as [mirose@sunnyvale.ca.gov](mailto:mirose@sunnyvale.ca.gov). Manage your [email preferences](#).

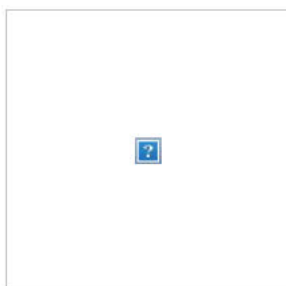
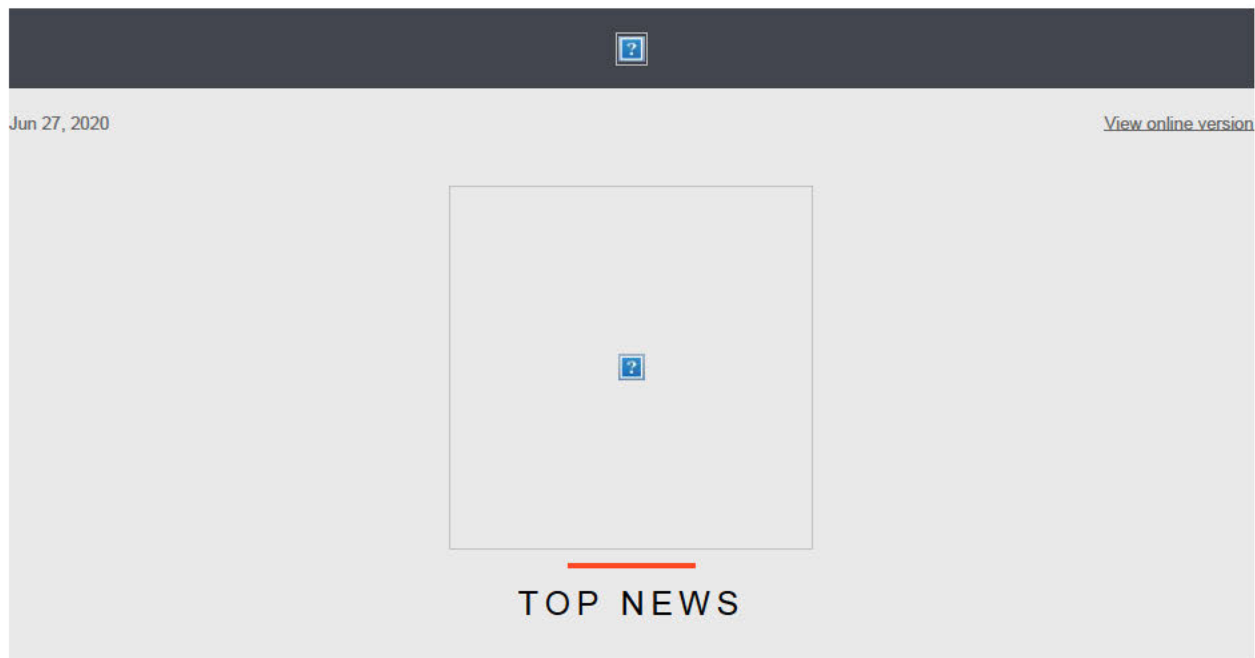
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

[Contact Us](#) | [Privacy Policy](#) | [Unsubscribe](#)

**From:** [Police Top Stories](#)  
**To:** [qviera@ci.sunnyvale.ca.us](mailto:qviera@ci.sunnyvale.ca.us)  
**Subject:** Top 5 News & Articles of the Week  
**Date:** Saturday, June 27, 2020 8:03:53 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



### Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police Department were reportedly ambushed early Saturday morning while responding to a call for service.

[READ MORE](#)



### Three North Carolina Officers Fired Over Hate Speech

Piner reportedly said he is "ready" for the civil war and martial law he believes is coming, saying, "we are just gonna go out and start slaughtering them..."

[READ MORE](#)



### Minneapolis Takes First Steps Toward Disbanding Police

## Department

The head of the new department would be somebody with "non-law-enforcement experience in community safety services, including but not limited to public health and/or restorative justice approaches."

[READ MORE](#)

---

## NYPD Officers May be Planning July 4 Strike, NY Post Reports

The paper says a pair of flyers making the rounds among NYPD officers are encouraging them to call out sick July 4. "NYPD cops will strike on July 4th to let the city have their independence without cops," the message, which is being passed among cops via text, according to Post sources.

[READ MORE](#)

---



## New Jersey Trooper Thrown from Patrol Vehicle in Horrific Crash

A trooper with the New Jersey State Police trooper was thrown 30 feet from his patrol vehicle in a vehicle collision with a dump truck Monday on the New Jersey Turnpike.

[READ MORE](#)

---

## Rasmussen Poll: Majority of Americans Want to Keep Police

A recent poll conducted by Rasmussen indicates that Americans value the role of the police and worry that increasing criticism of cops will make their communities less safe.

[READ MORE](#)

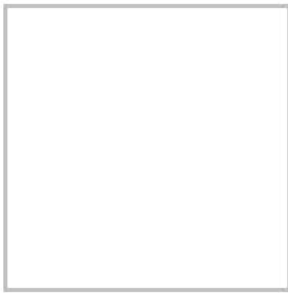
---



## Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

[READ MORE](#)



## Senate Democrats Torpedo GOP's Police Reform Bill

On one major point of dissension between the parties, the Republican bill leaves intact the "qualified immunity" standard that Democrats want to erode, to make it easier for law enforcement officials to be sued for misconduct.

[READ MORE](#)



## Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

[READ MORE](#)



## Mock Lynching of Mannequin in Police Uniform Found in Florida

A mock lynching of a mannequin wearing a police uniform was found hanging over an interstate highway in Florida over the weekend.

[READ MORE](#)







## FREE WHITEPAPERS

---

- ☐ SPECIAL REPORT: Drug Enforcement, Protection & Testing
- ☐ Police and the Coronavirus Pandemic
- ☐ SPECIAL REPORT: Fleet Management & Upfitting
- ☐ Special Report: Preventing & Preparing for Workplace Attacks
- ☐ Best Practices for Setting Up and Implementing a First Responder Network
- ☐ Special Report: Software & Mobile Apps
- ☐ Special Report: Ballistic Protection
- ☐ The Top 5 Emerging Technologies Police Agencies Can't Do Without
- ☐ How Technology Mitigates Threats at Large-Scale Events
- ☐ Special Report: Critical Incident Response
- ☐ Special Report: Upfitting & Fleet Management



## POLICE MAGAZINE

You are currently subscribed as [gvierra@ci.sunnyvale.ca.us](mailto:gvierra@ci.sunnyvale.ca.us). Manage your [email preferences](#).

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

[Contact Us](#) | [Privacy Policy](#) | [Unsubscribe](#)

**From:** [ZDNet](#)  
**To:** [michael.spath](#)  
**Subject:** Microsoft is closing its retail stores permanently  
**Date:** Friday, June 26, 2020 8:00:42 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



## ZDNet Tech Today

June 26, 2020

placeholder



Ex-Intel engineer: Apple turned away from Intel over Skylake CPU bugs



More than 75% of all vulnerabilities reside in indirect dependencies

## Microsoft is closing its physical retail stores

[READ FULL STORY](#)



SpaceX Starlink threat? Democrats propose \$100bn US-wide fiber broadband project

### RELATED

- [I went to a reopened Apple Store and listened to the silence](#)
- [Microsoft completes phase one of porting OpenJDK for Windows 10 on ARM devices](#)
- [Microsoft removes manual deferrals from Windows Update by IT pros 'to prevent confusion'](#)



DDoS botnet coder gets 13 months in prison



IBM mocks a startup and the question is what are you doing, IBM?

---

placeholder



For business customers, Microsoft's Windows 10 documentation is an unruly mess

[READ FULL STORY](#)

placeholder



Ethical contact tracing: How to balance privacy and data gathering

[WATCH THE VIDEO](#)

placeholder



Robotics in business: Everything humans need to know

[READ FULL STORY](#)

placeholder



The ultimate Windows 10 information hub: Everything you need in one place

[READ FULL STORY](#)

---

THIS WEEK ON ZD NET



## Top stories

- [1. BlueLeaks: Data from 200 US police departments & fusion centers published online](#)
- [2. New WastedLocker ransomware demands payments of millions of USD](#)

3. [Windows 10 critical process failure: Microsoft admits June updates are triggering reboots](#)

4. [Adobe wants users to uninstall Flash Player by the end of the year](#)

[See more >](#)



## TechRepublic

1. [What your personal identity and data are worth on the Dark Web](#)

2. [Universities are using clever tech solutions to prep for the fall](#)

3. [William Shatner explores the world of blockchain with new digital trading cards](#)

4. [How to prepare your organization for a global pandemic](#)

[Read more >](#)

IN CASE YOU MISSED IT	
-----------------------	--

# Software developers: We won't take a pay cut just to work remotely

placeholder

Most tech workers wouldn't be happy with Facebook's localized salaries, which are set to take effect next year.

[READ FULL STORY](#)

MORE SPONSORED RESEARCH

## Third party vendor policy

Downloads from [TechRepublic Premium](#)

DOWNLOAD NOW

## IT Hiring Kit: Programmer

Tools & Templates from [TechRepublic Premium](#)

DOWNLOAD NOW

## TechRepublic Real World Guide: Creating a Disaster Plan

eBooks from [TechRepublic Premium](#)

DOWNLOAD NOW

## Feature comparison: E-commerce services and software

Tools & Templates from [TechRepublic Premium](#)

VIEW THIS NOW

This newsletter is a service of ZDNet.com.  
To update your account, please visit our  
Subscription Center.

[Unsubscribe](#) | [Help](#) | [Privacy policy](#)

[Trouble viewing this?](#) [Read Online](#)


Copyright CBS Interactive, Inc.  
All rights reserved. ZDNet is a registered service  
mark of CBS Interactive, Inc.






ZDNet  
235 Second Street  
San Francisco, CA 94105  
U.S.A.




**From:** [Dark Reading Daily](#)  
**To:** [lbargueno@sunnyvale.ca.gov](mailto:lbargueno@sunnyvale.ca.gov)  
**Subject:** Another Record-Breaking DDoS Attack Signals Shift in Criminal Methods  
**Date:** Friday, June 26, 2020 6:08:05 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



Follow Dark Reading:  


June 26, 2020



## LATEST SECURITY NEWS & COMMENTARY

**Another Record-Breaking DDoS Attack Signals Shift in Criminal Methods**  
Malicious botnet sources explode in new attacks that push boundaries in terms of volume and duration.

**7 Tips for Effective Deception**  
The right decoys can frustrate attackers and help detect threats more quickly.

**Criminals Turn to IM Platforms to Avoid Law Enforcement Scrutiny**  
Researchers from IntSights observed a sharp increase in the use of popular instant messaging apps over the past year among threat groups.


**Lucifer Malware Aims to Become Broad Platform for Attacks**  
The recent spread of the distributed denial-of-service tool attempts to exploit a dozen web-framework flaws, uses credential stuffing, and is intended to work against a variety of operating systems.

**Vulnerabilities Declining in Open Source, But Slow Patching Still a Problem**  
Even as more code is produced, indirect dependencies continue to undermine security.

**Contact Tracing & Threat Intel: Broken Tools & Processes**  
How epidemiology can solve the people problem in security.

**Better Collaboration Between Security & Development**  
Security and development teams must make it clear why their segment of the development life cycle is relevant to the other teams in the pipeline.

MORE NEWS & COMMENTARY



## HOT TOPICS

**'GoldenSpy' Malware Hidden in Tax Software Spies on Companies Doing Business in China**  
Advanced persistent threat (APT) campaign aims to steal intelligence secrets from foreign companies operating in China.

**Long-Term Effects of COVID-19 on the Cybersecurity Industry**  
The maelstrom of change we're going through presents a unique opportunity to become enablers. And to do that requires flexibility.

**What Will Cybersecurity's 'New Normal' Look Like?**

## EDITORS' CHOICE

**10 Tips for Maintaining Information Security During Layoffs**  
Insider cyberthreats are always an issue during layoffs -- but with record numbers of home-office workers heading for the unemployment line, it has never been harder to maintain cybersecurity during offboarding.

**Black Hat Survey: Breach Concerns Hit Record Levels Due to COVID-19**  
Annual "Black Hat USA Attendee Survey" indicates unprecedented concern over possible compromises of enterprise networks and US critical infrastructure.

## NEW FROM THE EDGE

**How to Wring Every Last Drop Out of Your Security Budget**  
In the face of tighter budgets and lowered spending forecasts due to the pandemic, optimizing and improving the efficiency of security programs -- without sacrificing integrity -- has never been more important.

## Tech Resources

**7 Experts on Database Security**

**Case Study: Scaled Up InfoSec Risk & Compliance**

**How to Find the Right Management for Your Cloud**

**If Not Now, When?**

**2020 Predictions in Application Security, Data Privacy, and Artificial Intelligence**

**Dartmouth Transforms the Campus Experience with AI-Driven Insight and Automation**

**Cybersecurity for Remote Workers: How to Secure Every Device, Everywhere**

ACCESS TECH LIBRARY NOW

**Why Performance Testing is More Critical Today**  
In this InformationWeek webinar, experts will help enterprise teams understand what they should expect from performance testing solutions and how to put them to work most efficiently.

**Enabling a Smooth DX Transformation in the Post-Pandemic New Tomorrow**

The coronavirus pandemic has forced changes for much of the business world, cybersecurity included. What can we expect going forward?

[MORE](#)

The winding down of COVID-19 has everyone pondering The New Tomorrow, and no doubt you will be reviewing the state of your current networks and networking plans created previously. This likely means transforming your network architectures and security strategies, which ...

[MORE WEBINARS](#)



## FEATURED REPORTS

[The New Face of IT Automation](#)

[Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR](#)

[MORE REPORTS](#)

## CURRENT ISSUE



**How Cybersecurity Incident Response Programs Work (and Why Some Don't)**

[DOWNLOAD THIS ISSUE](#)

[SUBSCRIBE NOW](#)

[BACK ISSUES](#) | [MUST READS](#) | [TECH DIGEST](#)

## PRODUCTS & RELEASES

[Authomize Secures \\$6M Seed Funding for Automated Authorization and Security](#)

[WatchGuard Technologies Report Finds Two-Thirds of Malware is Encrypted, Invisible Without HTTPS Inspection](#)

[Armorblox Announces Box and Slack Integrations to Protect Remote Workforces Across Communication Platforms](#)

[MORE PRODUCTS & RELEASES](#)

## Dark Reading Daily

— Published By [Dark Reading](#)

Informa Tech

303 Second St., Suite 900 South Tower, San Francisco, CA 94107

To update your profile, change your e-mail address, or unsubscribe, [click here](#).

To opt-out of any future Dark Reading Daily Newsletter emails, please respond [here](#).

Thoughts about this newsletter? [Give us feedback](#).

## Keep This Newsletter Out Of Your SPAM Folder

Don't let future editions go missing. Take a moment to add the newsletter's address to your anti-spam white list:

If you're not sure how to do that, ask your administrator or ISP. Or check your anti-spam utility's documentation.

We take your privacy very seriously. Please review our [Privacy Statement](#).



**From:** [CLA Public Section](#)  
**To:** [Melissa Tronquet](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, June 26, 2020 3:12:40 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive](#) (999,909 articles)



[North America](#) | [Global](#)

**USA**

[North America](#)

[Employee Benefits & Pensions](#)



### **The place of private equity in a 401(k) plan's investment lineup**

**DLA Piper**

Fiduciaries of defined benefit pension plans have increasingly used alternative asset classes as a part of the plan's overall investment portfolio in...

### **IRS Releases Anticipated Expanded Guidance on Retirement Plan Provisions of the CARES Act**

**Michael Best & Friedrich LLP**

The CARES Act, passed just under three months ago, contained various provisions designed to offer certain relief to retirement plan sponsors and...

### **What Employers Should Know about ACA Shared Responsibility Payments**

**Proskauer Rose LLP**

A recently released redacted report from the Treasury Inspector General for Tax Administration (TIGTA) offers some helpful insights for employers who...

### **IRS Issues Proposed Regulations for Tax-Exempt Organizations Paying Excess Executive Compensation**

**Jackson Lewis PC**



The IRS issued proposed regulations under Section 4960 of the Internal Revenue Code of 1986, as amended (the “Code”), which was added as part of the...

---

### **The Good Parts of the New Rules Regarding Distributions from IRA and Plan Interests**

**Dickinson Wright**

The SECURE ACT (Setting Every Community Up for Retirement Enhancement Act) was included as part of the massive December 2019 appropriations bill. The...

---

### **Additional Guidance for Coronavirus-Related Distributions and Loans**

**Baker McKenzie**

On June 19, 2020, the IRS released Notice 2020-50 (the Notice) which provides additional guidance on tax-favored distributions from retirement plans...

---

### **Proposed Treasury Regulations Provide Potential Compensation Excise Tax Relief for Foundations Related to Business Organizations**

**Baker & Hostetler LLP**

Proposed Treasury Regulations published earlier this month contain limited relief for tax-exempt entities. If followed carefully, those regulations...

---

### **IRS Expands Eligibility for Coronavirus-Related Retirement Plan Distributions, Loans, and Loan Suspensions Under the CARES Act**

**Winston & Strawn LLP**

On June 19, 2020, the Internal Revenue Service (IRS) issued Notice 2020-50, which makes a number of updates and clarifications for plan sponsors and...

---

### **IRS Eases COVID Distribution Rules: More Individuals Can Withdraw or Borrow From Retirement Accounts**

**Nelson Mullins Riley & Scarborough LLP**

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) permitted coronavirus-related distributions (CRDs) from qualified retirement...

---

### **LGBTQ Title VII Ruling May Impact Your Employee Benefit Plan**

**McDermott Will & Emery**

Bostock definitively states that Title VII’s prohibition against employment discrimination “because of ... sex” bars not only discrimination based on...

---

### **COVID-19: Impact on Benefits & Other Issues | Webinar**

**Graydon Head & Ritchey LLP**

Last week, Graydon’s Lyndsey Barnett, Employee Benefits and Executive Compensation attorney partnered with VonLehman CPA & Advisory Firm and Joanna...

---

### **Zombie PCORI Fee III - The Form Rises**

**Graydon Head & Ritchey LLP**

As discussed in our prior blog posts, the PCORI fee, thought dead in 2019, was

reinstated and the amount updated. Knowing the new fee amount of \$2.54...

---

### **New Legislation Includes Employee Benefits Changes: Why M&A Practitioners Should 'CARE'**

**Morgan Lewis**

Financial assistance and other relief provided to employers under the Coronavirus Aid, Relief, and Economic Security Act (the CARES Act) will have a...

---

### **Is an Italy Pension Taxable in the US? FBAR & FATCA**

**Golding & Golding**

As with many foreign countries, the Italian pension system follows the common three (3) Pillar structure, which combines State, Occupational, and...

---

### **Qualified Retirement Plan Updates: The Changing Landscape for Communication with Participants**

**Schulte Roth & Zabel LLP**

In February 2020, the U.S. Supreme Court issued a ruling that narrowed the definition of "actual knowledge" in a case that focused on the electronic...

---

### **IRS Expands Definition of Qualified Individual for Loans and Coronavirus-Related Distributions under the CARES Act**

**Haynes and Boone LLP**

Notice 2020-50 provides additional guidance to taxpayers and sponsors of qualified retirement plans regarding coronavirus-related distributions and...

---

### **IRS Issues Helpful Guidance for Retirement Plans Under the CARES Act**

**Bradley Arant Boult Cummings LLP**

The Internal Revenue Service (IRS) recently issued Notice 2020-50 to provide retirement plans with guidance under the Coronavirus Aid, Relief, and...

---

## **Employment & Labor**



### **Preparing your workforce: how to avoid legal landmines when bringing employees back**

**McDermott Will & Emery**

The COVID-19 pandemic has put unprecedented strain on organisations of all sizes across all industries. The uncertainty of the new normal is...

---

### **Employment & Labor in Texas**

Texas

**Ogletree Deakins**

A structured guide to employment and labor law in Texas

---

### **Employment & Labor in New Mexico**

New Mexico

**Holland & Hart LLP**

A structured guide to employment and labor law in Mexico

---

### **Employment & Labor in Ohio**

Ohio

### **Taft Stettinius & Hollister LLP**

A structured guide to employment and labor law in Ohio

---

### **Employment and labor law in Tennessee** Tennessee

#### **Bass, Berry & Sims PLC**

A structured guide to employment and labor in Tennessee

---

### **U.S. Supreme Court Rules that Workplace Discrimination on the Bases of Sexual Orientation and Gender Identity is Prohibited Under Title VII**

#### **Foster Swift Collins & Smith PC**

In a significant ruling that has major implications for employers and employees, the U.S. Supreme Court, in the case of *Bostock v. Clayton County*...

---

### **Coming July 1: What Chicago employers need to know about the new paid sick leave, minimum wage and fair workweek rules** Illinois

#### **Thompson Coburn LLP**

The City of Chicago has revised its paid sick leave and minimum wage rules, amended its paid sick leave ordinance, passed a COVID-19 anti-retaliation...

---

### **Supreme Court to Resolve CFAA Circuit Split**

#### **McGuireWoods LLP**

Following an FBI sting, police sergeant Nathan Van Buren was convicted under the federal Computer Fraud and Abuse Act ("CFAA") for selling license...

---

### **Nobody Gets Antibody (Testing): EEOC Forbids Employers from Using Antibody Testing for Re-Entering Workplace**

#### **Bradley Arant Boult Cummings LLP**

The EEOC just amended its Q&A document on COVID-19 testing to address what COVID-19 testing employers can require. At this time (and it could change) ...

---

### **Supreme Court Rules Title VII Prohibits Discrimination Based Upon Sexual Orientation and Transgender Status - Part II**

#### **Breazeale Sachse & Wilson LLP**

On Monday I sent out an update that the U.S. Supreme Court had ruled that an employer who fires an employee for being gay or transgender violates...

---

### **Appeals court rejects AFL-CIO suit seeking to compel OSHA to issue COVID-19 emergency temporary standard** District of Columbia

#### **Reed Smith LLP**

On May 18, the AFL-CIO filed a petition for a writ of mandamus in the U.S. Court of Appeals for the District of Columbia Circuit to compel the...

---

### **Indiana Enters Stage 4 of Reopening Plan** Indiana

#### **Jackson Lewis PC**

Indiana continues to move through its five-stage, "Back on Track" plan to reopen the state. Stage 4 is set to begin on June 12, 2020. With certain...



---

## **OSHA issues new guidance on face coverings in light of COVID-19**

### **Thompson Coburn LLP**

As businesses adjust in response to COVID-19 and, in some cases, reopen after a temporary closure, issues may arise related to face covering...

---

## **What California Employers Should Know About Face Coverings** California

### **Jackson Lewis PC**

On June 18th the California Department of Public Health issued guidance broadly mandating that individuals in California wear face coverings in most...

---

## **Maryland Sexual Harassment Reporting Requirements About to Take Effect**

Maryland

### **Vedder Price PC**

Maryland's Disclosing Sexual Harassment in the Workplace Act (the "Act") became law on October 1, 2018. The Act prohibits employers, regardless of...

---

## **COVID-19 Whistleblower Protection Bill Introduced Into Congress**

### **Proskauer Rose LLP**

On June 15, 2020, Senator Kamala Harris and Representatives Jackie Speier and Jamie Raskin introduced the COVID-19 Whistleblower Protection Act (the...

---

## **COVID-19 Agency Update: OSHA Issues Guidance on Reopening for Non-Essential Businesses; EEOC Addresses Antibody Testing and Reasonable Accommodations, Harassment and Discrimination; SBA Provides New PPP Application**

### **Shawe Rosenthal LLP**

Several federal agencies have recently issued additional COVID-19 guidance of interest to employers, including the Occupational Safety and Health...

---

## **U.S. Supreme Court's Rules That Title VII Protects LGBT Workers, Likely To Expand The EEOC's Eye On Employers**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In a landmark decision for gay and transgender employees, the U.S. Supreme Court held in *Bostock v. Clayton County, Georgia*, No...

---

## **Nothing Comes Close To The Golden Coast: California Requires Masks** California

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: As counties begin loosening local restrictions and summer approaches, and in an effort to preempt a rise in COVID-19 cases, the...

---

## **Top Five Labor Law Developments for May 2020**

### **Jackson Lewis PC**

The National Labor Relations Board (NLRB) implemented several parts of its new election rule that were not enjoined by a federal district court judge...

---

## **DOT extends period for remote interviews after positive drug test results**

### **Constangy Brooks Smith & Prophete LLP**

The increased flexibility will be in effect through September 30. The U.S. Department of Transportation has extended the period during which...

---

### **Supreme Court Rules that Title VII Protects LGBT Workers**

#### **Graydon Head & Ritchey LLP**

Until today, June 15, 2020, the question of whether federal law prohibits discrimination against gay, lesbian, and transgender employees was...

---

### **Expanding the definition of sex: SCOTUS rules employers cannot discriminate based on sexual orientation or gender identity.**

#### **Reed Smith LLP**

On June 15, 2020, the U.S. Supreme Court issued a landmark decision in *Bostock v. Clayton County, Georgia*, No. 17-1618 (U.S. Jun. 15, 2020), which...

---

### **DHS Extends Guidance Relaxing Form I-9 Requirements until July 19**

#### **Greenberg Traurig LLP**

In March 2020, the Department of Homeland Security (DHS) issued revised guidance on I-9 compliance in light of employer office closures around the...

---

### **Question of the Day: COVID-Related Lawsuit Protection**

Iowa

#### **Fredrikson & Byron PA**

As the economy continues to reopen, businesses—even those taking all appropriate precautions—have questioned what liability they may face if COVID...

---

### **NLRB moves ahead with new election regs that were not blocked by federal judge**

#### **Constangy Brooks Smith & Prophete LLP**

The National Labor Relations Board has announced that it will move forward with parts of its new election regulations that were not blocked by a May...

---

### **THE NAME OF THE GAME IS THE FRAME**

#### **Graydon Head & Ritchey LLP**

Yesterday's historic decision by the United States Supreme Court in *Bostock v. Clayton County* is welcome news to supporters of LGBTQ rights...

---

### **The Big EZ? SBA Forgiveness Applications Are Revised, Not Revamped**

#### **Adams and Reese LLP**

On June 17, the Small Business Administration (SBA) released two new Paycheck Protection Program (PPP) loan-forgiveness application forms. The first...

---

### **Mexico Defeats Half a Billion ISDS Arbitration Claim Under NAFTA**

#### **Tereposky & DeRose LLP**

The Claimant alleged that his investment in a telecommunications company called Tele Fácil México S.A. De C.V. (Tele Fácil) had been unlawfully...

---



## **New York State Reduces Amount of Required Paid Voting Leave**

New York

### **Davis Wright Tremaine LLP**

Less than a year after expanding its Election Law, New York State returns to its prior requirement that employers provide employees with two hours of...

---

## **Supreme Court Rules LGBTQ Workers are Protected from Job Discrimination**

### **Loeb & Loeb LLP**

In a landmark decision, the U.S. Supreme Court ruled that a worker's sexual orientation or gender identity cannot be the basis of employment...

---

## **COVID-19 compliance forecast: What comes next for key industries?**

### **PRO Compliance**

Lexology PRO Compliance speaks to compliance leaders from the healthcare, financial services, insurance, IT and commercial sectors on what to expect from the new "business as usual" and enforcement. Conduct reviews, increased regulatory scrutiny and long-term digitisation are some key issues for compliance teams to prepare for.

---

## **Do You Have To Bargain With Your Predecessor's Union After You Bid On And Win A Contract?**

### **Barnes & Thornburg LLP**

Successor issues often pop up in the context of a sale or merger, including under labor law. Some may be surprised to learn that these issues also...

---

## **New Mask Requirements in Texas**

Texas

### **Littler Mendelson PC**

Between June 17 and June 19, 2020, four counties in Texas issued orders mandating that businesses develop and implement a "Health and Safety Policy"...

---

## **2020 Deferred Compensation Elections May be "Cancellable" Under New IRS Guidance**

### **Michael Best & Friedrich LLP**

While many aspects of Friday's IRS Notice on CARES Act provisions were anticipated (e.g., the expansion of the list of individuals who can qualify to...

---

## **New EEOC COVID-19 Guidance Updates Accommodation Obligations and Warns Against Return-to-Work Age and Pregnancy Discrimination and Harassment of Workers of Asian Descent**

### **Epstein Becker Green**

With regulators and lawmakers struggling to address the new wave of issues arising from employers reopening and bringing employees back to their...

---

## **COVID-19 Relief Triggers ERISA Participant Notice Requirements**

### **Kelley Drye & Warren LLP**

In response to the COVID-19 outbreak, Congress, the Department of Labor ("DOL") and the Internal Revenue Service ("IRS") have each offered temporary...

---

## **Facebook's New Content Moderation Appeals Process**

### **Crowell & Moring LLP**

Stung by repeated criticisms of content moderation decisions in which it either acted or refused to act to remove controversial content such as...

---

## **Trump Suspends Immigration to Remove "Competition" From U.S. Unemployed**

### **McCarter & English LLP**

Citing the overall unemployment rate in the United States, President Trump issued an expanded version of Proclamation 10014, titled "Suspension of...

---

## **SCOTUS: Discrimination Based on Sexual Orientation or Transgender Status is Sex Discrimination And Violates Federal Law**

### **FisherBroyles LLP**

An employer who fires or takes an adverse action against an individual merely for being gay or transgender violates Title VII of the Civil Rights Act...

---

## **How will the landmark Title VII decision in Bostock affect employer liability standards for LGBTQ+ employees?**

### **Thompson Coburn LLP**

As many had anticipated, by a 6-3 vote, the United States Supreme Court confirmed that it is unlawful under Title VII of the Civil Rights Act of 1964...

---

## **Seattle Enacts Gig Worker Paid Sick and Safe Time Ordinance During COVID-19 Crisis**

[Washington](#)

### **Jackson Lewis PC**

The Seattle City Council has enacted the Paid Sick and Safe Time for Gig Workers Ordinance, which temporarily provides paid sick and safe time (PSST)...

---

## **Have You Thought About ... Whether You Can Rescind Job Offers?**

### **Brownstein Hyatt Farber Schreck LLP**

In the face of the coronavirus pandemic, many companies closed or significantly reduced operations. As they are slowly ramping back up, their...

---

## **Maryland's Anti-Harassment Reporting Is Due July 1, 2020**

[Maryland](#)

### **Davis Wright Tremaine LLP**

With the start of summer 2020, many businesses have fully transitioned to the "new normal" of remote work. Employers and employees alike may have...

---

## **In a Landmark Decision, Supreme Court Rules Title VII Protects LGBTQ+ Workers**

### **Montgomery McCracken Walker & Rhoads LLP**

Today, the United States Supreme Court ruled that Title VII of the Civil Rights Act of 1964 prohibits discrimination on the basis of sexual...

---

## **Global Solutions: What's up Doc? The Role of Designated Medical Providers in Returning Employees to Work**

[Audio](#)

### **Ogletree Deakins**



In this Episode of the Global Solutions series by Ogletree Deakins' Cross-Border practice group, Carolyn Knox and Rebecca Marks discuss the role of...

---

#### **HHS Issues Final Rule on Section 1557**

**Seyfarth Shaw LLP**

Under Section 1557 of the Affordable Care Act ("Section 1557"), health programs and activities that receive federal financial assistance cannot...

---

#### **Minnesota Supreme Court Rejects Challenges to Minneapolis Sick and Safe Ordinance**

[Minnesota](#)

**Jackson Lewis PC**

The Minnesota Supreme Court (5-2) has upheld the Minneapolis Sick and Safe Time Ordinance, ruling state law does not preempt the Ordinance, and it...

---

#### **OSHA Issues New Business Reopening Guidance**

**Brownstein Hyatt Farber Schreck LLP**

As many nonessential businesses begin to slowly reopen, they have been left to navigate workplace safety questions without much federal guidance...

---

#### **US COVID-19: 4 Takeaways from the EEOC's New Guidance on Antibody Testing, Older Workers, and Accommodations**

**Bryan Cave Leighton Paisner LLP**

With more and more states reopening their economies, employers are facing a barrage of new requirements from state and local governments. But...

---

#### **California Employer Considerations and Best Practices for Returning to Work in the Week of COVID-19**

[California](#)

**Buchalter**

Currently in "Stage 2: Lower-risk workplaces" of the Resilience Roadmap - Retail (curbside and delivery only); related logistics and manufacturing...

---

#### **The USMCA's Facility-Specific Rapid Response Labor Mechanism: Are You Ready for It?**

**Akin Gump Strauss Hauer & Feld LLP**

The Facility-Specific Rapid Response Labor Mechanism (RRLM) in the United States-Mexico-Canada Agreement (USMCA) establishes an entirely...

---

#### **With Pennsylvania Non-Competes, As in Life, Timing is Everything**

[Pennsylvania](#)

**Faegre Drinker Biddle & Reath LLP**

In Pennsylvania, it has long been known that waiting until after the start of employment to have an employee sign a non-competition agreement comes...

---

#### **Connecticut Employers: Don't Forget Your Harassment Training and Notice Requirements**

[Connecticut](#)

**Davis Wright Tremaine LLP**

As detailed in our prior advisory, per Connecticut's "Time's Up Act," all employers are now subject to mandatory anti-harassment and posting...

---

## **EEOC Says No Mandatory Antibody Tests for COVID-19**

### **Barnes & Thornburg LLP**

The Equal Employment Opportunity Commission (EEOC) issued revised guidance about COVID-19 and the Americans with Disabilities Act on June 17, 2020...

---

## **New York Releases Phase Three Guidance for Reopening of Restaurants / Food Services and Personal Care Businesses**

New York

### **Epstein Becker Green**

Continuing New York State's four-phased plan for reopening nonessential businesses and expanding essential businesses in the state ("New York...

---

## **Bostock v. Clayton County, Georgia - What It May Mean for Group Health Plans**

### **Haynes and Boone LLP**

The U.S. Supreme Court's recent decision in *Bostock v. Clayton County, Georgia* held that Title VII of the Civil Rights Act of 1964 protects the...

---

## **UPDATE: COVID-19 Presents Another Opportunity for Leave Sharing**

### **Graydon Head & Ritchey LLP**

In a prior blog post, we discussed how COVID-19 presented a potential opportunity for employers to set up a leave-sharing program for those affected...

---

## **Public Nuisance Claims Emerge In COVID-19 Workplace Litigation Filings**

California

### **Barnes & Thornburg LLP**

In addition to other trends Barnes & Thornburg's Wage and Hour Practice Group is monitoring, this week, we noted the filing of several somewhat novel...

---

## **Updated California Face Covering Rules New EEOC And OSHA Reopening Guidance Local Government Rules For Reopening**

California

### **Stradling Yocca Carlson & Rauth**

The California Department of Public Health (CDPH) released updated guidance on the use of face coverings as the state sees an uptick in COVID-19...

---

## **Supreme Court Holds Employment Discrimination Based on Sexual Orientation and Gender Identity Constitute Sex Discrimination under Title VII**

### **Kramer Levin Naftalis & Frankel LLP**

On June 15, the United States Supreme Court ruled that Title VII of the Civil Rights Act of 1964 prohibits employers from discriminating against...

---

## **Trump Administration Considering Possible Changes to Nonimmigrant Visa Programs**

### **Fakhoury Global Immigration**

President Trump issued a proclamation on April 22, 2020 restricting the ability of certain foreign nationals from using immigrant visas (IVs) to enter...

---



## **President Trump Issues Proclamation Suspending Entry of Certain Foreign Workers**

### **Akin Gump Strauss Hauer & Feld LLP**

On June 22, 2020, President Trump signed a Presidential Proclamation (the "Proclamation") that extends the entry suspension...

---

## **New Order from Arizona Governor and New OSHA Guidance Put Multi-State Employers in a Quandary with Reopening Plans**

Arizona

### **Stinson LLP**

Arizona's Governor Doug Ducey issued an executive order laying out efforts to contain the spread of COVID-19. This executive...

---

## **SBA Revises PPP Loan Forgiveness Application and Issues EZ Forgiveness Application**

### **Haynsworth Sinkler Boyd PA**

Following the adoption of the Paycheck Protection Program Flexibility Act (PPP Flexibility Act), the Small Business Administration (SBA) has released...

---

## **Today in Washington - June 18, 2020: COVID-19 Updates**

Washington

### **Hall Render Killian Heath & Lyman PC**

Yesterday, the Senate Health Education Labor and Pensions Committee held a hearing to consider which telehealth expansion provisions should be...

---

## **Restart: Getting back to business amid COVID-19**

### **DLA Piper**

As businesses have begun to resume activities, they are faced with many challenges. Restart - a guide for employers - contains the main points every...

---

## **Ohio General Assembly Enacts Sweeping Changes to Workers' Compensation Law**

Ohio

### **Vorys Sater Seymour and Pease LLP**

Sweeping changes to the Ohio Workers' Compensation Act were made when Am. Sub. H.B. 81 was signed into law by Governor Mike DeWine on June 16, 2020...

---

## **Recent Supreme Court Decision Creates Basis For Challenge To HHS's Rescission Of Anti-Discrimination Protections**

### **Squire Patton Boggs**

Most readers are likely familiar with the landmark decision issued by the U.S. Supreme Court last week, in which the Court held that Title VII...

---

## **In Historic Decision, U.S. Supreme Court Rules Title VII Prohibits LGBTQ Employment Discrimination**

### **Barnes & Thornburg LLP**

The importance of this week's U.S. Supreme Court decision related to LGBTQ rights cannot be overstated. The full opinion in *Bostock v. Clayton Cty...*

---

## **COVID-19 Washington Update: June 18, 2020**



### **Kelley Drye & Warren LLP**

Today, the RESTAURANTS Act of 2020 was introduced by Senators Wicker (R-MS) and Sinema (D-AZ) and Representatives Blumenauer (D-OR) and...

---

### **OSHA issues return-to-work guidance for non-essential businesses**

#### **Hogan Lovells**

On Thursday, June 18, the Occupational Safety and Health Administration (OSHA) published a pamphlet with “guidance to assist employers and workers in...

---

### **Struggle Creates Innovation: Technology and Data Privacy for Contractors**

#### **Bradley Arant Boult Cummings LLP**

As the coronavirus (COVID-19) spread around the world, most businesses were forced to close their doors temporarily and take steps towards working...

---

### **Class Action Survival Guide - The Top Five Things That Employers Need To Defend Post-COVID-19 Litigation**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: As employers embark on reopening their businesses and implementing return to work plans, they face a potential wave of workplace...

---

### **Trade Tool Kit for a Successful Transition from NAFTA to CUSMA**

#### **Blake Cassels & Graydon LLP**

On July 1, 2020, the Canada-United States-Mexico Agreement (CUSMA) will come into force, replacing the existing North American Free Trade Agreement...

---

### **COVID-19: Quick State by State Reference Tool Regarding Reopening in New England States**

#### **Pierce Atwood LLP**

In response to the COVID-19 pandemic and its threat to public health from in-person contact, every state in New England issued orders closing or...

---

### **As the Entertainment Industry Gets Back to Business, COVID-19 Compliance Officers to Have a Starring Role**

#### **Venable LLP**

One of the key elements in the White Paper from the Industry-wide Labor-Management Safety Committee Task Force is the agreement among producers and...

---

### **All (clean and sanitized) hands on deck: What New York City office-based employers need to know to prepare for Phase Two**

#### **DLA Piper**

On April 26, 2020, Governor Andrew Cuomo announced a four-phased approach to reopening businesses in New York State in the wake of the coronavirus...

---

### **Leaders of Electric Cooperatives Discuss Safety Measures Taken to Protect the Safety and Health of Their Employees During COVID-19**

### **Eversheds Sutherland (US) LLP**

Senior electric coop leaders recently spoke with the National Rural Electric Cooperative Association (NRECA) and T&D World about safety measures being...

---

### **Moving forward: New York State Department of Health issues new protocols for returning employees to the workplace following COVID-19 infection or exposure**

New York

### **Reed Smith LLP**

As New York State businesses begin to reopen - a process we have detailed here - Empire State employers will increasingly be required to make...

---

### **A Win for Plaintiffs in Recent NC Ag-Gag Ruling**

North Carolina

### **Nexsen Pruet**

Much of a 2015 North Carolina law that was meant to stop activists from posing as farm workers in order to gain access to footage and information...

---

### **Workplace Safety Review Podcast: Episode 3 | Interview with Hamid Arabzadeh on OSHA Recordkeeping Regulations During COVID-19**

Audio

### **Greenberg Traurig LLP**

In this Episode, host Mike Taylor interviews Hamid Arabzadeh, Principle of HRA Environmental Consultants, regarding OSHA's recordkeeping regulations...

---

### **Austin and San Antonio-Area Businesses Now Required to Adopt Plans Mandating Face Coverings, But Fines May Be Imposed in San Antonio**

### **Ogletree Deakins**

On June 17, 2020, Bexar County Judge Nelson Wolff issued Executive Order NW-10, requiring all businesses operating in the county, which includes San...

---

### **California Issues Statewide Guidance for Mandatory Cloth Face Coverings**

California

### **Ogletree Deakins**

On June 18, 2020, the California Department of Public Health issued a statewide "Guidance for the Use of Face Coverings." Although the guidance is...

---

### **#WorkforceWednesday: Unionization Risks, Health Care Employers Reopen, Antibody Testing**

Video

### **Epstein Becker Green**

As businesses across the United States open up, workers may increasingly turn to unions to help support their safety. Employers should take steps to...

---

### **Diversity and Inclusion at Work: How U.S. Law Impacts Diversity & Inclusion Initiatives in the Context of the COVID-19 Pandemic**

Audio

### **Ogletree Deakins**

In this episode of our Diversity and Inclusion at Work series, Sarah Platt and Brazitte Poole discuss diversity and inclusion laws and initiatives to...

---



### **Question of the Day: Face Coverings in the Workplace**

#### **Fredrikson & Byron PA**

The Occupational Safety and Health Administration recently updated its information concerning cloth face coverings that are not covered by its...

---

### **Federal Circuit Sinks Claim for Submarine Construction Compliance Costs as Untimely Under the CDA**

#### **Vinson & Elkins LLP**

Government contractors operate in a constantly changing regulatory environment, and in certain circumstances, a contractor may be contractually...

---

### **Question of the Day: Anti-Discrimination Training in the Remote Workplace**

#### **Fredrikson & Byron PA**

Employers are at the confluence of a global pandemic and a worldwide focus on racial injustice. Even with some, or all, employees working remotely...

---

### **Information Requested on Pooled Employer Plan Prohibited Transaction Issues: Act Quickly to Help Shape Exemptive Relief**

#### **Morgan Lewis**

The US Department of Labor (DOL) published a Request for Information (RFI) on June 18 in the Federal Register on the subject of pooled employer plans...

---

### **Federal Protection for Businesses from Coronavirus Liability Starting to Take Shape**

#### **Phelps Dunbar LLP**

After an intense lobbying effort by the U.S. Chamber of Commerce, Senate Republicans are drafting legislation to provide broad coronavirus liability...

---

### **U.S. Supreme Court Issues Landmark Ruling Barring LGBT Workplace Discrimination**

#### **Fenwick & West LLP**

Yesterday, the U.S. Supreme Court issued a landmark 6-3 decision in a trio of linked cases (Altitude Express v. Zarda, Bostock v. Clayton County and...

---

### **EEOC Issues Updated Guidance on COVID-19 Antibody Testing**

#### **Greenberg Traurig LLP**

On June 17, 2020, the U.S. Equal Employment Opportunity Commission (EEOC) issued guidance (see A.7.) stating employers cannot require workers to...

---

### **Maximizing Workforce Agility**

#### **Baker McKenzie**

The COVID-19 pandemic is forcing companies to re-examine their work from home or remote work policies. There is no one size fits all plan. Many...

---

### **Podcast: UAE - Navigating the return to work after COVID-19 lock-downs**

#### **DLA Piper**

All businesses in the UAE have been affected in some way by the lockdown,

regardless of sector or size. Now that restrictions are being lifted across...

---

### **Emerging Technologies Washington Update- Jun 18, 2020**

#### **McGuireWoods Consulting LLC**

This week: Coronavirus response; Section 230 under fire again on both sides of the aisle; momentum grows for regulating facial recognition technology...

---

### **COVID-19: Key updates for compliance teams**

#### **PRO Compliance**

Lexology Pro Compliance takes a look at some of the most informative articles published on Lexology this fortnight for compliance teams to stay up-to-date, including key guidance from regulators around the world and practical tips to help businesses adapt to a new normal.

---

### **Refusing to Return to Work May Not Make Ohio Employees Ineligible for Unemployment Compensation**

Ohio

#### **Vorys Sater Seymour and Pease LLP**

Although businesses across the country are reopening, the threat of contracting COVID-19 remains. Accordingly, for many employees the choice to return...

---

### **Affordable Care Act No Longer Interpreted to Prohibit Discrimination Against Transgender Patients**

#### **Jackson Lewis PC**

Section 1557 of the Affordable Care Act ("ACA") contains anti-discrimination provisions, which include prohibitions on sex discrimination, that apply...

---

### **IRS Issues Proposed Regulations on Excess Nonprofit Executive Compensation**

#### **Greenberg Traurig LLP**

Section 4960 was added to the Code in 2017 as part of the Tax Cuts and JOBS Act. Section 4960 generally provides that if certain tax-exempt...

---

### **U.S. regulatory developments: EPA issues first in a series of rules restricting ethylene oxide emissions**

#### **Reed Smith LLP**

On June 1, 2020, the U.S. Environmental Protection Agency (EPA) announced final action to reduce emissions of ethylene oxide (EO) from certain...

---

### **Return to Work: Preparing for the Future Amid COVID-19**

California

#### **Latham & Watkins LLP**

Companies planning to reopen offices face numerous challenges, including how to handle employee illness, privacy rights, and more...

---

### **New Jersey's "Road Back": Rules of the Road, Exits Reached, and the Way Ahead**

New Jersey

#### **Epstein Becker Green**

In March 2020, New Jersey Governor Phil Murphy issued Executive Orders 104 and 107, closing or restricting all but certain designated "essential"...



---

## **Suspending Entry for Temporary Workers: What Employers Need to Know**

**Akerman LLP**

On Monday, President Trump issued a Proclamation restricting certain foreign workers from entering the U.S. through the end of 2020, claiming it is...

---

## **Supreme Court Holds that Title VII Prohibits Discrimination Based On Sexual Orientation and Gender Identity**

**Seyfarth Shaw LLP**

For decades, courts and practitioners have struggled with whether federal law protects employees against discrimination on the basis of sexual...

---

## **Are you ready for D.C. paid family/medical leave on July 1? Questions & Answers for employers, including benefits coordination**

**Hogan Lovells**

Benefits will be available to employees under the District of Columbia's paid family and medical leave program, known as D.C. Paid Family Leave...

---

## **IRS Guidance on Employer-Based Leave Donation Programs for COVID-19 Relief Organizations**

**Faegre Drinker Biddle & Reath LLP**

In recent years, it has become the norm for the IRS to respond to a federally declared disaster by issuing guidance enabling employers to establish...

---

## **Virginia Enacts Sweeping Employee Protection Laws**

Virginia

**Hunton Andrews Kurth LLP**

After a landmark 2019 election in which Democrats took control of the House of Delegates, Senate, and Governor's office for the first time in 26...

---

## **Supreme Court Holds that Title VII Prohibits Discrimination Based On Sexual Orientation and Gender Identity**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: For decades, courts and practitioners have struggled with whether federal law protects employees against discrimination on the...

---

## **Recent DOL guidance provides roadmap for private equity investments in 401(k) plans**

**Reed Smith LLP**

On June 3, 2020, the U.S. Department of Labor issued an information letter permitting individual account plans subject to the Employee Retirement...

---

## **CUSMA: Labour Rights and Provisions After NAFTA**

**Blake Cassels & Graydon LLP**

On July 1, 2020, the Canada-United States-Mexico Agreement (CUSMA) will be coming into force. This agreement will effectively replace the...

---

## **COVID-19: Weekly Oversight and Enforcement Report—Week of June 18, 2020**

### **Wilmer Cutler Pickering Hale and Dorr LLP**

The House Select Subcommittee on the Coronavirus Crisis launched an investigation into the disbursement of PPP funds by sending letters...

---

### **SBA Revises Loan Forgiveness Interim Final Rule: Implements Changes from the Paycheck Protection Program Flexibility Act**

#### **Potomac Law Group PLLC**

In prior alerts, we discussed the SBA's interim final rule on loan forgiveness, and changes to the Paycheck Protection Program (PPP) resulting from...

---

### **A Deeper Dive into Trade Secret Legal Analytics**

#### **Seyfarth Shaw LLP**

As a special feature of our blog—guest postings by experts, clients, and other professionals—please enjoy this blog entry from Rachel Bailey, a Legal...

---

### **Massachusetts Continues to Reopen: Step 2 of Phase 2 Begins June 22nd**

Massachusetts

#### **Morgan, Brown & Joy LLP**

On June 19, 2020, Governor Baker announced that the Massachusetts economy will begin the second step of Phase 2 of its Four-Phase Reopening Plan...

---

### **NLRB Tumbles From High-Wire in Circus Circus Dispute**

#### **Baker McKenzie**

Last week the D.C. Circuit Court of Appeals reversed a National Labor Relations Board's decision involving Weingarten rights, the application of its...

---

### **On the Basis of Text: SCOTUS Deals Victory for LGBTQ Rights Through the Words on the Page**

#### **McCarthy Tétrault LLP**

In a 6-3 opinion released on June 15, 2020, the U.S. Supreme Court held that Title VII of the Civil Rights Act of 1964 prohibits employment...

---

### **A Primer on Getting Employees Back to Production**

#### **Fox Rothschild LLP**

With restrictions beginning to soften following the months-long COVID-19 crisis, and producers eager to get back to production, but daunted by the...

---

### **Maryland Enters Phase Two: Non-Essential Retail Reopens with Restrictions**

Maryland

#### **Jackson Lewis PC**

Maryland Governor Larry Hogan has signed a new Executive Order allowing the reopening of more workplaces and non-essential businesses, subject to...

---

### **Allyship: How to Support Your Black Colleagues During This Racial Pandemic**

Audio

#### **Ogletree Deakins**

As the global community continues to grapple with issues of racial injustice, Sierra



Gray discusses how employers and employees can be allies in...

---

**Overview of government funding programs for U.S. based businesses operating in Canada and the UK** [Video](#)

**Gowling WLG**

In this webinar, the global professionals at Gowling WLG review various government funding programs to which Canadian and UK businesses can apply...

---

**California Employer Considerations and Best Practices for Returning to Work in the Wake of COVID-19** [California](#)

**Buchalter**

In this webinar, our speakers address local and state reopening orders and guidance, including industry-specific guidance; health and safety...

---

**Business as unusual: What role should business play in the battle for racial justice and equality?**

**Freshfields Bruckhaus Deringer**

"My advice to [CEOs] is to throw out the old playbook...More is going to be demanded of corporations, and more should be demanded, because they have a...

---

**Unnecessary Roughness: NLRB Calls Foul on Union for Workplace Investigation Interference**

**Barnes & Thornburg LLP**

Few things can frustrate human resources professionals or personnel administrators as much as individuals who interfere with a workplace...

---

**What the Traveler Saw: Handling Employee Vacation Requests During COVID-19**

**Baker McKenzie**

Even though vacation plans may be hampered by face coverings and social distancing this summer, US employers are still likely to see requests for...

---

**Supreme Court Extends Equal Employment Protections to LGBTQ Workers**

**Barnes & Thornburg LLP**

The Supreme Court, divided 6-3, issued its long-awaited decision in *Bostock v. Clayton County, Georgia*, holding that an employer who fires an...

---

**Question of the Day: Sexual Orientation and Transgender Identity Discrimination**

**Fredrikson & Byron PA**

What is the significance of today's U.S. Supreme Court ruling on sexual orientation and transgender identity discrimination and what steps should...

---

**New York Department of Health Issues Interim Guidance for Employees Returning to Work Following COVID-19 Infection or Exposure, Retroactively Revising Phase One and Two Industry-Specific Guidance** [New York](#)

**Epstein Becker Green**

One of the biggest concerns for New York employers as they plan or begin to reopen or expand their operations under the four-phase New York Forward...

---

### **Supreme Court Rules Title VII protects LGBT+ Employees from Workplace Discrimination: Practical Implications for Employers**

#### **Greenberg Traurig LLP**

What do a gay child-welfare advocate from Georgia, a transgender funeral home employee from Michigan, and a gay skydiving instructor from New York...

---

### **"The answer is clear": Title VII Protects Gay and Transgender Employees from Employment Discrimination**

#### **Phelps Dunbar LLP**

Title VII of the Civil Rights Act of 1964 prohibits discrimination on the basis of sex. The U.S. Supreme Court held Monday that this prohibition...

---

### **Paycheck Protection Program - Where Are We Now? An Up-to-Date Guide to the Paycheck Protection Program**

#### **Proskauer Rose LLP**

Since the enactment of the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") on March 27, 2020, the U.S. Small Business...

---

### **Extended Remote Workforce (Video Chat)**

[Video](#)

#### **Baker McKenzie**

As companies begin to reopen, a new trend has emerged - the idea of permanently remote employees. During this 15-minute moderated discussion, we will...

---

### **EEOC Issues New Guidance on COVID-19**

#### **Morgan Lewis**

The US Equal Employment Opportunity Commission (EEOC) issued its most recent round of Q&As on June 11 offering guidance to employers on the Americans...

---

### **COVID-19 に関する 対応における取締役 会の検討事項**

#### **Weil Gotshal & Manges LLP**

世界的に広がる新型コロナウイルス（ COVID-19 ）の影響により 世界中のビジネス が大きな困難に直面している この前代未聞の状況下ほど 取締役会によるリスク管理 が重要と...

---

### **Making the Most of Returning to the Office**

[Illinois](#)

#### **Amal Law Group**

With communities across Illinois, the nation, and the world returning to the office, attorneys and law firms are no doubt part of the masses. In a...

---

### **Ninth Circuit Clarifies Requirements for Article III Standing in Certain FCRA Cases**

#### **Squire Patton Boggs**



In a class action involving an allegation that an employer failed to give the “stand-alone” disclosure that is required under the Fair Credit...

---

### **Pandemic Leads to Accommodation Claims under Federal and State Laws** New

York

#### **Jackson Lewis PC**

The New York District Office of the Equal Employment Opportunity Commission recently commented that it had received an increasing number of charges...

---

### **Update on everything you need to know about New York's business reopening plan [Updated as of June 15]** New York

#### **Reed Smith LLP**

As we previously detailed here and here, New York State Governor Andrew Cuomo recently outlined guidelines for when Empire State businesses can...

---

### **Question of the Day: Diversity and Inclusion Efforts in the Workplace**

#### **Fredrikson & Byron PA**

As businesses proceed with reopening, COVID concerns are not the only thing on employees' minds. Many employers are finding their workplaces...

---

### **Proposed 4960 Excise Tax Regulations Issued**

#### **Patterson Belknap Webb & Tyler LLP**

On June 5, 2020, the Internal Revenue Service (“IRS”) issued proposed regulations on the Excise tax on excess tax-exempt organization executive...

---

### **Social Media Posts During Turbulent Times: FAQs on Employee Rights and Employer Responsibilities**

#### **Ogletree Deakins**

Many people have commented on social media regarding the anti-racist movement that has been gaining strength in the wake of police officers killings...

---

### **U.S. Supreme Court Makes Pride Month History by Holding That Title VII Bars Job Discrimination Against LGBT+ Workers**

#### **Dykema Gossett PLLC**

Unexpectedly siding with the liberal wing of the Court, Justice Neil Gorsuch penned a 6-3 decision in *Bostock v. Clayton County*, holding that Title...

---

### **Emails to Your Personal Attorney May Not Be Privileged If Sent or Received on a Work-Provided Email Address** Michigan

#### **Foster Swift Collins & Smith PC**

Emails with your personal attorney may not be confidential and protected by the attorney-client privilege if sent from or received at a work-provided...

---

### **Third Thursdays with Ruthie: Strategies for Effective Responses to Discussions About Race** Audio

#### **Ogletree Deakins**

In this Episode of our Third Thursday series, Ruthie Goodboe is joined by Luther

Wright, Jr. To discuss strategies employers can use to respond to...

---

**No Good Deed Goes Unpunished: Return to Work May Mean Reduced Protections for Trade Secrets and Customer Goodwill**

**Seyfarth Shaw LLP**

Tens of millions of employees have been laid off or furloughed as a result of the COVID-19 pandemic. Now that the reopening process has begun in most...

---

**Sexual Orientation and Gender Identity Protected Characteristics Under Title VII**

**Taft Stettinius & Hollister LLP**

In a landmark decision issued on June 15, 2020, the Supreme Court held in *Bostock v. Clayton County, Georgia* that sexual orientation and gender...

---

**EEOC provides updated guidance related to excluding high-risk workers, required accommodations, and pandemic-based harassment**

**Reed Smith LLP**

As we previously posted, the Centers for Disease Control and Prevention CDC recently issued guidance (CDC) recently issued guidance on reopening the...

---

**All (clean and sanitized) hands on deck: What New York City office-based employers need to know to prepare for Phase Two**

**DLA Piper**

On April 26, 2020, Governor Andrew Cuomo announced a four-phased approach to reopening businesses in New York State in the wake of the coronavirus...

---

**Have You Thought About ... Modifying Your Employment Policies Upon Reopening?**

**Brownstein Hyatt Farber Schreck LLP**

Many companies modified certain policies (whether formally or informally) during the initial COVID-19 crisis to address furloughs and reduced working...

---

**Thoughts for Employers Celebrating Juneteenth for the First Time**

**Mintz**

As the national conscience has elevated after the death of George Floyd regarding social justice and racial equality, many employers have begun to...

---

**SAG-AFTRA Issues Covid Safety Guidelines**

**Frankfurt Kurnit Klein & Selz PC**

SAG-AFTRA, along with the Director's Guild of America, the International Alliance of Theatrical Stage Employees, the International Brotherhood of...

---

**In Landmark Decision, U.S. Supreme Court Expands LGBTQ Protections in Employment**

**Cozen O'Connor**

On Monday, June 15, 2020, the U.S. Supreme Court issued a historic decision holding that LGBTQ individuals are protected from discrimination under...

---



## **New OSHA Guidance for Businesses Returning to Work**

**Jackson Lewis PC**

Late last week, the Occupational Safety and Health Administration ("OSHA") issued new guidance for employers that are reopening their businesses and...

---

## **Diversity & Inclusion at Work: Global Laws & Compliance**

[Audio](#)

**Ogletree Deakins**

In this Episode of our Diversity & Inclusion at Work series, Kimya Johnson and Bonnie Puckett discuss how employers with global workforces can create...

---

## **Question of the Day: Identity Theft and Unemployment**

**Fredrikson & Byron PA**

Several employers have notified us that they received written notice from their state unemployment agency of unemployment applications for one or...

---

## **#WorkforceWednesday: SCOTUS Decision on LGBTQ Employees, EEOC on Older Workers Returning to Work**

[Video](#)

**Epstein Becker Green**

It's #WorkforceWednesday. This week, we saw a landmark employment law decision and received clarifications on return-to-work issues involving older...

---

## **U.S. Supreme Court: Title VII Prohibits Discrimination Based on Sexual Orientation and Transgender Status**

**Lewis Rice LLC**

Last week, the United States Supreme Court held that individuals whose employment was terminated because of their sexual orientation or transgender...

---

## **US COVID-19: EEO Reminders to Include in Return to Work Communications**

**Bryan Cave Leighton Paisner LLP**

As employers prepare their "Return To Work" plans, clear communications to employees about protocols and expectations will be critically important...

---

## **DOL Introduces New Safe Harbor for Retirement Plan Disclosures; Health and Welfare Plans Remain Subject to Existing Safe Harbor E-Disclosure Rules**

**Hall Benefits Law**

On May 27, 2020, the Department of Labor ("DOL") published a final rule on electronic disclosures of ERISA-required documents (the "Final Rule") that...

---

## **OSHA and EEOC Expand Guidance to Employers Regarding COVID-19**

**Squire Patton Boggs**

The Occupational Safety and Health Administration (OSHA) and U.S. Equal Employment Opportunity Commission (EEOC) recently published guidance...

---

## **COVID-19 Lawsuits and Claims Increasing in Courts Nationwide**

**Littler Mendelson PC**

As the United States continues to struggle with the devastating impact of the COVID-19 pandemic on health, safety, and the economy, it is likely that...

---

## **Considerations for Employers Returning To Work Amidst Social Unrest and COVID-19**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In light of recent events, the Employment Law Lookout Blog provides some reflection and thought on returning to work in uncertain...

---

## **Video Chat Series (6th Installment): Employment Lessons from the Early Reopeners**

[Video](#)

### **Baker McKenzie**

We hope you have found our video chat series helpful and informative. We are continuing this series of quick and bite-sized video chats, where our...

---

## **Protecting confidential information in a work-from-home world**

### **Reed Smith LLP**

In non-compete and trade secret litigation, key evidence of employee misconduct often comes to light through a forensic examination of the employee's...

---

## **EEOC Provides Further Guidance Regarding How COVID-19 Affects Employers' Legal Obligations**

### **Taft Stettinius & Hollister LLP**

On June 11, 2020, the Equal Employment Opportunity Commission (EEOC) once again updated its guidance regarding how the COVID-19 pandemic affects an...

---

## **Supreme Court Decision Likely Expands the Reach of Fair Lending Laws to Protect Sexual Orientation and Gender Identity**

### **McGuireWoods LLP**

In a landmark case last week, the Supreme Court held in *Bostock v. Clayton Co.*, Ga. That the prohibition on sex-based discrimination in employment is...

---

## **NLRB Explains Past Practice Analysis and ULP Defense under Raytheon Decision**

### **Jackson Lewis PC**

The National Labor Relations Board (NLRB) has explained the "past practice" analysis it applies in determining whether a unionized employer's...

---

## **Supreme Court Surprises with a 6-3 Decision in Favor of Gay and Transgender Workers**

### **Vinson & Elkins LLP**

Nearly five years ago, I was driving south on Highway 59 to visit a client's facility. At 9 a.m., I pulled over on the shoulder near Edna, Texas, got...

---

## **NLRB GC Issues Guidance Memo Laying Out Changes to Evidence Collection in Unfair Labor Practice Investigations**

### **Proskauer Rose LLP**

NLRB General Counsel Peter Robb issued a Memorandum on June 17th setting forth new guidelines for how Regions conduct unfair labor practice...

---



---

## **EEOC Issues Guidance on Antibody Testing**

**Ogletree Deakins**

On June 17, 2020, the U.S. Equal Employment Opportunity Commission (EEOC) issued an update to its COVID-19 Technical Assistance Questions & Answers...

---

## **COVID-19 Employment Legislation and Litigation FAQs**

**Ogletree Deakins**

For the last several months, employers have been required to learn how COVID-19 spreads, how to maintain or resume safe work environments, and how to...

---

## **Minimum Wage Increases in July 2020: Are You Prepared?**

**Baker McKenzie**

Across the country, minimum wage rates will increase July 1 in several counties, cities and states. A few jurisdictions have postponed their...

---

## **Recent Seventh Circuit Title VII Sex Discrimination Case Offers Reminders for Employers About the Need for Consistency in Employment Practices and Decisions**

**Krieg DeVault**

Litigation rarely goes to trial and employment law is no exception. However, a recent opinion from the Seventh Circuit Court of Appeals in Joll v...

---

## **Supreme Court Justices Dissent: The Opposition to Extending Title VII's Protections to Gay and Transgender Employees**

**Ogletree Deakins**

On June 15, 2020, the Supreme Court of the United States, in a 6-3 decision, held Title VII of the Civil Rights Act of 1964's prohibition of sex...

---

## **Leslie Jordan: Unlikely Instagram King Celebrates a Historic Pride Month**

**Ford & Harrison LLP**

If you haven't been following actor and comedian Leslie Jordan's Instagram feed throughout the coronavirus pandemic, you have been missing out on a...

---

## **Easy Pickins For The EEOC - Again**

**FisherBroyles LLP**

I'm getting tired of repeatedly blogging that health care and medical providers are at serious risk of EEOC enforcement actions for alleged...

---

## **U.S. OSHA Issues Guidance on Returning to Work**

**Jenner & Block LLP**

On June 18, 2020, U.S. OSHA issued its "Guidance on Returning to Work," ("Reopening Guidance") compiling best practices and existing regulatory...

---

## **Let the Masking Debate Continue, but Maybe Not in Our Hospitals**

**Ogletree Deakins**

In 2015, long before COVID-19 emerged, a hospital disciplined and discharged a

recruiter in its HR department who refused to obtain a...

---

**Responding to the Uptick in Union Organizing During the COVID-19 Pandemic**  
**Fox Rothschild LLP**

Employers throughout the country are deciding how best to reopen their operations given the ongoing public health crisis and resulting government...

---

**OSHA's Guidance for Reopening Non-Essential Businesses**  
**Michael Best & Friedrich LLP**

Continuing its recent trend of issuing workplace guidance regarding the COVID-19 pandemic, the Occupational Safety and Health Administration (OSHA)...

---

**Dallas County Requires Health and Safety Policies for All Commercial Entities**  
**Frost Brown Todd LLC**

On June 19, 2020, Dallas County implemented a new Order requiring all commercial entities within the county to develop and implement health and safety...

---

**Ninth Circuit Rejects Plaintiffs' Claims in Trio of ADA Disability Access Cases**  
**Ogletree Deakins**

In a big win for Starbucks and all other restauranteurs, retailers, and places of public accommodation, the U.S. Court of Appeals for the Ninth...

---

**First Circuit Rules on Post-employment Restrictions as COVID-19 Restrictions Ease and Employees Return to Work**  
**Ogletree Deakins**

As employers reopen their businesses following closures or reductions in operations required during the COVID-19 pandemic, many are grappling with...

---

**NLRB Gives Green Light to Confidentiality Provisions in Individual Arbitration Agreements**  
**Proskauer Rose LLP**

In many private arbitration agreements entered into in the non-union context, employers and employees agree that the proceedings shall remain...

---

**OSHA Issues New Guidance Document for Reopening Non-Essential Businesses**  
**Michael Best & Friedrich LLP**

On June 18, 2020, the Occupational Safety and Health Administration (OSHA) issued a guidance document for reopening non-essential businesses during...

---

**Accommodating Older Workers During the COVID-19 Pandemic**  
**Vinson & Elkins LLP**

We have all seen the data: Eighty percent of the people who have died of COVID-19 in the United States have been 65 or older. While these numbers may...

---

**US Supreme Court Says Sexual Orientation and Gender Identity Discrimination Violate Federal Law**



### **Lane Powell PC**

Title VII, the federal law that prohibits discrimination on the basis of sex or gender, prohibits discrimination on the basis of sexual orientation...

---

**Beltway Buzz, June 19, 2020**

### **Ogletree Deakins**

On June 15, 2020, the Supreme Court of the United States released its historical decision...

---

### **New York Employers: Remember to Comply With Anti-Harassment Requirements, Even in a Remote Work World**

New York

### **Davis Wright Tremaine LLP**

As we have discussed previously, New York State and New York City have enacted legislation placing specific requirements on employers to address...

---

### **Title VII Protects LGBTQ Employees, U.S. Supreme Court Rules**

### **Duane Morris LLP**

On June 15, 2020, the Supreme Court of the United States issued a landmark decision holding that an employer who fires an individual merely for being...

---

### **OSHA Provides Updated Guidance on Workplace Safety as Employees Return to Work**

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

Many businesses are anxious to resume operations after closing or scaling back because of COVID-19. However, trends in North Carolina COVID-19...

---

### **Eleventh Circuit Confirms that Religious Accommodations Are a Two-Way Street**

### **Hall Render Killian Heath & Lyman PC**

In a recent opinion, the Eleventh Circuit Court of Appeals addressed the employer's and the employee's responsibilities in relation to claims...

---

### **Supreme Court Decision Prohibiting LGBTQ Discrimination in Employment Could Have Important Implications for Schools**

### **Frost Brown Todd LLC**

Recently, the Supreme Court in *Bostock v. Clayton* held that discrimination in employment based on an employee's sexual orientation or transgender...

---

### **EEOC Issues Guidance on Workplace Accommodations and Avoiding Discrimination**

### **Nelson Mullins Riley & Scarborough LLP**

In addressing the protections for "workers at higher risk," the U.S. Equal Employment Opportunity Commission ("EEOC") recently issued guidance called...

---

### **OSHA Issues Three-Phase Guidance On Return To Work for Non-Essential Businesses**

### **Nelson Mullins Riley & Scarborough LLP**

The U.S. Department of Labor's Occupational Safety and Health Administration ("OSHA") issued new recommendations, called Guidance on Returning to...

---

**Not Today Corona: EEOC Prohibits Testing Employees for Antibodies**

**Sheppard Mullin Richter & Hampton LLP**

On June 17, the Equal Employment Opportunity Commission ("EEOC" or "Commission") issued new guidance to employers forbidding the administration of...

---

**OSHA Issues New Guidance for Reopening Nonessential Businesses**

**Quarles & Brady LLP**

Last week, the Occupational Safety and Health Administration ("OSHA") issued new guidance for nonessential businesses to consider when reopening...

---

**The FLSA and Temperature Checks: The Doctrine of "Integral and Indispensable" Comes to the Forefront**

**Fox Rothschild LLP**

The other day I went to the eye doctor and, before I could go in, an employee checked my temperature. This phenomenon is going to become perhaps a...

---

**Supreme Court: Title VII Prohibits Discrimination Because of Sexual Orientation or Gender Identity**

**Paul Hastings LLP**

In a landmark ruling, the U.S. Supreme Court has held that Title VII of the Civil Rights Act of 1964 prohibits discrimination in employment because of...

---

**OSHA [Sort of] Clarifies Employers' Obligations Regarding Cloth Face Coverings**

**Vinson & Elkins LLP**

Some states have issued orders requiring employers to provide cloth face coverings to employees as a condition for reopening. The Occupational Safety...

---

**How Turbulent Times Might Impact Executive Contracts and Compensation**

**Frost Brown Todd LLC**

Executive employment contracts and compensation have been more heavily scrutinized for the last couple of decades, especially for public companies...

---

**Supreme Court Decrees Title VII Prohibits Discrimination Based Upon Sexual Orientation and Gender Identification**

**Sirote & Permutt PC**

Yesterday, June 15, 2020, the U.S. Supreme Court rendered a landmark 6-3 decision authored by President Trump appointee, Justice Neil Gorsuch, and...

---

**Supreme Court Rules That Title VII Protects LGBTQ Employees**

**Mintz**

In a landmark opinion, the U.S. Supreme Court ruled that Title VII of the Civil Rights Act of 1964 protects gay, lesbian, and transgender employees...

---



## **Getting Clean, Back to Routine and Ready to Be Seen: New OSHA and CDC Guidance on Employees Returning to Worksites After COVID-19 Shutdowns**

### **Bradley Arant Boult Cummings LLP**

OSHA and the CDC have each recently issued new guidance for employers as more and more employees make their way back to on-site work following the...

---

## **Supreme Court Decisions Clarify Gender Discrimination Question for LGBTQ Community**

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

On Monday, June 15, 2020, the United States Supreme Court issued a landmark ruling in three companion cases that provides much-needed clarity as to...

---

## **Second Circuit Upholds Fluctuating Work Week Despite Potential Payroll Issues**

### **Baker & Hostetler LLP**

More than 75 years ago, just four years after the passage of the Fair Labor Standards Act (FLSA), the United States Supreme Court recognized what has...

---

## **Global Solutions Episode 2: What's up, Doc? Designated Occupational Medical Providers' Roles in Reopening During COVID-19**

### **Ogletree Deakins**

In preparing global strategies for monitoring employee health, employers with international workforces may want to be aware that occupational...

---

## **Judge Jackson Explains the Basis for Her Invalidation of the Board's Election Regulations**

### **Sheppard Mullin Richter & Hampton LLP**

As we previously discussed earlier this month, District Court Judge Ketanji Brown Jackson issued an Order in American Federation of Labor and Congress...

---

## **[UPDATED] Coronavirus: US Federal and state governments work quickly to enable remote online notarization and SBA PPP loans to meet global crisis**

[Florida](#)

[Georgia](#)

[Maryland](#)

[Pennsylvania](#)

### **DLA Piper**

(This alert contains information which is current as of June 17, 2020. We are actively monitoring state and federal activities in this rapidly...

---

## **Is COVID-19 a Work-Related Illness?**

### **King & Spalding LLP**

On May 19, 2020, the United States Department of Labor's Occupational Safety and Health Administration ("OSHA") issued "Revised Enforcement Guidance...

---

## **Contact tracing apps: the promise and perils of automated tracking of COVID-19 exposure**

### **DLA Piper**

As state and local stay-in-place restrictions continue to ease and organizations resume or ramp up operations in the wake of the coronavirus disease...

---



## **OSHA FAQs Generally Add to the Confusion but Clarify a Few Key Issues - For Now**

### **Michael Best & Friedrich LLP**

Following its recent issuance of COVID-19 guidance for the construction industry, the Occupational Safety and Health Administration (OSHA) has issued...

---

## **IRS Issues Guidance on Employer COVID-19 Leave-Based Charitable Donation Payments**

### **Haynes and Boone LLP**

In Notice 2020-46, the IRS provided guidance allowing employers to make cash payments to certain charitable organizations in exchange for vacation...

---

## **DOL Confirms Private Equity Can Be Small Components of Defined Contribution Plan Investments**

### **Schulte Roth & Zabel LLP**

Earlier this month, the U.S. Department of Labor ("DOL") issued an Information Letter confirming the widely held view that private equity can be small...

---

## **U.S. Supreme Court Issues Ruling on Title VII Protections for Sexual Orientation and Transgender Status**

### **Krieg DeVault**

On Monday, June 15, 2020, the Supreme Court of the United States issued a landmark decision, *Bostock v. Clayton County*. In this 6-3 opinion, the...

---

## **Title VII applies to bias based on LGBT status, Supreme Court says**

### **Constangy Brooks Smith & Prophete LLP**

And what employers need to do . . . Assuming they haven't already. NOTE FROM ROBIN: The following is the content of a bulletin we published on June...

---

## **Non-Compete News: No-Hire Provisions Under the Georgia Restrictive Covenants Act**

[Georgia](#)

### **Ford & Harrison LLP**

The Georgia Restrictive Covenants Act (O.C.G.A. § 13-8-50, et seq.) ("RCA") governs restrictive covenant agreements in Georgia...

---

## **New Physician Non-Compete Provisions**

### **Ice Miller LLP**

Effective July 1, 2020, a new Indiana law will require certain provisions to be included in physician non-compete agreements in order for the...

---

## **Rejection of Collective Bargaining Agreements as Part of COVID-19 Related Chapter 11 Reorganization**

### **Michael Best & Friedrich LLP**

Employers with unionized workforces have inquired about the possibility of rejecting collective bargaining agreements as part of a Chapter 11...

---

## **Returning to Work Post-Shutdown, Part II: Addressing the Economic Impact of**

## **COVID-19**

### **Faegre Drinker Biddle & Reath LLP**

In this second instalment in our series examining the challenges U.K. employers are likely to face in the coming months, Faegre Drinker's London labor...

---

### **'But-For' Causation Under Bostock**

#### **Ogletree Deakins**

The recent Bostock v. Clayton County, Georgia decision, in which the Supreme Court of the United States ruled that an employer that fires an...

---

### **Gold Dome Report - June 24, 2020**

#### **Nelson Mullins Riley & Scarborough LLP**

With only two legislative days remaining in the 2020 Legislative Session, floor activity in the House and Senate hit a fever pitch as legislators...

---

### **EEOC to Employers: No Mandatory Antibody Tests**

#### **Fox Rothschild LLP**

On June 17, 2020, the Equal Employment Opportunity Commission weighed in on the question of whether an employer can mandate COVID-19 antibody tests...

---

### **New Virginia Law: Accommodations for Pregnant Employees, Handbook Changes**

#### **McGuireWoods LLP**

Virginia's regular 2020 legislative session enacted many new laws protecting employee rights. As previously reported, these new laws include adding...

---

### **Worker's Compensation Exclusivity—A Remedy for COVID-19 Claims?**

#### **Ice Miller LLP**

Businesses of all types, essential and non-essential alike, are reopening under a myriad of guidelines from our cities, states, and federal...

---

### **DOL Introduces New Safe Harbor for Retirement Plan Disclosures; Health and Welfare Plans Remain Subject to Existing Safe Harbor E-Disclosure Rules**

#### **Hall Benefits Law**

On May 27, 2020, the Department of Labor ("DOL") published a final rule on electronic disclosures of ERISA-required documents (the "Final Rule") that...

---

### **EEOC COVID-19 Guidance: Return-to-Work Antibody Testing Prohibited**

#### **Wilson Elser**

On June 17, 2020, the Equal Employment Opportunity Commission (EEOC) updated its technical assistance guidance to clarify that the Americans with...

---

### **Coronavirus - Refusing to Return to Work**

#### **Riker Danzig Scherer Hyland & Perretti LLP**

As New Jersey gradually reopens for business, the Department of Labor has issued new guidance relating to the return to work and unemployment...

---



## **How Much Can Employers Control Employees' Summer Travel During COVID-19? A lot.**

**Krieg DeVault**

As the country begins to reopen and employees begin taking summer vacations, employers are receiving more questions and having to make more decisions...

---

## **SCOTUS Holds That Title VII Prohibits Discrimination Because of Sexual Orientation and/or Transgender Status**

**Spencer Fane LLP**

On June 15, 2020, the Supreme Court held that Title VII's prohibition of "sex" discrimination also prohibits discrimination because of sexual...

---

## **COVID-19 Hero Highlights: Biscuitville Provides Southern Hospitality to Frontline Workers, Students**

**Brooks Pierce McLendon Humphrey & Leonard LLP**

Biscuitville, a Greensboro, North Carolina-based quick-service restaurant, is known for its scratch-made biscuits and homestyle Southern breakfast...

---

## **Federal Court Denies Conditional Certification of Collective Action Involving Restaurant Managers**

**Hunton Andrews Kurth LLP**

A federal district court in Florida recently declined to conditionally certify a nationwide collective action brought under the Fair Labor Standards...

---

## **New NLRB Election Rules Partially Invalidated**

**Stinson LLP**

The National Labor Relations Board (NLRB) faces yet another road block to fully implementing its new election rules. The final rule, issued at the...

---

## **Update: FHFA Announces Further Extension on Moratorium on Foreclosures and Evictions**

**Morgan Lewis**

The Federal Housing Finance Agency (FHFA) announced on June 17 that Fannie Mae and Freddie Mac (the GSEs) are once again extending their moratorium...

---

## **COVID-19 Washington Update: June 17, 2020**

**Kelley Drye & Warren LLP**

Today, the RESTAURANTS Act of 2020 was introduced by Senators Wicker (R-MS) and Sinema (D-AZ) and Representatives...

---

## **More on the Return to Work: the EEOC Issues New COVID-19 Related Guidance**

**Baker McKenzie**

On June 11 and June 17, 2020, the EEOC updated "What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws," its Q&A...

---

## **Troutman Sanders Weekly Consumer Financial Services COVID-19 Newsletter**

### **Troutman Sanders LLP**

Like most industries today, Consumer Finance Services businesses are being significantly impacted by the novel coronavirus (COVID-19). Troutman...

---

### **NLRB Severely Limits Jurisdiction Over Religious Schools**

#### **Cozen O'Connor**

On June 10, 2020, a three-member panel of the National Labor Relations Board issued a decision limiting its own jurisdiction over the faculty of...

---

### **Global Equity Services Clients & Friends Newsletter - June 2020**

#### **Baker McKenzie**

While we been focused on the impact of the pandemic and related stock market volatility on compensation and benefit plans, we did want to highlight...

---

### **Supreme Court's Pro-LGBTQ Ruling: What It Means and Related Legislative Solutions**

#### **Nelson Mullins Riley & Scarborough LLP**

In *Bostock v. Clayton County, Ga.*, the U.S. Supreme Court (SCOTUS) changed the face of LGBTQ civil rights across the country. The landmark 6-3...

---

### **COVID-19 Update: OSHA and EEOC Guidance on Returning to Work**

#### **Paul Weiss**

The Occupational Safety and Health Administration (the "OSHA") has issued guidance (the "OSHA Guidance") for "non-essential businesses" that have...

---

### **COVID-19: OSHA Issues New Guidance for Reopening Non-Essential Businesses**

#### **Wilmer Cutler Pickering Hale and Dorr LLP**

On June 18, 2020, the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) issued new COVID-19 related guidance to assist...

---

### **Top Five Employment Law Liabilities Facing Employers Post-Pandemic**

#### **Hunton Andrews Kurth LLP**

The COVID-19 pandemic has exposed employers to an influx of novel employment law issues. Many employers already have experienced an uptick in related...

---

### **Reopening: Can an Employer Require Antibody Testing For Returning Employees?**

#### **Frankfurt Kurnit Klein & Selz PC**

Last week, the EEOC updated its COVID-19-related guidance for employers, titled *What You Should Know About COVID-19 and the ADA, the Rehabilitation...*

---

### **Department of Labor Publishes Request for Information on Pooled Employer Plans**

#### **Faegre Drinker Biddle & Reath LLP**

The Setting Every Community Up for Retirement Enhancement (SECURE) Act of 2019 created a new type of plan that may begin operating in 2021 called a...



---

**Blurred Lines: Title VII Compliance in the Remote Era****Gordon Rees Scully Mansukhani**

The remote workforce is expanding. Many businesses have been finding ways to capitalize upon technological advancements - even before the COVID-19...

---

**DOL Sheds Light on Permissible Private Equity Components in Individual Account/Defined Contribution Plan Asset Allocation Funds****Pepper Hamilton LLP**

On June 3, the U.S. Department of Labor (DOL) issued an Information Letter (Letter)<sup>1</sup> concerning private equity investments within an...

---

**Environment & Climate Change****EPA Continues Aggressive Pesticide Enforcement: Amazon and eBay Ordered to Stop Sale of Certain Pesticides Claiming Efficacy Against COVID-19****Taft Stettinius & Hollister LLP**

On June 10, 2020, the U.S. Environmental Protection Agency (EPA) ordered Amazon Services LLC (Amazon) and eBay Inc. (eBay) to immediately stop...

---

**Privacy v. Contact Tracing Apps | Fracking Pollution Criminal Charges | Loans at 251% Interest****Cozen O'Connor**

COVID-19 Attorneys General Express Concern Over Contact Tracing Apps The National Association of Attorneys General ("NAAG") sent a letter signed by a...

---

**EPA Declines to Set Drinking Water Limits for Perchlorate****Troutman Sanders LLP**

As anticipated, the Environmental Protection Agency (EPA) announced on June 18, 2020, that it will not regulate perchlorate, a substance primarily...

---

**D.C. Mayor Signs Coronavirus Support Congressional Review Emergency Amendment Act of 2020**[Washington](#)**Kelley Drye & Warren LLP**

Last week, Washington D.C. Mayor Muriel Bowser signed the Coronavirus Support Congressional Review Emergency Amendment Act of 2020 (the "Act") into...

---

**Texas State Implementation Plan Suit Stayed in the Fifth Circuit**[Texas](#)**Sidley Austin LLP**

The U.S. Court of Appeals for the Fifth Circuit has stayed a lawsuit, Sierra Club v. EPA, brought by a coalition of environmental groups concerning...

---

**Water Board Adopts Final Definition of Microplastics in Drinking Water****Nossaman LLP**

This week, on June 16, the California State Water Resources Control Board ("State Water Board") unanimously adopted a definition for microplastics...

---



## **NJDEP Extends Comment Period for Proposed Revisions to Remediation Standards Due to Pandemic**

New Jersey

### **Goldberg Segalla LLP**

The New Jersey Department of Environmental Protection (NJDEP) is required to develop remediation standards for contaminated sites to be protective of...

---

## **Ninth Circuit Climate Change Ruling Opens Door to Increased Litigation**

### **King & Spalding LLP**

The past three years have seen a wave of tort lawsuits brought by local governments and one state seeking to hold fossil fuel companies liable for...

---

## **Despite COVID-19 concerns, CARB continues to advance its regulation of air emissions for shipping industry; hearing set for late June**

California

### **Reed Smith LLP**

The California Air Resources Board (CARB) will conduct a public Board hearing later this month as it continues its efforts to expand the State's...

---

## **California Amends Its Low Carbon Fuel Standard ("LCFS")**

California

### **King & Spalding LLP**

Pressing forward with its efforts to address climate change, the California Air Resources Board ("CARB") finalized amendments to its innovative LCFS...

---

## **First the advice, now the order**

### **Frankfurt Kurnit Klein & Selz PC**

Back in April, EPA told eight technology companies - including Facebook, Ebay and Shopify -- that "unscrupulous dealers are using their platforms" to...

---

## **EPA Officially Adds PFAS Chemicals to TRI Reporting Program**

### **Kelley Drye & Warren LLP**

Earlier today, U.S. EPA officially added 172 specific per- and poly-fluoroalkyl substances (PFAS) to the list of chemicals reportable each year under...

---

## **After the Stay-At-Home Order: Water Management Best Practices for Re-Opening Buildings**

### **Troutman Sanders LLP**

As businesses across the country begin to re-open, many will be hypervigilant about the safety of indoor spaces. While stay-at-home orders may be...

---

## **Federal Court Denies Nationwide Stay of Navigable Waters Protection Rule**

### **Latham & Watkins LLP**

New definition of "waters of the United States" takes effect June 22, 2020 everywhere except Colorado under split decisions...

---

## **Colorado District Court Judge Stays Trump Administration's Navigable Waters Protection Rule**

Colorado

### **Brownstein Hyatt Farber Schreck LLP**

On June 19, 2020, Judge William Martinez of the U.S. District Court for the District of Colorado entered an administrative stay of the recently...

---

### **EPA Requires TRI Reporting of PFAS for Year 2020**

#### **Troutman Sanders LLP**

This week, the U.S. Environmental Protection Agency (EPA) crystalized a new requirement that facilities manufacturing, processing, or otherwise using...

---

### **P3s to Combat Climate Change**

#### **Bilzin Sumberg**

We recently wrote an op-ed about the role that P3s can play in mitigating the effects of climate change. In that piece, we explained that an...

---

### **Trial Concludes in Challenge to EPA's Denial of Fluoride Petition**

#### **Bergeson & Campbell PC**

During the week of June 15, 2020, the U.S. District Court for the Northern District of California heard from the U.S. Environmental Protection...

---

### **Oil and Gas Pipelines are Clogged, at Least for Now**

#### **Breazeale Sachse & Wilson LLP**

A recent ruling by a single federal district judge in Montana has sent a shockwave through the oil and gas industry. By vacating the U.S. Army Corps...

---

### **Ohio's New Brownfield Regulatory Reform Legislation** Ohio

#### **Vorys Sater Seymour and Pease LLP**

On June 16, 2020, Governor DeWine signed House Bill 168 into law. The bill is designed to encourage brownfield redevelopment and reinvestment in the...

---

### **COVID-19 stimulus response to make or break our ability to meet carbon emissions targets**

#### **Clyde & Co LLP**

In a report published on Thursday, the International Energy Agency set out a global blueprint for a green recovery to COVID-19, reforming energy...

---

### **Effluent Limits for Stormwater - California Takes the Lead with Limits Effective July 1, 2020** California

#### **Troutman Sanders LLP**

Under the Clean Water Act, stormwater is considered a nonpoint source. Accordingly, benchmark standards and best management practices have been used...

---

### **Trump Track: Surprise! New WOTUS Rule Leads to Conflicting Rulings** Colorado

#### **Davis Wright Tremaine LLP**

It was clear to everyone, including this humble blogger, that EPA's new rule defining Waters of the United States (WOTUS) would bring little...

---

### **PFAS SNUR Finalized Without "Safe Harbor" Provisions**



### **Jenner & Block LLP**

On June 22, 2020, U.S. EPA issued a final TSCA significant new use rule (SNUR) for long-chain perfluoroalkyl carboxylate (LCPFAC) and perfluoroalkyl...

---

### **EPA Grants Petitions to Add First Chemical to Hazardous Air Pollutants List Since 1990**

#### **Sidley Austin LLP**

On June 18, 2020, the U.S. Environmental Protection Agency (EPA) published a Federal Register Notice granting petitions to add n-propyl bromide...

---

### **EPA Limits State and Tribal Authority with Final Clean Water Act Section 401 Certification Rule**

#### **Winston & Strawn LLP**

On June 1, 2020, the U.S. Environmental Protection Agency (EPA) finalized the "Clean Water Act Section 401 Certification Rule." Issued in response to...

---

### **US Fish and Wildlife Service Continues Work to Narrow Application of Migratory Bird Treaty Act**

#### **Latham & Watkins LLP**

A new draft environmental impact statement on the scope of liability under the MBTA available for public comment...

---

### **Federal Court Denies Preliminary Relief in Challenge to WOTUS Replacement Rule, Finding Plaintiffs Did Not Show a Likelihood of Success on Merits**

#### **Michael Best & Friedrich LLP**

In the first major ruling in numerous cases challenging a final rule redefining "waters of the United States" (WOTUS), a California federal court on...

---

### **ESG in European Private Equity: The Effects of COVID-19**

#### **Latham & Watkins LLP**

Increasing interest in ESG issues presents an opportunity for sponsors to re-evaluate their existing ESG strategies...

---

### **Land and Water Conservation Fund Clears First Congressional Hurdle for Permanent Funding**

#### **Squire Patton Boggs**

What happened: Last week the Senate passed a landmark piece of legislation - the Great American Outdoors Act. Under the legislation, the Land and...

---

### **EPA Finalizes Its Perchlorate Decision**

#### **Holland & Knight LLP**

The U.S. Environmental Protection Agency (EPA) issued a press release on June 18, 2020, indicating it has determined that perchlorate does not meet...

---

### **Animal Rights Challenge to Fish & Wildlife Service Sport Trophy Decision Fails in D.C. Circuit**

[District of Columbia](#)

#### **Duane Morris LLP**

In *Center for Biological Diversity v. Bernhardt*, \_\_\_ F.3d \_\_\_, No. 19-5152 (D.C. Cir. June 16, 2020), the U.S. Court of Appeals for the District of...

---

### **Water Storage and Dam Management Strategies in Light of Climate Change Impacts**

**Nossaman LLP**

There can be little argument that many of the more than 90,000 dams in this country are in need of immediate attention. The catastrophic failure of...

---

### **Companies Entering the Disinfectant and Sanitizer Markets Should Proceed With Caution**

**Baker & Hostetler LLP**

As COVID-19 swept across the country in March 2020, it became abundantly clear to anyone who visited a grocery store that the United States was...

---

## **Internet & Social Media**



**Do most banks and financial service companies take the position that the use of third party behavioral advertising cookies is, or is not, the “sale” of personal information?**

**Bryan Cave Leighton Paisner LLP**

Almost all banks and financial institutions that utilize third party behavioral advertising cookies have taken the position that the collection of...

---

### **Rethinking Consumer Privacy Litigation**

**Squire Patton Boggs**

“[M]odern enterprise and invention have, through invasions upon . . . Privacy, subjected [people] to mental pain and distress, far greater than could...

---

### **Facebook to Allow Users to Block all Political Advertising**

**Frankfurt Kurnit Klein & Selz PC**

Yesterday, Facebook announced that it will allow Facebook and Instagram users to block all social issue, electoral, or political advertising from...

---

### **NIST Releases Cybersecurity Guidance for Manufacturers of IoT Devices**

**Sheppard Mullin Richter & Hampton LLP**

As a part of its Cybersecurity for IoT Program, NIST recently released two publications with the goal of providing cybersecurity guidance and best...

---

### **FTC COPPA Settlement with App Developer Highlights Penalty Policy Considerations**

**Keller and Heckman LLP**

A recent Federal Trade Commission (FTC) settlement with an online game company that allegedly tracked children illegally highlights some important...

---

### **Hot Topics in Advertising & Marketing: COVID-19, Financial Services, and More - An ACC Legal Quick Hit**



## **Venable LLP**

Hot Topics in Advertising & Marketing: COVID-19, Financial Services, and More  
An ACC Legal Quick Hit Financial Services Network Wednesday, May 27...

---

## **Episode 11: Expected Developments in M&A Transactions in the TMT Sector**

Audio

## **Baker McKenzie**

TMT Talk continues to identify issues relevant to the Technology, Media, and Telecommunications sector, as companies determine their next steps and...

---

## **Do banks and financial service companies that use third party behavioral advertising cookies deploy cookie notices?**

## **Bryan Cave Leighton Paisner LLP**

Approximately 78% of banks and financial institutions that deploy a significant number of third party behavioral advertising cookies on their...

---

## **Instagram Users: Post at Your Own Risk. Your Public Content May Be Legally Sublicensed**

New York

## **Venable LLP**

On April 13, 2020, a federal district court in the Southern District of New York[1] held in *Sinclair v. Ziff Davis, LLC, and Mashable, Inc.*...

---

## **The Communication Decency Act and the DOJ's Proposed Solution: No Easy Answers**

Wisconsin

## **Proskauer Rose LLP**

Section 230 of the Communications Decency Act ("CDA"), 47 U.S.C. §230, enacted in 1996, is often cited as the most important law supporting the...

---

## **Tracking Kids Through Your App? Think Again.**

## **Mintz**

Klepto Cats and Dogs have been "stealing" children's personal information without parental consent and using it for targeted advertising. Bad dog...

---

## **Regulatory Hurdles for Sports Betting in Illinois During COVID-19**

Illinois

## **Thompson Coburn LLP**

By way of history, on May 14, 2018, the United States Supreme Court struck down the Professional and Amateur Sports Protection Act which outlawed...

---

## **Civil Rights Organizations Call for Facebook Advertising Boycott**

## **Frankfurt Kurnit Klein & Selz PC**

A coalition of civil rights organizations has called for advertisers to stop advertising on Facebook in July in response to "Facebook's repeated...

---

## **New York Department of Financial Services announces remote online testing for insurance licensing exams**

New York

## **Buckley LLP**

On June 11, the New York Department of Financial Services announced that



remote online proctored testing will be available beginning on June 15, 2020...

---

#### **What domain name to select?**

##### **Stange Law Firm PC**

Having a webpage is vital for almost any law firm. The reality is that a webpage for a law firm is a necessity. A webpage can be a source of gaining...

---

#### **NIST Provides Important Guidance For IOT Industry**

##### **Mintz**

More prevalent than ever before, Internet of Things ("IOT") devices, a term that includes connected "smart" devices, such as internet connected TVs...

---

#### **Episode 321: Using the internet to cause emotional distress is a felony?** Audio

##### **Step toe & Johnson LLP**

This is the week when the movement to reform Section 230 of the Communications Decency Act got serious. The Justice Department released a substantive...

---

#### **FDA Developments: COVID Rapid Antibody Tests**

##### **Greenspoon Marder LLP**

This past week, five new EUA authorizations for serology tests were posted. The pace of authorizations has picked up — as has enforcement of claims...

---

#### **COVID-19 UPDATE: New Jersey Court Embraces Virtual Deposition As The New Norm** New Jersey

##### **Ansa Assuncao LLP**

A Middlesex County Superior Court judge has ordered the plaintiff in a slip-and-fall lawsuit to appear for deposition remotely via Zoom or other...

---

#### **Electronic Data exclusion cries out for Judicial Interpretation**

##### **Gowling WLG**

Cybercrime, once a thing of science fiction, is growing in frequency and sophistication. While there is growing desire for business to access...

---

#### **Credential stuffing during COVID-19: Cybersecurity firm purchased over 500,000 Zoom account credentials on the dark web and hacker forums**

##### **K&L Gates**

In what could only be adding fuel to the fire that is the growing concern over Zoom's privacy and data security risks, it has been reported that over...

---

#### **Facebook Ordered to Turn Over Internal Investigation Documents to Massachusetts Attorney General** Massachusetts

##### **Nutter McClennen & Fish LLP**

Judge Davis of the BLS ordered Facebook to produce documents to Massachusetts Attorney General Maura Healey (AG). The AG obtained the order while...

---

## **Ransomware: Mitigating Risk and Avoiding Mistakes**

### **Quislex Inc**

Ransomware has come a long way since the 1989 "AIDS Trojan." Distributed by diskette, it encrypted the file names and directories of its victims...

---

## **Privacy Issues of U.S. Collection of Social Media Information from Visa Applicants**

### **Jackson Lewis PC**

The Department of State (DOS) has been collecting (and maintaining) information on social media use from all visa applicants (immigrant and...

---

## **Undeterred CFTC Unanimously Approves Three Proposed Rules, Two Final Rules at First Virtual Open Meeting**

### **K&L Gates**

The Commodity Futures Trading Commission (CFTC or Commission) recently held its first virtual open meeting and unanimously approved three proposed...

---

## **Texas Comptroller's Office Implements New Sourcing Rule for Internet Sales and Announces End of Internet Access Tax**

[Texas](#)

### **Baker McKenzie**

As the weather is heating up, the Texas tax front continues to bring hot and exciting developments in the Lone Star State. Two of the latest updates...

---

## **Twin Proposals Would Reform Section 230's Liability Protections and Broadly Affect Online Content**

### **Covington & Burling LLP**

On Wednesday, two proposals were unveiled that would reform the scope of Section 230 of the Communications Decency Act of 1996. Section 230 immunizes...

---

## **Sweating the Details: Court Analyzes User Interface to Uphold Online Arbitration Clause**

### **Morrison & Foerster LLP**

Online service providers typically seek to mitigate risk by including arbitration clauses in their user agreements. In order for such agreements to...

---

## **Risk Mitigation For Social Media Cos. In Light Of Trump Order**

### **Rothwell, Figg, Ernst & Manbeck, PC**

On May 28, President Donald Trump issued an Executive Order on preventing online censorship targeting the Communications Decency Act, or CDA, titled...

---

## **Knobbe Practice Series: Online Brand Enforcement Webinar**

[Video](#)

### **Knobbe Martens**

Attorneys Susan Natland and Jesssica Sganga discuss how your company can protect its valuable intellectual property rights by developing and/or...

---

## **Giving the players their fix**



## **DLA Piper**

When many would have had their eyes on the sneak peaks released by Sony of their eagerly awaited PlayStation 5, another games titan was wrestling...

---

## **Rhode Island passes SSUTA legislation**

Rhode Island

### **Eversheds Sutherland (US) LLP**

On June 18, Rhode Island's legislature passed H 7532, which expands the state's tax base to computer software and streaming entertainment to comply...

---

## **FTC Pounces on Maker of Children's App Menagerie**

### **Baker & Hostetler LLP**

HyperBeard used third-party collectors to build ad profiles...

---

## **The brave new world of virtual notarization**

Massachusetts

### **Robins Kaplan LLP**

The COVID-19 pandemic and consequent state and federal guidelines forced people to work from home before they were able to take steps so that they...

---

## **Alleged Privacy Law Violations Create Potential \$5 Billion Issue For Google**

### **Mintz**

In a proposed class action lawsuit filed in the U.S. District Court for the Northern District of California, Google is facing a potential \$5 billion...

---

## **Legal Practice**



## **Watch Remotely Ethical: "Can I Practice Law Under a Trade Name?"**

### **Frankfurt Kurnit Klein & Selz PC**

In our latest episode of Remotely Ethical, we discuss a recent change to the New York Rules of Professional Conduct, which permits lawyers to provide...

---

## **Are "Litigation Holds" Protected by the Privilege or the Work Product Doctrine?**

### **McGuireWoods LLP**

With pandemic-triggered litigation predicted to increase, corporations' lawyers undoubtedly will address the possible duty to impose "litigation..."

---

## **The Latin American General Counsel**

### **CMS Legal**

The first CMS General Counsel report in the Latin America region, "The Latin American GC: Rising to the challenge", explores the development of the...

---

## **Judges Albright, Lynn, and Tigar Encourage Argument by Junior Lawyers**

### **Winston & Strawn LLP**

On June 12, 2020, the Federal Circuit Bar Association, Berkeley Center for Law & Technology, Berkeley Judicial Institute, ChIPs, and CLI presented a...

---

## **Are the Client's Estate Planning Consultations with Counsel Privileged?**

### **Nelson Mullins Riley & Scarborough LLP**

Confidential communications from a client to her lawyer for the purpose of obtaining legal advice are generally deemed to be privileged. Lawyers are...

---

#### **Treat Truncated Voir Dire as Useless**

##### **Holland & Hart LLP**

Okay, my title is purposefully provocative, but it is not an exaggeration. Based on a recently released, first-of-its-kind, comprehensive study on the...

---

#### **Does a client transaction raise flags? You might have a duty to inquire further**

##### **Thompson Hine LLP**

If a South American investor asks you to take delivery of \$1 million cash in your law office, to deposit it into a client account and then wire it to...

---

#### **Can Withholding Privileged Communications Support an “Adverse Inference”?**

##### **McGuireWoods LLP**

The attorney-client privilege rests on a grand societal purpose — encouraging clients to safely share with their lawyers all the pertinent facts, so...

---

#### **Consider COVID Attitude Changes, Part 8: Population Density Matters**

##### **Holland & Hart LLP**

As I write this, a crowd of Trump supporters is entering the BOK Center in Tulsa, Oklahoma, to attend the President's first mid-pandemic rally. In...

---

#### **Legal Tech**



#### **6 Organizational Risks Solved with Contract Management Software**

##### **ContractWorks**

Contract management software has the potential to transform legal department operations and improve efficiency and productivity. It enables in-house...

---

#### **Projects & Procurement**



#### **AAG Delrahim Touts Success of DOJ's Procurement Collusion Strike Force on International Stage**

##### **Crowell & Moring LLP**

The U.S. Justice Department recently recommended that other countries consider focusing on collusion in government procurement, touting the early...

---

#### **Industry & DoD Push for Delay in Implementing the Section 889(a)(1)(B) Prohibition**

##### **Crowell & Moring LLP**

Section 889(a)(1)(B) of the FY 2019 NDAA, scheduled to become effective on August 13, 2020, bars the Government from entering into a contract, or...

---

#### **Beware Rogue Employees with a Taste for Fraud**

##### **Stinson LLP**

As if more evidence were needed, a recent Department of Justice (DOJ)



indictment provides another reminder of the importance of an effective...

---

**Fastest 5 Minutes: COVID-19 Guidance and Enforcement, DoD OIG, and FAR News (June 17)** [Audio](#)

**Crowell & Moring LLP**

This week's episode covers COVID-19 guidance and enforcement, DoD OIG, and FAR news and is hosted by partner Peter Eyre and counsel Yuan Zhou. Crowell...

---

**First Pandemic Response Accountability Committee Report Emphasizes Government-Wide Concerns About Fraud and Grant Management**

**Crowell & Moring LLP**

On Wednesday, June 17, 2020, the Pandemic Response Accountability Committee ("PRAC"), composed of 21 Offices of Inspector General overseeing agencies...

---

**A Sixth Circuit victory for False Claims Act defendants: Relators are "agents" of the government for purposes of the public disclosure bar**

**Reed Smith LLP**

In a significant win for False Claims Act ("FCA") defendants, the Sixth Circuit, in a unanimous, precedential decision, held that a relator is the...

---

**Technology Week in Iowa 2020**

**McKee Voorhees & Sease PLC**

Iowa Governor Kim Reynolds signed a proclamation designating the third week in June as Technology Week in Iowa with the first one taking place the...

---

**Public Policy Daily Briefing - June 22, 2020**

**Squire Patton Boggs**

With summer officially underway in America and the number of new coronavirus cases in the US continuing to rise, President Donald Trump is doubling...

---

**COVID-19 Relief Programs: Mitigating and Responding To Enforcement Risk**

**Mintz**

Since the early days of the pandemic, Mintz's COVID-19 Compliance & Enforcement Defense Task Force has closely monitored and advised clients on the...

---

**Medicaid Drug Rebate Program proposed rule on value-based pricing, line extension, PBM accumulators**

**Hogan Lovells**

On June 17, 2020, the Centers for Medicare & Medicaid Services (CMS) issued a Proposed Rule ([link](#)) that Would materially modify current Medicaid Drug...

---

**DOJ Announces First Increase To FCA Civil Penalties Since 2018**

**Sidley Austin LLP**

The 2015 Balanced Budget Act (BBA) requires that federal agencies make



inflationary adjustments to civil monetary penalties on a yearly basis to...

---

## Public Policy Daily Briefing - June 23, 2020

Connecticut

Georgia

### Squire Patton Boggs

Five weeks after passing the US\$3 trillion HEROES Act, House Democrats are moving to pass a companion measure, the Moving Forward Act, that would add...

---

## Does CAS Make Sense?

Audio

### Crowell & Moring LLP

Partner Nicole Owren-Wiest appeared on an episode of Baker Tilly's Fed Talks podcast to discuss Cost Accounting Standards. The episode addresses...

---

## DOJ Touts the Success of its Procurement Collusion Strike Force and Seeks a Global Effort on This Front

### Steptoe & Johnson LLP

Last year, the Department of Justice Antitrust Division announced that it was creating a Procurement Collusion Strike Force (Strike Force) to focus...

---

## Safeway Prevails on Motion for Summary Judgment in Whistleblower Pharmacy Usual and Customary Pricing Case

### Quarles & Brady LLP

A federal judge for United States District Court for the Central District of Illinois granted Safeway, Inc.'s motion of summary judgment in a...

---

## Federal Circuit Splits on Blue & Gold Question in Insero

### Covington & Burling LLP

It's a big deal in the government contracts community whenever the Federal Circuit weighs in on a bid protest. And it is a particularly big deal when...

---

## National P3 Update - Transportation

### Bilzin Sumberg

This installment of our National P3 Update focuses on transportation. While the transportation sector has dominated the U.S. P3 market over the last...

---

## Public-Private Partnerships in a Post-Pandemic World

### Frost Brown Todd LLC

While COVID-19 has forced many people and businesses to take a timeout from their everyday activities, the critical infrastructure upon which their...

Public



---

## Six Tips for Defending Foreign Language Witness Depositions

### Winston & Strawn LLP

Defending the deposition of a witness who speaks a foreign language presents significant challenges for defense counsel. As an initial matter, it is...

---

## COVID-19: Impact on State and Local Government Finance - Key Risks for

## **Government Vendors, Lenders and Bondholders**

Audio

### **Mayer Brown**

The economic contraction caused by the COVID-19 pandemic is having a significant impact on US state and local government finances. Mayer Brown...

---

## **DEA Signals that Substantive SOM Guidance is Not Likely Forthcoming**

### **Cote Law PLLC**

On January 20, 2020, the Government Accountability Office (GAO) released its report . The report, mandated by Congress in the SUPPORT Act, focuses...

---

## **Reopening Oregon: Where Are We Now and What Does It Mean?**

Oregon

### **Davis Wright Tremaine LLP**

On May 7, 2020, Oregon Governor Kate Brown outlined a three-phase approach to reopening Oregon's businesses beginning May 15, 2020. The phased...

---

## **New York Car Dealership Settles Discrimination Claims with FTC - Agency Leaders Call for More Rulemaking to Regulate Auto Finance Pricing**

### **Troutman Sanders LLP**

A New York franchise motor vehicle dealer agreed in May to pay \$1.5 million to the Federal Trade Commission to settle charges that the dealership...

---

## **U.S. COVID-19: California SB 939 Remains on Hold Indefinitely in the Appropriations Suspense File**

California

### **Bryan Cave Leighton Paisner LLP**

On June 9, 2020, the California Senate Appropriations Committee placed SB 939 in the Suspense File for further evaluation as the fiscal impact of the...

---

## **New York City to Enter Phase 2 of State's Reopening Plan on June 22**

New York

### **Davis Wright Tremaine LLP**

Mayor Bill de Blasio has announced that New York City will enter Phase 2 of the "NY Forward" reopening plan on Monday, June 22, 2020. To date, seven...

---

## **Florida Senator Rubio Introduces Federal Name, Image, and Likeness Legislation**

Florida

### **Jackson Lewis PC**

Although Florida Governor Ron DeSantis has just signed into law Florida's state name, image and likeness legislation, Florida U.S. Senator Marco...

---

## **Take Video, But Secure a Warrant to Run Facial Recognition Software**

### **Womble Bond Dickinson (US) LLP**

Last week's tech company announcements about facial recognition software startled me, but probably not for the reason you might imagine....

---

## **Supreme Court Ruling Upholds DACA Program**

### **Duane Morris LLP**

On June 18, 2020, a narrowly divided Supreme Court of the United States held that the Court can review the Deferred Action for Childhood Arrivals...



---

## **US Executive Branch Update - June 18, 2020**

### **Squire Patton Boggs**

This report provides a snapshot of the US Executive Branch priorities via daily schedules and the prior day's press releases...

---

## **DEA Poised to Roll Out Three Regulations in the Coming Months**

### **Cote Law PLLC**

It appears that the Drug Enforcement Administration (DEA) is on the cusp of publishing a new regulation in the next few weeks, with two more to follow...

---

## **ED Issues Interim Final Rule on Student Eligibility for HEERF Funding While Courts Grant Preliminary Injunctions**

### **Cooley LLP**

After weeks of confusion over the US Department of Education's guidance following its quick rollout of the Higher Education Emergency Relief Fund...

---

## **Coronavirus: The Hill and the Headlines - COVID-19 D.C. Update - June 18, 2020**

Washington

### **Hogan Lovells**

Your guide to the latest Hill developments, news narratives, and media headlines provided by the Hogan Lovells Government Relations and Public Affairs...

---

## **Financial Daily Dose 6.18.2020 | Top Story: SEC Intervenes to Halt Bankrupt Hertz's Planned Stock Sales**

### **Robins Kaplan LLP**

Some rare last-minute SEC intervention forced Hertz to suspend its planned sale of up to \$500 million in shares of the bankrupt car-rental company...

---

## **Legislation for Business Immunity from Civil Liability for COVID-19 Claims Is Trending**

### **Wilson Elser**

Legislators in multiple jurisdictions are moving forward with laws that provide businesses with varying degrees of immunity from civil liability for...

---

## **Groceries and Beer, a One Stop Shop: How a Potential Ballot Question Could Make This True**

Massachusetts

### **Bowditch & Dewey LLP**

When Massachusetts voters pick up their ballots this November, they may be asked to decide whether all food stores in the Commonwealth should be able...

---

## **Governor Newsom Orders All Californians to Wear Masks in Public**

California

### **Manatt Phelps & Phillips LLP**

On Thursday, June 18, 2020, Governor Newsom and California's Department of Public Health (CDPH) issued an Order requiring all Californians to wear...

---

## **Governor Newsom Signs Law Ordering Mail-in Ballots for November Election**

California

### **Manatt Phelps & Phillips LLP**

On Thursday, June 18, 2020, Governor Gavin Newsom signed into law legislation that requires election officials in California to mail a ballot to...

---

### **Old North State Report - June 19, 2020**

#### **Nelson Mullins Riley & Scarborough LLP**

With the GOP convention being moved to Jacksonville, Fla., many business leaders from Charlotte, N.C., including Republicans...

---

### **A Win for Dreamers: Supreme Court Rejects Bid to end DACA**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The Supreme Court allows DACA to proceed on the grounds that DHS did not meet the regulatory Administrative Procedures Act...

---

### **COVID-19: New York State and New York City Press Conference Weekly Highlights**

New York

#### **Manatt Phelps & Phillips LLP**

Governor Cuomo and Mayor de Blasio provide daily press briefings on the status of New York State and New York City's COVID-19 response. Below, please...

---

### **Body language can matter in the family court**

#### **Stange Law Firm PC**

In any court date in the Family Court, there are a lot of moving parts. For example, if there is a trial or evidentiary hearing, parties are often...

---

### **DACA Survives: SCOTUS Blocks Trump Administration Bid to End Deferred Action for Childhood Arrivals Program**

#### **Ogletree Deakins**

On June 18, 2020, the Supreme Court of the United States issued its decision in DHS v. Regents of the University of California, No. 18-587...

---

### **Scaling the (Geo)Fence: New York Lawmakers Push to Outlaw Geofence Warrants amid Ongoing National Debate for Police Reform**

New York

#### **Duane Morris LLP**

In the wake of national protests against police brutality surrounding the death of George Floyd, and ongoing national debate for police reform, New...

---

### **Gold Dome Report - June 19, 2020**

#### **Nelson Mullins Riley & Scarborough LLP**

While families around the state prepare to celebrate Father's Day weekend, members of the Georgia General Assembly continue to work into the evening...

---

### **Worcester License Commission's Outdoor Table Service Applications**

Massachusetts

#### **Bowditch & Dewey LLP**

Pursuant to the Governor's Executive Order No. 35 issued June 1, 2020 and the



Worcester City Manager's Executive Order issued June 3, 2020, the...

---

**HHS Posts Section 1557 Final Rule and Walks Back Sex-Based Discrimination Protections: Enter *Bostock v Clayton County Bd. of Commissioners***

**Hall Render Killian Heath & Lyman PC**

On June 12, 2020, CMS and the Office for Civil Rights of Health and Human Services ("HHS") posted a display copy of a new final rule that implements...

---

**Missouri extends executive order regarding remote notary services** Missouri

**Buckley LLP**

On June 11, the Missouri governor issued an Executive Order extending, among others, Executive Order 20-08 relating to remote notary services, which...

---

**Update: Legislation for Business Immunity from Civil Liability for COVID-19 Claims Is Trending**

**Wilson Elser**

Louisiana has joined North Carolina, Oklahoma, Utah and Wyoming in adopting laws that grant businesses immunity from civil liability for claims...

---

**EducationCounsel Supports Efforts to Protect Rights of Transgender Students Across the Country**

**Nelson Mullins Riley & Scarborough LLP**

Through its long-standing engagement with GLSEN, a national nonprofit dedicated to promoting and supporting LGBTQ+ inclusive schools...

---

**DEA Proposes 21% Increase in Registration Fees**

**Cote Law PLLC**

To support this doom and gloom prediction, DEA points to several reasons to justify the fee increase. They include, but are not limited to, the...

---

**Gold Dome Report - June 20, 2020**

**Nelson Mullins Riley & Scarborough LLP**

It may be Saturday and the first day of summer, but it is also Legislative Day 35 under the Gold Dome. In a rare weekend convening that was the result...

---

**California Governor Releases New Guidance in Response to COVID-19 Rise**

California

**Gordon Rees Scully Mansukhani**

On June 18, 2020, California's Office of the Governor released new guidance for all Californians in response to the rise in cases for COVID-19. The...

---

**Gold Dome Report - June 18, 2020**

**Nelson Mullins Riley & Scarborough LLP**

What a day under the Gold Dome! The budget, hate crimes legislation, tobacco tax increase efforts, CON amendments, etc. All of these issues are...

---

**CBD Advertisements: What CBD Companies and Celebrity Influencers Need to**



## Know

### Venable LLP

An increasing number of celebrities and social media personalities are endorsing the use of cannabidiol (CBD) products through social media. Many of...

---

## California Department of Health Issues New Guidance on Face Coverings

California

### Davis Wright Tremaine LLP

Under the direction of Governor Gavin Newsom, the California Department of Public Health has issued revised statewide guidance requiring cloth face...

---

## Gold Dome Report - June 22, 2020

### Nelson Mullins Riley & Scarborough LLP

Although the House and Senate each had robust Rules and committee calendars for Legislative Day 36, all eyes were looking towards signals to a...

---

## COVID-19: Massachusetts Begins Step 2 of Phase 2 on June 22

Massachusetts

### Pierce Atwood LLP

Earlier this month, Massachusetts Governor Charlie Baker issued Order 37 initiating Phase 2 of the Commonwealth's four-phased Reopening Plan. The...

---

## President Signs Bill Targeting Human Rights Violators in China into Law

### Baker McKenzie

On June 17, 2020, the President signed the Uyghur Human Rights Policy Act of 2020 into law. The law authorizes the President to impose sanctions on...

---

## UPDATE: California Assembly Adjourns Without Reconsidering Sweeping Mortgage Relief Bill

California

### Troutman Sanders LLP

Yesterday, Troutman Sanders LLP's Consumer Financial Services Law Monitor reported that AB-2501, a proposed bill allowing for homeowners to defer...

---

## U.S. Supreme Court Strikes Down Trump Administration's Rescission of DACA in Department of Homeland Security v. Regents of the University of California

California

### Mintz

Today, in a 5-4 decision, the U.S. Supreme Court upheld three lower court rulings holding that Trump's 2017 move to rescind the Deferred Action for...

---

## North Carolina General Assembly Week in Review

North Carolina

### McGuireWoods Consulting LLC

The North Carolina General Assembly was in full swing this week as legislators aim to adjourn short session by next week. A number of bills ranging...

---

## The Pandemic Has Made It Easier for Plaintiffs to Tell Their Story

### Proskauer Rose LLP

In many respects, the pandemic has created the perfect storm for plaintiff

attorneys, especially in employment cases. By now we are all too familiar...

---

### **Foreign Gift Reporting: New Online Portal Continues Compliance Pressure on Postsecondary Institutions**

**Duane Morris LLP**

On June 22, 2020, the U.S. Department of Education published an electronic announcement reminding institutions of higher education of their mandatory...

---

### **Coronavirus: The Hill and the Headlines - COVID-19 D.C. Update - June 22, 2020**

Washington

**Hogan Lovells**

Your guide to the latest Hill developments, news narratives, and media headlines provided by the Hogan Lovells Government Relations and Public Affairs...

---

### **COVID-19: US State Policy Report - June 23, 2020**

Wisconsin

**Squire Patton Boggs**

This report captures the shifting state, territorial and local government policies and guidance in response to the COVID-19 pandemic and reopening of...

---

### **COVID-19: US State Policy Report - June 18, 2020**

Wisconsin

**Squire Patton Boggs**

This report captures the shifting state, territorial and local government policies and guidance in response to the COVID-19 pandemic and reopening of...

---

### **Gold Dome Report - June 23, 2020**

**Nelson Mullins Riley & Scarborough LLP**

Stars aligned in the Capitol today as the House and Senate reached agreement on the most closely watched issue during the reconvening of the 2020...

---

### **Have Friday Nights replaced Saturday for 'Massacres'? Trump's Stealthy Attempts to Undermine Justice**

**Morvillo Abramowitz Grand Iason & Anello PC**

Some still remember waking to the news following one fateful evening - October 20, 1973, when then-President Richard Nixon, embroiled in the...

---

### **US Executive Branch Update - June 23, 2020**

**Squire Patton Boggs**

This report provides a snapshot of the US Executive Branch priorities via daily schedules and the prior day's press releases...

---

### **Title IX Celebrates 48th Anniversary Amidst Pandemic, Economic, and Societal Challenges**

**Nelson Mullins Riley & Scarborough LLP**

June 23, 2020, marks the 48th anniversary of the enactment of Title IX, the comprehensive federal law prohibiting discrimination on the basis of sex...

---

### **Bowditch Legal Podcasts: Estate Planning Strategies to Use in This Down**



## Market [Audio](#)

### **Bowditch & Dewey LLP**

Listen to Bowditch partner and estate planning attorney Rebecca MacGregor discuss estate planning strategies to use during this down market.

---

## **COVID-19 Washington Update: June 22, 2020**

### **Kelley Drye & Warren LLP**

On Friday, SBA and the Treasury Department announced an agreement with bipartisan leaders of the Senate Committee on Small Business...

---

## **Key Changes to US Shelter-In-Place / Reopening Orders [Current as of June 19]**

### **Baker McKenzie**

The Governors of Georgia, Hawaii, Vermont and Wyoming extended their State's shelter in place orders...

---

## **President Trump to Nominate SEC Chair Clayton as U.S. Attorney for SDNY**

### **Cadwalader Wickersham & Taft LLP**

Attorney General William P. Barr announced that President Donald J. Trump will nominate SEC Chair Jay Clayton as U.S. Attorney for the Southern...

---

## **Federal Courts Issue Guidance for Jury Trials During COVID-19: What Litigators Need to Know**

### **Jackson Lewis PC**

The U.S. Courts' COVID-19 Judicial Task Force has released guidance on conducting jury trials and convening grand juries during the pandemic. The...

---

## **The Unfolding Shape of the New National Security Law for Hong Kong**

### **Akin Gump Strauss Hauer & Feld LLP**

Following the decision taken by China's National People's Congress to adopt a new National Security Law (the "Security Law") for the Hong Kong...

---

## **Senate Introduces the "Safeguarding American Innovation Act," Targeting Foreign Influence and Unreported Foreign Ties in Research**

### **Ropes & Gray LLP**

Last Thursday, June 18, a long-awaited, bipartisan bill to address the federal government's concerns about "foreign influence" in research, the...

---

## **Bowditch Legal Podcasts: Overlooked Estate Planning Tools [Audio](#)**

### **Bowditch & Dewey LLP**

Listen to Bowditch partner and estate planning attorney Rebecca MacGregor discuss what estate planning tools might have been overlooked before...

---

## **US Executive Branch Update - June 19, 2020**

### **Squire Patton Boggs**

This report provides a snapshot of the US Executive Branch priorities via daily schedules and the prior day's press releases...

---

## **US Executive Branch Update - June 22, 2020**

### **Squire Patton Boggs**

This report provides a snapshot of the US Executive Branch priorities via daily schedules and the prior day's press releases

---

## **SEC Names New Associate Director in the Division of Enforcement**

### **Cadwalader Wickersham & Taft LLP**

The SEC named Jennifer S. Leete the new Associate Director in the Division of Enforcement. Ms. Leete will succeed Antonia Chion, who retired in...

---

## **Coronavirus: The Hill and the Headlines - COVID-19 D.C. Update - June 23, 2020**

Washington

### **Hogan Lovells**

Your guide to the latest Hill developments, news narratives, and media headlines provided by the Hogan Lovells Government Relations and Public Affairs...

---

## **Covid-19: Government Measures**

### **Linklaters LLP**

Covid-19: Government Measures March 2020 In response to the outbreak of Covid-19, governments around the world are introducing measures and...

---

## **US Executive Branch Update - June 24, 2020**

### **Squire Patton Boggs**

This report provides a snapshot of the US Executive Branch priorities via daily schedules and the prior day's press releases...

---

## **Boise, Idaho Is First In The Nation To Reintroduce COVID-19 Restrictions**

Idaho

### **Bryan Cave Leighton Paisner LLP**

Ada County - home to Boise, Idaho - entered Phase IV of Idaho's Reopening Plan on June 13, 2020, but on Wednesday, June 24, 2020, will return to...

---

## **Presidential Proclamation Extends Green Card Limitations and Reduces Temporary Visas**

### **Thompson Hine LLP**

Yesterday, President Trump extended his April proclamation limiting the issuance of green cards and additionally put in place limits on temporary...

---

## **New Ways of Notarization During the COVID Pandemic**

### **Squire Patton Boggs**

If you regularly have documents notarized as part of your practice, you're probably like me. Under normal circumstances, you probably have the...

---

## **Coronavirus: The Hill and the Headlines - COVID-19 D.C. Update - June 24, 2020**

Washington

### **Hogan Lovells**

Your guide to the latest Hill developments, news narratives, and media headlines provided by the Hogan Lovells Government Relations and Public Affairs...



---

## **U.S. Expands Syria Sanctions By Targeting Non-U.S. Persons Who Support the Assad Regime**

### **Dechert LLP**

The U.S. Government, through the Treasury Department's Office of Foreign Assets Control ("OFAC"), has imposed comprehensive sanctions against Syria...

---

## **Massachusetts Updates Sector-Specific Safety Standards for Phase 2 Step 2 of Economic Reopening**

Massachusetts

### **Greenberg Traurig LLP**

Effective June 22, 2020, Massachusetts moves into Step 2 of Phase 2 of the Four-Phase Reopening Plan. Businesses permitted to reopen in Step 2 can...

---

## **California Requires Face Masks as Coronavirus Cases Increases**

California

### **Greenberg Traurig LLP**

As California enters Stage 2 of its "Resilience Roadmap" plan to reopen, California Governor Gavin Newsom and the California Department of Public...

---

## **States Expand COVID-19-Related Immunity and Provide Guidance to Businesses Reopening**

### **Winston & Strawn LLP**

Along with the expansive tort liability immunity offered by the recent Declaration of the Secretary of the Department of Health and Human Services...

---

## **Comparing Presidential Healthcare Campaign Policy Positions**

### **Manatt Phelps & Phillips LLP**

Healthcare is one of several key issues on voters' minds in the upcoming presidential election. According to a June CNN poll, healthcare is near the...

---

## **New York State Police and Criminal Justice Reforms Enacted Following George Floyd's Death**

New York

### **Greenberg Traurig LLP**

The death of George Floyd, an unarmed and handcuffed African-American man, during an encounter with now-fired City of Minneapolis police officers...

---

## **European regulatory update for asset managers**

Audio

### **Ropes & Gray LLP**

Welcome to the fourth installment of Ropes & Gray's European regulatory podcast for asset managers. These fortnightly podcasts and accompanying...

---

## **COVID-19: US State Policy Report - June 22, 2020**

Wisconsin

### **Squire Patton Boggs**

This report captures the shifting state, territorial and local government policies and guidance in response to the COVID-19 pandemic and reopening of...

---





## Global

### Employment & Labor



#### **COVID-19 Labor Law FAQ for Employers in Mainland Southeast Asia**

**Tilleke & Gibbins**

The COVID-19 pandemic has led to shutdowns, lockdowns, and quarantines around the world, forcing companies into drastic cost-cutting measures to...

#### **Global: COVID-19: Protecting Minds in Uncertain Times - An Employer's Guide to Securing the Mental Health of Their Workforce**

**Baker McKenzie**

In this special webcast by our regional Employment & Compensation team, Baker McKenzie Employment Partners Michael Michalandos, Celeste Ang and Rowan...

#### **Protection from dismissal: the rules for employee representatives in 10 key jurisdictions**

**Ius Laboris**

To what extent are (non) elected employee representatives of the Works Council protected against dismissal under local legislation? In this report...

### Environment & Climate Change



#### **Aviation Industry Sustainability Must Include New International Waste Rules**

**Baker McKenzie**

The aviation industry has been hard-hit by the recent pandemic. In many, though not all countries, environmental performance conditions have been...

#### **The principles of ecologically sustainable development in Australia and internationally**

**Corrs Chambers Westgarth**

The meaning of ecologically sustainable development (ESD) has been described as "elusive", as it differs from one jurisdiction to another...

#### **Are you reframing your future or is the future reframing you?**

**EY Law**

The world changed in March. The COVID-19 pandemic has strained health care systems to breaking point, put much of the global economy...

#### **South Africa: COVID-19 and the imperative for sustainable development**

**ENSafrica**

Many articles ask readers to imagine a post Coronavirus (COVID-19) world. However, it is difficult to do so when we have no idea when the pandemic...

### Internet & Social Media



#### **Will Virtual Shareholder Meetings Become the New Normal?**

### **Hunton Andrews Kurth LLP**

One novel feature of the 2020 proxy season has been the surge in virtual shareholder meetings. For example, one provider of virtual meeting services...

### **ISO-konforme Datenschutzinformation und Einwilligung im Onlinebereich**

#### **Knyrim Trieb Rechtsanwälte**

Die Welt der internationalen Normung ist einen ISO/IEC-Standard reicher. Letzte Woche wurde für die Themenbereiche der Datenschutzinformation und der...

### **Éléments de stratégie de gestion de portefeuilles de noms de domaine en temps de pandémie**

#### **IP Twins**

L'analyse des décisions UDRP rendues à l'issue de procédures commencées pendant la pandémie de COVID-19 rappelle l'impossibilité de prévoir tous les...

#### Legal Practice



### **Essential soft skills for lawyers - author Kim Tasso's research findings**

#### **Globe Law and Business**

Between August 2019 and March 2020 I analysed information relating to the importance of soft skills within and beyond the legal profession. I...

#### Projects & Procurement



### **A non-exhaustive list of recent measures aimed at curbing the spread of Coronavirus (COVID-19)**

#### **ENSafrica**

World: The World Tourism Organization (UNWTO) has released a set of guidelines to help tourism sector emerge stronger and more sustainably from...

### **Africa Business in Brief - ISSUE 356 | 14 JUN 2020**

#### **ENSafrica**

Africa: Africa's aviation industry will suffer an estimated revenue loss of USD8.103-billion this year as a result of COVID-19 pandemic, according to...

#### Public



### **Nuevas realidades para América Latina de la protección a la consulta previa con CIDH sentencia**

#### **Holland & Knight LLP**

La Corte Interamericana de Derechos Humanos (CIDH) emitió sentencia en el caso de Comunidades Indígenas Miembros de la Asociación Lhaka Honhat...

### **High Court holds s.236(3) of the Insolvency Act 1986 does not have extra-territorial effect, except where the EU Insolvency Regulation applies**

#### **Herbert Smith Freehills LLP**

The High Court has held that s.236 of the Insolvency Act 1986 ("IA 1986") does



not have extra-territorial effect, so that the court is not generally...

## Other top stories

**Updated Country-by-Country Guide: Government Measures Taken in Response to COVID-19**

---

**What did you miss? Five things that happened while all eyes were on COVID-19**

---

**July 2020 Visa Bulletin -Backlogs Persist, but India Advances at a Quicker Pace**

---

**COVID-19: How to mitigate the next phase of compliance risks**

---

**Colorado Implements New Paid Sick Leave Requirements Extending Beyond COVID-19 Issues**

---

**Illinois Bankruptcy Court Takes First Swing at Applying Force Majeure to Nonperformance Due to COVID-19**

---

**Data Sharing Without Borders**

---

**EEOC Delivers Hefty Fine for Disability Discrimination**

---

**Legally Bombed: Reese Witherspoon's Clothing Company Earns Failing Grade on 'Free Dress' Giveaway**

---

**Six Strategies for Effective AML Compliance That Avoids Regulatory Scrutiny**

---

## International developments

**Employment & Labor in Canada - Quebec (Quebec)**

---

**UK immigration beyond lockdown**

---

**UK Drops Consumer Online ADR Requirement Due to Brexit**

---

**Keeping Data Secure While Working Remotely**

---

**Publishers Sue Internet Archive for free access to E-books**

---

**Covid-19: a practical guide to data protections practices in workplace testing in the UK - France - Germany**

---

**Singapore: retrenchment benefits**

---

**Minimum Wage increase 2020 - wages rise by 1.75%**

---

**Project finance in Turkey**

---

**Project finance in Thailand**

---

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law

[Contact Lexology](#)

[About Lexology](#)



© 2006-2020 Law Business Research



From: [Homeland Security News Wire](#)  
To: [info@hcn.org](mailto:info@hcn.org)  
Subject: Visas & Business | Virus & Violence | Irish Police Lessons  
Date: Thursday, June 25, 2020 4:16:17 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)

?

?

## DAILY REPORT

BIOMETRICS BORDER/IMMIG. BUSINESS CYBERSECURITY DETECTION DISASTERS GOVERNMENT INFRASTRUCTURE  
PUBLIC HEALTH PUBLIC SAFETY REGIONAL SCI-TECH SURVEILLANCE TERRORISM TRANSPORTATION WATER

Thursday 25 June 2020 vol. 14 no. 124

### Terrorism

## Growing Terrorism Threats: Iran-backed groups, IS in Africa, and White Supremacists: State Dept. Report

The Trump administration, noting significant victories against global terrorism, says Iran continues to increase its support for extremists, while IS is increasing its presence in Africa and Southeast Asia. Attacks by white supremacists are on the rise, and the terrorism threat posed by white nationalists is of particular concern.

[Read more](#)

### Visas & the economy

## Visa Ban Strikes Another Blow at Cross-Border Labor Flows

By Rob Garver

President Donald Trump's executive order this week to extend and expand a ban on issuing visas to certain classes of foreign workers — ostensibly to preserve 525,000 jobs for hard-pressed American workers — was celebrated by advocates of decreased immigration. But business leaders and economists worry that in addition to doing short-term damage to some sectors of the U.S. economy, it could also make talented professionals from overseas less willing to relocate to the United States in the future.

[Read more](#)

?

### Extremism

## Viruses and Violence: How COVID-19 Has Impacted Extremism

By Stevie Kiesel

In April 2020, the Tony Blair Institute acknowledged that “extremist groups are beginning to recognize the scale of the COVID-19 pandemic, seeing opportunities to exploit fears, exacerbate tensions and mobilize supporters while government are occupied with trying to address COVID-19.” Extremists across the ideological spectrum have incorporated the pandemic into their messaging and their operations, though groups have differed on just what COVID-19 means and how to best exploit the pandemic and its resultant unrest.

[Read more](#)

### Cybersecurity education

## UA Little Rock to Offer New Bachelor's Degree in Cybersecurity

The University of Arkansas at Little Rock is introducing a new four-year degree program in cybersecurity in the fall 2021 semester to help meet the

rising demand for cybersecurity professionals. The university says the new degree program will attract more government and industry jobs to the region, while helping to fill a growing need for more trained cybersecurity professionals.

[Read more](#)

#### First responders

### Gear Treated with “Forever Chemicals” Poses Risk to Firefighters

Firefighters face occupational hazards on a daily basis. Now, new research shows they face additional risk just by gearing up. Fabric used for firefighter turnout gear tested positive for the presence of per- and polyfluorinated alkyl substances (PFAS), according to a new study.

[Read more](#)

#### Energy security

### Uncertainty in Renewable Energy Regulation Leads to Electricity Price Volatility

Incorporating renewable energies into the electricity system entails a certain degree of volatility in the electricity price owing to the intermittent nature of generation by plants of this type. However, a study by the UPV/EHU shows that the greatest volatility is caused when unexpected regulatory changes are made in the renewable sector. What disrupts economic players most is uncertainty.

[Read more](#)

#### Argument

### Nuclear Alarmism: Proliferation and Terrorism

Alarmism about nuclear weapons is common coin in the foreign policy establishment, John Mueller writes. He notes that during the course of the Cold War, for example, the chief concern was that the weapons would somehow go off, by accident or by intention, devastating the planet in the process. More recently, the worry has been that terrorists would get their hands on nuclear weapons. Concerns about the dangers inherent in nuclear proliferation and in nuclear terrorism certainly seem overwrought, Mueller writes, concluding: “There may be reason for concern, or at least for interest and watchfulness. But alarm and hysteria (not to mention sleeplessness) are hardly called for.”

[Read more](#)

#### Perspective

### Northern Ireland’s Lessons for American Policing

Not that long ago, Americans would regularly go to Northern Ireland to offer advice on reforming the region’s notoriously repressive policing. Martin S. Flaherty writes that happily for Northern Ireland, and tragically for the United States, the lessons now run in the other direction. The 1998 Good Friday Agreement changed Northern Ireland, and one of the major changes was a profound reform of policing methods – and of the police itself: The Royal Ulster Constabulary (RUC), Northern Ireland’s police force, which reflected the Protestant majority almost exclusively, was replaced with the Police Service of Northern Ireland (PSNI), which was much more reflective of Northern Ireland’s society and sensibilities. ““None of this is to say that policing in Northern Ireland today lacks problems or critics. But the PSNI is nonetheless widely regarded as a substantial step in the right direction,” Flaherty writes. “Those seeking a hopeful model for change would do well to look to a land where change once seemed hopeless.”

[Read more](#)

#### Our picks

### Bioterrorists Cooperation | Russia Targets U.S. Infrastructure | EMP First Strike, and more

- Far-Right Obsession with Bioterror Could Lead to Work with al-Qaeda, Iran
- Sahara Dust Cloud Looms Over Cuba, Caribbean and Florida
- China is Retooling, and Russia Seeks Harm to Critical Infrastructure

- U.S. Soldier's Alleged Connection to Satanic Nazi Extremist Group Renews Calls to Ban It
- Neo-Nazi Memoir Describes Terror Group's Acid-Soaked Ram Sacrifice
- Lawsuit Alleges Scientific Misconduct at U.S. Nuclear Weapons Lab
- How the U.S. military has failed to address white supremacy in its ranks
- Rise in Far-Right and Islamic Extremism Activity in Ireland Last Year, Says Europol
- China Has "First-Strike" Capability to Melt U.S. Power Grid with Electromagnetic Pulse Weapon
- What Are the Key Tenets of China's Propaganda Regime? – Analysis

[Read more](#)

## Also noted

- Local de-radicalization programs effectively combat extremism: study
- U.S. Economic Losses from Severe Weather During May Topped \$4 Billion: Aon
- Securing voter registration databases takes on added importance in pandemic, DHS official says
- DDoSecrets' mission is 'unchanged' in wake of 'Blue Leaks' Twitter ban
- Senate Republicans target encryption with bill aimed at Apple, Facebook, other tech giants

[Read more](#)

---

BIOMETRICS | BORDER/IMMIG. | BUSINESS | CYBERSECURITY | DETECTION | DISASTERS | GOVERNMENT | INFRASTRUCTURE  
PUBLIC HEALTH | PUBLIC SAFETY | REGIONAL | SCI-TECH | SURVEILLANCE | TERRORISM | TRANSPORTATION | WATER

---

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)

---

Advertising & Marketing [advertise@newswirepubs.com](mailto:advertise@newswirepubs.com)

Editorial [editor@newswirepubs.com](mailto:editor@newswirepubs.com)

General [info@newswirepubs.com](mailto:info@newswirepubs.com)

2010-2011 © News Wire Publications, LLC News Wire Publications, LLC

220 Old Country Road | Suite 200 | Mineola | New York | 11501

[Permissions and Policies](#)



Homeland Security News Wire, 220 Old Country Road, Suite 200, Mineola, NY 11501

SafeUnsubscribe™ [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)


[Forward email](#) | [Update Profile](#) | [About our service provider](#)






Sent by [hsnewswire@newswirepubs.com](mailto:hsnewswire@newswirepubs.com)




**From:** [Dark Reading Weekly](#)  
**To:** [lbargueno@sunnyvale.ca.gov](mailto:lbargueno@sunnyvale.ca.gov)  
**Subject:** What Will Cybersecurity's "New Normal" Look Like? | Cloud Threats and Priorities  
**Date:** Thursday, June 25, 2020 8:36:26 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



Follow Dark Reading:  


June 25, 2020



## LATEST SECURITY NEWS & COMMENTARY

**What Will Cybersecurity's 'New Normal' Look Like?**  
The coronavirus pandemic has forced changes for much of the business world, cybersecurity included. What can we expect going forward?

**'GoldenSpy' Malware Hidden in Tax Software Spies on Companies Doing Business in China**  
Advanced persistent threat (APT) campaign aims to steal intelligence secrets from foreign companies operating in China.

**Cybercrime Infrastructure Never Really Dies**  
Despite the takedown of the "CyberBunker" threat operators in 2019, command-and-control traffic continues to report back to the defunct network address space.

**Black Hat Survey: Breach Concerns Hit Record Levels Due to COVID-19**  
Annual "Black Hat USA Attendee Survey" indicates unprecedented concern over possible compromises of enterprise networks and US critical infrastructure.


**Firmware Flaw Allows Attackers to Evade Security on Some Home Routers**  
Networking devices sold under at least one major brand have a firmware vulnerability that allows hackers to take control of the device, a cybersecurity firm claims.

**Long-Term Effects of COVID-19 on the Cybersecurity Industry**  
The maelstrom of change we're going through presents a unique opportunity to become enablers. And to do that requires flex bility.

**Average Cost of a Data Breach: \$116M**  
Sensitivity of customer information and time-to-detection determine financial blowback of cybersecurity breaches.

**How to Secure Machine Learning**  
Part two of a series on avoiding potential security risks with ML.

[MORE NEWS & COMMENTARY](#)



## HOT TOPICS

**What's Anonymous Up to Now?**  
The hacker group recently took credit for two high-profile incidents -- but its actions aren't quite the same as they once were, some say.

## EDITORS' CHOICE

**Cloud Threats and Priorities as We Head Into the Second Half of 2020**  
With millions working from home and relying on the cloud, security leaders are under increasing pressure to keep their enterprises breach-free.

**COVID-19: Latest Security News & Commentary**  
Check out Dark Reading's updated, exclusive news and commentary surrounding the coronavirus pandemic.

**Have Your Say: Dark Reading Video News Desk Seeks Reader Contributions**  
We've got questions for you on black infosec, burnout, vulnerabilities, COVID-19, and much more. Send us your video responses and we'll play them in our News Desk broadcast during Black Hat Virtual.

## NEW FROM THE EDGE

**How to Wring Every Last Drop Out of Your Security Budget**  
In the face of tighter budgets and lowered spending forecasts due to the pandemic, optimizing and improving the efficiency of security programs -- without sacrificing integrity -- has never been more important.

## Tech Resources

[How to Find the Right Management for Your Cloud](#)

[Increase Your Cyber Defense Effectiveness](#)

[How to Build a 'DefenderSphere' Map for OT Security](#)

[Headline Vulnerabilities: How Media Coverage Shapes the Perception of Risk](#)

[SANS Whitepaper: Practical Industrial Control System Cybersecurity](#)

[Dartmouth Transforms the Campus Experience with AI-Driven Insight and Automation](#)

[Secure Everywhere: The power of integrated internet, endpoint, and email security](#)

[ACCESS TECH LIBRARY NOW](#)

[Why Performance Testing is More Critical Today](#)



**Hosting Provider Hit With Largest-Ever DDoS Attack**  
Likely looking to make a statement, attackers targeted specific websites hosted by a single provider with a 1.44 terabit-per-second distributed denial-of-service attack, according to Akamai.

**Healthcare CISOs Share COVID-19 Response Stories**  
Cybersecurity leaders discussed the threats and challenges that arose during the pandemic, and how they responded, during a virtual roundtable.

[MORE](#)

In this InformationWeek webinar, experts will help enterprise teams understand what they should expect from performance testing solutions and how to put them to work most efficiently.

#### **IT Automation: Scaling to the Future**

Experts will examine the layers of automation and orchestration in IT operations, and how they can provide high availability and greater scale for modern applications and business demands.

[MORE WEBINARS](#)

## **FEATURED REPORTS**

### **CyberSecurity Trends 2020**

#### **2020 SANS Cyber Threat Intelligence (CTI) Survey**

This new survey from the SANS Institute explores how cyber threat intelligence has evolved over the last year.

[MORE REPORTS](#)

## **CURRENT ISSUE**



**How Cybersecurity Incident Response Programs Work  
(and Why Some Don't)**

[DOWNLOAD THIS ISSUE](#)

[SUBSCRIBE NOW](#)

[BACK ISSUES](#) | [MUST READS](#) | [TECH DIGEST](#)

## **PRODUCTS & RELEASES**

**WatchGuard Technologies Report Finds Two-Thirds of Malware is Encrypted, Invisible Without HTTPS Inspection**

**Blueliv and King & Union Announce Threat Intelligence Partnership**

**Authomize Secures \$6M Seed Funding for Automated Authorization and Security**

**Small Businesses Continue to Underestimate Cyberthreats Even as More Work Remotely**

**RangeForce Debuts New Cyberskills Platform**

[MORE PRODUCTS & RELEASES](#)

### **Dark Reading Weekly**

— Published By **Dark Reading**

Informa Tech

303 Second St., Suite 900 South Tower, San Francisco, CA 94107

### **Keep This Newsletter Out Of Your SPAM Folder**

Don't let future editions go missing. Take a moment to add the newsletter's address to your anti-spam white list:

To update your profile, change your e-mail address, or unsubscribe, [click here](#).

To opt-out of any future Dark Reading Weekly Newsletter emails, please respond [here](#).

Thoughts about this newsletter? [Give us feedback](#).

If you're not sure how to do that, ask your administrator or ISP. Or check your anti-spam utility's documentation.

We take your privacy very seriously. Please review our [Privacy Statement](#).

**From:** [While You Were Working SmartBrief](#)  
**To:** [angelachan@sunnyvale.ca.gov](mailto:angelachan@sunnyvale.ca.gov)  
**Subject:** Women continued to pay the "child penalty" ... Limited research suggested coronavirus might trigger diabetes ... A dust storm from Africa hit Florida ... Canned wine came of age  
**Date:** Wednesday, June 24, 2020 1:51:56 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



Created for [angelachan@sunnyvale.ca.gov](mailto:angelachan@sunnyvale.ca.gov) | [Web Version](#)

June 24, 2020

CONNECT WITH SMARTBRIEF ☐ ☐ ☐



News, Not Noise

SIGN UP · SHARE



THIS HAPPENED

Women continued to pay the "child penalty"

## Women continued to pay the "child penalty"



(PH LIPPE HUGUEN/Getty Images)

**Why it matters:** Experts concluded long ago that the career earnings of women often suffer the cost of a "child penalty." New research suggests two policies often prescribed to reduce the child penalty show differing outcomes. Subsidized, high-quality child care was shown to reduce the child penalty by as much as 25%. Meanwhile, increased allotments of paternity leave, aimed at enabling fathers to handle more child care responsibilities, have done little to reduce the child penalty. **Full Story:** [USC News \(University of Southern California\)](#) (6/24)



## Twitter twisted itself into knots over "BlueLeaks"

**Why it matters:** Twitter has found itself in a bit of a sticky wicket over the banning of the primary account associated with "BlueLeaks," which is a trove of internal documents pilfered from law enforcement agencies. Twitter claims it banned the account because the documents were hacked and could cause real-world harm. But when pressed about why the account was banned while accounts linked to groups like WikiLeaks and Anonymous remain active, Twitter has so far failed to provide any logical answers. **Full Story:** [Ars Technica](#) (6/23)



## A "Godzilla dust storm" from the Sahara Desert hit Florida



**Why it matters:** A spike in coronavirus cases might not be the only respiratory concern hitting the Sunshine State. A massive dust storm that originated in the Sahara Desert has crossed the Atlantic and is expected to diminish air quality in Florida and other Gulf states. Such dust clouds are a regular occurrence, but this version is abnormally large.**Full Story:** [LiveScience](#) (6/24)



## Google started fact-checking images

**Why it matters:** The old adage "seeing is believing" died long ago, so this is just another nail in that coffin.**Full Story:** [TechRadar \(UK\)](#) (6/24)



## The FCC pondered an easier-to-remember suicide prevention hotline

**Why it matters:** Pop quiz: Do you know the phone number for the suicide prevention hotline in your area? In the US, the national number is 1-800-273-8255 (TALK). But that might change soon when the FCC votes on changing the number to 988. This seems like a good idea because in times of mental crisis, a number that is easier to remember might save lives.**Full Story:** [Engadget](#) (6/23)



## These 6 things made meetings and email more effective

**Why it matters:** We've all been in meetings that should have been an email and read emails that were waaaaaaa too long. This article highlights six steps to maximize the use of email and meetings, including weekly chunks of time where no meetings are scheduled.**Full Story:** [The Boston Consulting Group](#) (6/17)



---

### SMARTTALK



## The coronavirus shifted the education landscape

**Why it matters:** We tried something new. My colleague Kanoe Namahoe covers the Education sector for SmartBrief, so she's had a front-row seat as the coronavirus disrupted education from kindergarten all the way up through colleges and universities.

Rather than ask Kanoe to write some long article, I thought I'd just invite her to have a chat about the lessons learned from the last few months. She also shared some excellent sources you can follow to keep tabs on how the future of education is taking shape.

**Send me your feedback:** What do you think of this kind of content? [Shoot me an email](#) to let me know if you found it valuable ... or how it could be improved.

---

## FOR YOUR VIEWING PLEASURE

### NASA simulated sunsets on other planets

**Why it matters:** Considering how much love we give sunsets here at WYWW, I just couldn't resist sharing these sunsets that are out of this world. **Full Story:** [CNET](#) (6/24)



---

## CORONAVIRUS CORNER

### Limited research suggested coronavirus might trigger diabetes

**Why it matters:** Like much of the medical research associated with the coronavirus, there is still more work to be done, but early evidence suggests the virus might trigger diabetes in some people. Right now, this is just a hypothesis. But studies like this are yet another reminder that while patients might survive the coronavirus, that doesn't mean the virus will leave their long-term health unscathed. **Full Story:** [Nature \(free content\)](#) (6/24)

---

## ON THE ROAD WITH WYWW

### Archaeologists found new clues about Stonehenge

**Why it matters:** Today's dose of mental vacationing takes you to one of the most mystical places on Earth.

The discovery of deep pits surrounding Durrington Walls, a large Neolithic hedge located

about two miles from Stonehenge, answered some questions about the humans who lived in the area 4,500 years ago. **Full Story:** [Smithsonian](#) (6/2020)



## THE DAGGER BALL

### Restarting high school sports seemed unlikely

**Why it matters:** I have a sneaky suspicion many high schools will have to backpedal faster than Deion Sanders away from plans to restart athletics this fall. While pro sports leagues and some colleges have the medical and financial resources to afford regular testing for the coronavirus, that is not the case for most high schools. **Full Story:** [The Conversation](#) (6/24)



## YOUR FUTURE

- [...Might include airlines getting smarter about managing delays](#)

University of Illinois (6/22)

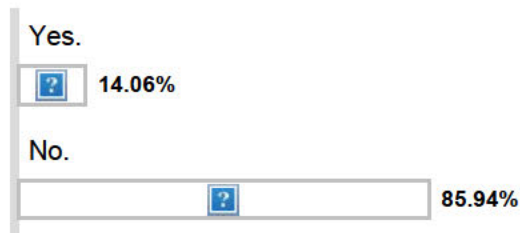
- [...Can include getting a free Whopper from Burger King](#)

CNET (6/24)

## SURVEY RESULTS

*Here are the results of yesterday's reader poll. There were 1,201 responses.*

### Do you keep a regular journal?



## HAPPY HOUR FUN

### Canned wine came of age

**Why it matters:** Trends in direct-to-consumer alcohol sales have powered the growth of

canned wine. The stigma once associated with such wines has receded as quality has improved. **Full Story:** [Forbes](#) (6/24)



**POLL QUESTION:**

**Have you tried canned wine?**

☐ Yes.

☐ No.

---

#### WYWW PLAYLIST

### "Red Red Wine" by UB40

There is a [WYWW playlist](#) on Spotify to keep track of all the songs listed in this space.

[Click here](#) to follow the playlist.



---

#### ENJOY THE VIEW



## Sunset in Paris



(Mr. Le Papillon)

## Sunset in Paris

If you look really close, you can see Place de la Concorde aligned with the Arc de Triomphe. This photo was submitted by Mr. Le Papillon. **Full Story:** [Flickr](#) (6/24)



---

## ABOUT THE EDITORS

### Sean McMahon



*Since I joined SmartBrief in 2003, I have produced content on a variety of topics including finance, energy, infrastructure, politics, telecommunications and international development.*

*Wow. I knew the sweet, flowing locks of my pandemic haircut were loooooong, but that video made me realize just how long. Oof.*

*If you like WYWW, hate WYWW or want to submit a story, [shoot me an email](#). Yes, I actually read them.*

The kindest compliment you can pay to WYWW is to send [this link](#) to your friends, family and colleagues so they can subscribe. Thanks!



*No matter where you're from, your dreams are valid.*

Lupita Nyong'o,  
actress, writer



Sharing While You Were Working SmartBrief with your network keeps the quality of content high and these newsletters free.

**Help Spread the Word**

**SHARE**

Or copy & share your personalized link:

**[smartbrief.com/wyww/?referrerId=kiisjVSSMX](https://smartbrief.com/wyww/?referrerId=kiisjVSSMX)**



SmartBrief publishes more than 200 free industry newsletters - [Browse our portfolio](#)

[Sign Up](#) | [Update Profile](#) | [Advertise with SmartBrief](#)

[Unsubscribe](#) | [Privacy policy](#)

**CONTACT US: [FEEDBACK](#) | [ADVERTISE](#)**



SmartBrief, Inc.®, 555 11th ST NW, Suite 600, Washington, DC 20004

**From:** [While You Were Working SmartBrief](#)  
**To:** [mrodriguez@sunnyvale.ca.gov](mailto:mrodriguez@sunnyvale.ca.gov)  
**Subject:** Women continued to pay the "child penalty" ... Limited research suggested coronavirus might trigger diabetes ... A dust storm from Africa hit Florida ... Canned wine came of age  
**Date:** Wednesday, June 24, 2020 1:51:51 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



Created for [mrodriguez@sunnyvale.ca.gov](mailto:mrodriguez@sunnyvale.ca.gov) | [Web Version](#)

June 24, 2020

CONNECT WITH SMARTBRIEF ☐ ☐ ☐



News, Not Noise

SIGN UP · SHARE



THIS HAPPENED

Women continued to pay the "child penalty"

## Women continued to pay the "child penalty"



(PH LIPPE HUGUEN/Getty Images)

**Why it matters:** Experts concluded long ago that the career earnings of women often suffer the cost of a "child penalty." New research suggests two policies often prescribed to reduce the child penalty show differing outcomes. Subsidized, high-quality child care was shown to reduce the child penalty by as much as 25%. Meanwhile, increased allotments of paternity leave, aimed at enabling fathers to handle more child care responsibilities, have done little to reduce the child penalty. **Full Story:** [USC News \(University of Southern California\)](#) (6/24)



## Twitter twisted itself into knots over "BlueLeaks"

**Why it matters:** Twitter has found itself in a bit of a sticky wicket over the banning of the primary account associated with "BlueLeaks," which is a trove of internal documents pilfered from law enforcement agencies. Twitter claims it banned the account because the documents were hacked and could cause real-world harm. But when pressed about why the account was banned while accounts linked to groups like WikiLeaks and Anonymous remain active, Twitter has so far failed to provide any logical answers. **Full Story:** [Ars Technica](#) (6/23)



## A "Godzilla dust storm" from the Sahara Desert hit Florida



**Why it matters:** A spike in coronavirus cases might not be the only respiratory concern hitting the Sunshine State. A massive dust storm that originated in the Sahara Desert has crossed the Atlantic and is expected to diminish air quality in Florida and other Gulf states. Such dust clouds are a regular occurrence, but this version is abnormally large.**Full Story:** [LiveScience](#) (6/24)



## Google started fact-checking images

**Why it matters:** The old adage "seeing is believing" died long ago, so this is just another nail in that coffin.**Full Story:** [TechRadar \(UK\)](#) (6/24)



## The FCC pondered an easier-to-remember suicide prevention hotline

**Why it matters:** Pop quiz: Do you know the phone number for the suicide prevention hotline in your area? In the US, the national number is 1-800-273-8255 (TALK). But that might change soon when the FCC votes on changing the number to 988. This seems like a good idea because in times of mental crisis, a number that is easier to remember might save lives.**Full Story:** [Engadget](#) (6/23)



## These 6 things made meetings and email more effective

**Why it matters:** We've all been in meetings that should have been an email and read emails that were waaaaaaa too long. This article highlights six steps to maximize the use of email and meetings, including weekly chunks of time where no meetings are scheduled.**Full Story:** [The Boston Consulting Group](#) (6/17)



---

### SMARTTALK



## The coronavirus shifted the education landscape

**Why it matters:** We tried something new. My colleague Kanoe Namahoe covers the Education sector for SmartBrief, so she's had a front-row seat as the coronavirus disrupted education from kindergarten all the way up through colleges and universities.

Rather than ask Kanoe to write some long article, I thought I'd just invite her to have a chat about the lessons learned from the last few months. She also shared some excellent sources you can follow to keep tabs on how the future of education is taking shape.

**Send me your feedback:** What do you think of this kind of content? [Shoot me an email](#) to let me know if you found it valuable ... or how it could be improved.

---

## FOR YOUR VIEWING PLEASURE

### NASA simulated sunsets on other planets

**Why it matters:** Considering how much love we give sunsets here at WYWW, I just couldn't resist sharing these sunsets that are out of this world. **Full Story:** [CNET](#) (6/24)



---

## CORONAVIRUS CORNER

### Limited research suggested coronavirus might trigger diabetes

**Why it matters:** Like much of the medical research associated with the coronavirus, there is still more work to be done, but early evidence suggests the virus might trigger diabetes in some people. Right now, this is just a hypothesis. But studies like this are yet another reminder that while patients might survive the coronavirus, that doesn't mean the virus will leave their long-term health unscathed. **Full Story:** [Nature \(free content\)](#) (6/24)

---

## ON THE ROAD WITH WYWW

### Archaeologists found new clues about Stonehenge

**Why it matters:** Today's dose of mental vacationing takes you to one of the most mystical places on Earth.

The discovery of deep pits surrounding Durrington Walls, a large Neolithic hedge located

about two miles from Stonehenge, answered some questions about the humans who lived in the area 4,500 years ago. **Full Story:** [Smithsonian](#) (6/2020)



## THE DAGGER BALL

### Restarting high school sports seemed unlikely

**Why it matters:** I have a sneaky suspicion many high schools will have to backpedal faster than Deion Sanders away from plans to restart athletics this fall. While pro sports leagues and some colleges have the medical and financial resources to afford regular testing for the coronavirus, that is not the case for most high schools. **Full Story:** [The Conversation](#) (6/24)



## YOUR FUTURE

- [...Might include airlines getting smarter about managing delays](#)

University of Illinois (6/22)

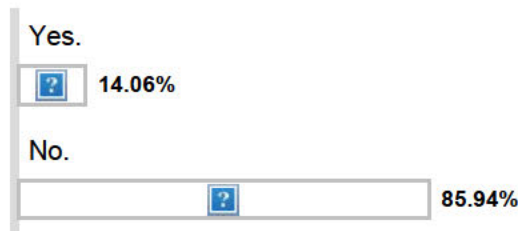
- [...Can include getting a free Whopper from Burger King](#)

CNET (6/24)

## SURVEY RESULTS

*Here are the results of yesterday's reader poll. There were 1,201 responses.*

### Do you keep a regular journal?



## HAPPY HOUR FUN

### Canned wine came of age

**Why it matters:** Trends in direct-to-consumer alcohol sales have powered the growth of

canned wine. The stigma once associated with such wines has receded as quality has improved. **Full Story:** [Forbes](#) (6/24)



**POLL QUESTION:**

**Have you tried canned wine?**

☐ Yes.

☐ No.

---

#### WYWW PLAYLIST

### "Red Red Wine" by UB40

There is a [WYWW playlist](#) on Spotify to keep track of all the songs listed in this space.

[Click here](#) to follow the playlist.



---

#### ENJOY THE VIEW



## Sunset in Paris



(Mr. Le Papillon)

## Sunset in Paris

If you look really close, you can see Place de la Concorde aligned with the Arc de Triomphe. This photo was submitted by Mr. Le Papillon. **Full Story:** [Flickr](#) (6/24)



---

## ABOUT THE EDITORS

### Sean McMahon



*Since I joined SmartBrief in 2003, I have produced content on a variety of topics including finance, energy, infrastructure, politics, telecommunications and international development.*

*Wow. I knew the sweet, flowing locks of my pandemic haircut were loooooong, but that video made me realize just how long. Oof.*

*If you like WYWW, hate WYWW or want to submit a story, [shoot me an email](#). Yes, I actually read them.*

The kindest compliment you can pay to WYWW is to send [this link](#) to your friends, family and colleagues so they can subscribe. Thanks!



*No matter where you're from, your dreams are valid.*

Lupita Nyong'o,  
actress, writer



Sharing While You Were Working SmartBrief with your network keeps the quality of content high and these newsletters free.

**Help Spread the Word**

**SHARE**

Or copy & share your personalized link:

**[smartbrief.com/wyww/?referrerId=hPcTodaQtF](https://smartbrief.com/wyww/?referrerId=hPcTodaQtF)**



SmartBrief publishes more than 200 free industry newsletters - [Browse our portfolio](#)

[Sign Up](#) | [Update Profile](#) | [Advertise with SmartBrief](#)

[Unsubscribe](#) | [Privacy policy](#)

**CONTACT US: [FEEDBACK](#) | [ADVERTISE](#)**



SmartBrief, Inc.®, 555 11th ST NW, Suite 600, Washington, DC 20004

**From:** [InvestigativeSupportInquiry](mailto:InvestigativeSupportInquiry@ncric.ca.gov)  
**To:** [mhutchison@sunnyvale.ca.gov](mailto:mhutchison@sunnyvale.ca.gov)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 10:15:14 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 6/14/2017 was potentially compromised. The request was submitted under case number 17-4416 for the Other Case Support team. The tracking number provided to you upon submission was 20170092.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



**From:** [InvestigativeSupportInquiry](#)  
**To:** [Clyde Cheng](#)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 10:14:35 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 7/12/2017 was potentially compromised. The request was submitted under case number 17-2010 for the Other Case Support team. The tracking number provided to you upon submission was 20170114.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

**From:** [InvestigativeSupportInquiry](mailto:InvestigativeSupportInquiry@ncric.ca.gov)  
**To:** [aserrano@sunnyvale.ca.gov](mailto:aserrano@sunnyvale.ca.gov)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 10:13:11 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group "Distributed Denial of Secrets" posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 9/15/2017 was potentially compromised. The request was submitted under case number 17-2188 for the Other Case Support team. The tracking number provided to you upon submission was 20170178.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid "right and need-to-know" without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



**From:** [InvestigativeSupportInquiry](mailto:InvestigativeSupportInquiry@ncric.ca.gov)  
**To:** [bholt@sunnyvale.ca.gov](mailto:bholt@sunnyvale.ca.gov)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 10:13:08 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 9/28/2017 was potentially compromised. The request was submitted under case number 17-3535 for the Other Case Support team. The tracking number provided to you upon submission was 20170184.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

**From:** [InvestigativeSupportInquiry](#)  
**To:** [Clyde Cheng](#)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 10:08:18 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 7/17/2018 was potentially compromised. The request was submitted under case number 17-10247 for the Crime Strategies Unit team. The tracking number provided to you upon submission was 20180157.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

**From:** [InvestigativeSupportInquiry](#)  
**To:** [I Singh](#)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 10:08:13 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 8/6/2018 was potentially compromised. The request was submitted under case number 18-5932 for the team. The tracking number provided to you upon submission was 20180170.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.



UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

**From:** [InvestigativeSupportInquiry](mailto:InvestigativeSupportInquiry@ncric.ca.gov)  
**To:** [NKakis@sunnyvale.ca.gov](mailto:NKakis@sunnyvale.ca.gov)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 10:04:03 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 4/5/2019 was potentially compromised. The request was submitted under case number 19-957 for the Other Case Support team. The tracking number provided to you upon submission was 20190096.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

**From:** [InvestigativeSupportInquiry](mailto:InvestigativeSupportInquiry@ncric.ca.gov)  
**To:** [NKakis@sunnyvale.ca.gov](mailto:NKakis@sunnyvale.ca.gov)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 9:56:19 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 2/18/2020 was potentially compromised. The request was submitted under case number 19-8930 for the Crime Strategies Unit team. The tracking number provided to you upon submission was 20200035.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE



**From:** [InvestigativeSupportInquiry](mailto:InvestigativeSupportInquiry@mjorgensen@sunnyvale.ca.gov)  
**To:** [mjorgensen@sunnyvale.ca.gov](mailto:mjorgensen@sunnyvale.ca.gov)  
**Subject:** (U//LES) Potential Compromise of NCRIC Investigative Support Requests  
**Date:** Wednesday, June 24, 2020 9:54:50 AM

---

**ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.**

UNCLASSIFIED//**LAW ENFORCEMENT SENSITIVE**

(U//FOUO) On Friday evening, the group “Distributed Denial of Secrets” posted on Twitter a link to an expansive volume of law enforcement sensitive data, that was exfiltrated from a compromised online platform. An investigation is under way, with the Houston FBI office taking the lead, in partnership with cybersecurity resources from the fusion centers, DHS CISA, CIS & MS-ISAC, among others. Ongoing analysis suggests the majority of the data came from the Texas-based company that hosts our [www.ncric.org](http://www.ncric.org) and [www.nchidta.org](http://www.nchidta.org) websites, among numerous other law enforcement entities.

(U//FOUO) Based on conversations with the affected party, it is the opinion of the NCRIC Cybersecurity Team that the compromise has been solved and halted.

(U//LES) You are receiving this email to notify you that case information included in a NCRIC or NC HIDTA Investigative Support Request you submitted on 06/01/2020 was potentially compromised. The request was submitted under case number NO Case number assigned for the Threat Assessment or Strategic Support team. The tracking number provided to you upon submission was 20200103.

(U//FOUO) If you have additional questions, please reply to this email or contact us at [InvestigativeSupportInquiry@ncric.ca.gov](mailto:InvestigativeSupportInquiry@ncric.ca.gov)

Sincerely,

Mike L. Sena, Director

Report urgent threat information to the FBI-JTTF at (415) 553-7400

**Report suspicious activity to the NCRIC at <https://ncric.ca.gov>**

Handling Notice: This document is Unclassified//LAW ENFORCEMENT SENSITIVE (U//LES). This document is not subject to the California Information Practices Act and contains information that may be exempt from public release under exemptions provided by the California Public Records Act. Receipt of this information acknowledges an agreement to comply with all applicable laws protecting privacy, civil rights and civil liberties and further constitutes acceptance of all terms and conditions regarding its use, handling, storage, dissemination and destruction in accordance with laws relating to LAW ENFORCEMENT SENSITIVE information. This information is not to be released to the public, the media, or other personnel who do not have a valid “right and need-to-know” without approval of the NCRIC.

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE

**From:** [CyberScoop](#)  
**To:** [kbfooster@sunnyvale.ca.gov](mailto:kbfooster@sunnyvale.ca.gov)  
**Subject:** Why Twitter banned a WikiLeaks-style activist group  
**Date:** Wednesday, June 24, 2020 9:07:30 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

WEDNESDAY, JUNE 24, 2020



*More about Distributed Denial of Secrets, an emerging transparency group that was just banned from Twitter. An in-depth look at how the Pentagon is trying to improve contractors' cybersecurity. And exploring the value of U.S. cyber investigators abroad. This is CyberScoop for Wednesday, June 24.*



## Meet DDoSecrets, a transparency group trying to avoid WikiLeaks' fate

After Twitter blacklisted an anti-secrecy group for distributing a vast collection of data stolen from U.S. law enforcement agencies, a co-

founder of the WikiLeaks-style startup says it won't go away quietly. Distributed Denial of Secrets co-founder Emma Best says the group, which published 269 GB of police materials, is exploring its option for appeal, and getting set up on other social networks. Meanwhile, a longtime Anonymous scholar suggested that DDoSecrets represents the next logical step for the hacktivist movement. **Jeff Stone has the details.**

#### **Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **A Pentagon cyber plan comes down to 15 volunteers**

One of the biggest, most complicated projects in the defense industrial base isn't a new weapons system or cloud computing environment. It's the Cybersecurity Maturity Model Certification (CMMC), which is set to upend how the Department of Defense does business with 300,000 contractors who provide everything from advanced aircraft to the shoelaces in soldiers' boots. Effective security measures represent a key component of that effort, and the days when a contractor needs only to self-certify cyber compliance are coming to an end. Instead, the idea is to accredit thousands of people who will test companies against a new system of security controls. Without a CMMC certification, a company will not be able to land a DOD job (without a waiver). **Jackson Barnett goes deep at FedScoop.**

---

## **Why cyber attachés are worth it**

International cybercrime investigations present an array of increasingly complex and diffuse challenges. Getting multiple investigative organizations and the legal procedures that bind them to work together requires unprecedented collaboration. To keep pace with these evolving borderless and highly technical crimes in cyberspace, the FBI has been leaning on its cyber attachés, which



work with foreign partners to address the growing global threat. In this op-ed, two members of the Cyberspace Solarium Commission talk about what the program has done to take down criminals, and how it helps both the U.S. and foreign countries fight bureaucratic red tape when time is of the essence. [Read more here.](#)

**Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **Technologists slam new Senate encryption bill**

Republican Sens. Tom Cotton, Lindsey Graham and Marsha Blackburn just introduced a bill that would require device manufacturers to provide warranted law enforcement with access to encrypted communications. It's the most hardline encryption bill in years, and technologists immediately decried it. "2020 just keeps giving," tweeted Matthew Green, a professor at Johns Hopkins University. The bill would also offer a prize to engineers who can meet lawmakers' demands for building backdoors into encryption products, something that technologists say could weaken security for a huge number of people. But it also shows how much traction encryption hardliners have on Capitol Hill right now. [The crypto wars rage eternal.](#)

---

## **How do you fight off a ransomware attack?**

Ransomware has been one of the biggest threats in cybersecurity over the past few years. Hospitals, governments, cities, companies. They've all been impacted by this wave of malicious behavior. But what happens when an enterprise is hit? What goes on in the short term? How do you stop the bleeding? And how do you recover? On this episode of Securiosity, Greg Otto talks with David Macias, president of ITRMS, a IT service provider based in California. Macias, a victim of a ransomware attack, tells us how he recovered, what he learned, and what he tells his clients to do in order to

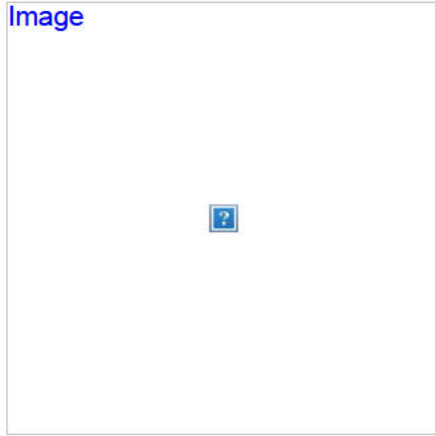


prevent a similar incident from occurring. [Listen here.](#)

---

## Tweet of the Day

Image



Finally a justification for that plug.

---

*[Want more? Catch our events for all things cybersecurity!](#)*

Copyright (c) 2020 CyberScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)

**From:** [CyberScoop](#)  
**To:** [smorton@ci.sunnyvale.ca.us](mailto:smorton@ci.sunnyvale.ca.us)  
**Subject:** Why Twitter banned a WikiLeaks-style activist group  
**Date:** Wednesday, June 24, 2020 9:07:21 AM

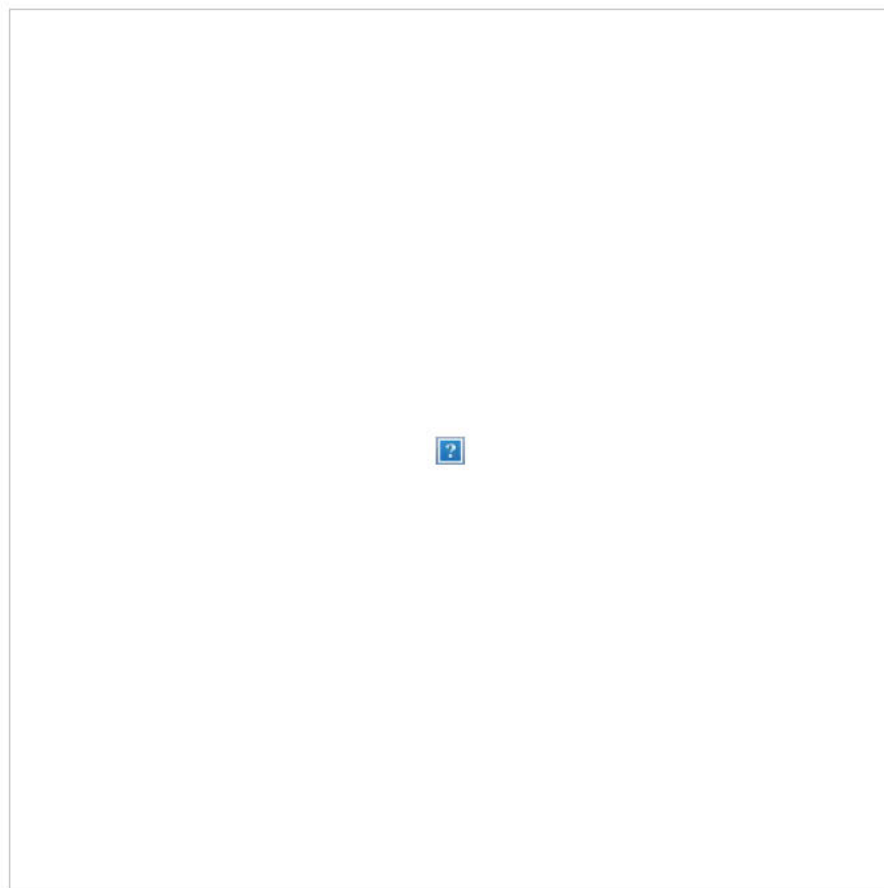
ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

WEDNESDAY, JUNE 24, 2020



*More about Distributed Denial of Secrets, an emerging transparency group that was just banned from Twitter. An in-depth look at how the Pentagon is trying to improve contractors' cybersecurity. And exploring the value of U.S. cyber investigators abroad. This is CyberScoop for Wednesday, June 24.*



## Meet DDoSecrets, a transparency group trying to avoid WikiLeaks' fate

After Twitter blacklisted an anti-secrecy group for distributing a vast collection of data stolen from U.S. law enforcement agencies, a co-

founder of the WikiLeaks-style startup says it won't go away quietly. Distributed Denial of Secrets co-founder Emma Best says the group, which published 269 GB of police materials, is exploring its option for appeal, and getting set up on other social networks. Meanwhile, a longtime Anonymous scholar suggested that DDoSecrets represents the next logical step for the hacktivist movement. **Jeff Stone has the details.**

#### **Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **A Pentagon cyber plan comes down to 15 volunteers**

One of the biggest, most complicated projects in the defense industrial base isn't a new weapons system or cloud computing environment. It's the Cybersecurity Maturity Model Certification (CMMC), which is set to upend how the Department of Defense does business with 300,000 contractors who provide everything from advanced aircraft to the shoelaces in soldiers' boots. Effective security measures represent a key component of that effort, and the days when a contractor needs only to self-certify cyber compliance are coming to an end. Instead, the idea is to accredit thousands of people who will test companies against a new system of security controls. Without a CMMC certification, a company will not be able to land a DOD job (without a waiver). **Jackson Barnett goes deep at FedScoop.**

---

## **Why cyber attachés are worth it**

International cybercrime investigations present an array of increasingly complex and diffuse challenges. Getting multiple investigative organizations and the legal procedures that bind them to work together requires unprecedented collaboration. To keep pace with these evolving borderless and highly technical crimes in cyberspace, the FBI has been leaning on its cyber attachés, which



work with foreign partners to address the growing global threat. In this op-ed, two members of the Cyberspace Solarium Commission talk about what the program has done to take down criminals, and how it helps both the U.S. and foreign countries fight bureaucratic red tape when time is of the essence. [Read more here.](#)

**Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **Technologists slam new Senate encryption bill**

Republican Sens. Tom Cotton, Lindsey Graham and Marsha Blackburn just introduced a bill that would require device manufacturers to provide warranted law enforcement with access to encrypted communications. It's the most hardline encryption bill in years, and technologists immediately decried it. "2020 just keeps giving," tweeted Matthew Green, a professor at Johns Hopkins University. The bill would also offer a prize to engineers who can meet lawmakers' demands for building backdoors into encryption products, something that technologists say could weaken security for a huge number of people. But it also shows how much traction encryption hardliners have on Capitol Hill right now. [The crypto wars rage eternal.](#)

---

## **How do you fight off a ransomware attack?**

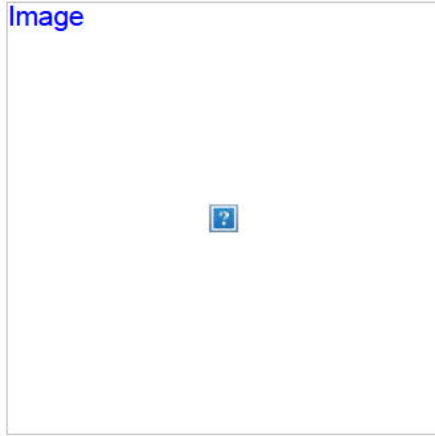
Ransomware has been one of the biggest threats in cybersecurity over the past few years. Hospitals, governments, cities, companies. They've all been impacted by this wave of malicious behavior. But what happens when an enterprise is hit? What goes on in the short term? How do you stop the bleeding? And how do you recover? On this episode of Securiosity, Greg Otto talks with David Macias, president of ITRMS, a IT service provider based in California. Macias, a victim of a ransomware attack, tells us how he recovered, what he learned, and what he tells his clients to do in order to

prevent a similar incident from occurring. [Listen here.](#)

---

## Tweet of the Day

Image



Finally a justification for that plug.

---

*[Want more? Catch our events for all things cybersecurity!](#)*

Copyright (c) 2020 CyberScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)



**From:** [CyberScoop](#)  
**To:** [lvo@sunnyvale.ca.gov](mailto:lvo@sunnyvale.ca.gov)  
**Subject:** Why Twitter banned a WikiLeaks-style activist group  
**Date:** Wednesday, June 24, 2020 9:03:51 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

WEDNESDAY, JUNE 24, 2020



*More about Distributed Denial of Secrets, an emerging transparency group that was just banned from Twitter. An in-depth look at how the Pentagon is trying to improve contractors' cybersecurity. And exploring the value of U.S. cyber investigators abroad. This is CyberScoop for Wednesday, June 24.*



## Meet DDoSecrets, a transparency group trying to avoid WikiLeaks' fate

After Twitter blacklisted an anti-secrecy group for distributing a vast collection of data stolen from U.S. law enforcement agencies, a co-

founder of the WikiLeaks-style startup says it won't go away quietly. Distributed Denial of Secrets co-founder Emma Best says the group, which published 269 GB of police materials, is exploring its option for appeal, and getting set up on other social networks. Meanwhile, a longtime Anonymous scholar suggested that DDoSecrets represents the next logical step for the hacktivist movement. **Jeff Stone has the details.**

#### **Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **A Pentagon cyber plan comes down to 15 volunteers**

One of the biggest, most complicated projects in the defense industrial base isn't a new weapons system or cloud computing environment. It's the Cybersecurity Maturity Model Certification (CMMC), which is set to upend how the Department of Defense does business with 300,000 contractors who provide everything from advanced aircraft to the shoelaces in soldiers' boots. Effective security measures represent a key component of that effort, and the days when a contractor needs only to self-certify cyber compliance are coming to an end. Instead, the idea is to accredit thousands of people who will test companies against a new system of security controls. Without a CMMC certification, a company will not be able to land a DOD job (without a waiver). **Jackson Barnett goes deep at FedScoop.**

---

## **Why cyber attachés are worth it**

International cybercrime investigations present an array of increasingly complex and diffuse challenges. Getting multiple investigative organizations and the legal procedures that bind them to work together requires unprecedented collaboration. To keep pace with these evolving borderless and highly technical crimes in cyberspace, the FBI has been leaning on its cyber attachés, which

work with foreign partners to address the growing global threat. In this op-ed, two members of the Cyberspace Solarium Commission talk about what the program has done to take down criminals, and how it helps both the U.S. and foreign countries fight bureaucratic red tape when time is of the essence. [Read more here.](#)

**Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **Technologists slam new Senate encryption bill**

Republican Sens. Tom Cotton, Lindsey Graham and Marsha Blackburn just introduced a bill that would require device manufacturers to provide warranted law enforcement with access to encrypted communications. It's the most hardline encryption bill in years, and technologists immediately decried it. "2020 just keeps giving," tweeted Matthew Green, a professor at Johns Hopkins University. The bill would also offer a prize to engineers who can meet lawmakers' demands for building backdoors into encryption products, something that technologists say could weaken security for a huge number of people. But it also shows how much traction encryption hardliners have on Capitol Hill right now. [The crypto wars rage eternal.](#)

---

## **How do you fight off a ransomware attack?**

Ransomware has been one of the biggest threats in cybersecurity over the past few years. Hospitals, governments, cities, companies. They've all been impacted by this wave of malicious behavior. But what happens when an enterprise is hit? What goes on in the short term? How do you stop the bleeding? And how do you recover? On this episode of Securiosity, Greg Otto talks with David Macias, president of ITRMS, a IT service provider based in California. Macias, a victim of a ransomware attack, tells us how he recovered, what he learned, and what he tells his clients to do in order to

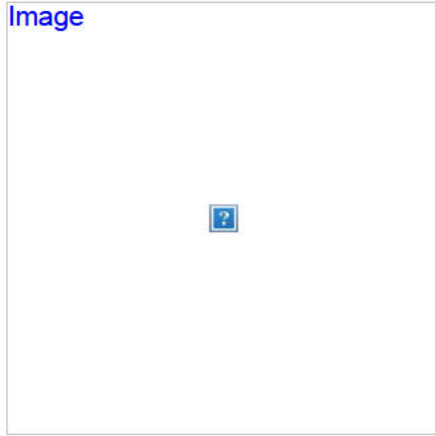


prevent a similar incident from occurring. [Listen here.](#)

---

## Tweet of the Day

Image



Finally a justification for that plug.

---

*[Want more? Catch our events for all things cybersecurity!](#)*

Copyright (c) 2020 CyberScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)

**From:** [CyberScoop](#)  
**To:** [jleung@sunnyvale.ca.gov](mailto:jleung@sunnyvale.ca.gov)  
**Subject:** Why Twitter banned a WikiLeaks-style activist group  
**Date:** Wednesday, June 24, 2020 9:03:35 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

WEDNESDAY, JUNE 24, 2020



*More about Distributed Denial of Secrets, an emerging transparency group that was just banned from Twitter. An in-depth look at how the Pentagon is trying to improve contractors' cybersecurity. And exploring the value of U.S. cyber investigators abroad. This is CyberScoop for Wednesday, June 24.*



## Meet DDoSecrets, a transparency group trying to avoid WikiLeaks' fate

After Twitter blacklisted an anti-secrecy group for distributing a vast collection of data stolen from U.S. law enforcement agencies, a co-



founder of the WikiLeaks-style startup says it won't go away quietly. Distributed Denial of Secrets co-founder Emma Best says the group, which published 269 GB of police materials, is exploring its option for appeal, and getting set up on other social networks. Meanwhile, a longtime Anonymous scholar suggested that DDoSecrets represents the next logical step for the hacktivist movement. **Jeff Stone has the details.**

#### **Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **A Pentagon cyber plan comes down to 15 volunteers**

One of the biggest, most complicated projects in the defense industrial base isn't a new weapons system or cloud computing environment. It's the Cybersecurity Maturity Model Certification (CMMC), which is set to upend how the Department of Defense does business with 300,000 contractors who provide everything from advanced aircraft to the shoelaces in soldiers' boots. Effective security measures represent a key component of that effort, and the days when a contractor needs only to self-certify cyber compliance are coming to an end. Instead, the idea is to accredit thousands of people who will test companies against a new system of security controls. Without a CMMC certification, a company will not be able to land a DOD job (without a waiver). **Jackson Barnett goes deep at FedScoop.**

---

## **Why cyber attachés are worth it**

International cybercrime investigations present an array of increasingly complex and diffuse challenges. Getting multiple investigative organizations and the legal procedures that bind them to work together requires unprecedented collaboration. To keep pace with these evolving borderless and highly technical crimes in cyberspace, the FBI has been leaning on its cyber attachés, which

work with foreign partners to address the growing global threat. In this op-ed, two members of the Cyberspace Solarium Commission talk about what the program has done to take down criminals, and how it helps both the U.S. and foreign countries fight bureaucratic red tape when time is of the essence. [Read more here.](#)

**Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **Technologists slam new Senate encryption bill**

Republican Sens. Tom Cotton, Lindsey Graham and Marsha Blackburn just introduced a bill that would require device manufacturers to provide warranted law enforcement with access to encrypted communications. It's the most hardline encryption bill in years, and technologists immediately decried it. "2020 just keeps giving," tweeted Matthew Green, a professor at Johns Hopkins University. The bill would also offer a prize to engineers who can meet lawmakers' demands for building backdoors into encryption products, something that technologists say could weaken security for a huge number of people. But it also shows how much traction encryption hardliners have on Capitol Hill right now. [The crypto wars rage eternal.](#)

---

## **How do you fight off a ransomware attack?**

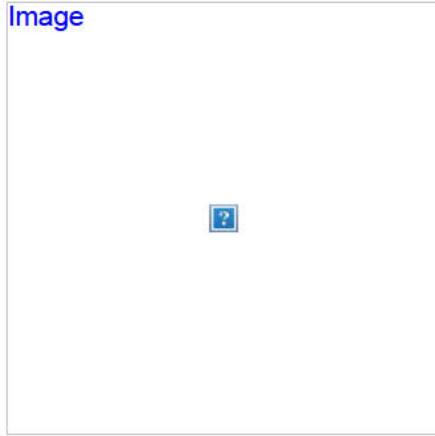
Ransomware has been one of the biggest threats in cybersecurity over the past few years. Hospitals, governments, cities, companies. They've all been impacted by this wave of malicious behavior. But what happens when an enterprise is hit? What goes on in the short term? How do you stop the bleeding? And how do you recover? On this episode of Securiosity, Greg Otto talks with David Macias, president of ITRMS, a IT service provider based in California. Macias, a victim of a ransomware attack, tells us how he recovered, what he learned, and what he tells his clients to do in order to

prevent a similar incident from occurring. [Listen here.](#)

---

## Tweet of the Day

Image



Finally a justification for that plug.

---

*[Want more? Catch our events for all things cybersecurity!](#)*

Copyright (c) 2020 CyberScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)



**From:** [ZDNet](#)  
**To:** [michael spath](#)  
**Subject:** Windows 10 updates trigger critical process failures  
**Date:** Wednesday, June 24, 2020 7:09:13 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**ZDNet Tech Today**

June 24, 2020

placeholder



New ransomware masquerades as COVID-19 contact-tracing app on your Android device



Apple macOS 11 Big Sur: Startup chime returns in revamped design, plus new battery section

## Windows 10 critical process failure: Microsoft admits June updates are triggering reboots

[READ FULL STORY](#)



Twitter bans DDoSecrets account over 'BlueLeaks' police data dump

### RELATED

- [Microsoft, stop feeding bugs to a billion Windows 10 users. Here's how](#)
- [Windows 7 and 8.1 users: Now Microsoft is pushing out new Edge browser to you, too](#)
- [New Windows Terminal preview is out: These are the latest features, says Microsoft](#)



Nvidia and Mercedes to roll out software-defined autonomous vehicles by 2024

Apple iPadOS 14 report card: There's room for



improvement

placeholder



Smart toilets could transform health tracking. Here's how

[READ FULL STORY](#)

placeholder



Using a neural network for COVID-19 detection

[WATCH THE VIDEO](#)

placeholder



Going back to the office? Here are five major tech problems that lie ahead of you

[READ FULL STORY](#)

placeholder



Will Apple Silicon kill the Hackintosh? The odds against a self-built MacOS Arm computer

[READ FULL STORY](#)

THIS WEEK ON ZD NET





## Security

1. [New WastedLocker ransomware demands payments of millions of USD](#)
2. [Safari 14 removes Flash, gets support for breach alerts, HTTP/3, and WebP](#)
3. [US Republican Senators develop Bill to end use of 'warrant-proof' encryption](#)
4. [80,000 printers are exposing their IPP port online](#)

[See more](#) >



## TechRepublic

1. [AI continues to flourish in business despite the pandemic and a turbulent economy](#)
2. [Zoom losing to Teams in the video conference race to the top](#)
3. [COVID-19 has become a powerful catalyst for rapid cloud migration](#)
4. [Technology might be the key to fighting the coronavirus](#)

[Read more](#) >

IN CASE YOU MISSED IT	
-----------------------	--

# Apple Silicon: Meet the new Mac, PC of the future

placeholder

Moving the Mac to its own chip architecture is just the first step. How quickly will Apple seize complete control of its ecosystem? Big Sur is not locked down -- yet.

[READ FULL STORY](#)

#### MORE SPONSORED RESEARCH

### Moving Forward to Zero Trust Security

White Papers from Akamai Technologies

[READ MORE](#)

### Hiring kit: Microsoft Power BI developer

Tools & Templates from TechRepublic Premium

[DOWNLOAD NOW](#)

### Spending too much in your Multicloud Environment?

eBooks from CloudHealth by VMware

[VIEW THIS NOW](#)

### Employee political activity policy

Downloads from TechRepublic Premium

[DOWNLOAD NOW](#)

This newsletter is a service of ZDNet.com.  
To update your account, please visit our  
Subscription Center.

[Unsubscribe](#) | [Help](#) | [Privacy policy](#)

[Trouble viewing this?](#) [Read Online](#)

Copyright CBS Interactive, Inc.  
All rights reserved. ZDNet is a registered service  
mark of CBS Interactive, Inc.

ZDNet  
235 Second Street  
San Francisco, CA 94105  
U.S.A.

**From:** [The IACP](#)  
**To:** [hchoi@sunnyvale.ca.gov](mailto:hchoi@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.  
**Date:** Wednesday, June 24, 2020 4:41:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings Hyun Choi

Wednesday, June 24, 2020



## POLICING & POLICY

Advertisement



### Top Senate Democrats Dismiss Republican Policing Reform Bill

The [AP](#) (6/23, Mascaro) reports Congress is "hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away." Ahead of a test vote Wednesday, Senate Majority Leader McConnell "acknowledged it may fall short," and the GOP bill's author, Sen. Tim Scott (R-SC), "warned against a partisan, political debate that chisels away confidence in the nation's institutions." [Reuters](#) (6/23, Morgan) similarly says "Democrats and Republicans...found themselves in a partisan deadlock on Tuesday."

**AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform.** The [AP](#) (6/23, Long, Fingerhut) reports

that Americans "overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation's criminal justice system." The new AP-NORC poll "also finds there is strong support for penalizing officers who engage in racially biased policing."

### Confronting Nazi Legacy Part Of German Police Training

The [New York Times](#) (6/23, Bennhold, Eddy) reports that "visiting a former concentration camp is mandatory for every future police officer in Berlin." To the Times, it is "one of the ways in which policing was fundamentally overhauled in Germany after World War II."

### Rhode Island Governor Signs Ban On 3D-Printed Weapons, "Ghost Guns"

The [AP](#) (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo "on Tuesday signed into law bills that ban 3D-printed guns and so-called 'ghost guns' in the state." The bills "are 'a matter of public health,' she said." The bills "were approved by the legislature last week," and "make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up to \$10,000. The laws take effect in 30 days."

### Seattle, Washington To End Anti-Loitering Law

[Fox News](#) (6/23, Carter) reports, "Seattle is moving to end a longstanding city law that allowed police to arrest someone for



loitering, if they are also suspected of being a possible drug offender or sex worker.” According to Fox News, “The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color.”

### Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The [AP](#) (6/23, Nadler, Amy) reports, “Georgia’s legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp’s desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders.” According to the AP, “The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support.”



The impact of an officer’s line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

[Review documents and resources.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Law Enforcement Concerned About Rash Of Gun-Store Robberies

[Politico](#) (6/23, Swan) reports, “A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country.” According to Politico, “In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau’s assistant director of field operations Tom Chittum told POLITICO. ‘It’s a lot of guns,’ Chittum said in an interview. ‘It’s the biggest spike I have ever seen of gun store burglaries.’” Chittum “said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists.”

### Gun Violence Spikes In New York City

The [New York Times](#) (6/23, Southall, Macfarquhar) reports, “It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.” The city “logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions.” New York “is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.” On Monday, Mayor Bill de Blasio “announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department.”

### Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The [Columbia \(SC\) State](#) (6/23, Monk) reports, “More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing.” According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests “were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018.” FBI South Carolina SAC Jody Norris said, “Even in the midst of a



pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina.” Also reporting are [WACH-TV](#) (6/23, Lanahan) and [WIS-TV](#) (6/23, Greene).

## GLOBAL SECURITY

### Suicide Bomber Targets Turkish Military Base In Somalia

The [New York Times](#) (6/23, Mohamed, Dahir) reports, “Two people were killed after a suicide bomber detonated his explosives outside Turkey’s largest overseas military base in Mogadishu on Tuesday.” The attack, which the Times says “bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway.”

The [AP](#) (6/23, Guled) says Tuesday’s attack marks “the first time Turkey’s largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group,” which “quickly claimed responsibility, according to its Radio al-Furqan affiliate.”

### Secret Recordings Detail Neo-Nazi Group’s Grooming, Recruiting Process

[Fox News](#) (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show “senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them.” The founder of the group, American Rinaldo Nazzaro, “who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons.” Fox reports Nazzaro “purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago.”

## ALSO IN THE NEWS

### FCC To Vote Next Month On Making “988” New Suicide Hotline Number

The [AP](#) (6/23, Arbel) reports the FCC “will vote in July on whether to make ‘988’ the number to reach a suicide prevention hotline.” The Commission explained that “phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected.”

## TUESDAY'S LEAD STORIES

- [US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police](#)
- [Swedish Rape Conviction Rates Rise 75% After Change In Law](#)
- [“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers](#)
- [NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally](#)

### Subscriber Tools

- [Change Email Address](#)
- [Send Feedback](#)
- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to hchoi@sunnyvale.ca.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media’s [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by [Bulletin Media](#) | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

**From:** [The IACP](#)  
**To:** [hsyu@sunnyvale.ca.gov](mailto:hsyu@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.  
**Date:** Wednesday, June 24, 2020 4:41:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings Hank Syu

Wednesday, June 24, 2020



## POLICING & POLICY

Advertisement



### Top Senate Democrats Dismiss Republican Policing Reform Bill

The [AP](#) (6/23, Mascaro) reports Congress is “hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away.” Ahead of a test vote Wednesday, Senate Majority Leader McConnell “acknowledged it may fall short,” and the GOP bill’s author, Sen. Tim Scott (R-SC), “warned against a partisan, political debate that chisels away confidence in the nation’s institutions.” [Reuters](#) (6/23, Morgan) similarly says “Democrats and Republicans...found themselves in a partisan deadlock on Tuesday.”

**AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform.** The [AP](#) (6/23, Long, Fingerhut) reports

that Americans “overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation’s criminal justice system.” The new AP-NORC poll “also finds there is strong support for penalizing officers who engage in racially biased policing.”

### Confronting Nazi Legacy Part Of German Police Training

The [New York Times](#) (6/23, Bennhold, Eddy) reports that “visiting a former concentration camp is mandatory for every future police officer in Berlin.” To the Times, it is “one of the ways in which policing was fundamentally overhauled in Germany after World War II.”

### Rhode Island Governor Signs Ban On 3D-Printed Weapons, “Ghost Guns”

The [AP](#) (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo “on Tuesday signed into law bills that ban 3D-printed guns and so-called ‘ghost guns’ in the state.” The bills “are ‘a matter of public health,’ she said.” The bills “were approved by the legislature last week,” and “make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up \$10,000. The laws take effect in 30 days.”

### Seattle, Washington To End Anti-Loitering Law

[Fox News](#) (6/23, Carter) reports, “Seattle is moving to end a longstanding city law that allowed police to arrest someone for



loitering, if they are also suspected of being a possible drug offender or sex worker.” According to Fox News, “The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color.”

### Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The [AP](#) (6/23, Nadler, Amy) reports, “Georgia’s legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp’s desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders.” According to the AP, “The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support.”



The impact of an officer’s line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

[Review documents and resources.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Law Enforcement Concerned About Rash Of Gun-Store Robberies

[Politico](#) (6/23, Swan) reports, “A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country.” According to Politico, “In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau’s assistant director of field operations Tom Chittum told POLITICO. ‘It’s a lot of guns,’ Chittum said in an interview. ‘It’s the biggest spike I have ever seen of gun store burglaries.’” Chittum “said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists.”

### Gun Violence Spikes In New York City

The [New York Times](#) (6/23, Southall, Macfarquhar) reports, “It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.” The city “logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions.” New York “is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.” On Monday, Mayor Bill de Blasio “announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department.”

### Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The [Columbia \(SC\) State](#) (6/23, Monk) reports, “More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing.” According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests “were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018.” FBI South Carolina SAC Jody Norris said, “Even in the midst of a

pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina.” Also reporting are [WACH-TV](#) (6/23, Lanahan) and [WIS-TV](#) (6/23, Greene).

## GLOBAL SECURITY

### Suicide Bomber Targets Turkish Military Base In Somalia

The [New York Times](#) (6/23, Mohamed, Dahir) reports, “Two people were killed after a suicide bomber detonated his explosives outside Turkey’s largest overseas military base in Mogadishu on Tuesday.” The attack, which the Times says “bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway.”

The [AP](#) (6/23, Guled) says Tuesday’s attack marks “the first time Turkey’s largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group,” which “quickly claimed responsibility, according to its Radio al-Furqan affiliate.”

### Secret Recordings Detail Neo-Nazi Group’s Grooming, Recruiting Process

[Fox News](#) (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show “senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them.” The founder of the group, American Rinaldo Nazzaro, “who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons.” Fox reports Nazzaro “purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago.”

## ALSO IN THE NEWS

### FCC To Vote Next Month On Making “988” New Suicide Hotline Number

The [AP](#) (6/23, Arbel) reports the FCC “will vote in July on whether to make ‘988’ the number to reach a suicide prevention hotline.” The Commission explained that “phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected.”

## TUESDAY'S LEAD STORIES

- [US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police](#)
- [Swedish Rape Conviction Rates Rise 75% After Change In Law](#)
- [“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers](#)
- [NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally](#)

### Subscriber Tools

- [Change Email Address](#)
- [Send Feedback](#)
- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to [hsyu@sunnyvale.ca.gov](mailto:hsyu@sunnyvale.ca.gov) as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media’s [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by [Bulletin Media](#) | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191



**From:** [The IACP](#)  
**To:** [jboone@sunnyvale.ca.gov](mailto:jboone@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.  
**Date:** Wednesday, June 24, 2020 4:41:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings James Boone

Wednesday, June 24, 2020



## POLICING & POLICY

Advertisement



### Top Senate Democrats Dismiss Republican Policing Reform Bill

The [AP](#) (6/23, Mascaro) reports Congress is “hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away.” Ahead of a test vote Wednesday, Senate Majority Leader McConnell “acknowledged it may fall short,” and the GOP bill’s author, Sen. Tim Scott (R-SC), “warned against a partisan, political debate that chisels away confidence in the nation’s institutions.” [Reuters](#) (6/23, Morgan) similarly says “Democrats and Republicans...found themselves in a partisan deadlock on Tuesday.”

**AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform.** The [AP](#) (6/23, Long, Fingerhut) reports

that Americans “overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation’s criminal justice system.” The new AP-NORC poll “also finds there is strong support for penalizing officers who engage in racially biased policing.”

### Confronting Nazi Legacy Part Of German Police Training

The [New York Times](#) (6/23, Bennhold, Eddy) reports that “visiting a former concentration camp is mandatory for every future police officer in Berlin.” To the Times, it is “one of the ways in which policing was fundamentally overhauled in Germany after World War II.”

### Rhode Island Governor Signs Ban On 3D-Printed Weapons, “Ghost Guns”

The [AP](#) (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo “on Tuesday signed into law bills that ban 3D-printed guns and so-called ‘ghost guns’ in the state.” The bills “are ‘a matter of public health,’ she said.” The bills “were approved by the legislature last week,” and “make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up \$10,000. The laws take effect in 30 days.”

### Seattle, Washington To End Anti-Loitering Law

[Fox News](#) (6/23, Carter) reports, “Seattle is moving to end a longstanding city law that allowed police to arrest someone for



loitering, if they are also suspected of being a possible drug offender or sex worker.” According to Fox News, “The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color.”

### Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The [AP](#) (6/23, Nadler, Amy) reports, “Georgia’s legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp’s desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders.” According to the AP, “The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support.”



The impact of an officer’s line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

[Review documents and resources.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Law Enforcement Concerned About Rash Of Gun-Store Robberies

[Politico](#) (6/23, Swan) reports, “A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country.” According to Politico, “In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau’s assistant director of field operations Tom Chittum told POLITICO. ‘It’s a lot of guns,’ Chittum said in an interview. ‘It’s the biggest spike I have ever seen of gun store burglaries.’” Chittum “said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists.”

### Gun Violence Spikes In New York City

The [New York Times](#) (6/23, Southall, Macfarquhar) reports, “It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.” The city “logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions.” New York “is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.” On Monday, Mayor Bill de Blasio “announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department.”

### Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The [Columbia \(SC\) State](#) (6/23, Monk) reports, “More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing.” According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests “were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018.” FBI South Carolina SAC Jody Norris said, “Even in the midst of a

pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina.” Also reporting are [WACH-TV](#) (6/23, Lanahan) and [WIS-TV](#) (6/23, Greene).

## GLOBAL SECURITY

### Suicide Bomber Targets Turkish Military Base In Somalia

The [New York Times](#) (6/23, Mohamed, Dahir) reports, “Two people were killed after a suicide bomber detonated his explosives outside Turkey’s largest overseas military base in Mogadishu on Tuesday.” The attack, which the Times says “bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway.”

The [AP](#) (6/23, Guled) says Tuesday’s attack marks “the first time Turkey’s largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group,” which “quickly claimed responsibility, according to its Radio al-Furqan affiliate.”

### Secret Recordings Detail Neo-Nazi Group’s Grooming, Recruiting Process

[Fox News](#) (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show “senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them.” The founder of the group, American Rinaldo Nazzaro, “who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons.” Fox reports Nazzaro “purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago.”

## ALSO IN THE NEWS

### FCC To Vote Next Month On Making “988” New Suicide Hotline Number

The [AP](#) (6/23, Arbel) reports the FCC “will vote in July on whether to make ‘988’ the number to reach a suicide prevention hotline.” The Commission explained that “phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected.”

## TUESDAY'S LEAD STORIES

- [US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police](#)
- [Swedish Rape Conviction Rates Rise 75% After Change In Law](#)
- [“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers](#)
- [NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally](#)

### Subscriber Tools

- [Change Email Address](#)
- [Send Feedback](#)
- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to jboone@sunnyvale.ca.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media’s [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by [Bulletin Media](#) | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191



**From:** [The IACP](#)  
**To:** [dsakurai@sunnyvale.ca.gov](mailto:dsakurai@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.  
**Date:** Wednesday, June 24, 2020 4:41:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings David Sakurai

Wednesday, June 24, 2020



## POLICING & POLICY

Advertisement



### Top Senate Democrats Dismiss Republican Policing Reform Bill

The [AP](#) (6/23, Mascaro) reports Congress is “hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away.” Ahead of a test vote Wednesday, Senate Majority Leader McConnell “acknowledged it may fall short,” and the GOP bill’s author, Sen. Tim Scott (R-SC), “warned against a partisan, political debate that chisels away confidence in the nation’s institutions.” [Reuters](#) (6/23, Morgan) similarly says “Democrats and Republicans...found themselves in a partisan deadlock on Tuesday.”

**AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform.** The [AP](#) (6/23, Long, Fingerhut) reports

that Americans “overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation’s criminal justice system.” The new AP-NORC poll “also finds there is strong support for penalizing officers who engage in racially biased policing.”

### Confronting Nazi Legacy Part Of German Police Training

The [New York Times](#) (6/23, Bennhold, Eddy) reports that “visiting a former concentration camp is mandatory for every future police officer in Berlin.” To the Times, it is “one of the ways in which policing was fundamentally overhauled in Germany after World War II.”

### Rhode Island Governor Signs Ban On 3D-Printed Weapons, “Ghost Guns”

The [AP](#) (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo “on Tuesday signed into law bills that ban 3D-printed guns and so-called ‘ghost guns’ in the state.” The bills “are ‘a matter of public health,’ she said.” The bills “were approved by the legislature last week,” and “make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up \$10,000. The laws take effect in 30 days.”

### Seattle, Washington To End Anti-Loitering Law

[Fox News](#) (6/23, Carter) reports, “Seattle is moving to end a longstanding city law that allowed police to arrest someone for

loitering, if they are also suspected of being a possible drug offender or sex worker.” According to Fox News, “The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color.”

### Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The [AP](#) (6/23, Nadler, Amy) reports, “Georgia’s legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp’s desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders.” According to the AP, “The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support.”



The impact of an officer’s line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

[Review documents and resources.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Law Enforcement Concerned About Rash Of Gun-Store Robberies

[Politico](#) (6/23, Swan) reports, “A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country.” According to Politico, “In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau’s assistant director of field operations Tom Chittum told POLITICO. ‘It’s a lot of guns,’ Chittum said in an interview. ‘It’s the biggest spike I have ever seen of gun store burglaries.’” Chittum “said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists.”

### Gun Violence Spikes In New York City

The [New York Times](#) (6/23, Southall, Macfarquhar) reports, “It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.” The city “logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions.” New York “is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.” On Monday, Mayor Bill de Blasio “announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department.”

### Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The [Columbia \(SC\) State](#) (6/23, Monk) reports, “More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing.” According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests “were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018.” FBI South Carolina SAC Jody Norris said, “Even in the midst of a



pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina.” Also reporting are [WACH-TV](#) (6/23, Lanahan) and [WIS-TV](#) (6/23, Greene).

## GLOBAL SECURITY

### Suicide Bomber Targets Turkish Military Base In Somalia

The [New York Times](#) (6/23, Mohamed, Dahir) reports, “Two people were killed after a suicide bomber detonated his explosives outside Turkey’s largest overseas military base in Mogadishu on Tuesday.” The attack, which the Times says “bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway.”

The [AP](#) (6/23, Guled) says Tuesday’s attack marks “the first time Turkey’s largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group,” which “quickly claimed responsibility, according to its Radio al-Furqan affiliate.”

### Secret Recordings Detail Neo-Nazi Group’s Grooming, Recruiting Process

[Fox News](#) (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show “senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them.” The founder of the group, American Rinaldo Nazzaro, “who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons.” Fox reports Nazzaro “purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago.”

## ALSO IN THE NEWS

### FCC To Vote Next Month On Making “988” New Suicide Hotline Number

The [AP](#) (6/23, Arbel) reports the FCC “will vote in July on whether to make ‘988’ the number to reach a suicide prevention hotline.” The Commission explained that “phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected.”

## TUESDAY'S LEAD STORIES

- [US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police](#)
- [Swedish Rape Conviction Rates Rise 75% After Change In Law](#)
- [“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers](#)
- [NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally](#)

### Subscriber Tools

- [Change Email Address](#)
- [Send Feedback](#)
- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to dsakurai@sunnyvale.ca.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media’s [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191



**From:** [The IACP](#)  
**To:** [afanucchi@sunnyvale.ca.gov](mailto:afanucchi@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: Top Senate Democrats Dismiss Republican Policing Reform Bill.  
**Date:** Wednesday, June 24, 2020 4:41:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings Ava Fanucchi

Wednesday, June 24, 2020



## POLICING & POLICY

Advertisement



### Top Senate Democrats Dismiss Republican Policing Reform Bill

The [AP](#) (6/23, Mascaro) reports Congress is “hitting an impasse on policing legislation, as key Senate Democrats on Tuesday opposed a Republican proposal as inadequate, leaving the parties to decide whether to take on the hard job of negotiating a compromise or walk away.” Ahead of a test vote Wednesday, Senate Majority Leader McConnell “acknowledged it may fall short,” and the GOP bill’s author, Sen. Tim Scott (R-SC), “warned against a partisan, political debate that chisels away confidence in the nation’s institutions.” [Reuters](#) (6/23, Morgan) similarly says “Democrats and Republicans...found themselves in a partisan deadlock on Tuesday.”

**AP-NORC Poll: Nearly All Americans Back Some Kind Of Criminal Justice Reform.** The [AP](#) (6/23, Long, Fingerhut) reports

that Americans “overwhelmingly want clear standards on when police officers may use force and consequences for officers who do so excessively, according to a new poll that finds nearly all Americans favor at least some level of change to the nation’s criminal justice system.” The new AP-NORC poll “also finds there is strong support for penalizing officers who engage in racially biased policing.”

### Confronting Nazi Legacy Part Of German Police Training

The [New York Times](#) (6/23, Bennhold, Eddy) reports that “visiting a former concentration camp is mandatory for every future police officer in Berlin.” To the Times, it is “one of the ways in which policing was fundamentally overhauled in Germany after World War II.”

### Rhode Island Governor Signs Ban On 3D-Printed Weapons, “Ghost Guns”

The [AP](#) (6/23, Pratt) reports that Rhode Island Gov. Gina Raimondo “on Tuesday signed into law bills that ban 3D-printed guns and so-called ‘ghost guns’ in the state.” The bills “are ‘a matter of public health,’ she said.” The bills “were approved by the legislature last week,” and “make it illegal to manufacture, import, sell, ship, deliver, possess, transfer or receive any such firearms. Anyone who violates the ban and is convicted could serve up to 10 years in prison and faces fines of up \$10,000. The laws take effect in 30 days.”

### Seattle, Washington To End Anti-Loitering Law

[Fox News](#) (6/23, Carter) reports, “Seattle is moving to end a longstanding city law that allowed police to arrest someone for

loitering, if they are also suspected of being a possible drug offender or sex worker.” According to Fox News, “The twin bills, passed unanimously by the Seattle City Council Monday, effectively block authorities from arresting someone for loitering in relation to a drug or a prostitution inquiry. Both laws, according to the Chicago-Kent Law Review, have historically targeted people of color.”

### Georgia Lawmakers Pass Bills On Hate Crimes, Enhanced Police Protections

The [AP](#) (6/23, Nadler, Amy) reports, “Georgia’s legislature on Tuesday passed hate crimes legislation deemed essential by business and many political leaders, sending the measure to Gov. Brian Kemp’s desk. The price Republicans exacted for moving that legislation forward was simultaneous passage of a separate bill that would mandate penalties for crimes targeting police and other first responders.” According to the AP, “The action comes after Senate Republicans had added police as a protected class to the hate crimes legislation last week in committee, but then later moved those protections to a separate bill in a deal between the parties. Democrats on Tuesday voted overwhelmingly against House Bill 838, which includes the increased protections for first responders. The hate crimes legislation, House Bill 426, had bipartisan support.”



The impact of an officer’s line-of-duty injury may continue beyond the initial event and hospitalization. Agencies can prepare to provide resources such as behavioral health and wellness or peer support services to officers and their families. The Line-of-Duty Serious Injury Considerations document and Concepts & Issues paper from the IACP Law Enforcement Policy Center provides guidelines for agencies to consider.

[Review documents and resources.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Law Enforcement Concerned About Rash Of Gun-Store Robberies

[Politico](#) (6/23, Swan) reports, “A rash of gun-store burglaries has alarmed law enforcement officials, and comes amid widespread protests that have been accompanied by incidents of looting and vandalism across the country.” According to Politico, “In the last days of May and first week of June, there were more than 90 attempted or successful burglaries of gun stores, according to the Bureau of Alcohol, Tobacco, and Firearms (ATF). More than 1,000 guns were stolen in that window of time, the bureau’s assistant director of field operations Tom Chittum told POLITICO. ‘It’s a lot of guns,’ Chittum said in an interview. ‘It’s the biggest spike I have ever seen of gun store burglaries.’” Chittum “said investigations into the surge of gun store burglaries are underway, and that some of the burglaries appeared to be part of broader looting. Other cases, he added, may have been the work of opportunists.”

### Gun Violence Spikes In New York City

The [New York Times](#) (6/23, Southall, Macfarquhar) reports, “It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.” The city “logged 125 shootings in the first three weeks of the month, more than double the number recorded over in same period last year, police data show. Gunmen opened fire during house parties, barbecues, dice games, and carried out coldly calculated street executions.” New York “is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.” On Monday, Mayor Bill de Blasio “announced that the city was sending more officers into the streets and declared he would not retreat from efforts to overhaul the Police Department.”

### Federal, Local Authorities Arrest 14 Suspects In South Carolina Car-Jacking, Drug Ring

The [Columbia \(SC\) State](#) (6/23, Monk) reports, “More than 200 federal and local law enforcement officers on Tuesday rounded up 14 members of an alleged Columbia-area violent gang whose members specialized in carjackings, armed robberies and drug dealing.” According to US Attorney Peter McCoy, who announced the arrests Tuesday, the arrests “were the result of a nearly two-year investigation by the FBI, the DEA and local law enforcement into a spike in gang-related violence in Richland, Lexington and Kershaw counties that began in July 2018.” FBI South Carolina SAC Jody Norris said, “Even in the midst of a



pandemic, the FBI and its task forces will continue to find and arrest drug traffickers who work against the people of South Carolina.” Also reporting are [WACH-TV](#) (6/23, Lanahan) and [WIS-TV](#) (6/23, Greene).

## GLOBAL SECURITY

### Suicide Bomber Targets Turkish Military Base In Somalia

The [New York Times](#) (6/23, Mohamed, Dahir) reports, “Two people were killed after a suicide bomber detonated his explosives outside Turkey’s largest overseas military base in Mogadishu on Tuesday.” The attack, which the Times says “bears the hallmarks of the Shabab terrorist group, was carried out just before 9 a.m. as recruits lined up for enlistment at Camp Turksom, where hundreds of Somali soldiers are trained and the new enrollment of dozens was underway.”

The [AP](#) (6/23, Guled) says Tuesday’s attack marks “the first time Turkey’s largest overseas military base has been attacked by the al-Qaida-linked al-Shabab extremist group,” which “quickly claimed responsibility, according to its Radio al-Furqan affiliate.”

### Secret Recordings Detail Neo-Nazi Group’s Grooming, Recruiting Process

[Fox News](#) (6/23, Chakraborty) reports on newly revealed secret recordings, first reported by the BBC, which show “senior members of The Base, a hate group started in the United States, interviewing young applicants, discussing their prospects and ways to radicalize them.” The founder of the group, American Rinaldo Nazzaro, “who now directs members of his group from St. Petersburg, Russia, is heard asking prospective members about their ethnicity, radicalization journey and their experience with weapons.” Fox reports Nazzaro “purportedly worked as an analyst for the FBI and as a contractor for the Pentagon before he left New York for Russia less than two years ago.”

## ALSO IN THE NEWS

### FCC To Vote Next Month On Making “988” New Suicide Hotline Number

The [AP](#) (6/23, Arbel) reports the FCC “will vote in July on whether to make ‘988’ the number to reach a suicide prevention hotline.” The Commission explained that “phone service providers will have until July 2022 to implement the new number, if the measure is approved in July, as expected.”

## TUESDAY'S LEAD STORIES

- [US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police](#)
- [Swedish Rape Conviction Rates Rise 75% After Change In Law](#)
- [“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers](#)
- [NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally](#)

### Subscriber Tools

- [Change Email Address](#)
- [Send Feedback](#)
- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to [afanucchi@sunnyvale.ca.gov](mailto:afanucchi@sunnyvale.ca.gov) as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media’s [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by [Bulletin Media](#) | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [hsyu@sunnyvale.ca.gov](mailto:hsyu@sunnyvale.ca.gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:21:40 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



---

**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.



The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.

## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

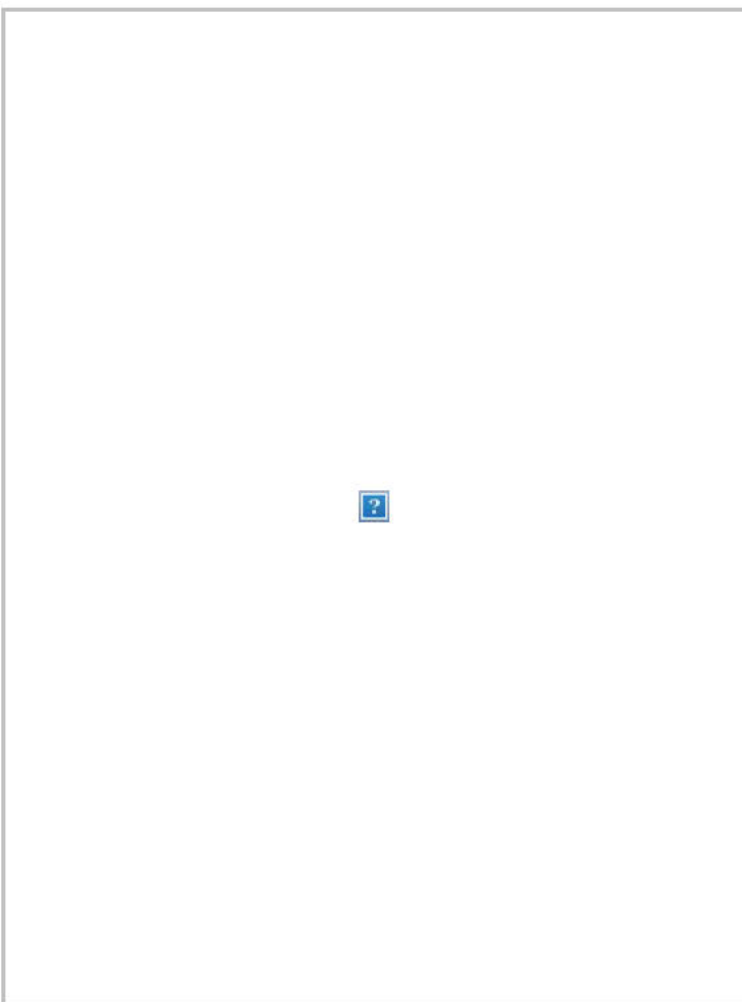
While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---



## Photo of the Day



[Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [hsyu@sunnyvale.ca.gov](mailto:hsyu@sunnyvale.ca.gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)





**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [JBoone@Sunnyvale.Ca.Gov](mailto:JBoone@Sunnyvale.Ca.Gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:20:50 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.

The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.

## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

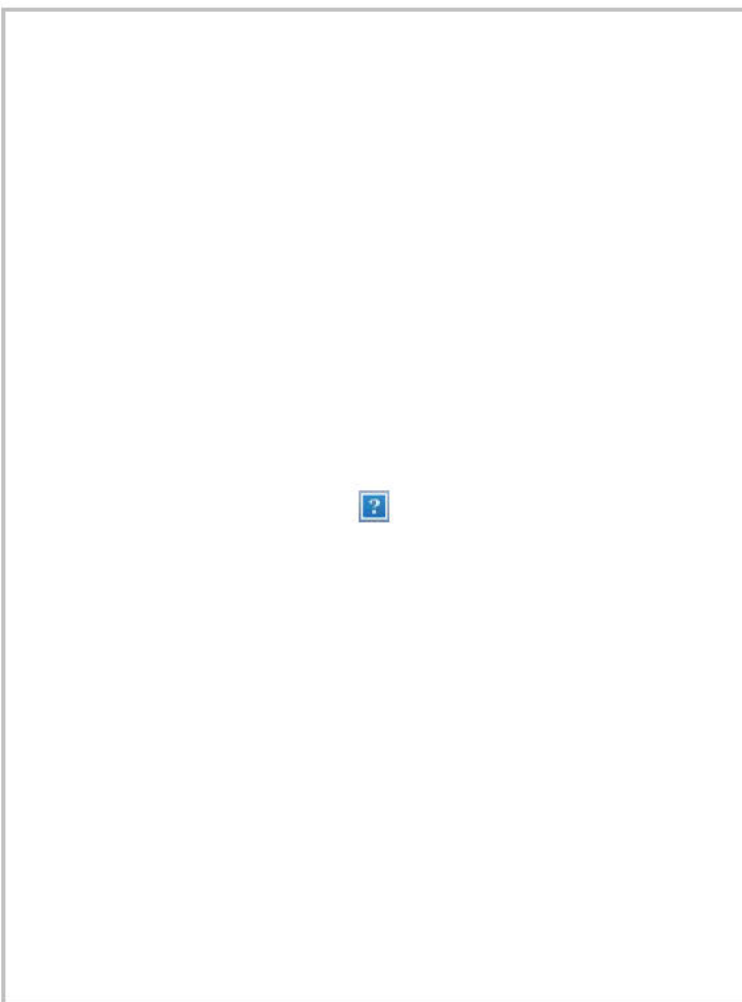
Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---





## Photo of the Day



### [Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [JBoone@Sunnyvale.Ca.Gov](mailto:JBoone@Sunnyvale.Ca.Gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)



**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [dsakurai@sunnyvale.ca.gov](mailto:dsakurai@sunnyvale.ca.gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:20:50 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.

The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.

## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.



## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

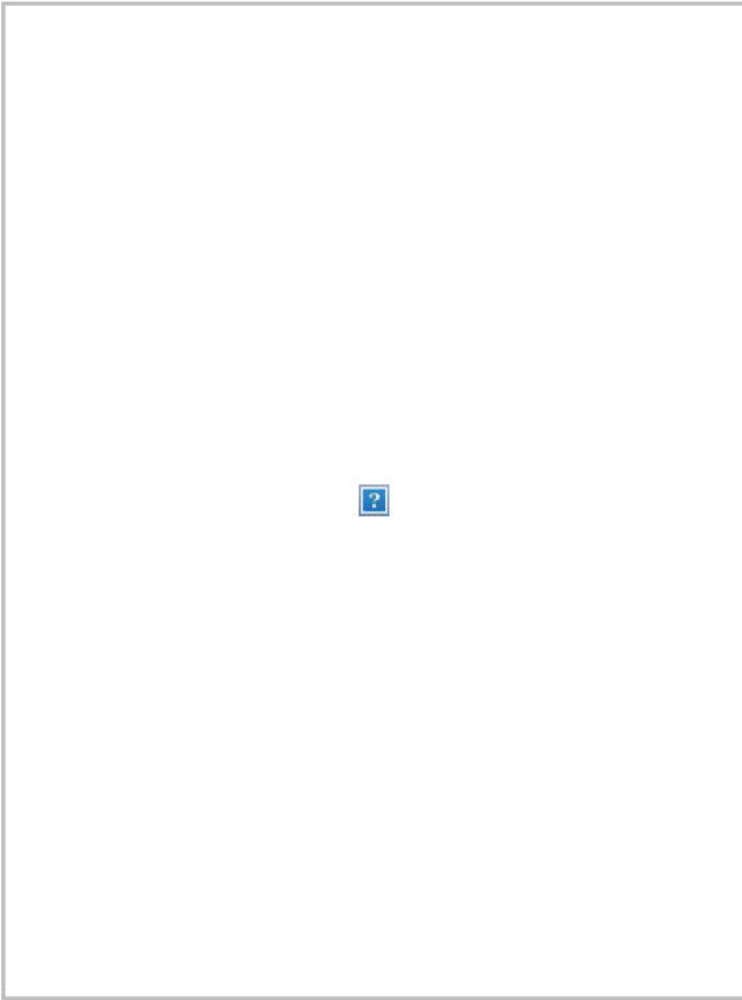
While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---



## Photo of the Day



### [Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [dsakurai@sunnyvale.ca.gov](mailto:dsakurai@sunnyvale.ca.gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)



**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [Hchoi@sunnyvale.ca.gov](mailto:Hchoi@sunnyvale.ca.gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:20:50 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.

The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.



## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

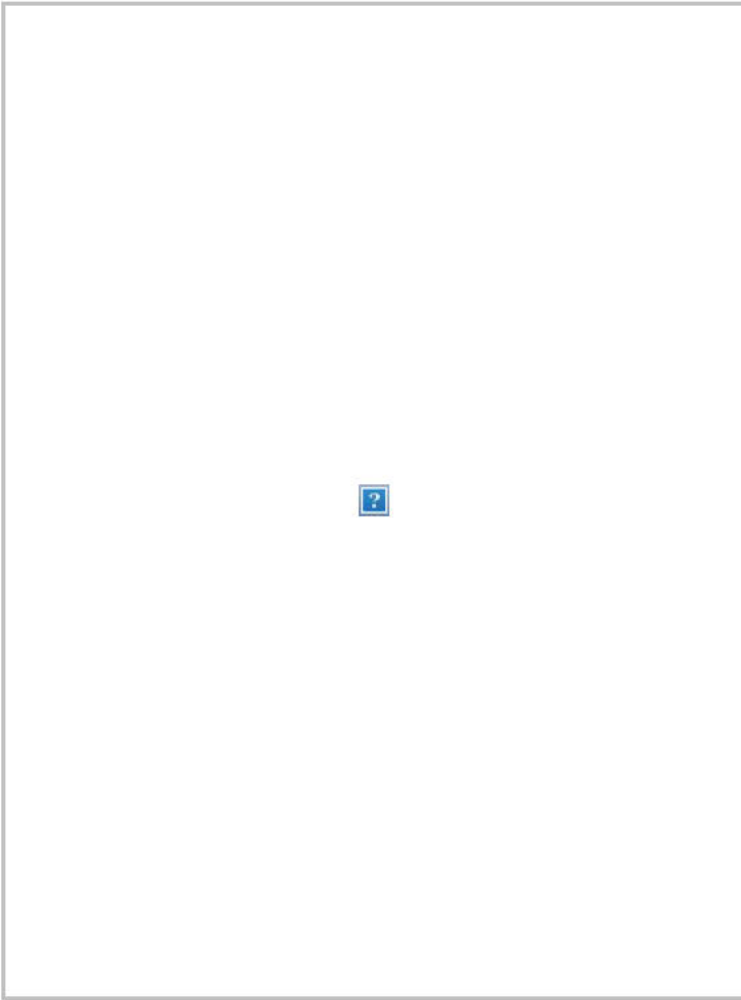
While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---



## Photo of the Day



[Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [Hchoi@sunnyvale.ca.gov](mailto:Hchoi@sunnyvale.ca.gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)



**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [jhunter@sunnyvale.ca.gov](mailto:jhunter@sunnyvale.ca.gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:20:15 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.

The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.



## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

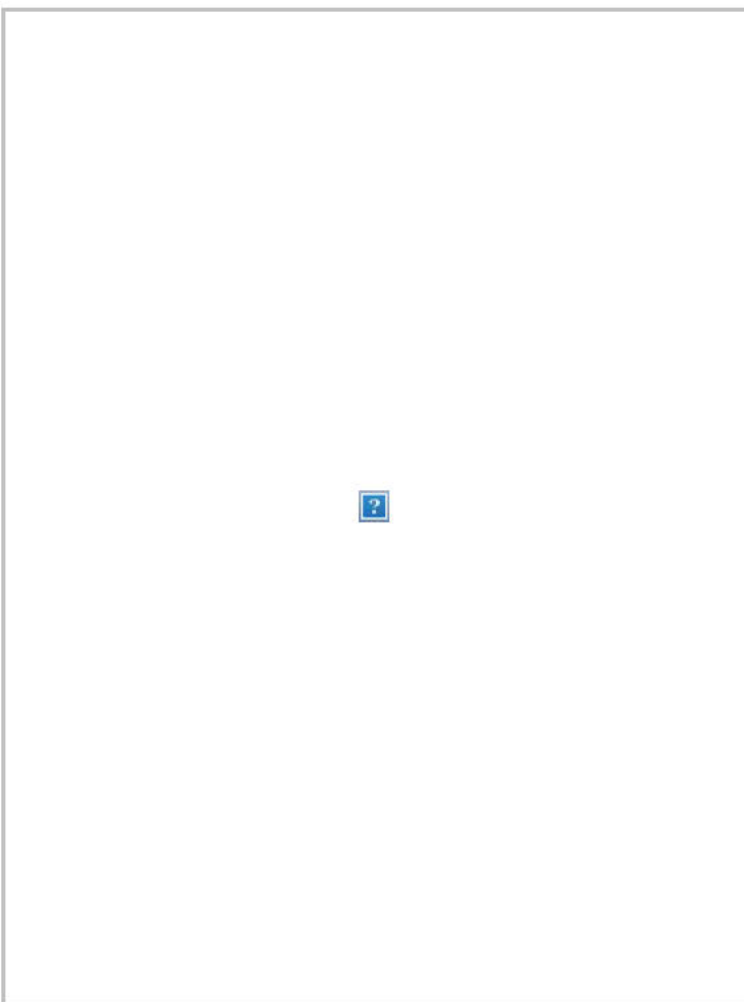
While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---



## Photo of the Day



### [Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [jhunter@sunnyvale.ca.gov](mailto:jhunter@sunnyvale.ca.gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)



**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [sdrewniany@sunnyvale.ca.gov](mailto:sdrewniany@sunnyvale.ca.gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:19:41 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.

The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.



## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

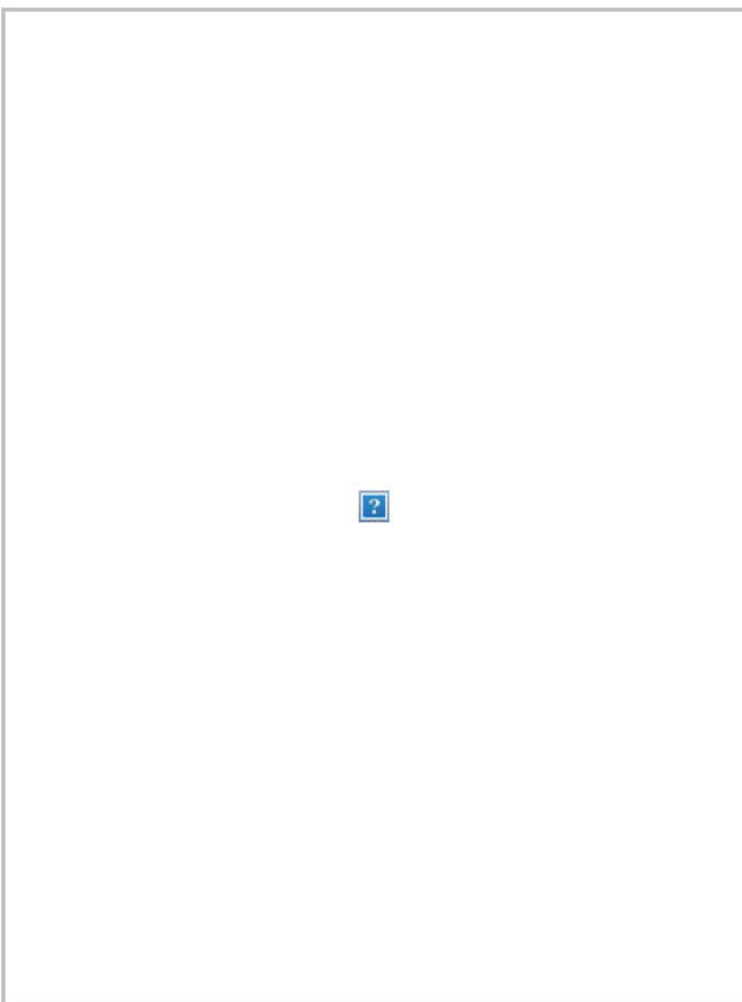
While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---



## Photo of the Day



### [Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [sdrewniany@sunnyvale.ca.gov](mailto:sdrewniany@sunnyvale.ca.gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)



**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [pngo@sunnyvale.ca.gov](mailto:pngo@sunnyvale.ca.gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:19:40 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.

The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.



## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

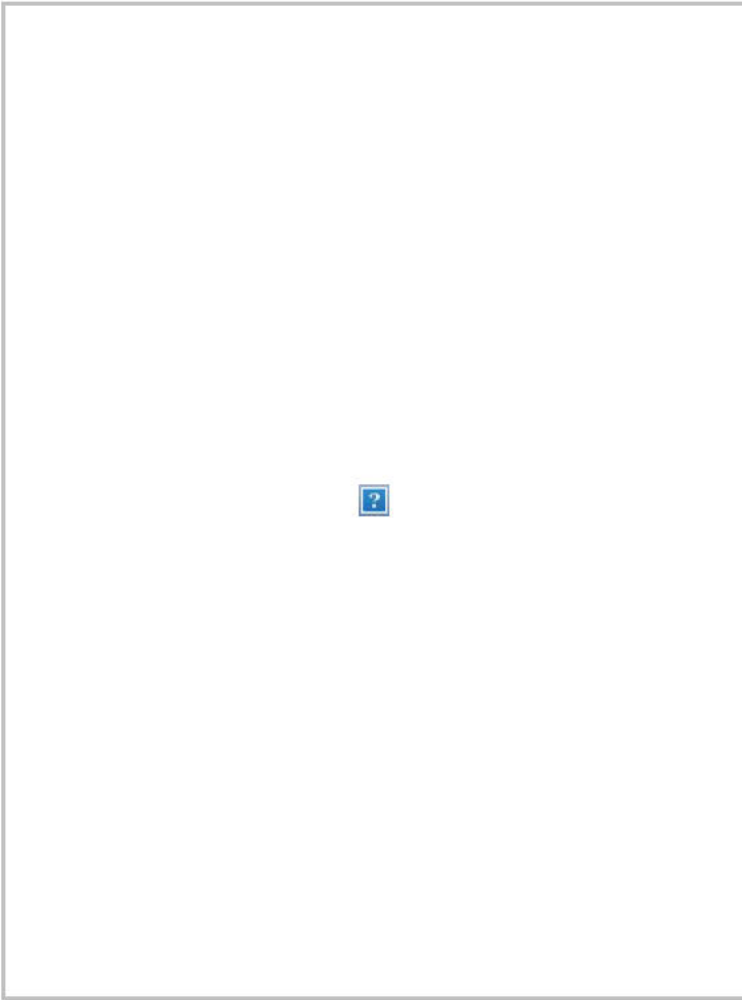
While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---



## Photo of the Day



### [Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [pngo@sunnyvale.ca.gov](mailto:pngo@sunnyvale.ca.gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)



**From:** [perf@memberclicks-mail.net](mailto:perf@memberclicks-mail.net) on behalf of [PERF Daily Clips](#)  
**To:** [Afanucchi@sunnyvale.ca.gov](mailto:Afanucchi@sunnyvale.ca.gov)  
**Subject:** PERF Daily Clips: Anonymous stole and leaked a megatrove of police documents  
**Date:** Wednesday, June 24, 2020 4:15:29 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



**Wednesday, June 24, 2020**

---

## **National News**

**WIRED:** [Anonymous stole and leaked a megatrove of police documents](#)

It's been the better part of a decade since the hacktivist group Anonymous rampaged across the internet, stealing and leaking millions of secret files from dozens of US organizations. Now, amid the global protests following the killing of George Floyd, Anonymous is back—and it's returned with a dump of hundreds of gigabytes of law enforcement files and internal communications.

On Friday of last week a leak-focused activist group known as Distributed Denial of Secrets published a 269-gigabyte collection of police data that includes emails, audio, video, and intelligence documents, with more than a million files in total. DDOSecrets founder Emma Best tells WIRED that the hacked files came from Anonymous—or at least a source self-representing as part of that group, given that under Anonymous' loose, leaderless structure anyone can declare themselves a member. Over the weekend, supporters of DDOSecrets, Anonymous, and protesters worldwide began digging through the files to pull out frank internal memos about police efforts to track the activities of protesters. The documents also reveal how law enforcement has described groups like the antifascist movement Antifa.

The massive internal data trove that DDOSecrets published was originally taken from a web development firm called Netsential, according to a law enforcement memo obtained by Krebs On Security. That memo, issued by the National Fusion Center Association, says that much of the data belonged to law enforcement "fusion centers" across the US that act as information-sharing hubs for federal, state, and local agencies. Netsential did not immediately respond to a request for comment.

## **New York Times: [Qualified immunity protection for police emerges as flash point amid protests](#)**

Once a little-known rule, qualified immunity has emerged as a flash point in the protests spurred by Mr. Floyd's killing and galvanized calls for police reform. In the vast majority of cases of police brutality, officers are never criminally prosecuted. For families of victims seeking some sort of relief through the justice system, qualified immunity presents another obstacle to obtaining financial or other damages. Even in the rare cases where the officers are charged, as in Mr. Floyd's death, the police can still claim qualified immunity if relatives or victims sue them.

Activists have seized on qualified immunity as what they see as one of the biggest problems with policing and argued that it shields officers from being held accountable in cases of misconduct. Police leaders said it was essential for officers' ability to respond to calls and to make split-second decisions.

Qualified immunity is a focal point of the new debate on Capitol Hill over how to address systemic racism in policing and use of excessive force. House Democrats unveiled a bill that would allow victims of police brutality to seek damages from their assailants. A competing Senate Republican bill made no mention of qualified immunity, and the White House press secretary, Kayleigh McEnany, called it a "total and complete nonstarter."

---

## **Local News**

### **New York Times: [Gun violence spikes in N.Y.C., intensifying debate over policing](#)**

It has been nearly a quarter century since New York City experienced as much gun violence in the month of June as it has seen this year.

The city logged 125 shootings in the first three weeks of the month, more than double the number recorded over the same period last year, police data show. Gunmen opened fire during house parties, barbecues and dice games, and carried out coldly calculated street executions.

The rising toll of gun violence has become part of a contentious debate over the future of policing in the wake of mass protests against police brutality. Police unions and their supporters have issued shrill warnings that the city was slipping into a high-crime era reminiscent of the early 1990s.

The city is not alone. Shootings are on the rise in other big cities across the country, including Chicago and Minneapolis, a trend that some conservatives have seized on to argue against the recent demands of protesters to cut police budgets and rein in officers.



## **NPR: [Seattle Police will return to precinct in protest zone, mayor says](#)**

Seattle Mayor Jenny Durkan says police will return to their East Precinct building, after a weekend in which three people were shot in the occupied zone known as the Capitol Hill Organized Protest, or CHOP. One of the victims died.

"In the near future, SPD will be peacefully returning to the East Precinct," Durkan said via Twitter, as she and Police Chief Carmen Best announced plans to take back control of the area formerly known as the Capitol Hill Autonomous Zone.

Seattle police need to work from the precinct to "ensure public safety" and respond to emergency calls, Durkan said.

## **KPBS San Diego: [Reports of child exploitation, trafficking increase during pandemic](#)**

Among the many social consequences of the coronavirus pandemic is that young people are spending more time than ever at home and on their phones.

This has made them more vulnerable to human traffickers who lurk on social media, say local law enforcement officials.

Reports of internet crime against juveniles in San Diego County, which mostly involve sharing illicit photos of minors, have tripled since the pandemic started, according to the San Diego County District Attorney's Office.

In April of 2019, there were 287 reports in the county. This April, the number shot up to more than 850, the DA's data show. The local numbers mirror a trend happening nationwide and across the world.

## **Chicago Tribune: [Saying Chicago police uphold 'racist and white supremacist values,' DePaul tutors refuse to work with officers taking classes, call for university to cut ties with department](#)**

After weeks of student calls to end educational programs that serve members of the Chicago Police Department, DePaul University Provost Salma Ghanem turned aside the demands on Monday, saying in a statement that "the actions of a few do not represent the (CPD officers) we teach."

The provost's statement also included an account from an unnamed police officer who said she was "devastated" by the students' appeal.

"As a CPD Latina I am proud to be who I am and for the past 12 years have worked tirelessly throughout my career to make a difference and I can bet my life savings that many officers (enrolled at DePaul) share the same feelings," she wrote.

## **AFP: [French police under new scrutiny after chokehold death](#)**

France's police faced new pressure Tuesday after the family of a delivery man who died after being arrested last January demanded a ban on chokeholds.

Cedric Chouviat got into a heated exchange with police after being stopped for a routine check near the Eiffel Tower in Paris before he was pinned down by several officers.

Chouviat, who has North African origins, said "I'm suffocating" seven times before his body went limp, according to a review of videos by investigators seen by AFP this week.

He was not breathing and had no pulse when emergency services arrived and brought him to hospital, where he was pronounced dead two days later.

Four officers were taken in for questioning last week in an inquiry into "involuntary homicide" but so far they have not faced disciplinary action.

---

## **Police Executive Appointments**

### **Global News: [Toronto Police Deputy Chief James Ramer named interim chief effective Aug. 1](#)**

Toronto Police Deputy Chief Ramer has been named the interim chief of police effective Aug. 1.

Ramer will remain as interim chief until the Toronto Police Services Board appoints a new chief.

The board made the announcement on Monday after an internal memo was sent to officers informing them of the decision.

The internal memo, obtained by Global News, was sent on behalf of current police Chief Mark Saunders, who announced he would be resigning at the end of July.

---

## **Good News of the Day**

### **ABC 13 Toledo (OH): [Toledo Police officers leave gift for child attacked by dog](#)**

A Toledo family is sending out a thank you to two Toledo Police officers that went above and beyond the call of duty.

Last week, JJ Knudsen was visiting a family member when she was attacked by a dog. Police officers and firefighters both arrived on the scene and JJ was taken to the hospital and rushed into surgery.

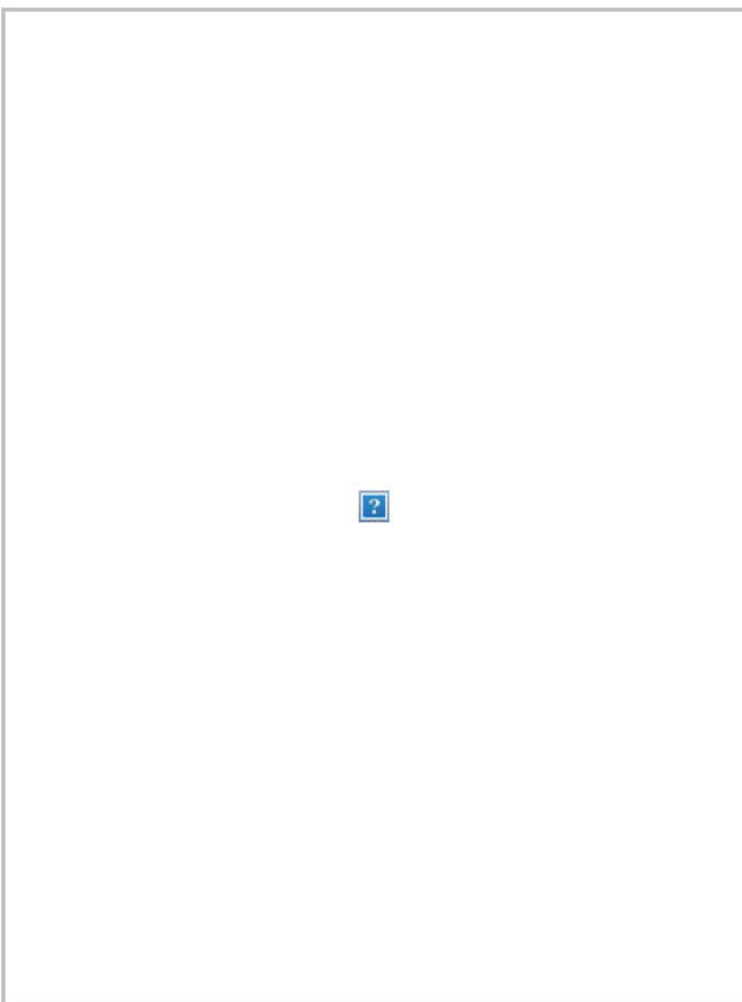
While at the hospital, her father noticed something on the family's security system. Two police officers that responded to the call tracked down the family's address, went to the house and placed a gift on the back porch.

Inside the bag was a baby doll and a Paw Patrol toy along with a card wishing the 4-year-old a speedy recovery.

---



## Photo of the Day



### [Sheboygan \(WI\) Police Department](#)

We had a nice visit today from Audrey. Audrey and her mom made us "survival bags." Thank you Audrey for the amazing bags.

---

To unsubscribe from clips, check "I do not want Daily Clips" in the [My Profile](#) section of the PERF website, or reply to this email with the word "unsubscribe."

---

This email was sent to [Afanucchi@sunnyvale.ca.gov](mailto:Afanucchi@sunnyvale.ca.gov) by [perfclips@policeforum.org](mailto:perfclips@policeforum.org)

Police Executive Research Forum • 1120 Connecticut Ave. NW DC, Suite 930, Washington, District of Columbia 20036, United States

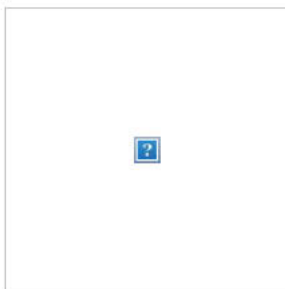
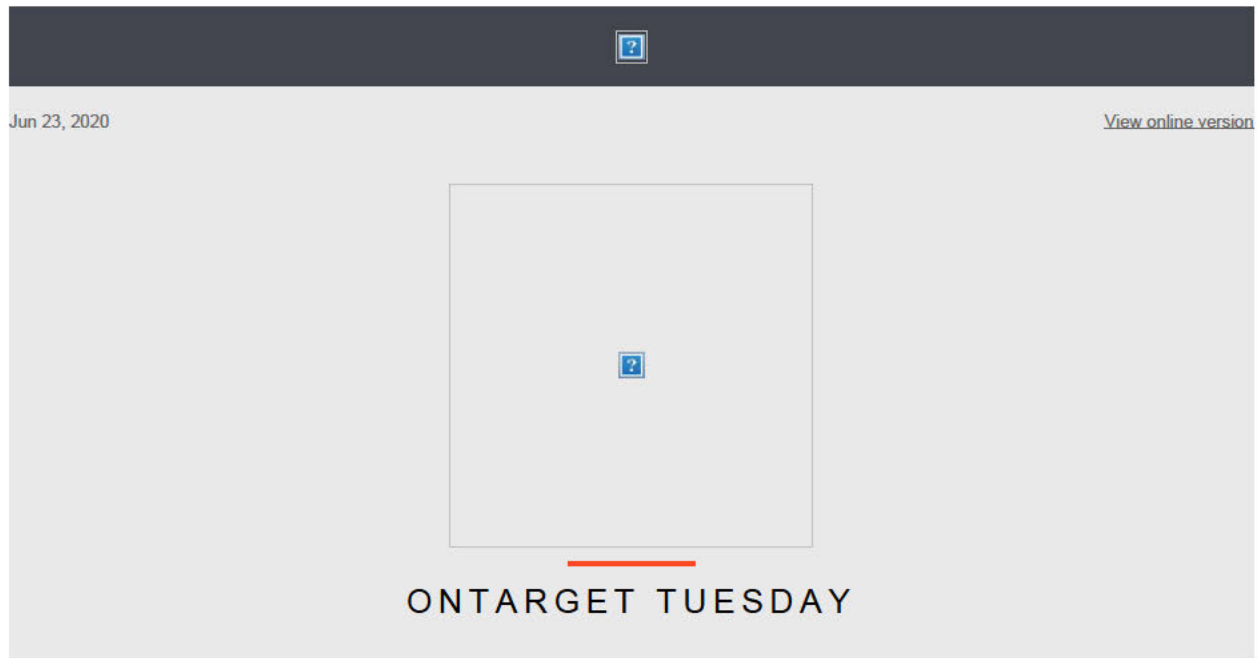
[Remove My Email or Manage Preferences](#) • [Privacy Policy](#)



**From:** [Police On Target](#)  
**To:** [mirose@sunnyvale.ca.gov](mailto:mirose@sunnyvale.ca.gov)  
**Subject:** Man Saves Officer from Wrecked Patrol Car  
**Date:** Tuesday, June 23, 2020 3:25:55 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



### **Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car**

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

[READ MORE](#)



---

### **Hackers Steals Massive Trove of Police Files, Post Them Online**

DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

[READ MORE](#)



---

### **Florida Officers Lured Into Ambush Attack at Call for Service**

Several officers with the Tampa (LF) Police



Department were reportedly ambushed early Saturday morning while responding to a call for service.

[READ MORE](#)



---

### **Maryland Officer Wounded by Gunfire Released from Hospital**

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

[READ MORE](#)



### **Responding to Domestic Disturbances**

A domestic disturbance call can involve anything from a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

[READ MORE](#)

---

### **Massachusetts Officer Injured in Attack During Interview at Police Station**

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

[READ MORE](#)



### **Oregon Officer Saves Infant from Burning Home**

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

[READ MORE](#)

---



## Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

[READ MORE](#)



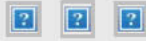
## Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut emissions. More importantly, they can do the job.

[READ MORE](#)

## FREE WHITEPAPERS

- ☐ SPECIAL REPORT: Drug Enforcement, Protection & Testing
- ☐ Police and the Coronavirus Pandemic
- ☐ SPECIAL REPORT: Fleet Management & Upfitting
- ☐ Special Report: Preventing & Preparing for Workplace Attacks
- ☐ Best Practices for Setting Up and Implementing a First Responder Network
- ☐ Special Report: Software & Mobile Apps
- ☐ Special Report: Ballistic Protection
- ☐ The Top 5 Emerging Technologies Police Agencies Can't Do Without
- ☐ How Technology Mitigates Threats at Large-Scale Events
- ☐ Special Report: Critical Incident Response
- ☐ Special Report: Upfitting & Fleet Management



## POLICE MAGAZINE

You are currently subscribed as mirose@sunnyvale.ca gov. Manage your [email preferences](#).

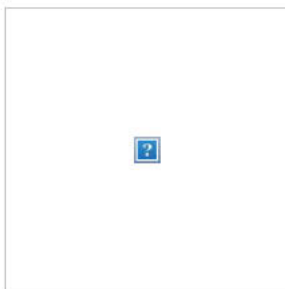
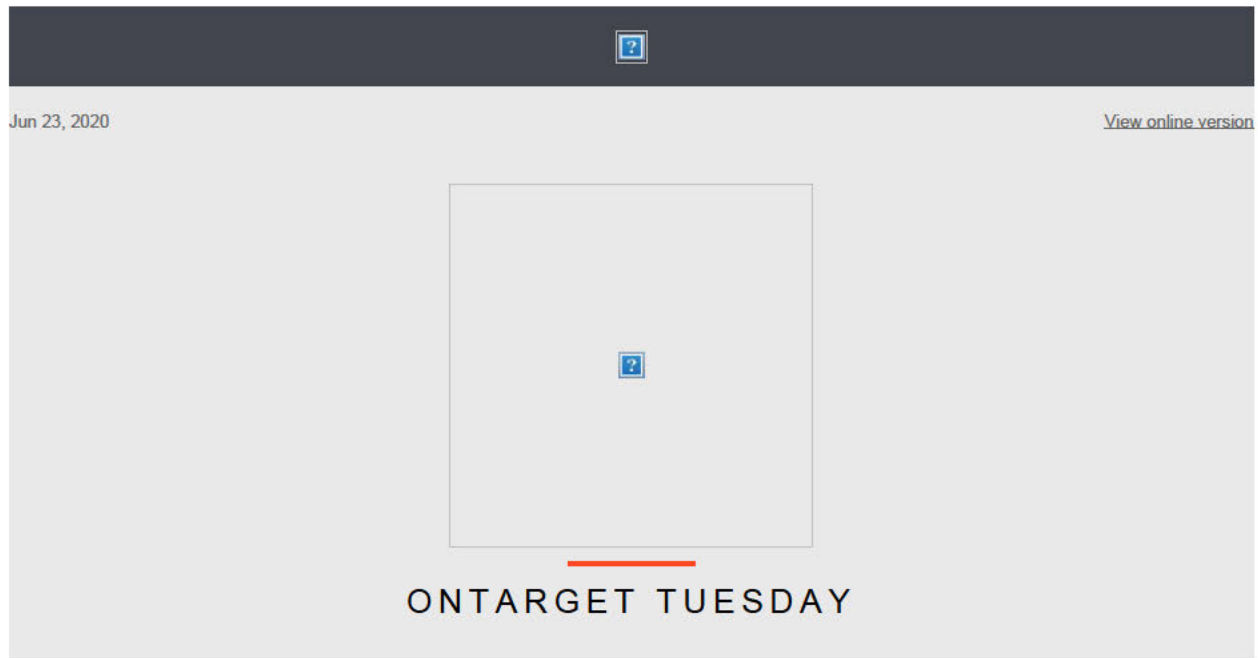
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

[Contact Us](#) | [Privacy Policy](#) | [Unsubscribe](#)

**From:** [Police On Target](#)  
**To:** [kkim@sunnyvale.ca.gov](mailto:kkim@sunnyvale.ca.gov)  
**Subject:** Man Saves Officer from Wrecked Patrol Car  
**Date:** Tuesday, June 23, 2020 3:25:52 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



## Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

[READ MORE](#)



---

## Hackers Steals Massive Trove of Police Files, Post Them Online

DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

[READ MORE](#)



---

## Florida Officers Lured Into Ambush Attack at Call for Service

Several officers with the Tampa (LF) Police



Department were reportedly ambushed early Saturday morning while responding to a call for service.

[READ MORE](#)



---

### **Maryland Officer Wounded by Gunfire Released from Hospital**

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

[READ MORE](#)



### **Responding to Domestic Disturbances**

A domestic disturbance call can involve anything from a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

[READ MORE](#)

---

### **Massachusetts Officer Injured in Attack During Interview at Police Station**

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

[READ MORE](#)



### **Oregon Officer Saves Infant from Burning Home**

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

[READ MORE](#)

---

## Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

[READ MORE](#)



## Hybrids Ready for Patrol

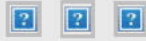
Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut emissions. More importantly, they can do the job.

[READ MORE](#)

## FREE WHITEPAPERS

- ☐ SPECIAL REPORT: Drug Enforcement, Protection & Testing
- ☐ Police and the Coronavirus Pandemic
- ☐ SPECIAL REPORT: Fleet Management & Upfitting
- ☐ Special Report: Preventing & Preparing for Workplace Attacks
- ☐ Best Practices for Setting Up and Implementing a First Responder Network
- ☐ Special Report: Software & Mobile Apps
- ☐ Special Report: Ballistic Protection
- ☐ The Top 5 Emerging Technologies Police Agencies Can't Do Without
- ☐ How Technology Mitigates Threats at Large-Scale Events
- ☐ Special Report: Critical Incident Response
- ☐ Special Report: Upfitting & Fleet Management





## POLICE MAGAZINE

You are currently subscribed as [kkim@sunnyvale.ca.gov](mailto:kkim@sunnyvale.ca.gov). Manage your [email preferences](#).

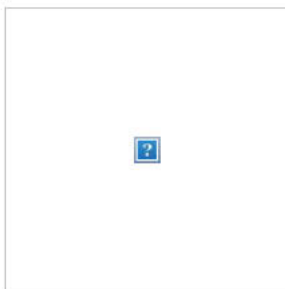
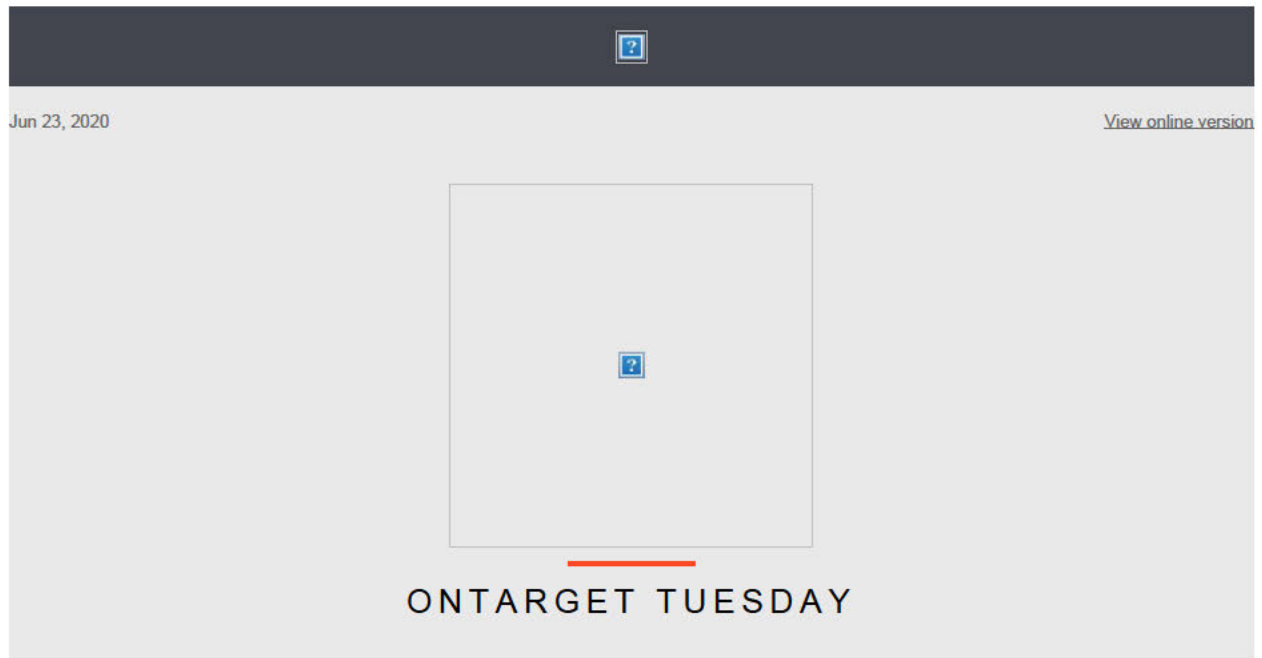
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

[Contact Us](#) | [Privacy Policy](#) | [Unsubscribe](#)

**From:** [Police On Target](#)  
**To:** [rhuihui@sunnyvale.ca.gov](mailto:rhuihui@sunnyvale.ca.gov)  
**Subject:** Man Saves Officer from Wrecked Patrol Car  
**Date:** Tuesday, June 23, 2020 3:25:28 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



### **Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car**

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

[READ MORE](#)



---

### **Hackers Steals Massive Trove of Police Files, Post Them Online**

DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

[READ MORE](#)



---

### **Florida Officers Lured Into Ambush Attack at Call for Service**

Several officers with the Tampa (LF) Police



Department were reportedly ambushed early Saturday morning while responding to a call for service.

[READ MORE](#)



### **Maryland Officer Wounded by Gunfire Released from Hospital**

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

[READ MORE](#)



### **Responding to Domestic Disturbances**

A domestic disturbance call can involve anything from a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

[READ MORE](#)

### **Massachusetts Officer Injured in Attack During Interview at Police Station**

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

[READ MORE](#)



### **Oregon Officer Saves Infant from Burning Home**

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

[READ MORE](#)

## Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

[READ MORE](#)



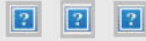
## Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut emissions. More importantly, they can do the job.

[READ MORE](#)

## FREE WHITEPAPERS

- ☐ SPECIAL REPORT: Drug Enforcement, Protection & Testing
- ☐ Police and the Coronavirus Pandemic
- ☐ SPECIAL REPORT: Fleet Management & Upfitting
- ☐ Special Report: Preventing & Preparing for Workplace Attacks
- ☐ Best Practices for Setting Up and Implementing a First Responder Network
- ☐ Special Report: Software & Mobile Apps
- ☐ Special Report: Ballistic Protection
- ☐ The Top 5 Emerging Technologies Police Agencies Can't Do Without
- ☐ How Technology Mitigates Threats at Large-Scale Events
- ☐ Special Report: Critical Incident Response
- ☐ Special Report: Upfitting & Fleet Management



## POLICE MAGAZINE

You are currently subscribed as rhuihui@sunnyvale.ca.gov. Manage your [email preferences](#).

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

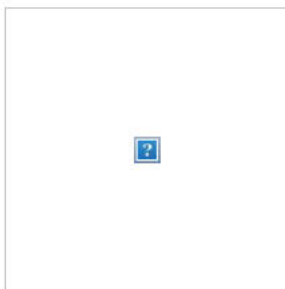
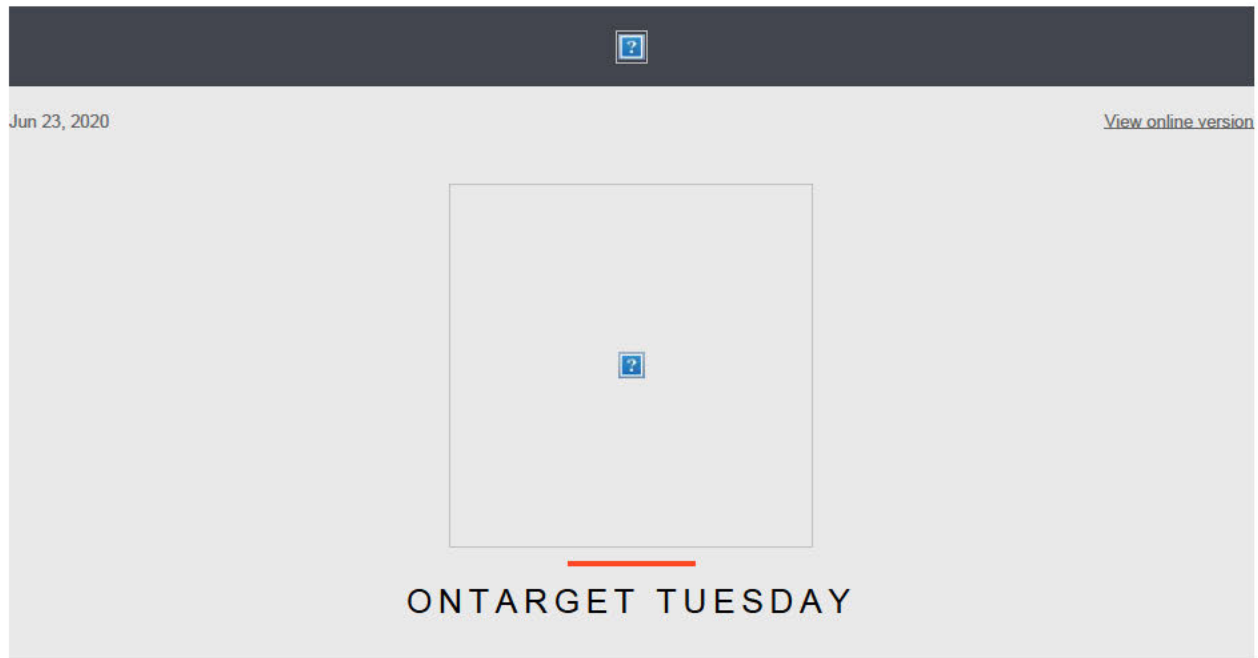
[Contact Us](#) | [Privacy Policy](#) | [Unsubscribe](#)



**From:** [Police On Target](#)  
**To:** [toki@sunnyvale.ca.gov](mailto:toki@sunnyvale.ca.gov)  
**Subject:** Man Saves Officer from Wrecked Patrol Car  
**Date:** Tuesday, June 23, 2020 3:25:27 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



### **Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car**

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

[READ MORE](#)



---

### **Hackers Steals Massive Trove of Police Files, Post Them Online**

DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

[READ MORE](#)



---

### **Florida Officers Lured Into Ambush Attack at Call for Service**

Several officers with the Tampa (LF) Police



Department were reportedly ambushed early Saturday morning while responding to a call for service.

[READ MORE](#)



### **Maryland Officer Wounded by Gunfire Released from Hospital**

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

[READ MORE](#)



### **Responding to Domestic Disturbances**

A domestic disturbance call can involve anything from a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

[READ MORE](#)

### **Massachusetts Officer Injured in Attack During Interview at Police Station**

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

[READ MORE](#)



### **Oregon Officer Saves Infant from Burning Home**

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

[READ MORE](#)

## Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

[READ MORE](#)



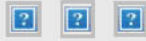
## Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut emissions. More importantly, they can do the job.

[READ MORE](#)

## FREE WHITEPAPERS

- ☐ SPECIAL REPORT: Drug Enforcement, Protection & Testing
- ☐ Police and the Coronavirus Pandemic
- ☐ SPECIAL REPORT: Fleet Management & Upfitting
- ☐ Special Report: Preventing & Preparing for Workplace Attacks
- ☐ Best Practices for Setting Up and Implementing a First Responder Network
- ☐ Special Report: Software & Mobile Apps
- ☐ Special Report: Ballistic Protection
- ☐ The Top 5 Emerging Technologies Police Agencies Can't Do Without
- ☐ How Technology Mitigates Threats at Large-Scale Events
- ☐ Special Report: Critical Incident Response
- ☐ Special Report: Upfitting & Fleet Management



## POLICE MAGAZINE

You are currently subscribed as [toki@sunnyvale.ca.gov](mailto:toki@sunnyvale.ca.gov). Manage your [email preferences](#).

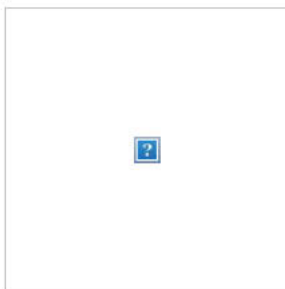
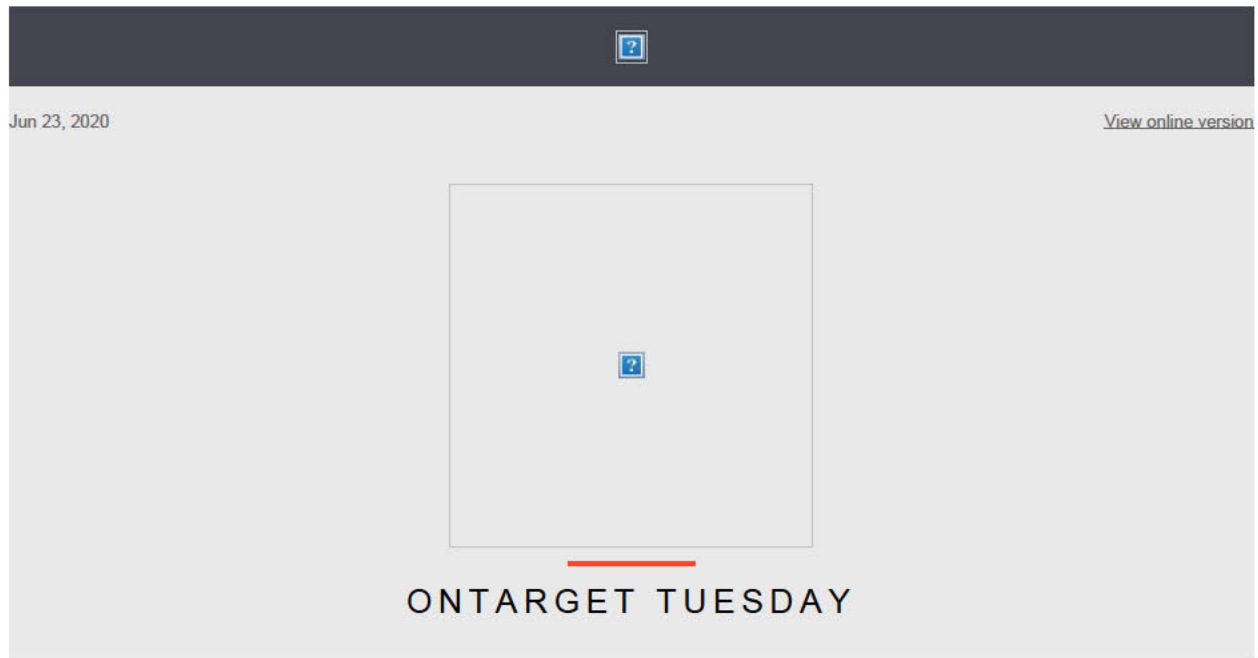
Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

[Contact Us](#) | [Privacy Policy](#) | [Unsubscribe](#)

**From:** [Police On Target](#)  
**To:** [qvierra@ci.sunnyvale.ca.us](mailto:qvierra@ci.sunnyvale.ca.us)  
**Subject:** Man Saves Officer from Wrecked Patrol Car  
**Date:** Tuesday, June 23, 2020 3:24:26 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



### **Pennsylvania Man Pulls Police Officer from Wrecked Patrol Car**

Daylan McLee was at a Fathers' Day event with family when he saw the police officer pinned to the ground by his patrol vehicle following a crash.

[READ MORE](#)



---

### **Hackers Steals Massive Trove of Police Files, Post Them Online**

DDoSecrets said the BlueLeaks archive indexes "ten years of data from over 200 police departments, fusion centers and other law enforcement training and support resources," and that "among the hundreds of thousands of documents are police and FBI reports, bulletins, guides and more."

[READ MORE](#)



---

### **Florida Officers Lured Into Ambush Attack at Call for Service**

Several officers with the Tampa (LF) Police





Department were reportedly ambushed early Saturday morning while responding to a call for service.

[READ MORE](#)



---

### **Maryland Officer Wounded by Gunfire Released from Hospital**

An officer with the Baltimore Police Department who was shot earlier this month while he tried to disperse a large crowd that had gathered to protest the in-custody death of George Floyd in Minneapolis has been released from the hospital.

[READ MORE](#)



### **Responding to Domestic Disturbances**

A domestic disturbance call can involve anything from a verbal dispute to a homicide. So we all need reminders of the danger of domestic disputes and ensure officers are taking all precautions.

[READ MORE](#)

---

### **Massachusetts Officer Injured in Attack During Interview at Police Station**

An officer with the Southborough (MA) Police Department was injured after he was reportedly assaulted with a weapon inside a police station on Monday night.

[READ MORE](#)



### **Oregon Officer Saves Infant from Burning Home**

An officer with the Astoria (OR) Police Department is being heralded as a hero for his quick actions late last week that are now only becoming public knowledge.

[READ MORE](#)

---

## Texas Officer Shot in Arm Following Vehicle and Foot Pursuit

An officer with the Watauga (TX) Police Department was shot in the arm by a suspect who led police on a vehicle chase, bailed out of the car and ran away, briefly eluding officers.

[READ MORE](#)



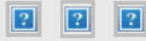
## Hybrids Ready for Patrol

Police vehicles with hybrid gas-electric engines will save law enforcement agencies money and cut emissions. More importantly, they can do the job.

[READ MORE](#)

## FREE WHITEPAPERS

- ☐ SPECIAL REPORT: Drug Enforcement, Protection & Testing
- ☐ Police and the Coronavirus Pandemic
- ☐ SPECIAL REPORT: Fleet Management & Upfitting
- ☐ Special Report: Preventing & Preparing for Workplace Attacks
- ☐ Best Practices for Setting Up and Implementing a First Responder Network
- ☐ Special Report: Software & Mobile Apps
- ☐ Special Report: Ballistic Protection
- ☐ The Top 5 Emerging Technologies Police Agencies Can't Do Without
- ☐ How Technology Mitigates Threats at Large-Scale Events
- ☐ Special Report: Critical Incident Response
- ☐ Special Report: Upfitting & Fleet Management



## POLICE MAGAZINE

You are currently subscribed as [gvierra@ci.sunnyvale.ca.us](mailto:gvierra@ci.sunnyvale.ca.us). Manage your [email preferences](#).

Bobit Business Media is located at 3520 Challenger Street, Torrance CA 90503

[Contact Us](#) | [Privacy Policy](#) | [Unsubscribe](#)

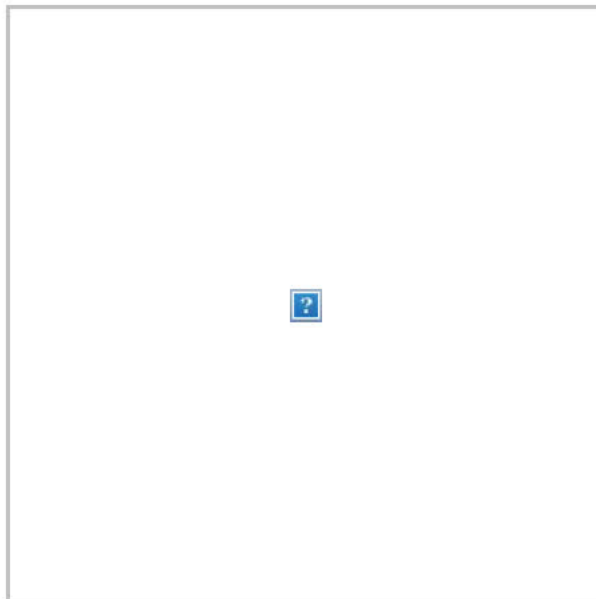
**From:** [PoliceOne Roll Call](#)  
**To:** [dklein@sunnyvale.ca.gov](mailto:dklein@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:27:19 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

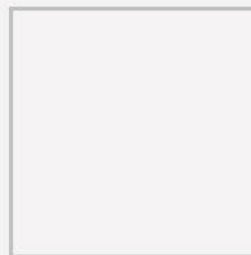
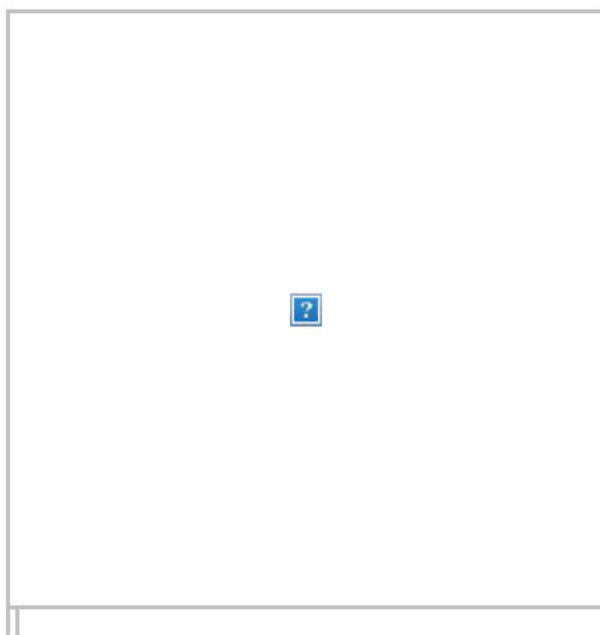
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

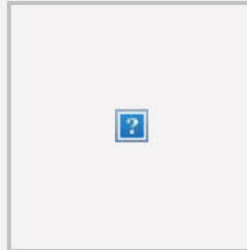


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

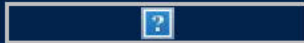
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

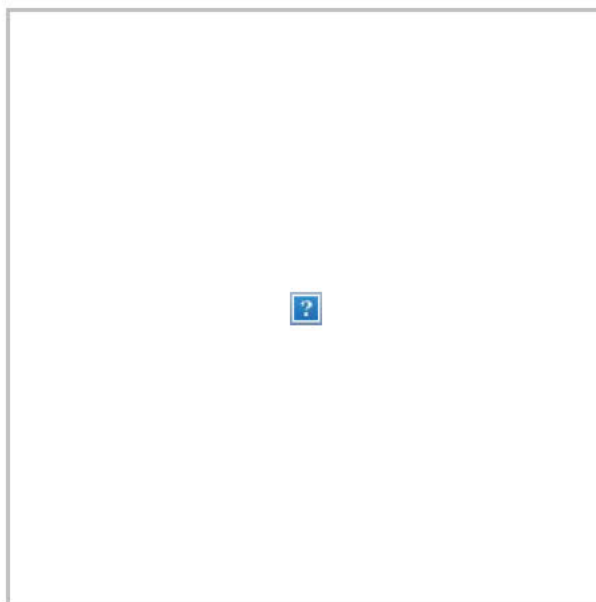
**From:** [PoliceOne Roll Call](#)  
**To:** [dchong@ci.sunnyvale.ca.us](mailto:dchong@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:27:12 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

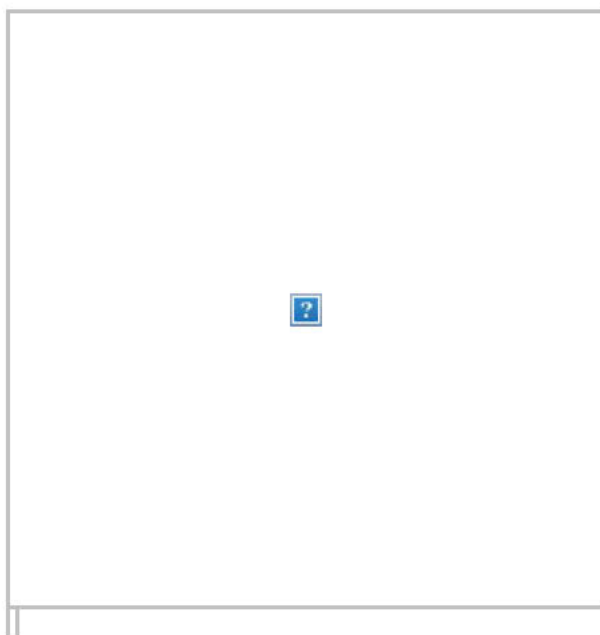
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

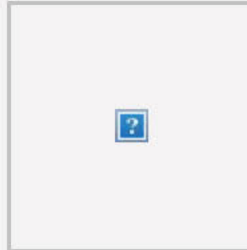


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

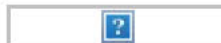
- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

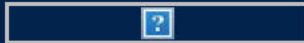
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

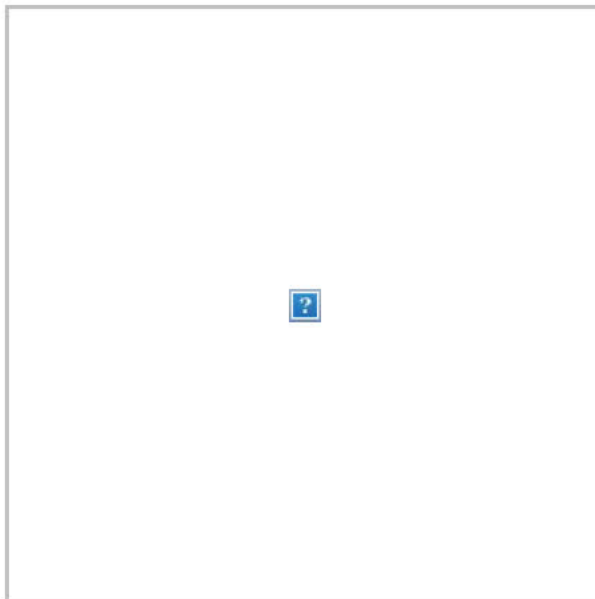
**From:** [PoliceOne Roll Call](#)  
**To:** [gvierra@sunnyvale.ca.gov](mailto:gvierra@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:26:55 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

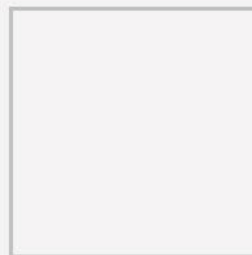
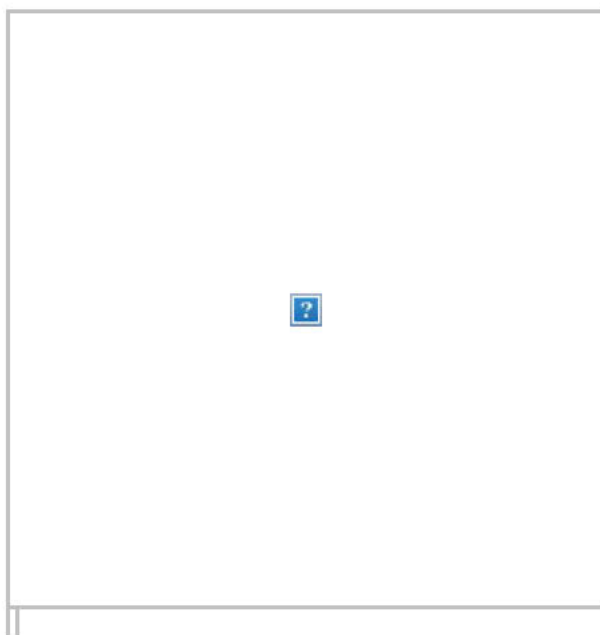
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

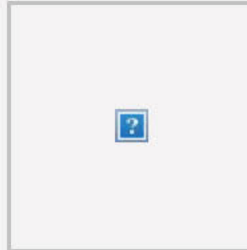


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



## Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



## Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



## Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

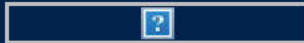
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



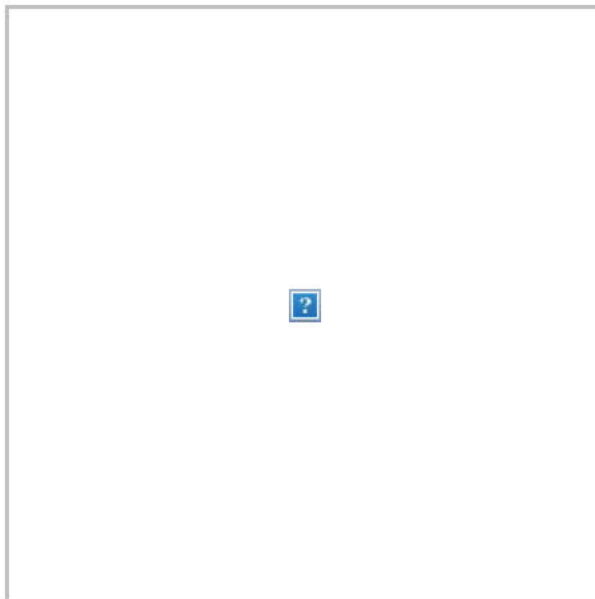
**From:** [PoliceOne Roll Call](#)  
**To:** [klemos@sunnyvale.ca.gov](mailto:klemos@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:26:50 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

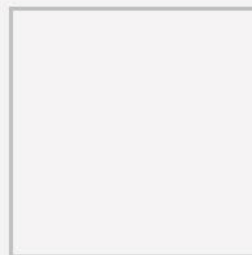
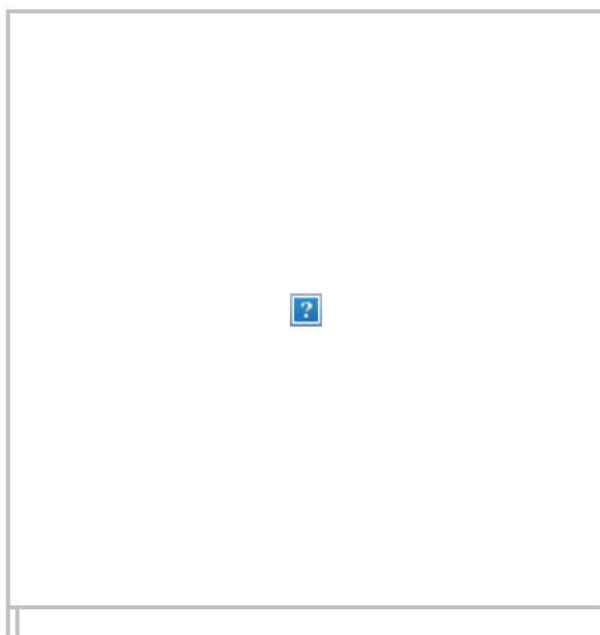
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

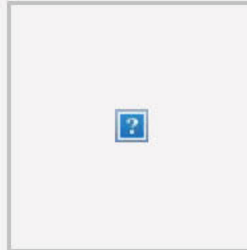


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

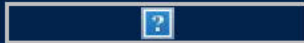
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

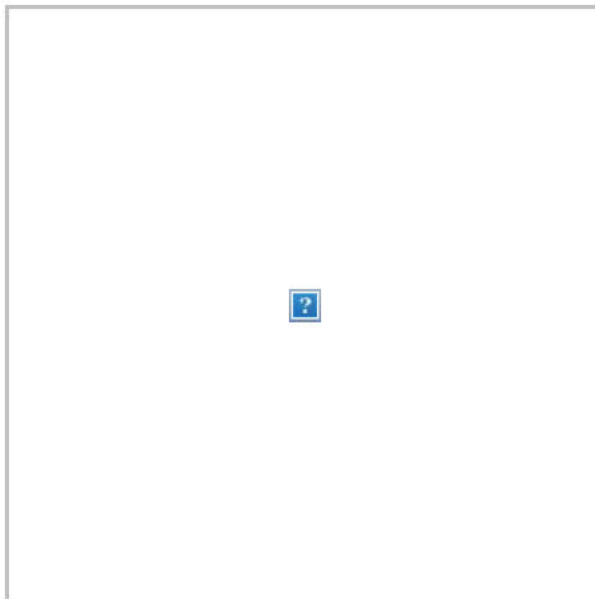
**From:** [PoliceOne Roll Call](#)  
**To:** [tfoley@ci.sunnyvale.ca.us](mailto:tfoley@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:26:39 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

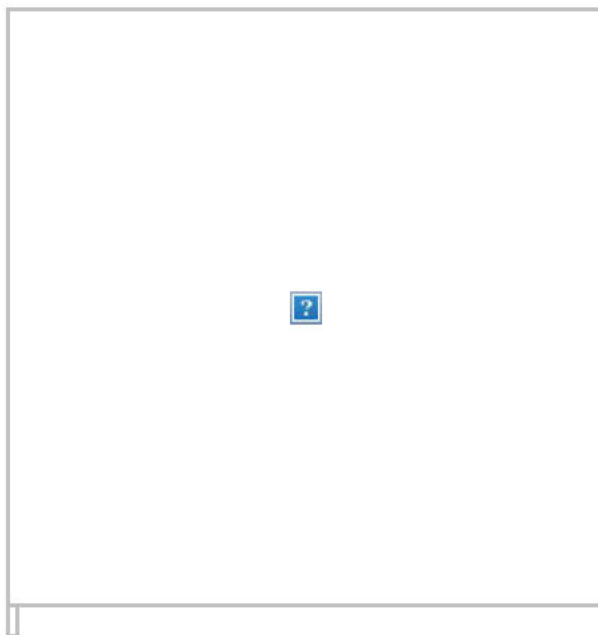
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

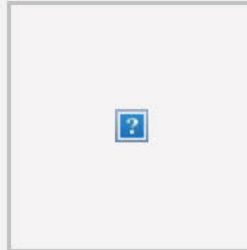


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

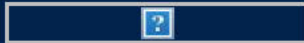
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

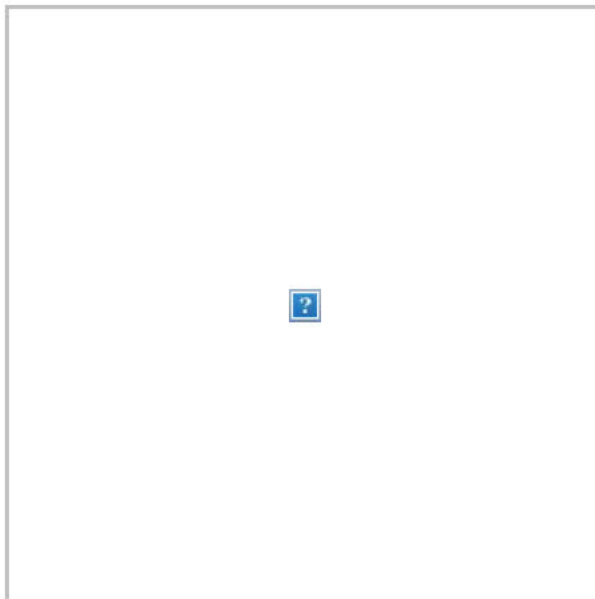
**From:** [PoliceOne Roll Call](#)  
**To:** [tgibo@sunnyvale.ca.gov](mailto:tgibo@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:26:32 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

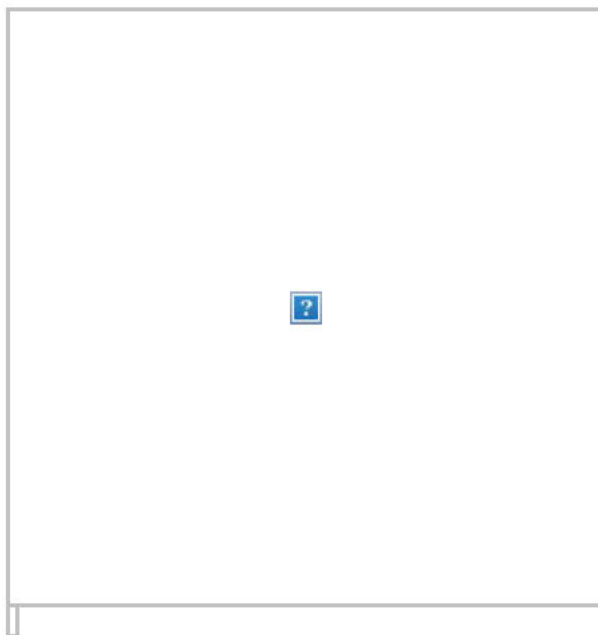
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

By Mike Callahan

The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan  
Marcou

We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

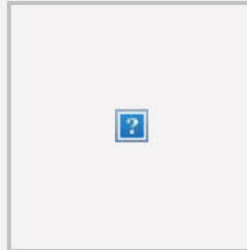


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

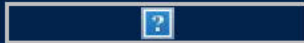
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

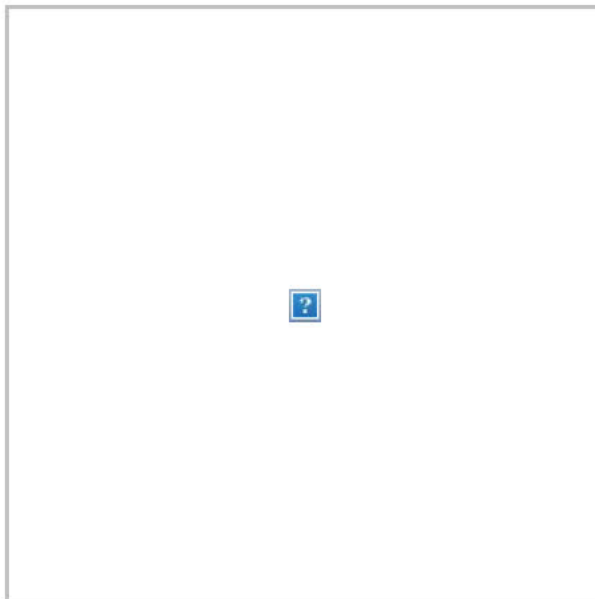
**From:** [PoliceOne Roll Call](#)  
**To:** [bwilkes@ci.sunnyvale.ca.us](mailto:bwilkes@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:26:32 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

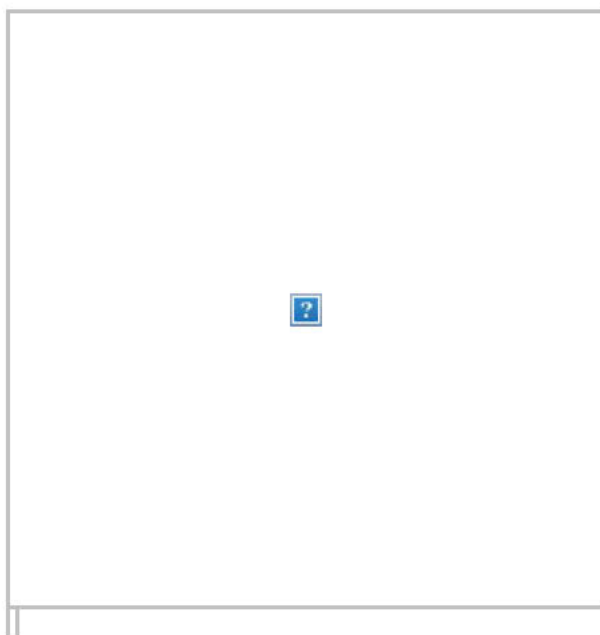
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

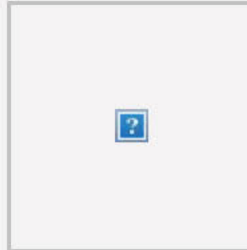


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

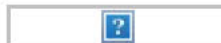
☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

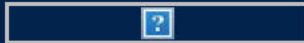
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

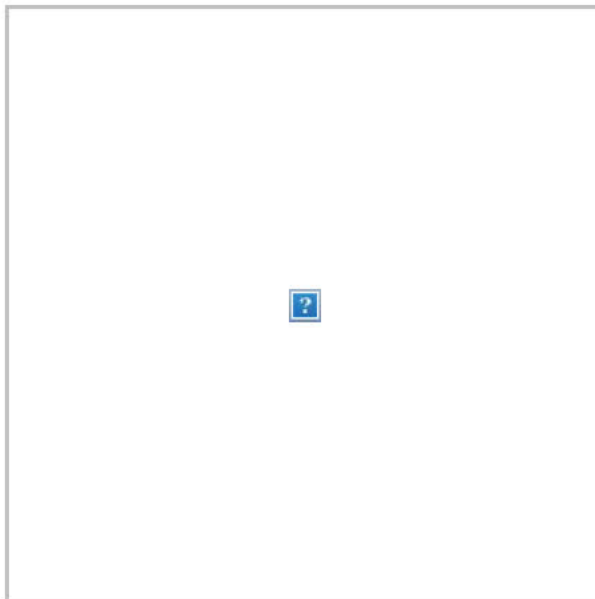
**From:** [PoliceOne Roll Call](#)  
**To:** [sgorshe@sunnyvale.ca.gov](mailto:sgorshe@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:26:19 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

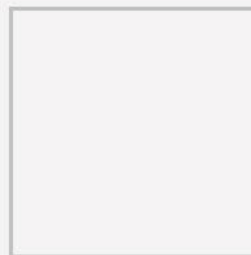
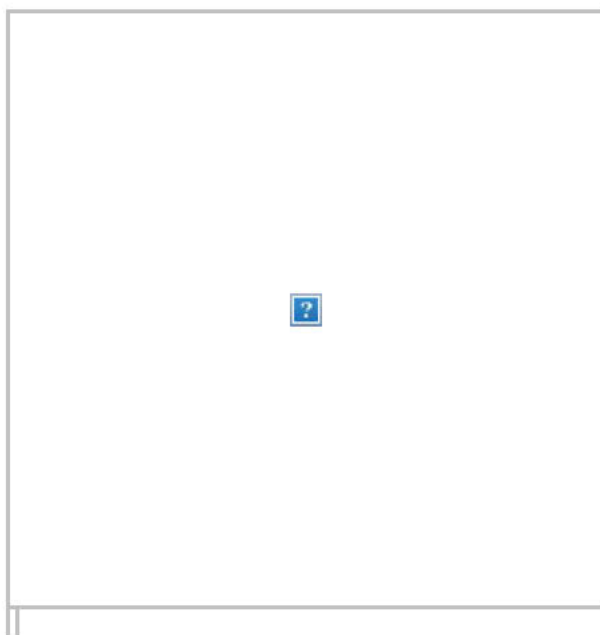
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

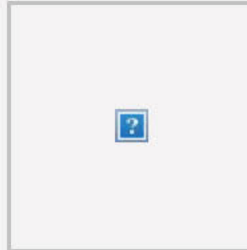


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



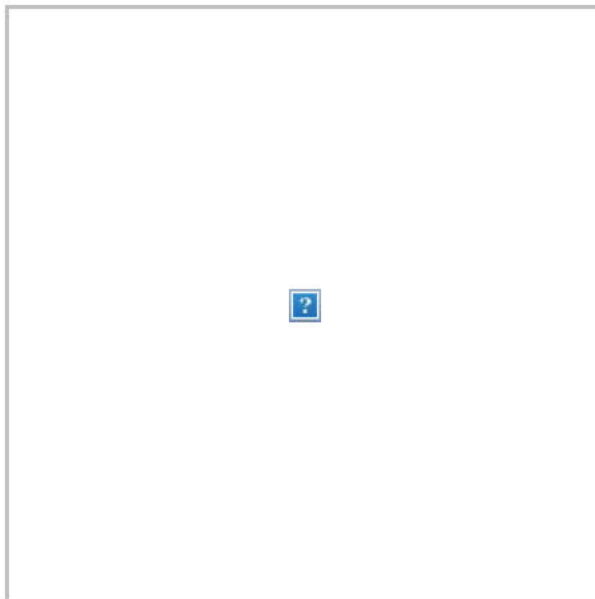
**From:** [PoliceOne Roll Call](#)  
**To:** [aserrano@sunnyvale.ca.gov](mailto:aserrano@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:26:01 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

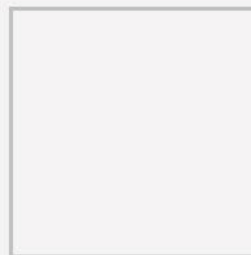
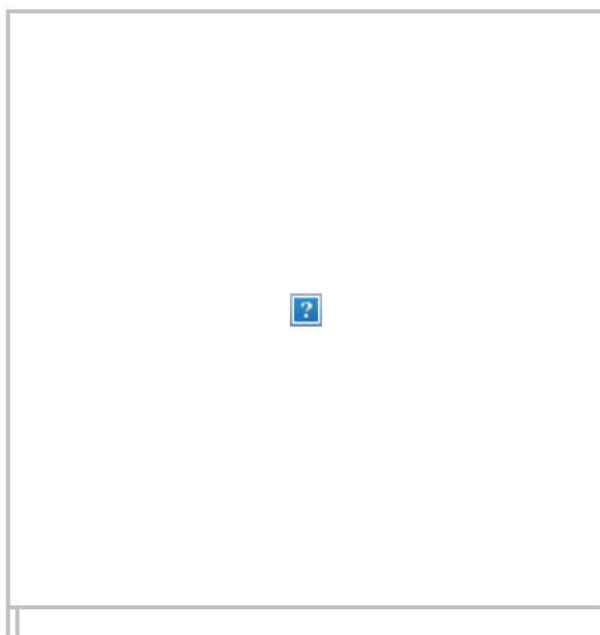
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

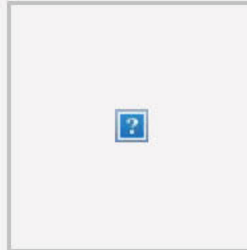


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

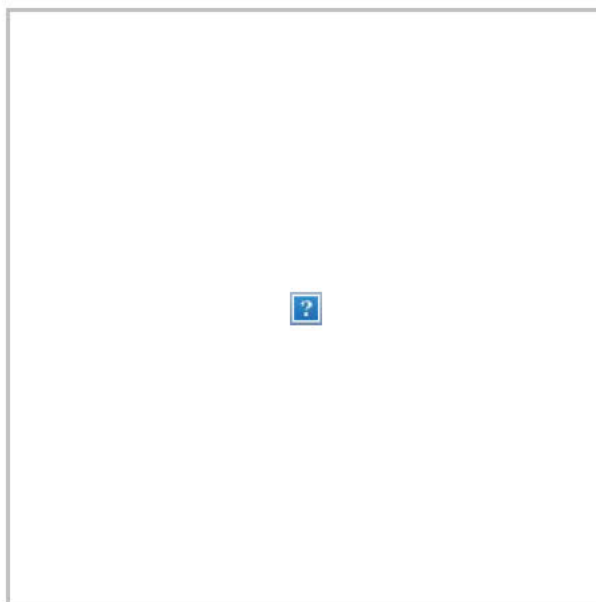
**From:** [PoliceOne Roll Call](#)  
**To:** [skotani@sunnyvale.ca.gov](mailto:skotani@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:55 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

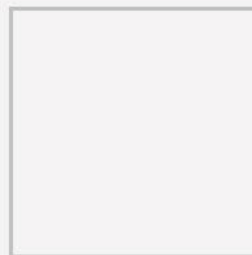
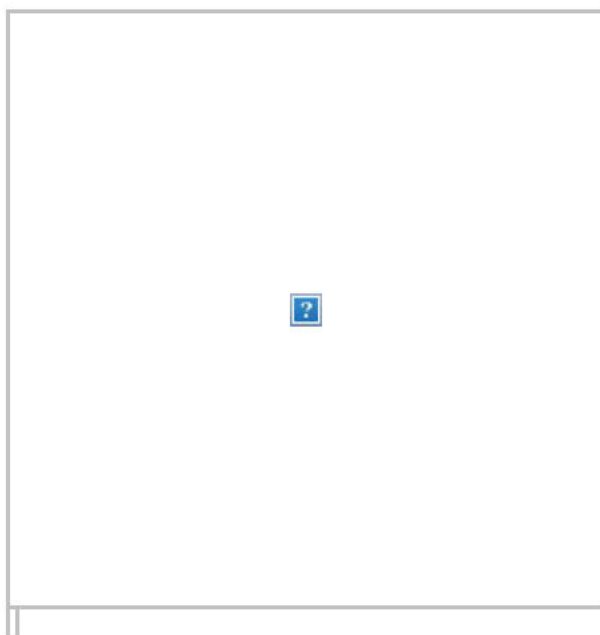
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

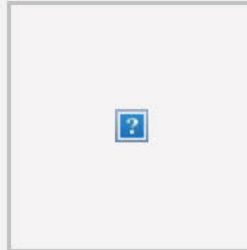


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

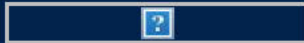
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

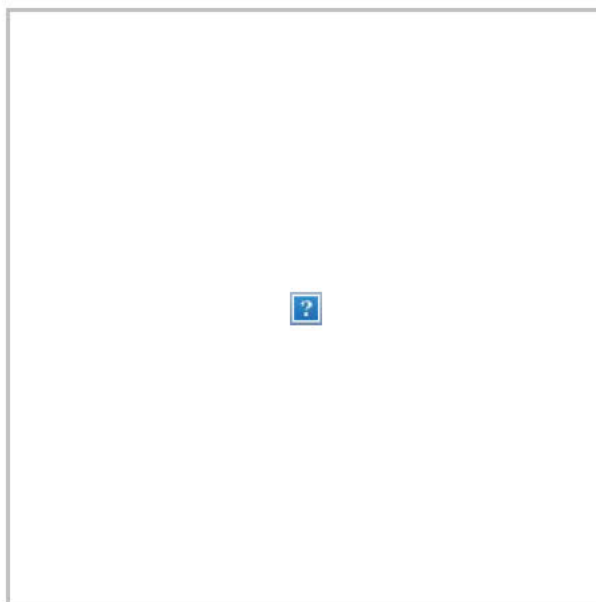
**From:** [PoliceOne Roll Call](#)  
**To:** [Jasselin@sunnyvale.ca.gov](mailto:Jasselin@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:52 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

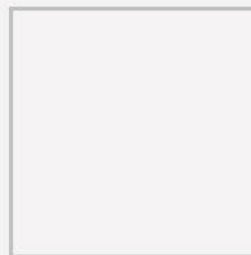
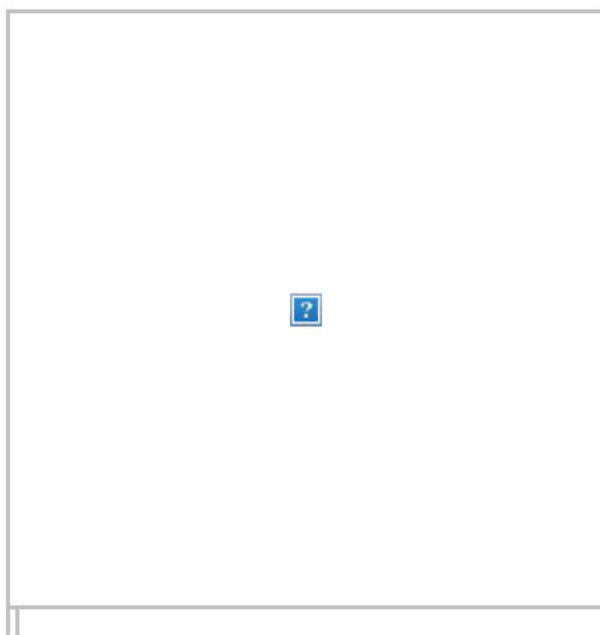
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

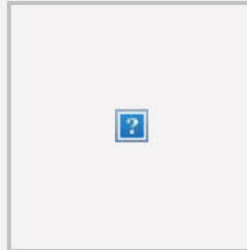


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

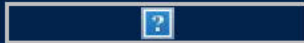
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

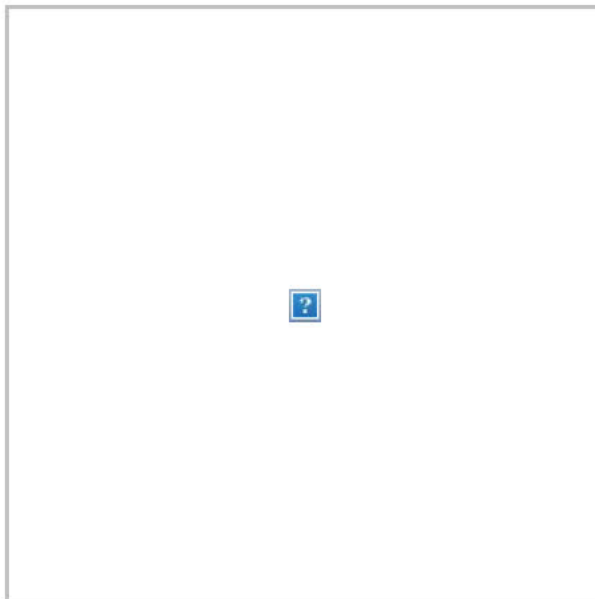
**From:** [PoliceOne Roll Call](#)  
**To:** [jkirk@ci.sunnyvale.ca.us](mailto:jkirk@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:42 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

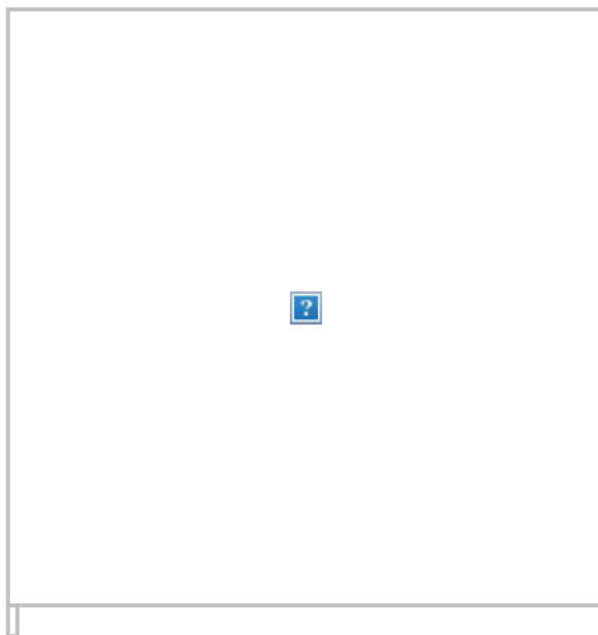
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

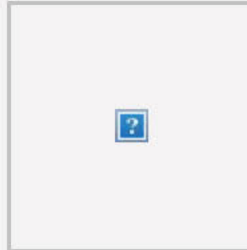


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

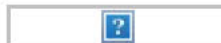
☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

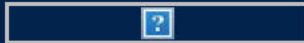
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

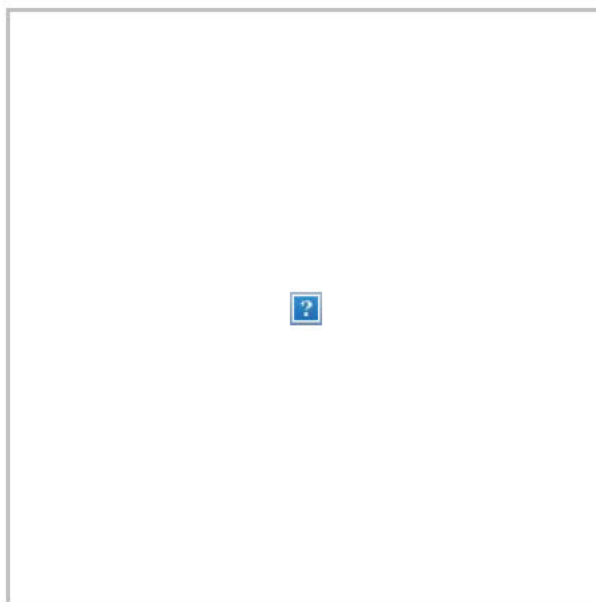
**From:** [PoliceOne Roll Call](#)  
**To:** [atani@ci.sunnyvale.ca.us](mailto:atani@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:39 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

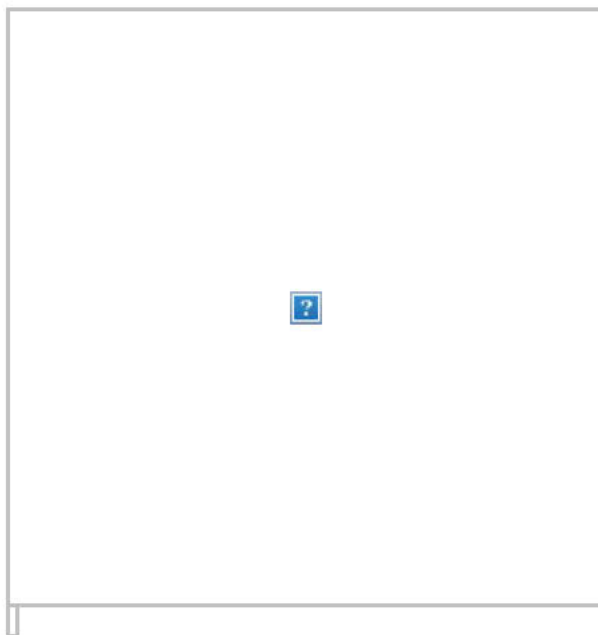
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

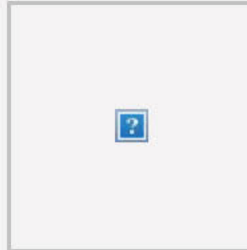


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

- ☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



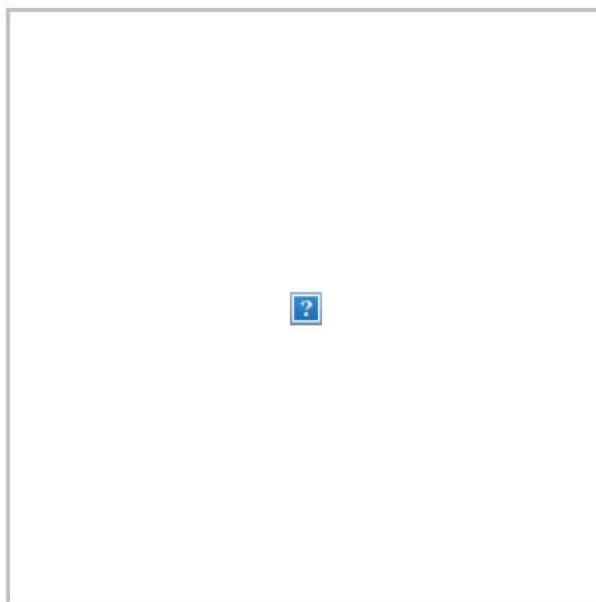
**From:** [PoliceOne Roll Call](#)  
**To:** [janton@ci.sunnyvale.ca.us](mailto:janton@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:36 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

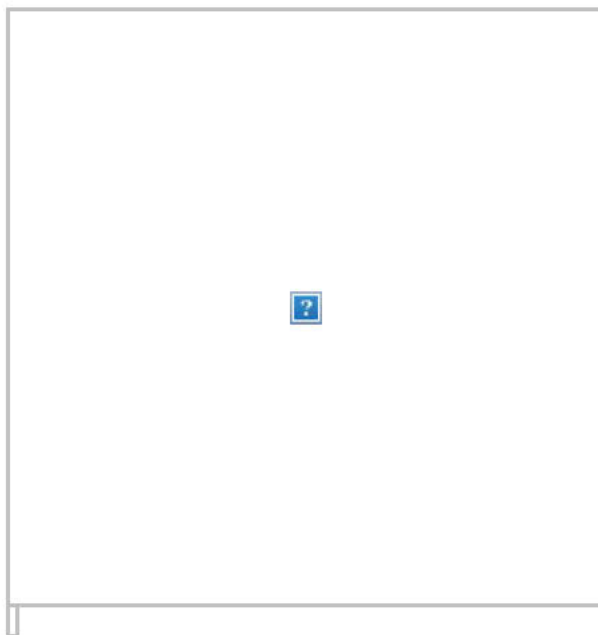
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

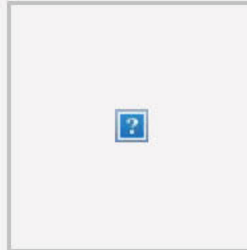


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

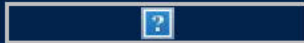
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

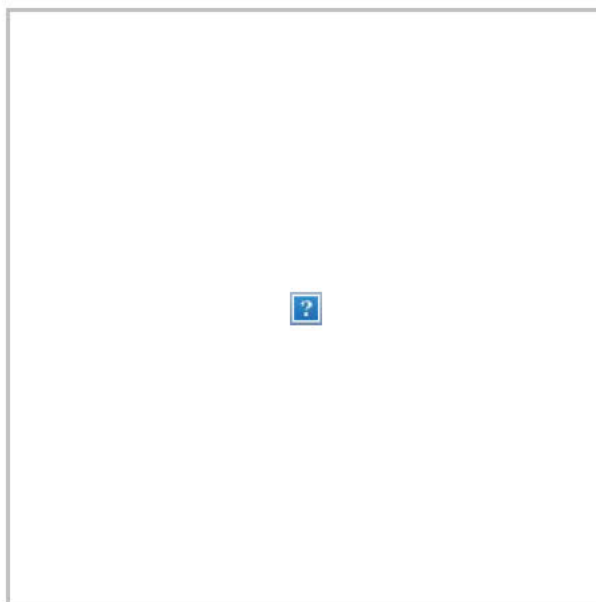
**From:** [PoliceOne Roll Call](#)  
**To:** [dodischer@ci.sunnyvale.ca.us](mailto:dodischer@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:30 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

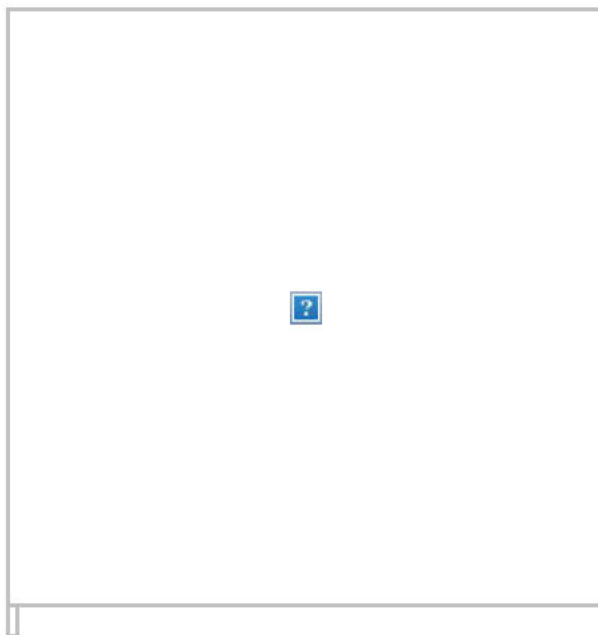
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

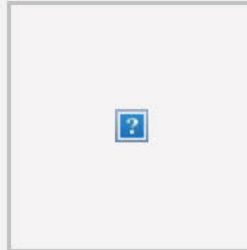


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

- ☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

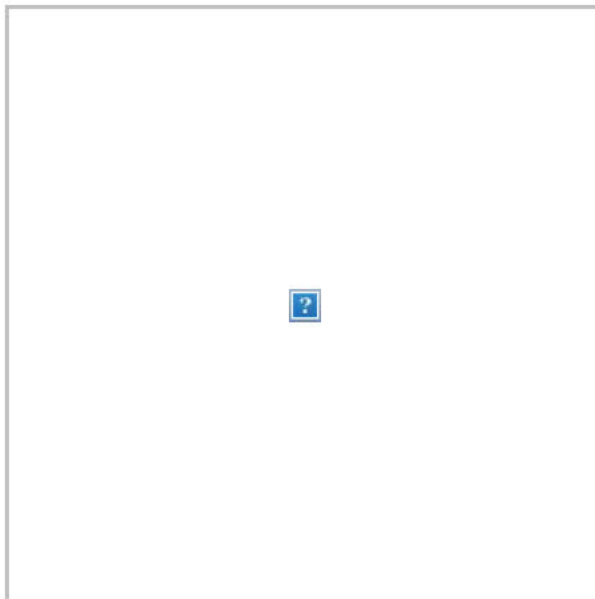
**From:** [PoliceOne Roll Call](#)  
**To:** [ramirez@ci.sunnyvale.ca.us](mailto:ramirez@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:30 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

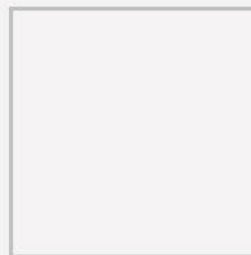
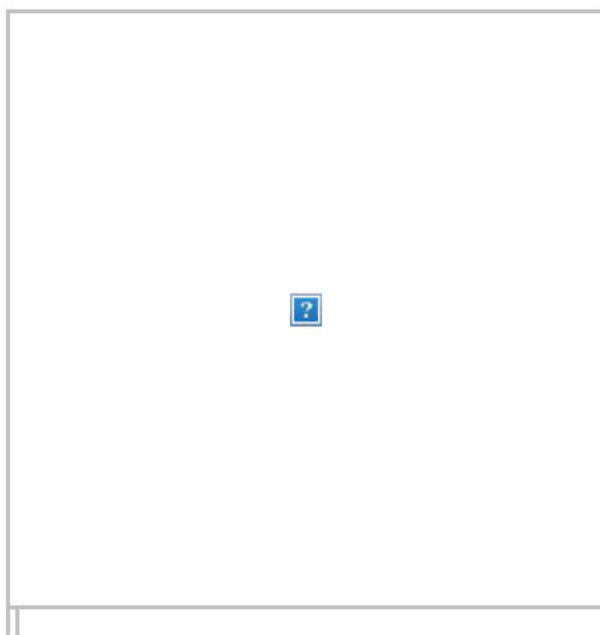
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

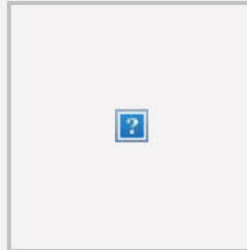


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

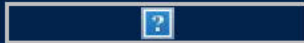
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

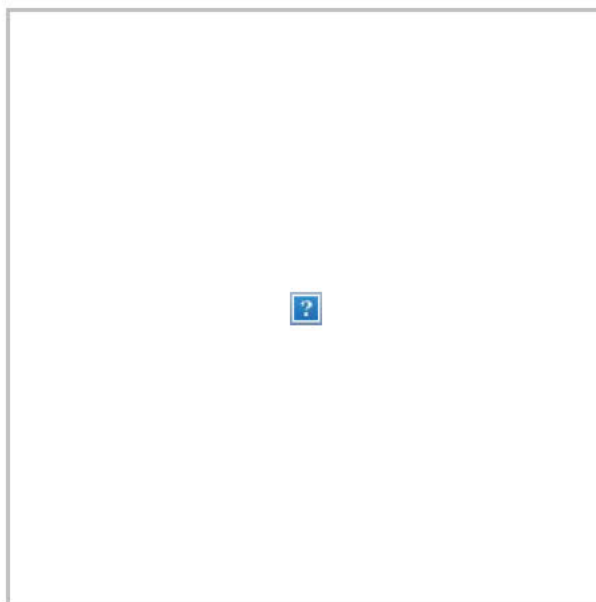
**From:** [PoliceOne Roll Call](#)  
**To:** [mplonka@ci.sunnyvale.ca.us](mailto:mplonka@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:24 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

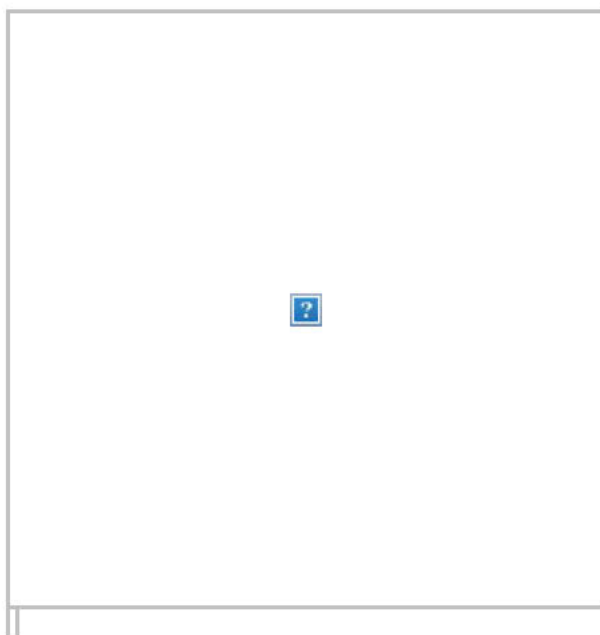
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

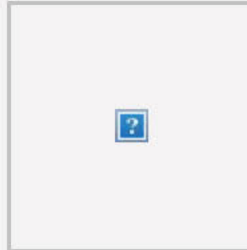


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

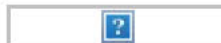
- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

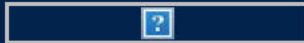
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

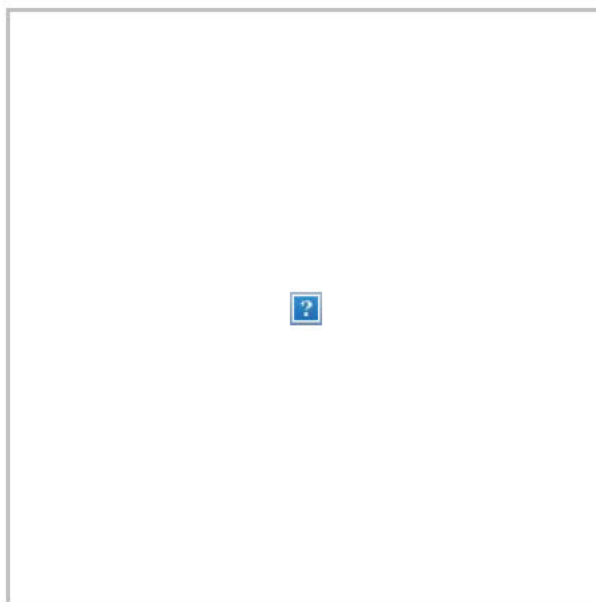
**From:** [PoliceOne Roll Call](#)  
**To:** [kjenks@ci.sunnyvale.ca.us](mailto:kjenks@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:19 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

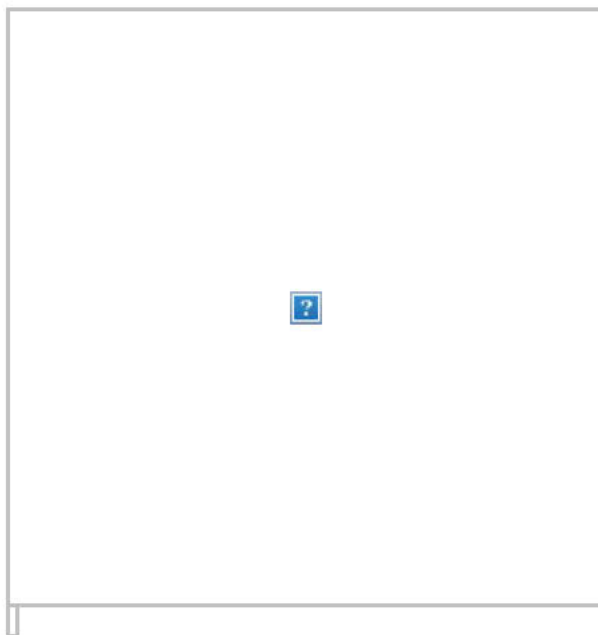
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

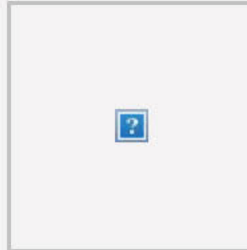


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

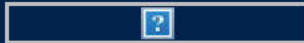
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



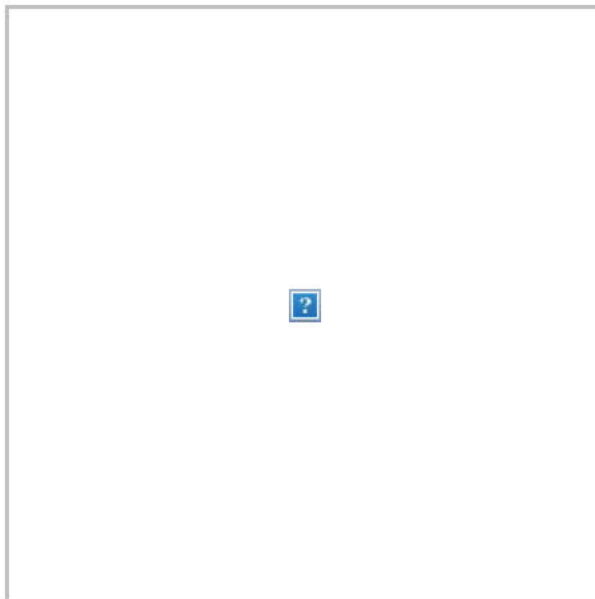
**From:** [PoliceOne Roll Call](#)  
**To:** [tsprayberry@sunnyvale.ca.gov](mailto:tsprayberry@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:18 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

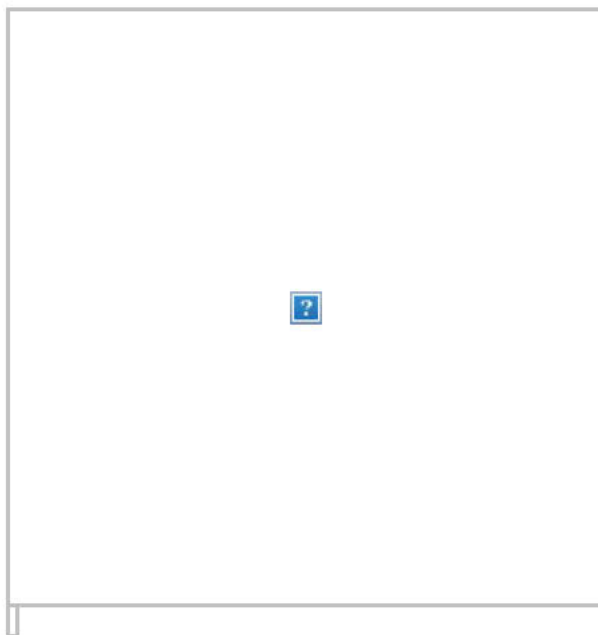
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

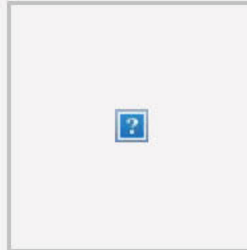


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

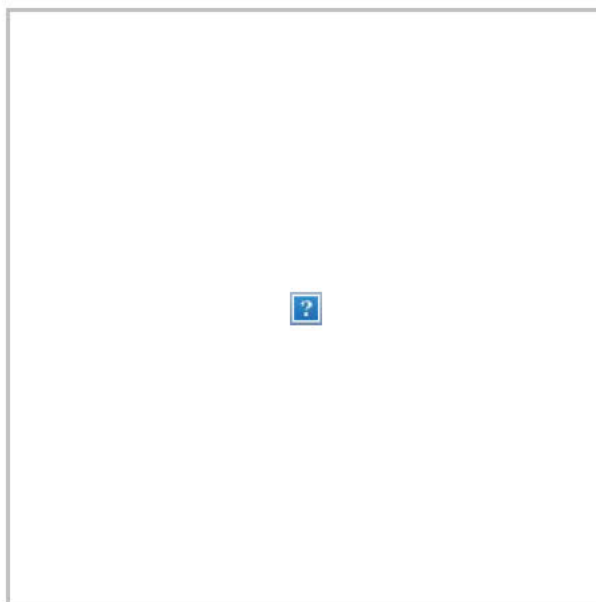
**From:** [PoliceOne Roll Call](#)  
**To:** [joramirez@ci.sunnyvale.ca.us](mailto:joramirez@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:16 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

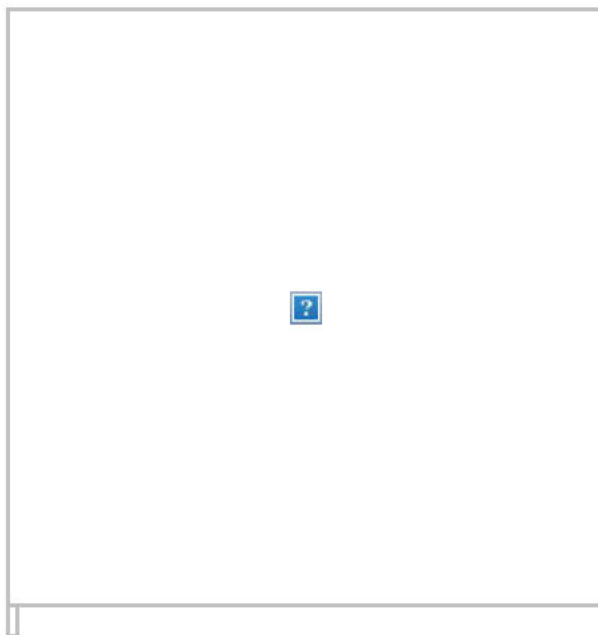
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

By Mike Callahan

The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan  
Marcou

We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

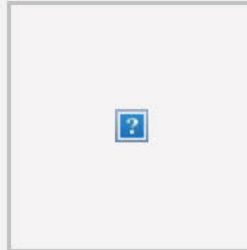


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

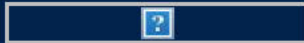
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

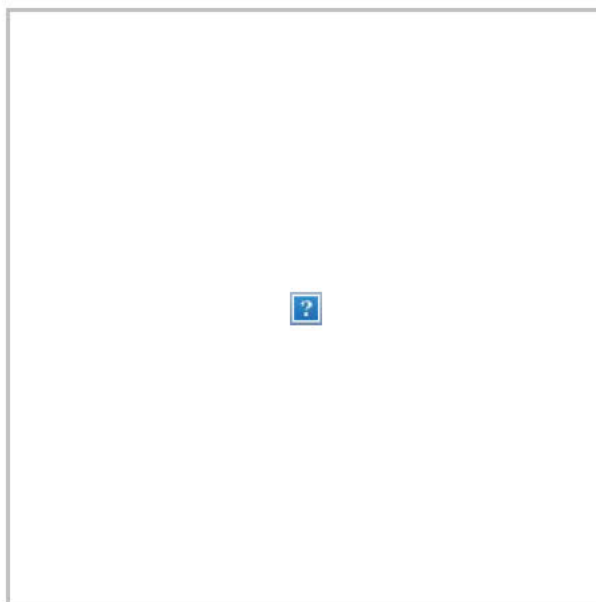
**From:** [PoliceOne Roll Call](#)  
**To:** [Kdedely@sunnyvale.ca.gov](mailto:Kdedely@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:16 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

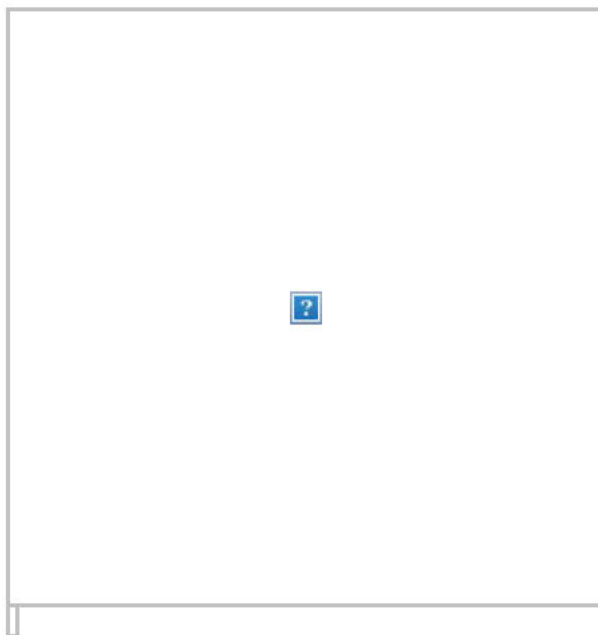
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

By Mike Callahan

The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan  
Marcou

We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins



Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

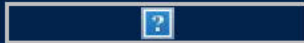
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

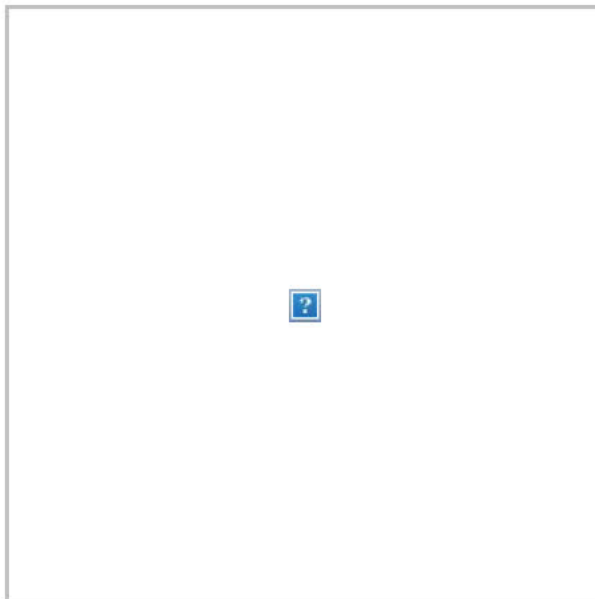
**From:** [PoliceOne Roll Call](#)  
**To:** [bmilitano@ci.sunnyvale.ca.us](mailto:bmilitano@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:14 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

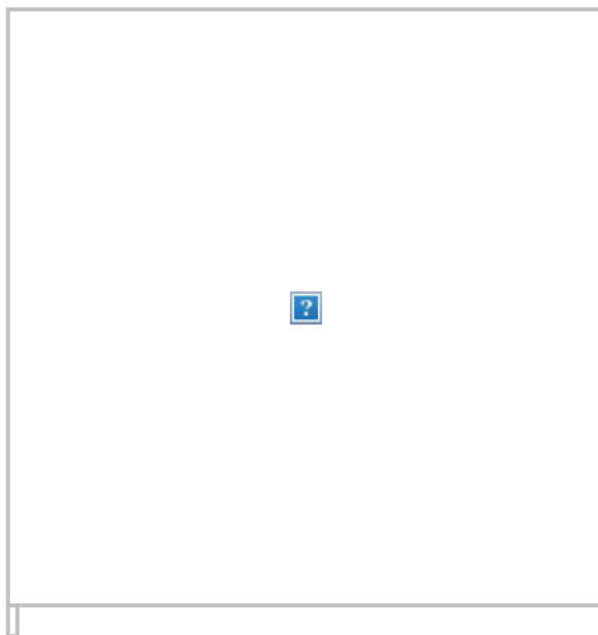
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

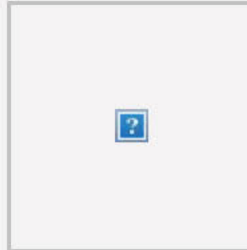


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

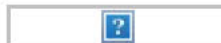
- ☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

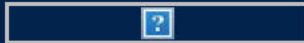
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

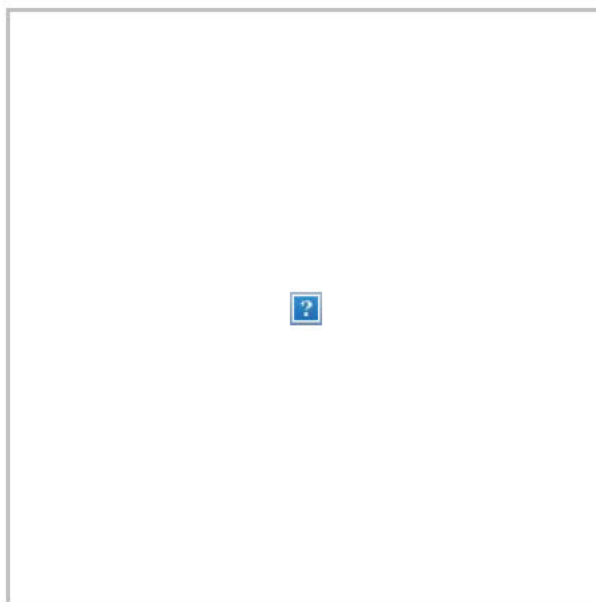
**From:** [PoliceOne Roll Call](#)  
**To:** [them@ci.sunnyvale.ca.us](mailto:them@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:10 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

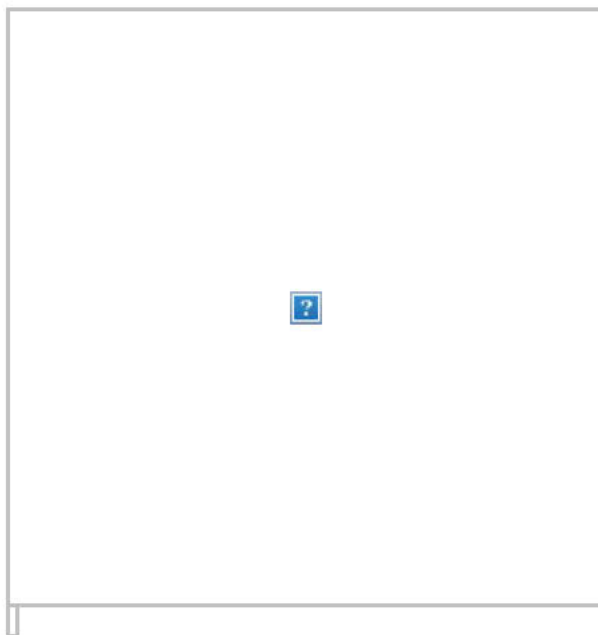
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

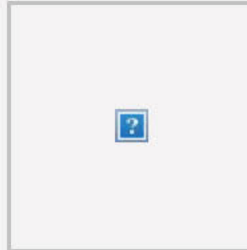


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



## Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



## Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



## Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

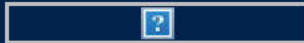
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



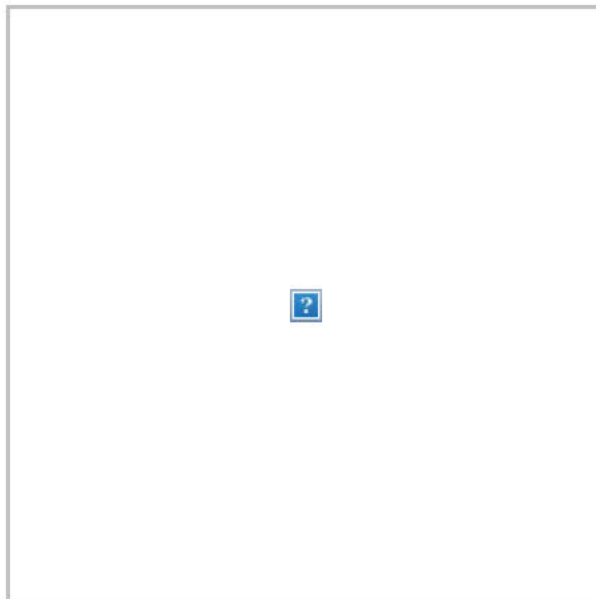
**From:** [PoliceOne Roll Call](#)  
**To:** [schen@ci.sunnyvale.ca.us](mailto:schen@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:09 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

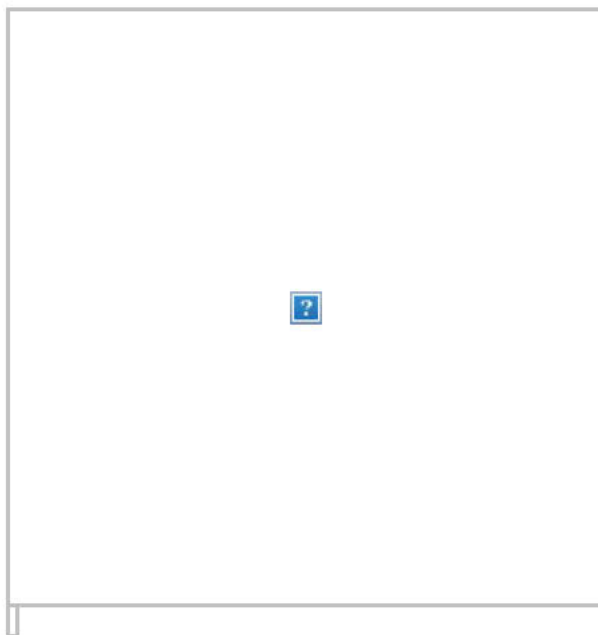
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

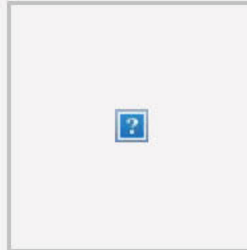


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

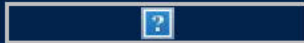
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

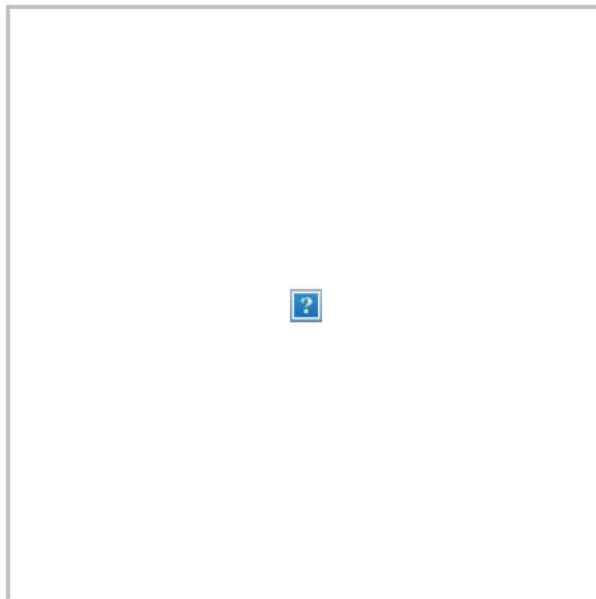
**From:** [PoliceOne Roll Call](#)  
**To:** [fmonge@ci.sunnyvale.ca.us](mailto:fmonge@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:09 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

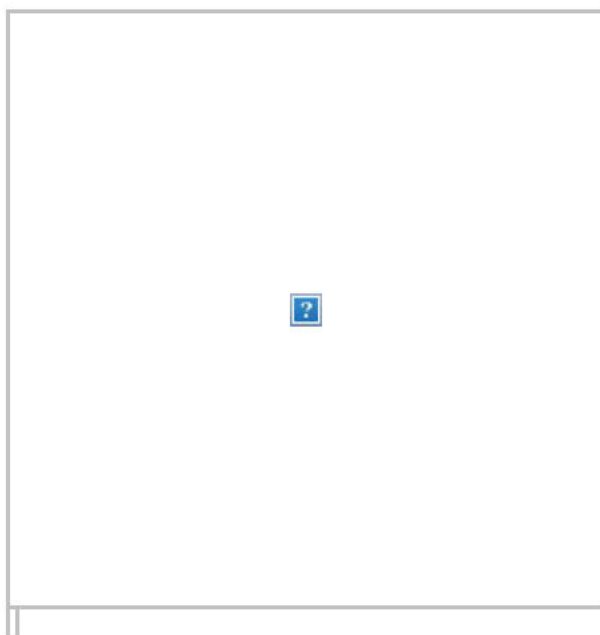
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins



Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

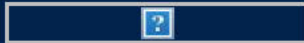
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

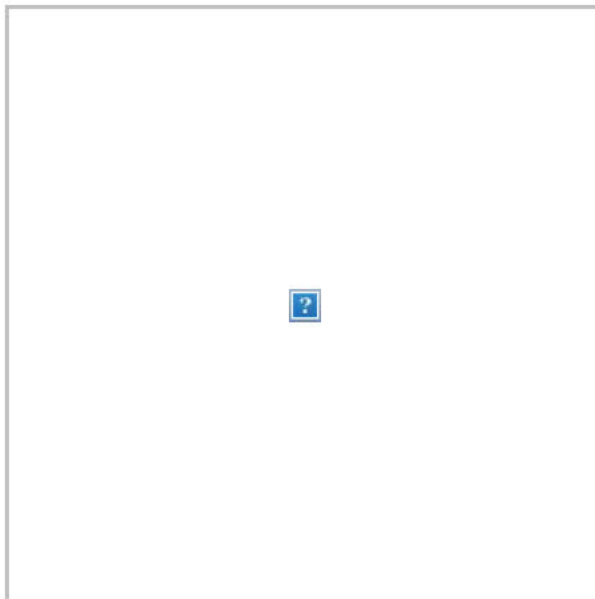
**From:** [PoliceOne Roll Call](#)  
**To:** [jboone@ci.sunnyvale.ca.us](mailto:jboone@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:06 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

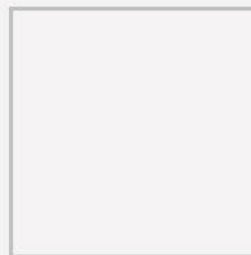
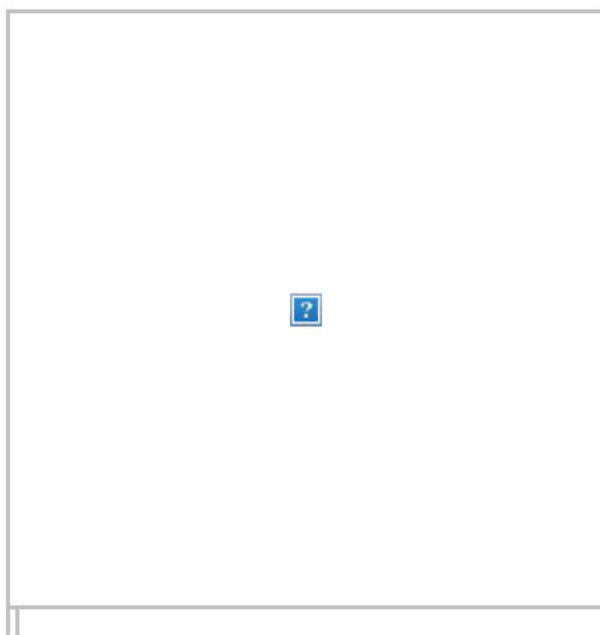
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

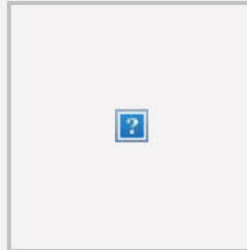


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

- ☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

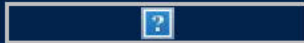
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

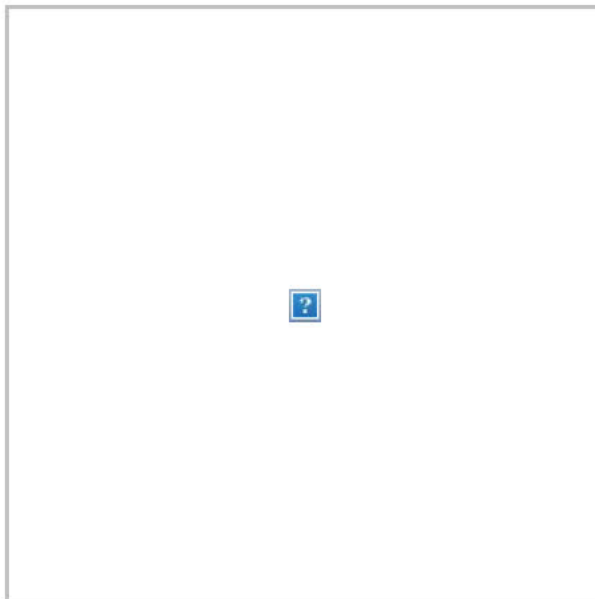
**From:** [PoliceOne Roll Call](#)  
**To:** [elarkin@sunnyvale.ca.gov](mailto:elarkin@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:25:05 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

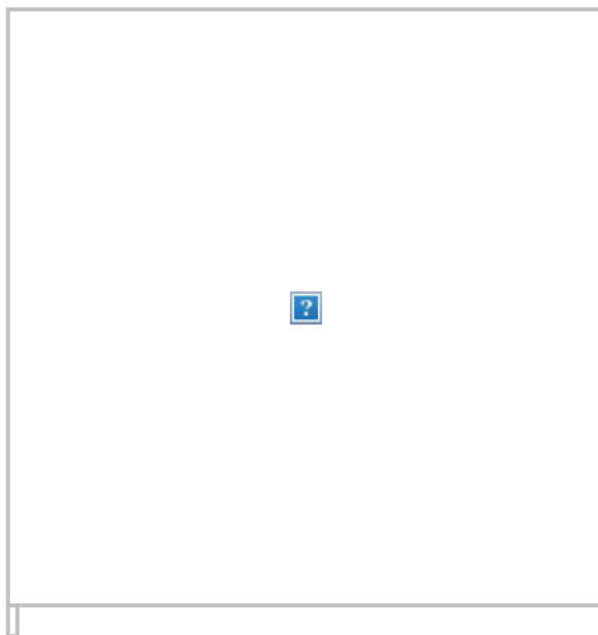
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

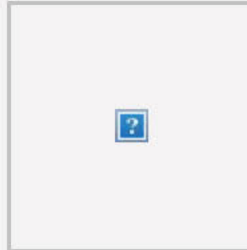


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

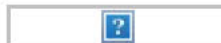
- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

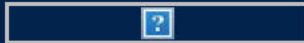
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

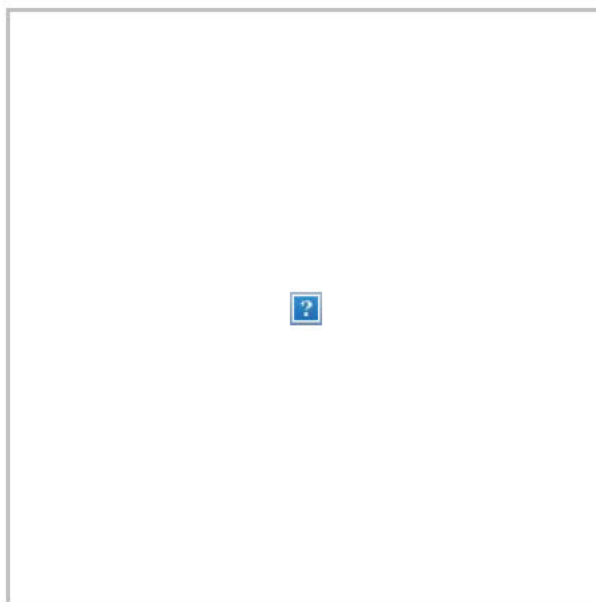
**From:** [PoliceOne Roll Call](#)  
**To:** [dapang@sunnyvale.ca.gov](mailto:dapang@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:59 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

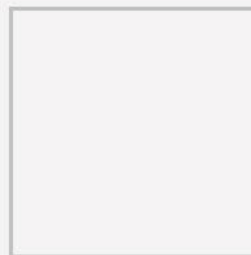
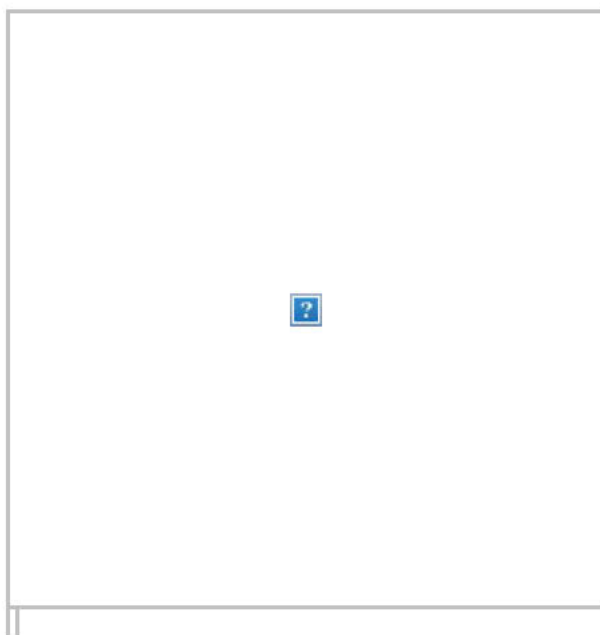
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

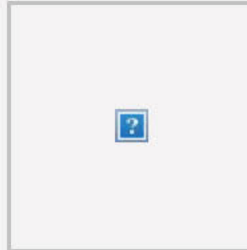


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



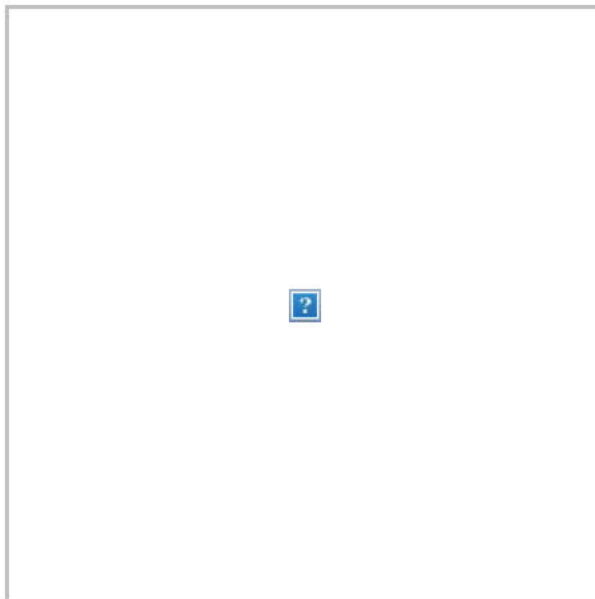
**From:** [PoliceOne Roll Call](#)  
**To:** [dsakurai@ci.sunnyvale.ca.us](mailto:dsakurai@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:52 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

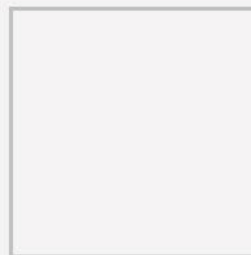
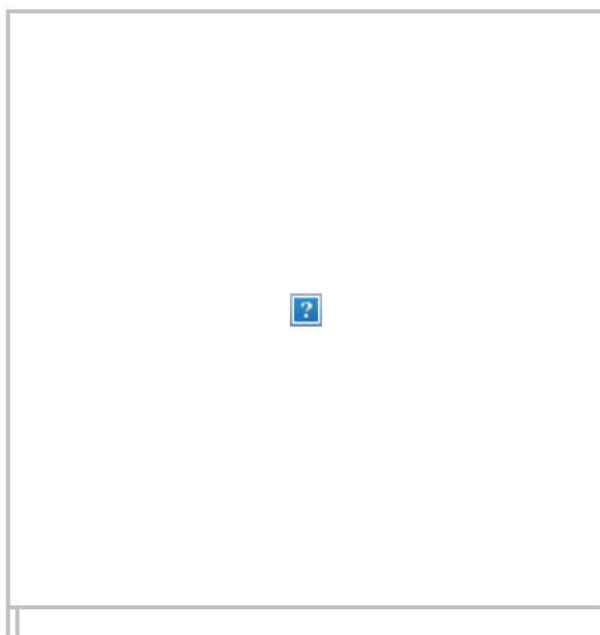
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

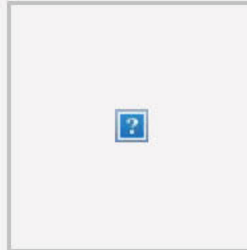


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

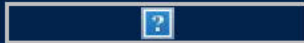
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

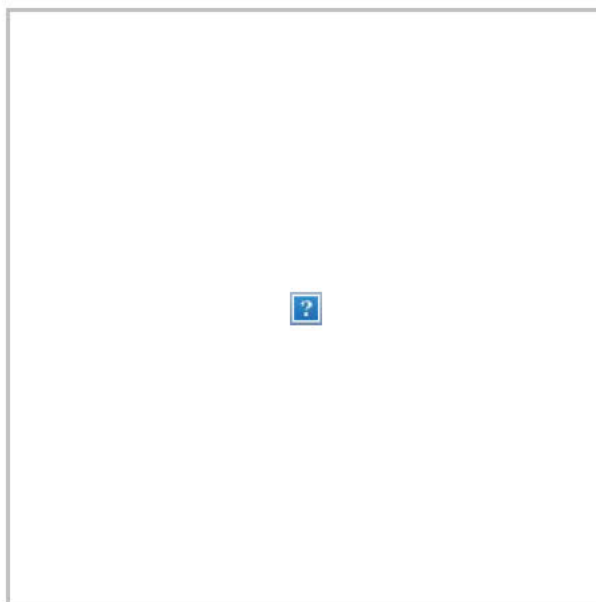
**From:** [PoliceOne Roll Call](#)  
**To:** [sstewart@sunnyvale.ca.gov](mailto:sstewart@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:49 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

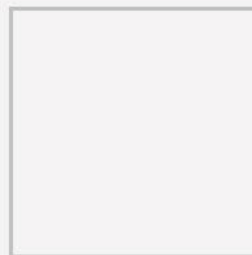
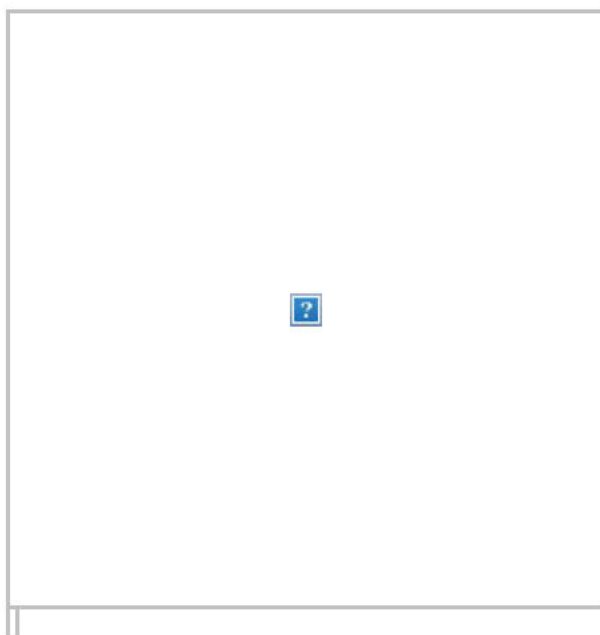
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

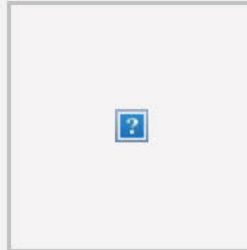


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

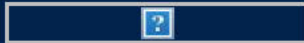
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

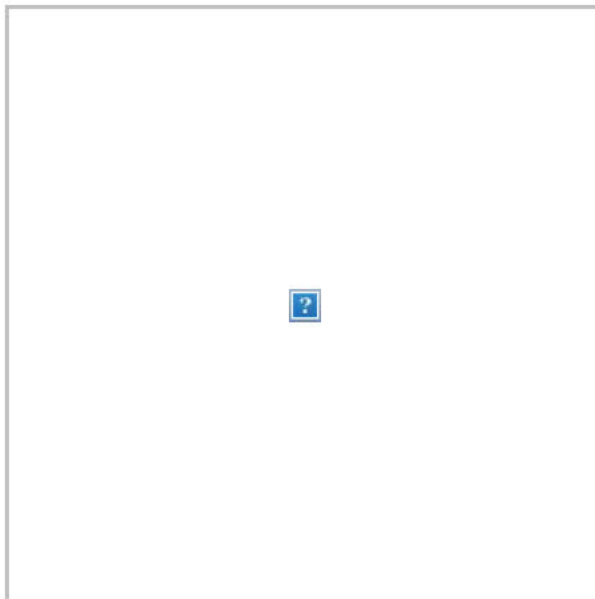
**From:** [PoliceOne Roll Call](#)  
**To:** [aherbert@sunnyvale.ca.gov](mailto:aherbert@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:40 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

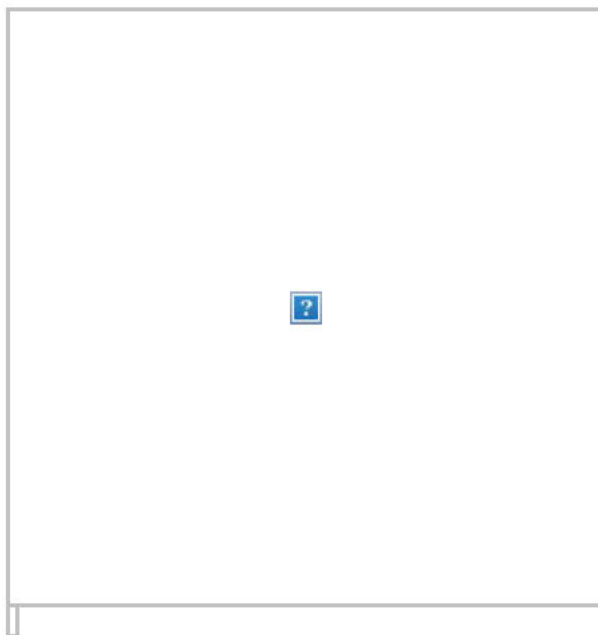
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

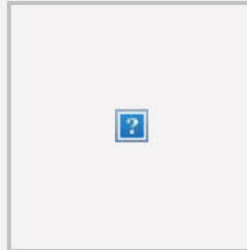


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

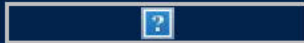
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

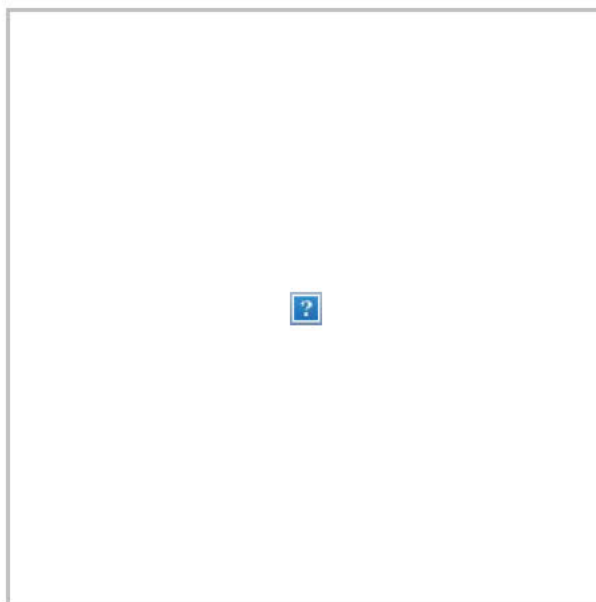
**From:** [PoliceOne Roll Call](#)  
**To:** [Jlockwood@sunnyvale.ca.gov](mailto:Jlockwood@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:38 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

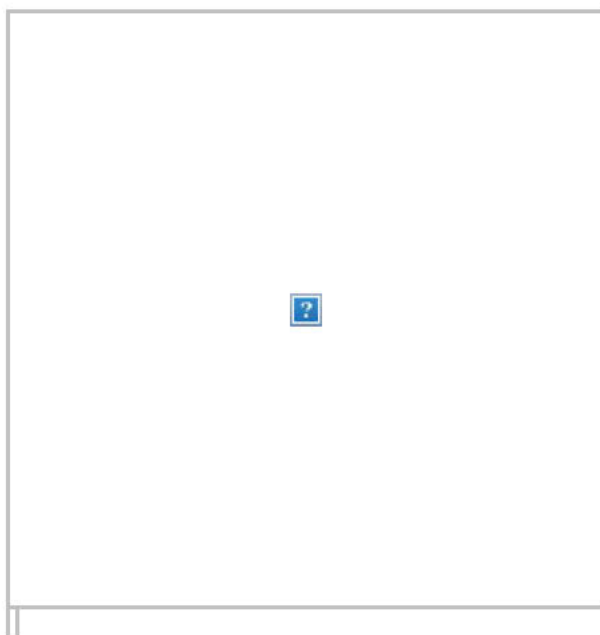
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

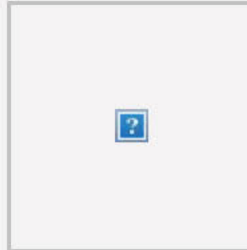


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

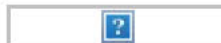
☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

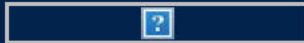
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

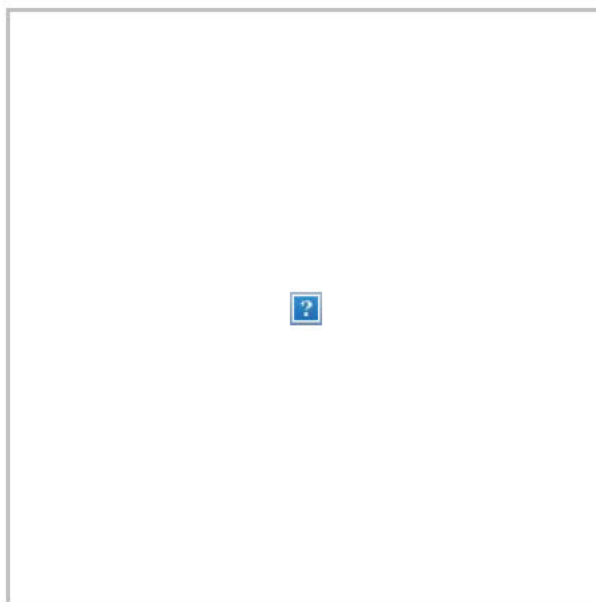
**From:** [PoliceOne Roll Call](#)  
**To:** [cketchum@sunnyvale.ca.gov](mailto:cketchum@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:38 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

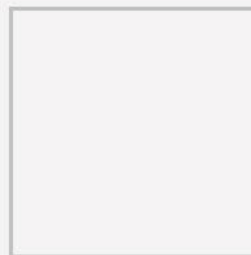
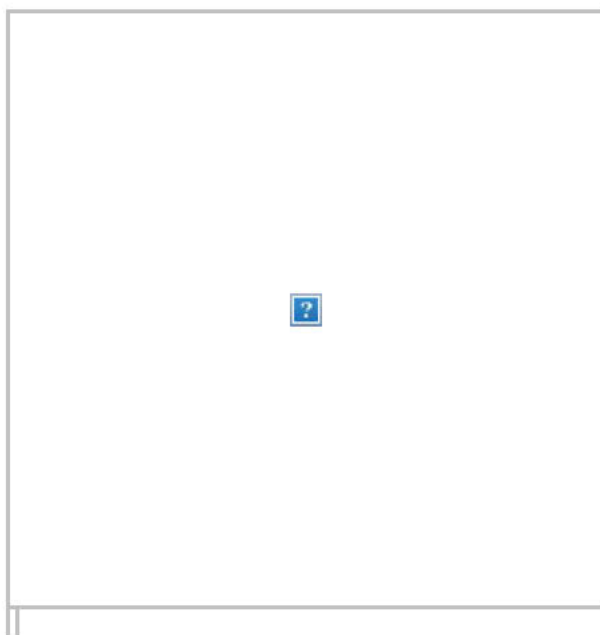
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

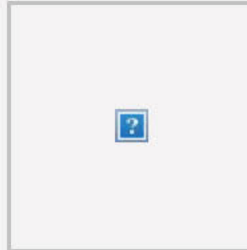


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

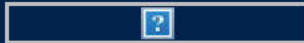
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



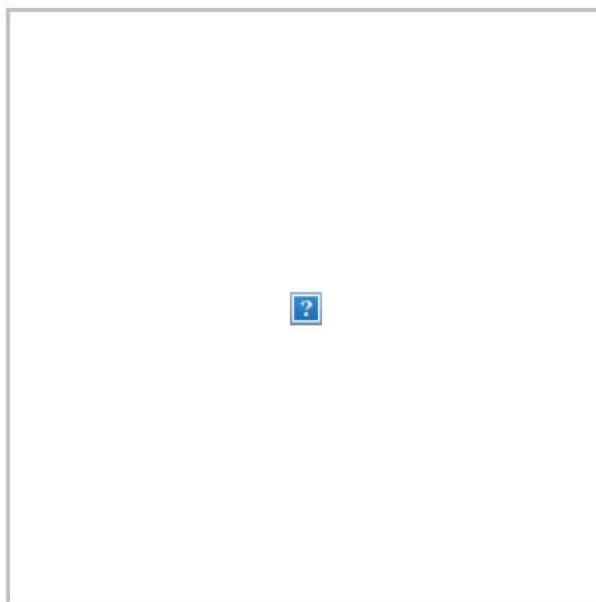
**From:** [PoliceOne Roll Call](#)  
**To:** [mpeel@sunnyvale.ca.gov](mailto:mpeel@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:28 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

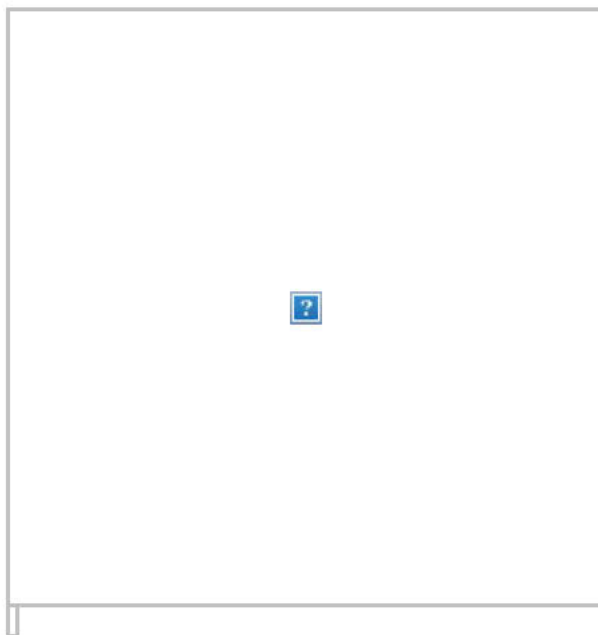
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

By Mike Callahan

The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

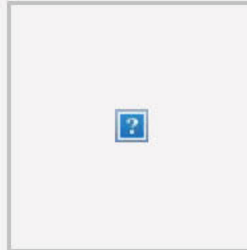


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

- ☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

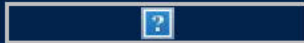
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

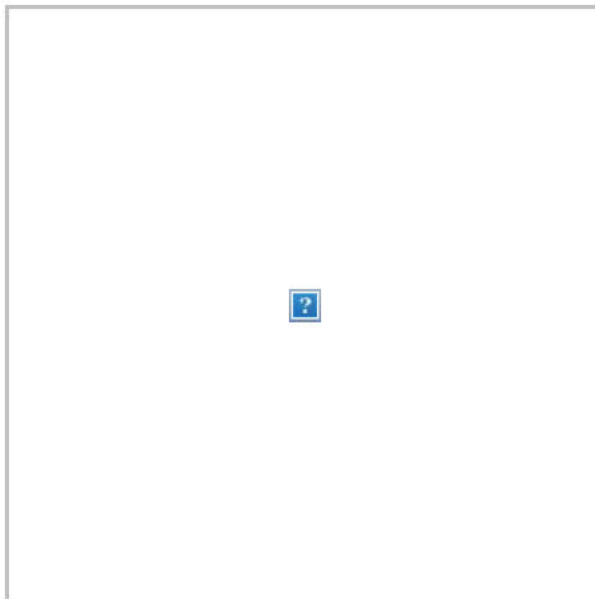
**From:** [PoliceOne Roll Call](#)  
**To:** [Skuhlmann@sunnyvale.ca.gov](mailto:Skuhlmann@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:22 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

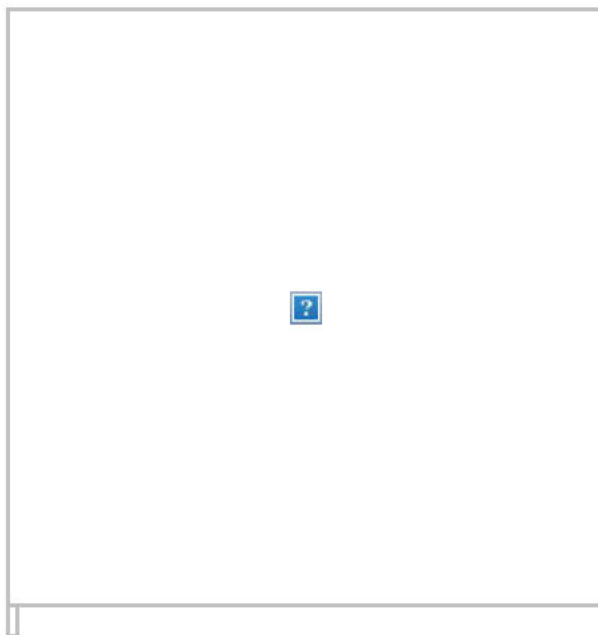
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

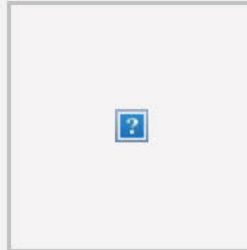


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

- ☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

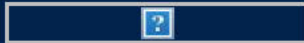
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

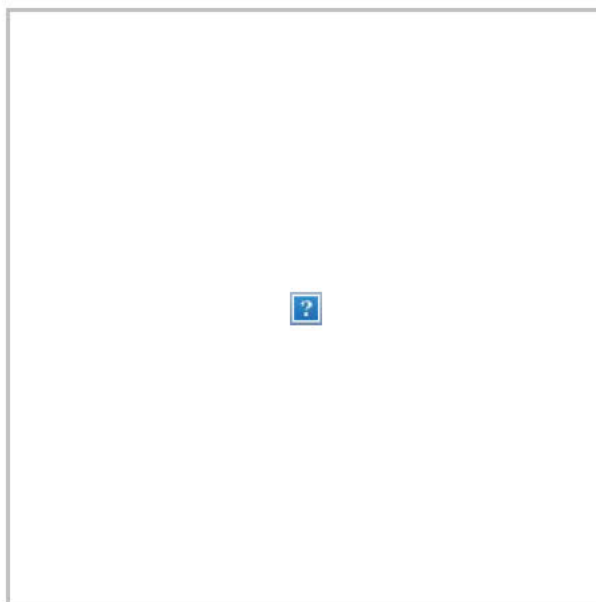
**From:** [PoliceOne Roll Call](#)  
**To:** [jgalazzo@sunnyvale.ca.gov](mailto:jgalazzo@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:22 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

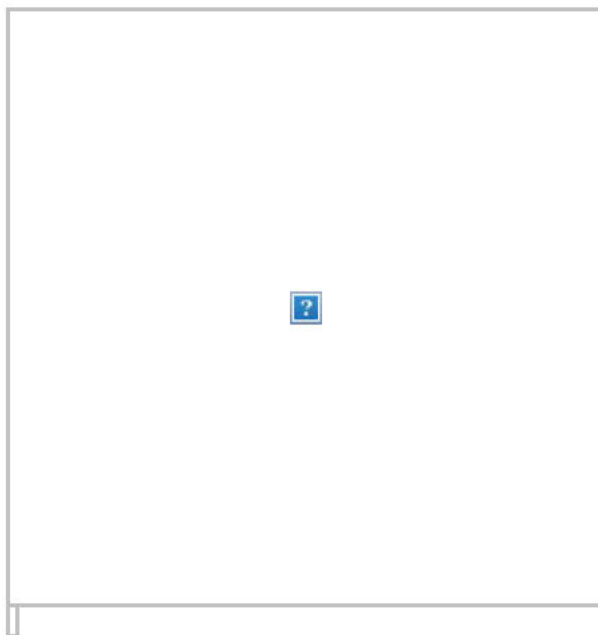
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

By Mike Callahan

The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan  
Marcou

We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins



Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

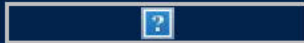
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

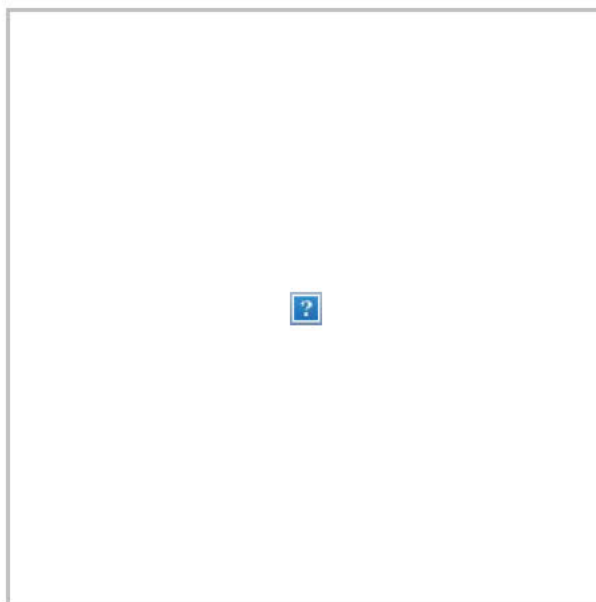
**From:** [PoliceOne Roll Call](#)  
**To:** [cabernathy@sunnyvale.ca.gov](mailto:cabernathy@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:16 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

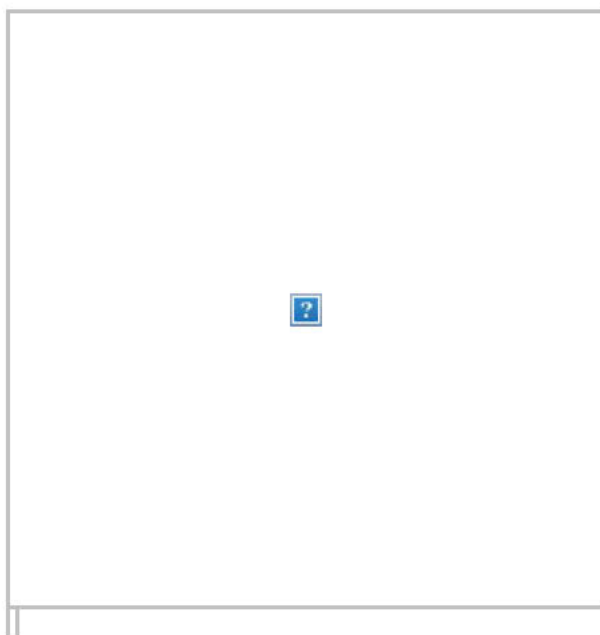
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

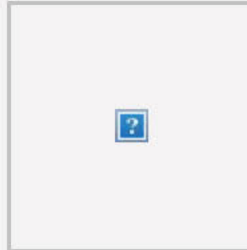


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

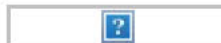
- ☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

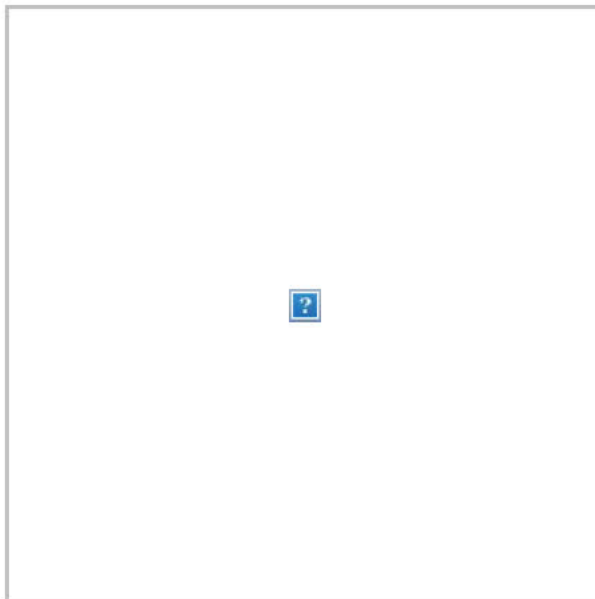
**From:** [PoliceOne Roll Call](#)  
**To:** [bgantt@sunnyvale.ca.gov](mailto:bgantt@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:11 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

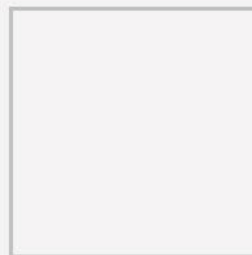
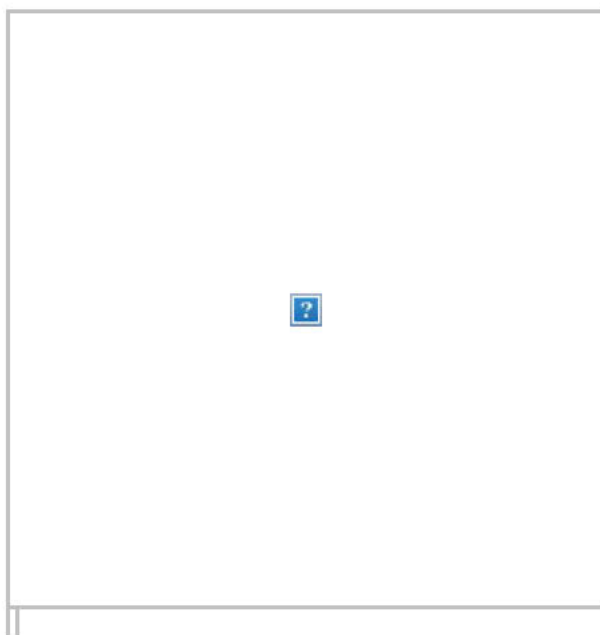
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

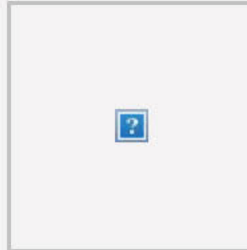


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

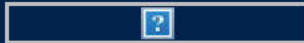
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



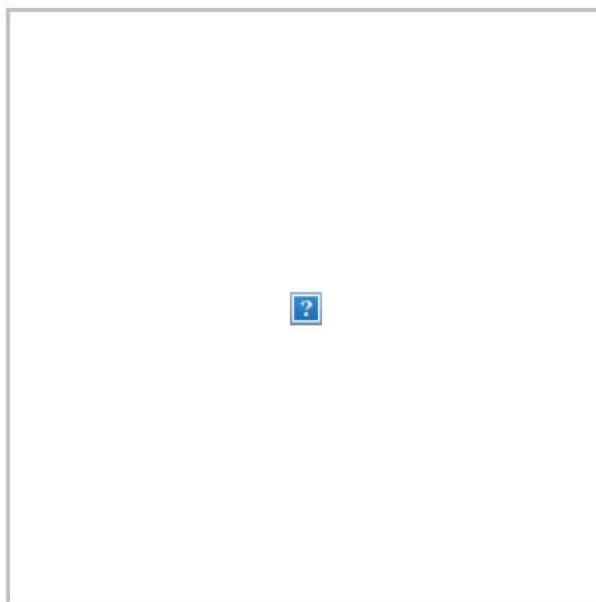
**From:** [PoliceOne Roll Call](#)  
**To:** [rhuihui@ci.sunnyvale.ca.us](mailto:rhuihui@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:24:00 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

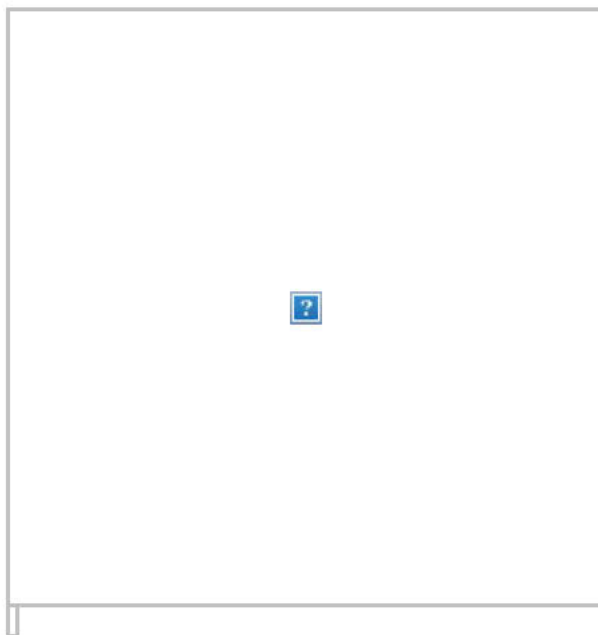
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

By Mike Callahan

The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan  
Marcou

We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

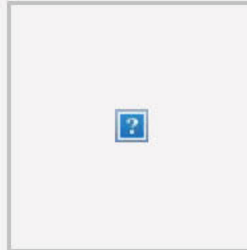


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

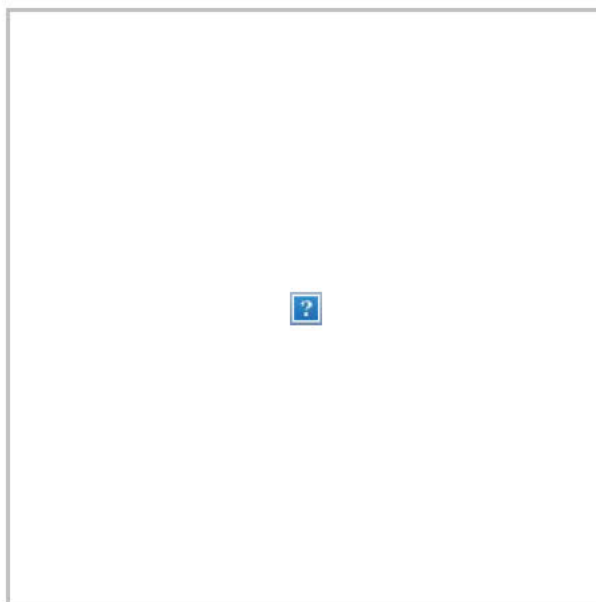
**From:** [PoliceOne Roll Call](#)  
**To:** [maguirre@ci.sunnyvale.ca.us](mailto:maguirre@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:23:59 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

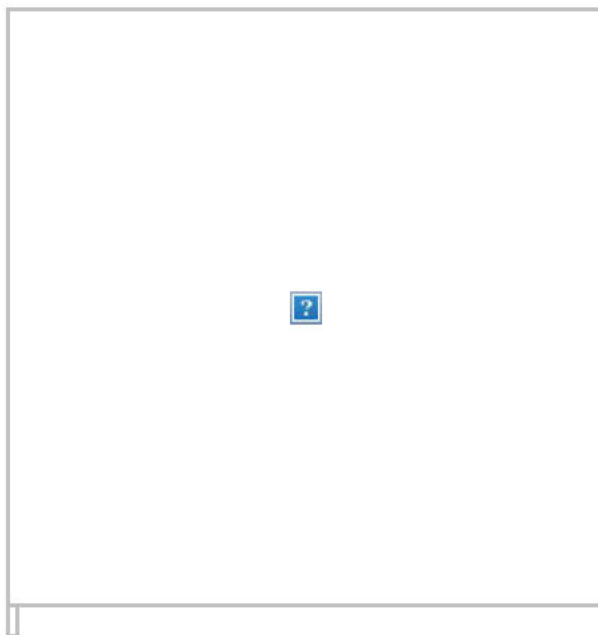
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

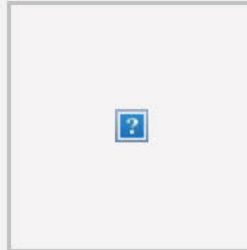


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

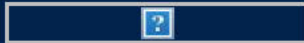
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

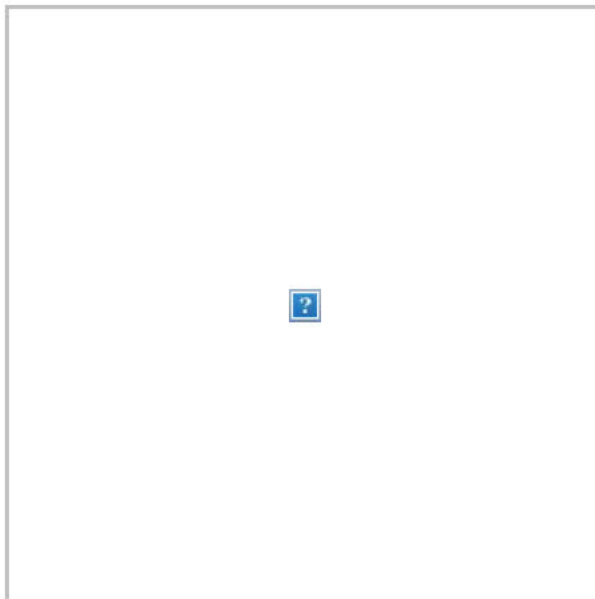
**From:** [PoliceOne Roll Call](#)  
**To:** [mirose@sunnyvale.ca.gov](mailto:mirose@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:23:56 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

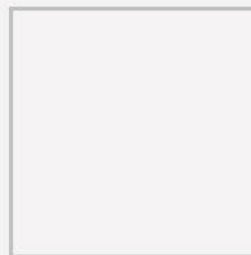
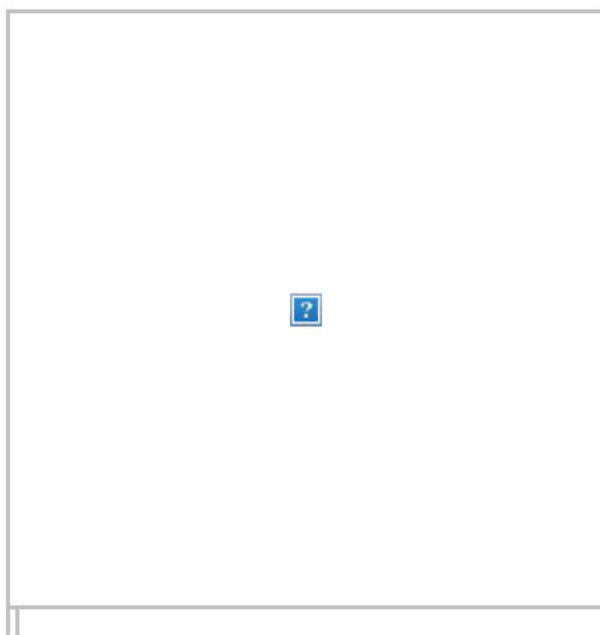
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

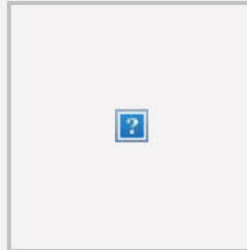


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

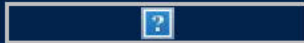
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

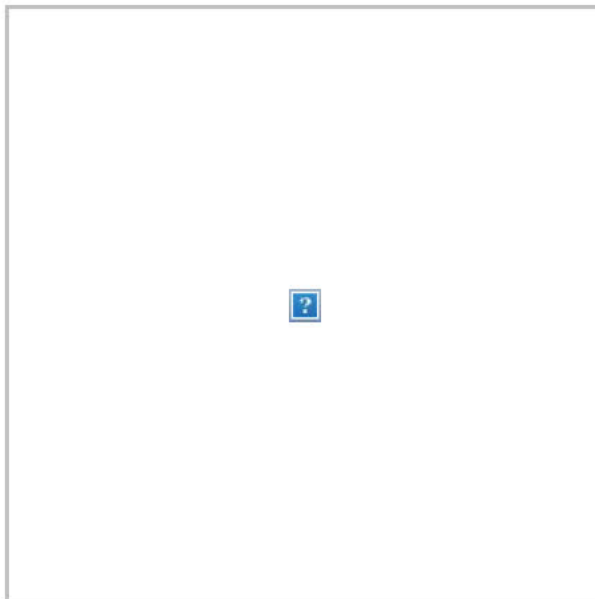
**From:** [PoliceOne Roll Call](#)  
**To:** [sgorshe@ci.sunnyvale.ca.us](mailto:sgorshe@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:23:37 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

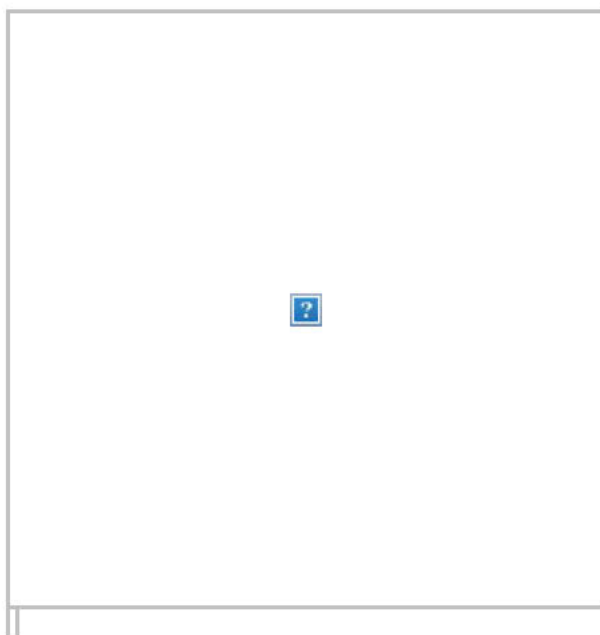
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins



Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

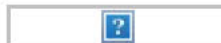
- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

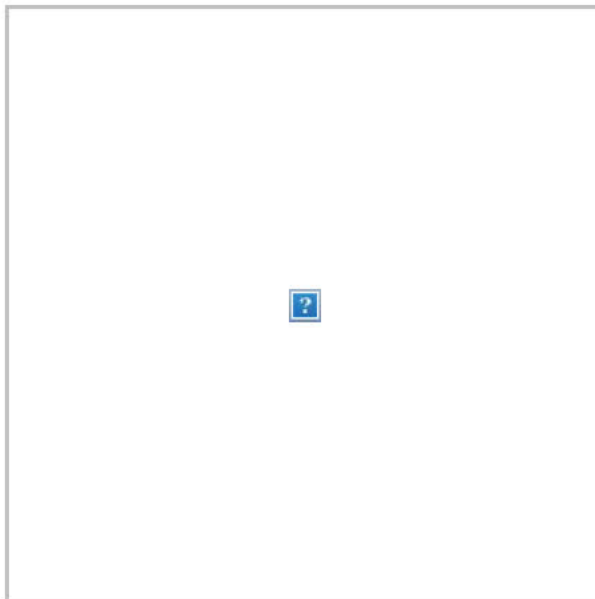
**From:** [PoliceOne Roll Call](#)  
**To:** [srocheville@sunnyvale.ca.gov](mailto:srocheville@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:23:24 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

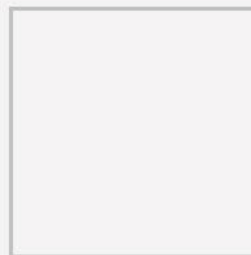
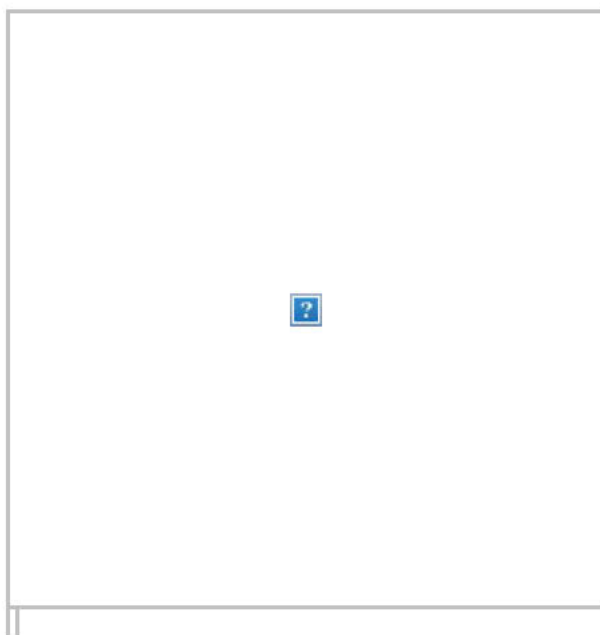
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

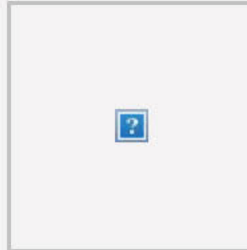


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

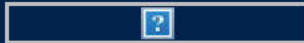
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



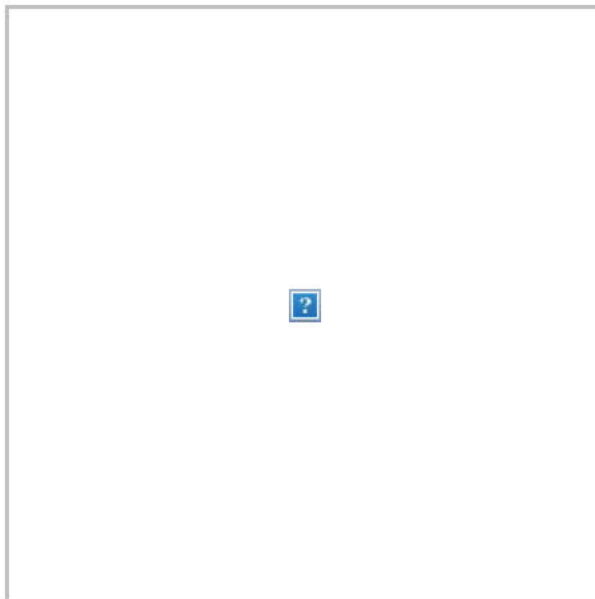
**From:** [PoliceOne Roll Call](#)  
**To:** [ssimpson@sunnyvale.ca.gov](mailto:ssimpson@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:23:08 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

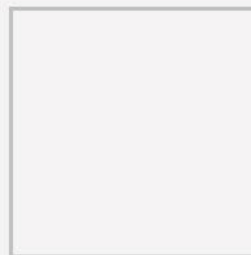
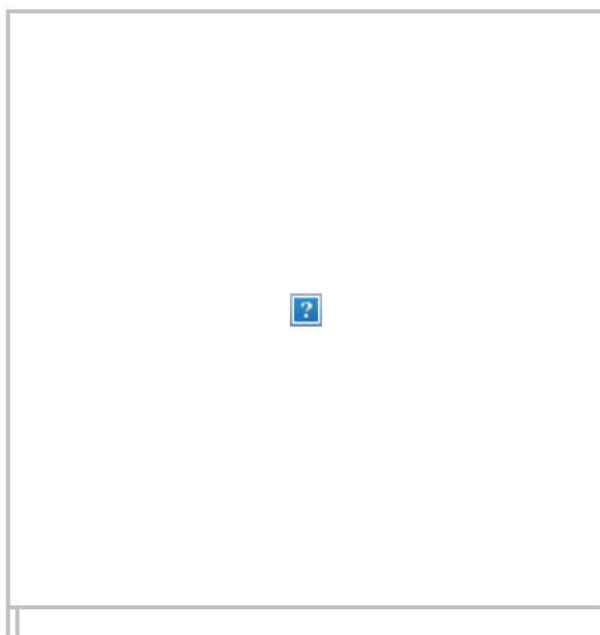
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

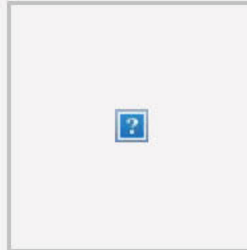


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



## Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



## Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



## Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

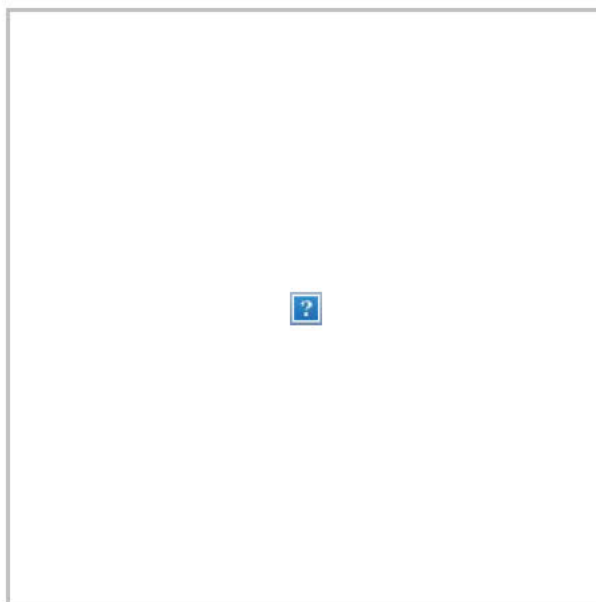
**From:** [PoliceOne Roll Call](#)  
**To:** [dswanger@ci.sunnyvale.ca.us](mailto:dswanger@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:22:53 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

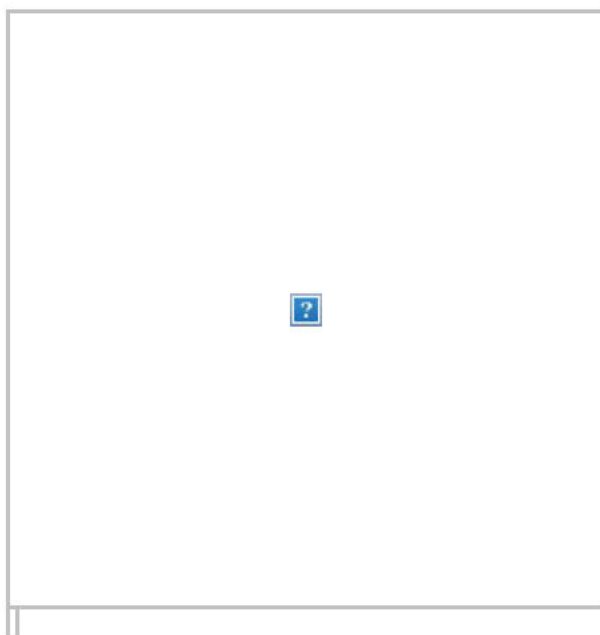
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

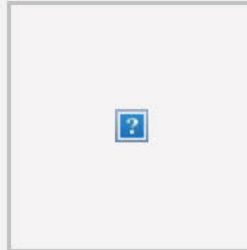


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

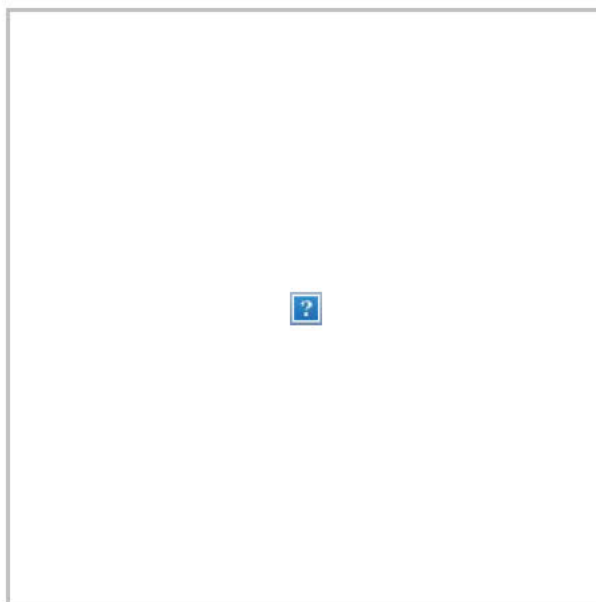
**From:** [PoliceOne Roll Call](#)  
**To:** [rcortez@sunnyvale.ca.gov](mailto:rcortez@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:22:51 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

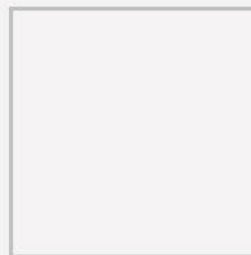
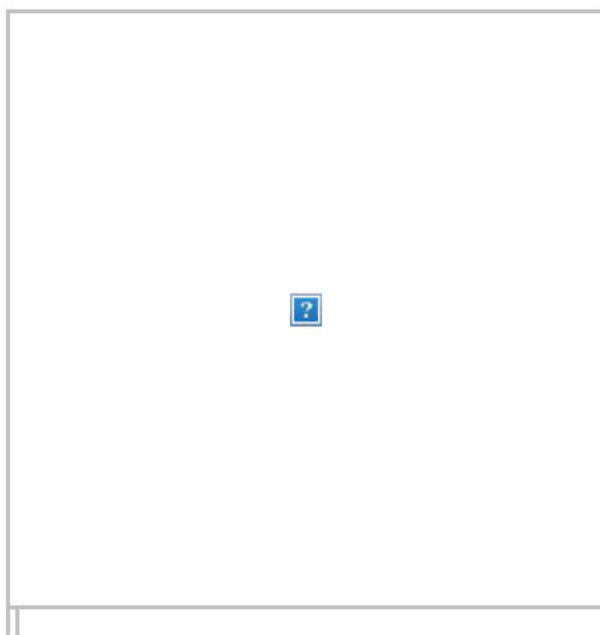
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

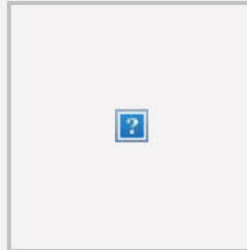


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

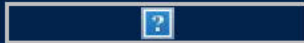
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

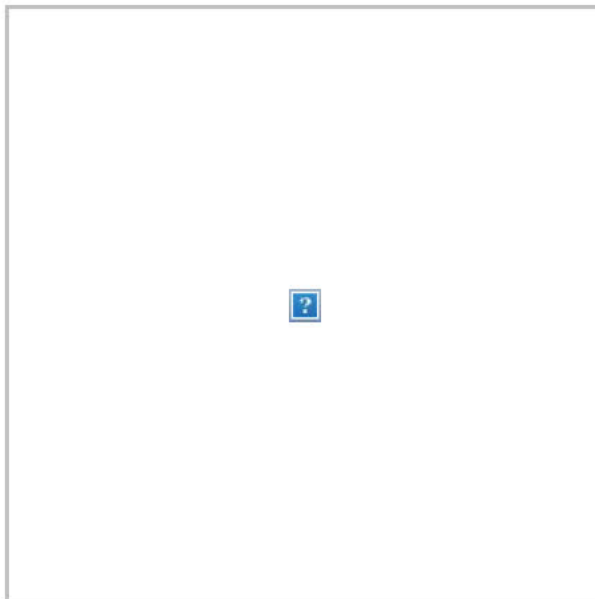
**From:** [PoliceOne Roll Call](#)  
**To:** [sdrewniany@sunnyvale.ca.gov](mailto:sdrewniany@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:22:43 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

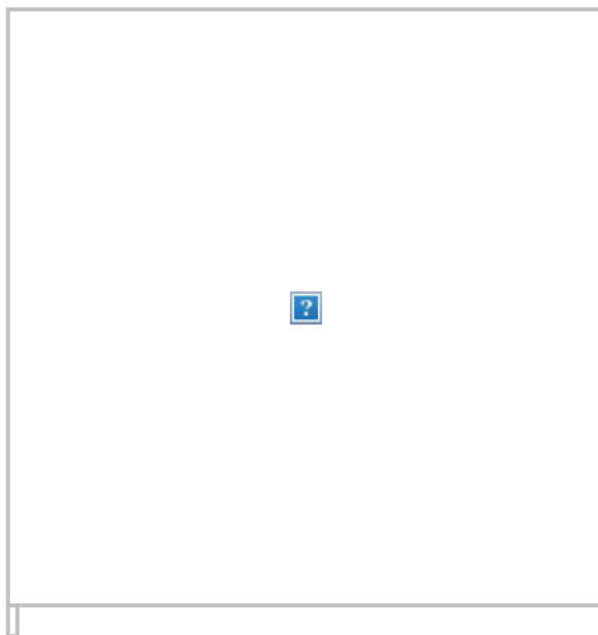
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan  
Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

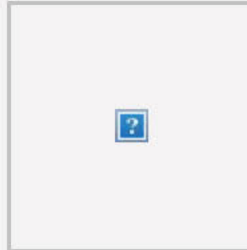


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

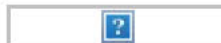
- ☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

- ☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

- ☐ performance evaluations. Download this white paper to learn how to



avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

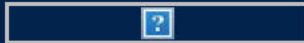
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

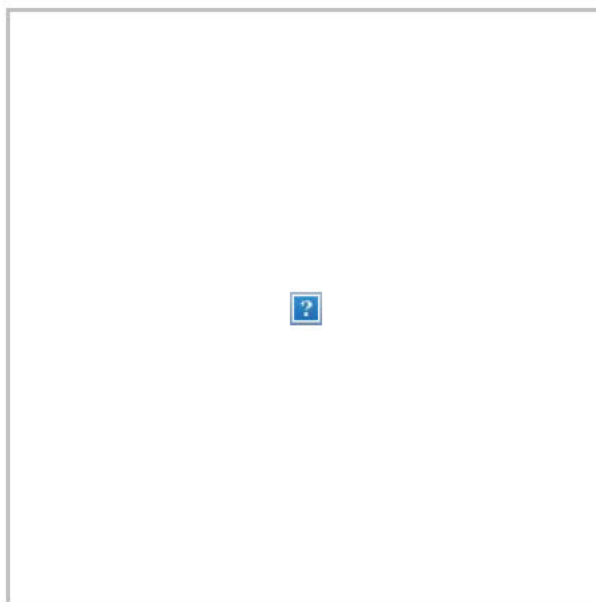
**From:** [PoliceOne Roll Call](#)  
**To:** [cabernathy@ci.sunnyvale.ca.us](mailto:cabernathy@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:22:40 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

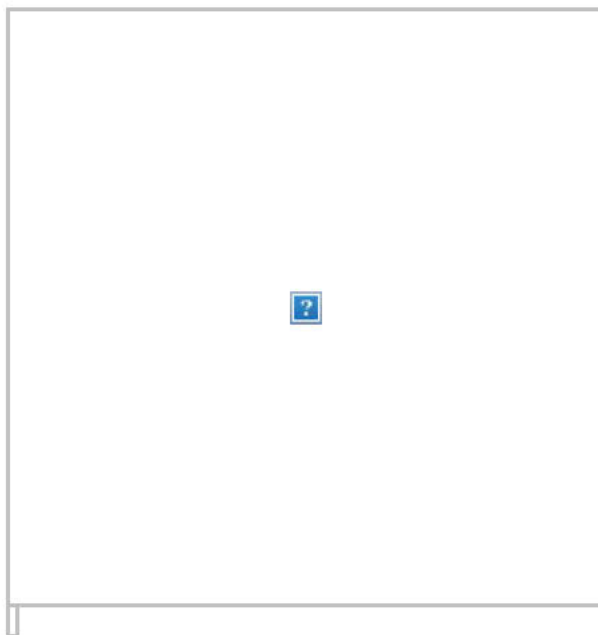
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

By Mike Callahan

The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

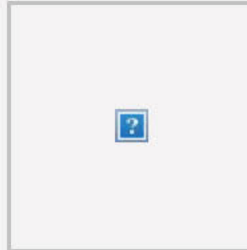


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.



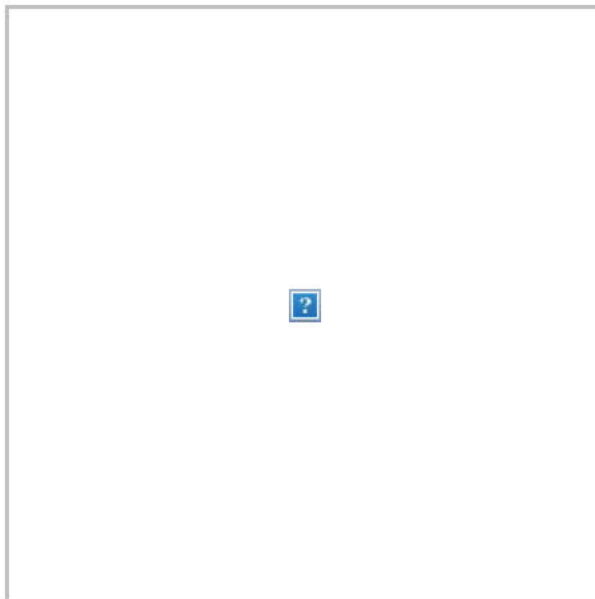
**From:** [PoliceOne Roll Call](#)  
**To:** [srocheville@ci.sunnyvale.ca.us](mailto:srocheville@ci.sunnyvale.ca.us)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:22:40 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

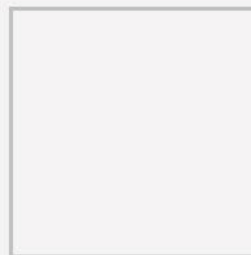
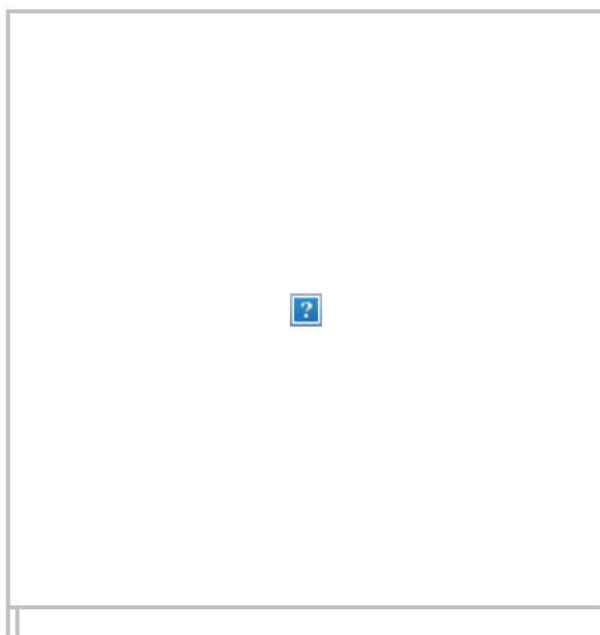
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

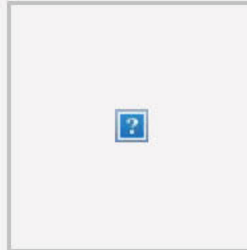


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

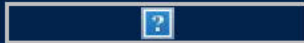
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

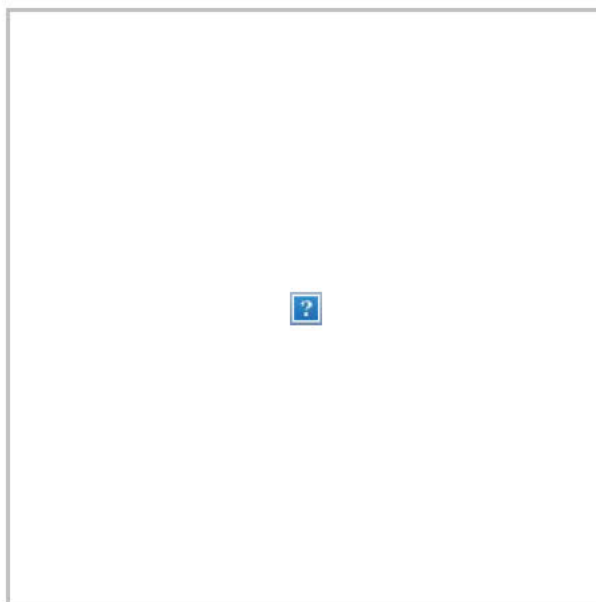
**From:** [PoliceOne Roll Call](#)  
**To:** [bmcmoore@sunnyvale.ca.gov](mailto:bmcmoore@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:22:20 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

[Democrats demand more changes, greater accountability in GOP police bill](#)

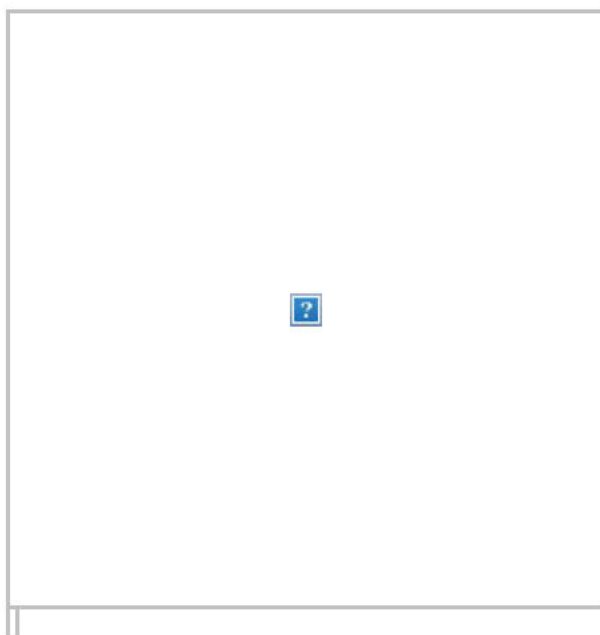
['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a





user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the

survival of our  
honorable  
profession

### Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins



Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

### Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

## OTHER HIGHLIGHTS



### Are you ready to testify?

By Val Van Brocklin

☐ Tips on being an effective witness



### Preparing for a court appearance

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



## SPONSORED CONTENT



### Performance evaluations in public safety: 4 common mistakes

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

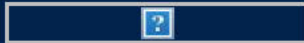
Claim your training credits.

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

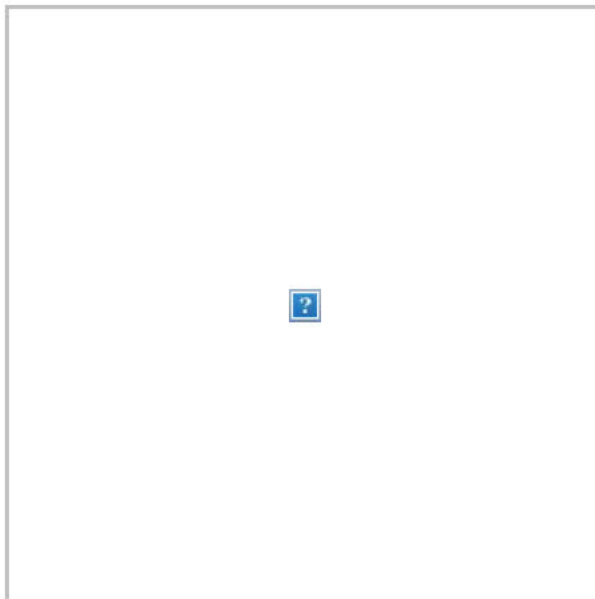
**From:** [PoliceOne Roll Call](#)  
**To:** [msmith@sunnyvale.ca.gov](mailto:msmith@sunnyvale.ca.gov)  
**Subject:** Bystander saves LEO from fiery crash; Hundreds of PDs targeted in hack  
**Date:** Tuesday, June 23, 2020 1:22:18 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

June 23, 2020 | [View as webpage](#)

## TOP STORIES



### Seattle mayor: City will reclaim police-free 'autonomous zone'

Seattle Mayor Jenny Durkan argued that police needed to be in the area to respond to reported crimes



[Minn. police union says it's been 'scapegoated' after Floyd death](#)

[Police investigate 3rd shooting near Seattle's 'occupied' protest zone](#)

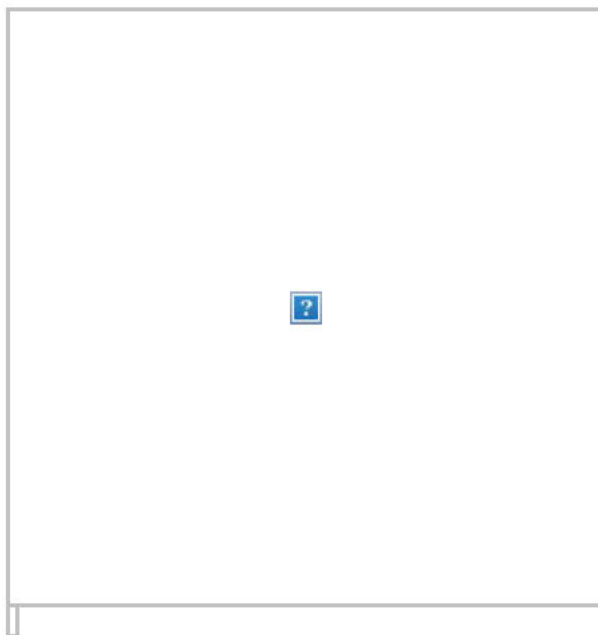
[Democrats demand more changes, greater accountability in GOP police bill](#)

['BlueLeaks' exposes files from hundreds of US police departments](#)

[Bystander helps save Pa. police officer following fiery crash](#)

### Aerial Intelligence With the DJI Matrice 300 RTK

Introducing the Matrice 300 RTK with Smart Pin and Track. PinPoint enables a



user to calculate an object's coordinates via a quick tap on the controller's screen. With Smart Track, identify and follow moving subjects with steady tracking and viewing.

[Learn more](#)

## FEATURED CONTENT



### **Analysis: What cops need to know about the changes to qualified immunity in Colorado**

□ By Mike Callahan  
The legislation creates a \$25,000 personal liability ceiling for officers found liable for state constitutional violations



### **My five sense worth on police reform**

By Lt. Dan Marcou

□ We must address some critical issues of grave importance to the



survival of our  
honorable  
profession

## Webinar: Managing Probation and Parole, Engaging With Vulnerable Citizens Via Smartphone Check-Ins

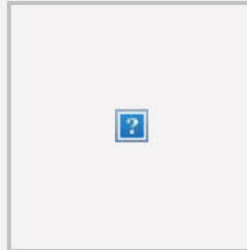


Watch this free, on-demand webinar with AWS and Acivilate to learn how an app can make oversight from a distance during the COVID-19 pandemic

easier.

[Watch it on-demand](#)

## Your In-Car Clutter May Prevent Airbags From Saving Your Life



Most police car-mounted components get in the way of airbag deployment zones and can endanger officers during serious collisions. Check out

the link below for more info.

[Learn how](#)

### OTHER HIGHLIGHTS



#### [Are you ready to testify?](#)

By Val Van Brocklin

☐ Tips on being an effective witness



#### [Preparing for a court appearance](#)

By Gordon Graham

☐ Follow these steps to ensure you are adequately prepped



### SPONSORED CONTENT



#### [Performance evaluations in public safety: 4 common mistakes](#)

A lot can go wrong with

☐ performance evaluations. Download this white paper to learn how to

avoid four common mistakes. [Learn more.](#)



#### FEATURED EDUCATION



#### **Advance Your Career, at Your Own Pace**

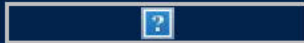
[Claim your training credits.](#)

#### FEATURED EDUCATION



#### **University of Cincinnati Online**

100% online bachelor's & master's in Criminal Justice programs. [Learn more!](#)



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. [Click here to unsubscribe.](#) Visit our [Customer Support page](#) to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

**From:** [Twitter](#)  
**To:** [Ava Fanucchi](#)  
**Subject:** Menlo Park PD shared "Testing and treatment"  
**Date:** Tuesday, June 23, 2020 9:38:24 AM

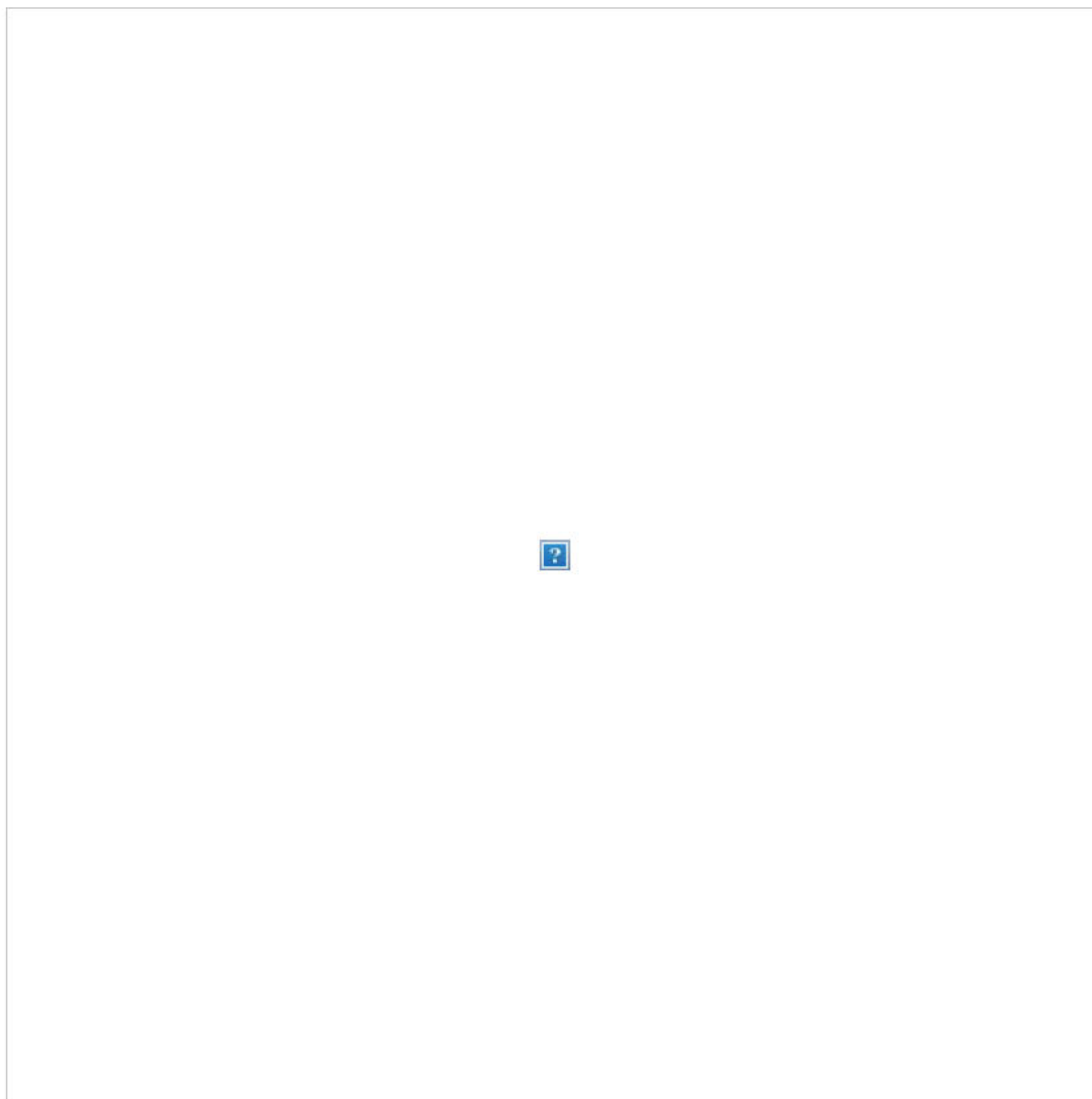
---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



## What's happening

Menlo Park PD shared



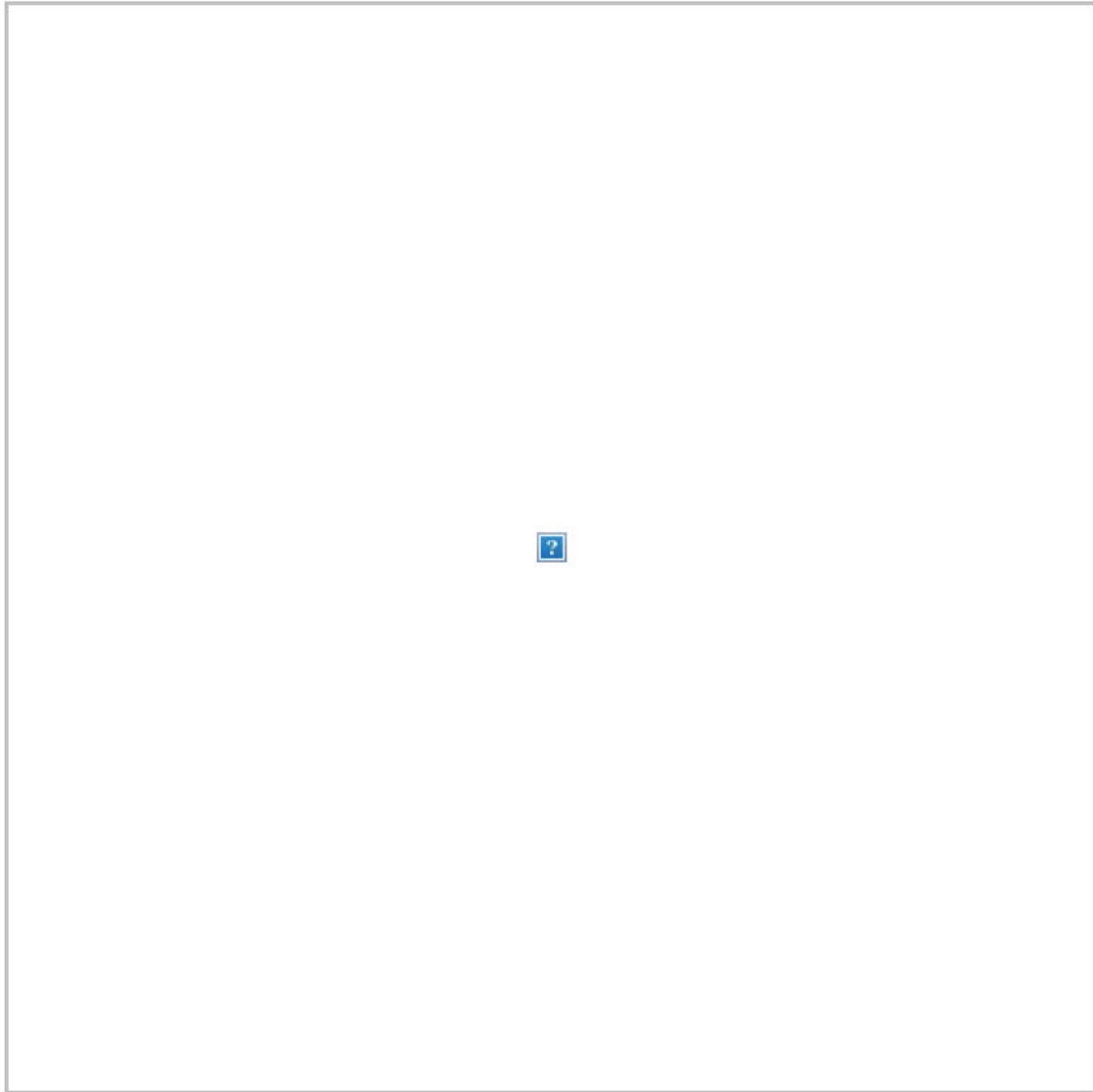
Testing and treatment

**Testing and treatment**

California is expanding coronavirus testing capacity daily. Governor Newsom announced COVID-19 Testing Task Force, a ...

[Read more at Twitter](#)

PoliceOne.com shared



PoliceOne

### **'BlueLeaks' exposes files from hundreds of US police departments**

The data was leaked after a breach at a Houston-based web development firm that handles websites for several PDs

[Read more at Twitter](#)

PoliceOne.com shared



PoliceOne

### **Moody's 'meth show' wins life sentences**

The message in this case is to always check for mobile phone and YouTube video recordings of stupid suspects self-inc...

[Read more at Twitter](#)

PoliceOne.com shared





PoliceOne

### **Ark. police officer killed in head-on, off-duty crash**

Jonesboro Police Department Officer Zachary Barton, 28, had just joined the department in March

[Read more at Twitter](#)

Santa Clara Police shared



California DMV

### **DMV Resumes Behind-the-Wheel Drive Tests with New Protocols on Friday - California DMV**

FOR IMMEDIATE RELEASE June 22, 2020 Canceled appointments will be rescheduled automatically New appointments will be a...

[Read more at Twitter](#)

NBC Bay Area shared



NBC Bay Area

## **FDA Warns Against Using 9 Potentially 'Toxic' Hand Sanitizer Products**

The Food and Drug Administration has warned against the use of nine hand sanitizer products manufactured by Eskbioche...

[Read more at Twitter](#)

[Help](#) | [Privacy](#) | [Reset password](#) | [Download app](#)

We sent this email to @apSunnyvaleDPS. [Unsubscribe](#)

Twitter, Inc. 1355 Market Street, Suite 900 San Francisco, CA 94103



**From:** [MS-ISAC Advisory](#)  
**To:** [Michael Aliperti](#); [Ben Spear](#)  
**Subject:** Message from the MS/EI-ISAC: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach - TLP: AMBER  
**Date:** Tuesday, June 23, 2020 9:07:01 AM  
**Attachments:** [image001.png](#)  
[image002.png](#)  
[image003.png](#)  
[image004.png](#)  
[image005.png](#)

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

**TLP: AMBER**

**TO: All MS-ISAC Members and Partners**

**DATE: June 23, 2020**

**SUBJECT: 200+ Police Departments, Fusion Centers Affected by #BlueLeaks Data Breach**

On June 19, 2020, a Twitter account announced the leak of 10 years of data from police departments, fusion centers, and other law enforcement-related entities currently being tracked on social media as #BlueLeaks. According to the National Fusion Center Association (NFCA), the leak is the result of a compromise at a third party web hosting company, Netsential.

The Twitter account is associated with Distributed Denial of Secrets (DDOS), a collective known for posting leaked or exfiltrated data. The post included a link to a Dark Web location hosting 269GB of files and emails including bulletins, advisories, and guides.

Upon receiving notification of this data breach, the MS-ISAC has confirmed the existence of the dataset and is currently working to analyze the specific contents of the data along with our federal, state, and local partners. At this time, some MS-ISAC products and correspondence have been identified in the leaked data due to the nature of our relationship with fusion centers and law enforcement entities. It is likely that cyber threat actors will utilize MS-ISAC information and/or other portions of the data dump to create tailored phishing campaigns or conduct other malicious cyber activity.

**Recommendations:**

- Be vigilant for new waves of phishing campaigns spoofing emails or products.
- Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain-Based Message Authentication Reporting and Conformance (DMARC), which will assist in ensuring that senders are unable to spoof your email domain. For assistance in implementing these controls, see the Global Cyber Alliance's DMARC Guide <https://dmarcguide.globalcyberalliance.org/#/>.
- Ensure anti-virus software is up to date.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

The MS-ISAC continues to monitor this situation closely and will release further information as appropriate.

24x7 Security Operations Center

Multi-State Information Sharing and Analysis Center (MS-ISAC)

Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)

31 Tech Valley Drive



East Greenbush, NY 12061  
[SOC@cisecurity.org](mailto:SOC@cisecurity.org) - 1-866-787-4722



**TLP: AMBER**

**Limited Disclosure, restricted to participants' organizations. Recipients may only share TLP: AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm.**

**<http://www.us-cert.gov/tlp/>**

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

.....

**From:** [ZDNet](#)  
**To:** [michael spath](#)  
**Subject:** 80,000 printers are exposing their IPP port online  
**Date:** Tuesday, June 23, 2020 7:50:35 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



## ZDNet Tech Today

June 23, 2020

placeholder



Apple Big Sur: What makes new macOS 'biggest update to design in over a decade'



Outlook not working? Microsoft works on fix for buggy June update

## 80,000 printers are exposing their IPP port online

[READ FULL STORY](#)



Apple to App Store developers: How to challenge our decisions

### RELATED

- [New WastedLocker ransomware demands payments of millions of USD](#)
- [This ransomware has learned a new trick: Scanning for point of sales devices](#)
- [Russia unbans Telegram](#)



Virgin Galactic inks deal with NASA to train astronauts for commercial space trips



WWDC 2020: 7 things you probably missed

---

placeholder



5G, video links and virtual consultations: The wireless future of healthcare

[READ FULL STORY](#)

placeholder



The Space Foundation workforce initiative

[WATCH THE VIDEO](#)

placeholder



Apple Silicon at WWDC 2020: Everything you need to know

[READ FULL STORY](#)

placeholder



Working from home: Security is still a confusing mess

[READ FULL STORY](#)

---

THIS WEEK ON ZD NET



## Security

1. [BlueLeaks: Data from 200 US police departments & fusion centers published online](#)
2. [Microsoft's 'Safe Documents' feature reaches general availability in](#)

Office 365

3. [New privacy and security features announced at Apple's WWDC 2020](#)
4. [Microsoft: These hackers got from a broken password to full control of a network - in just days](#)

[See more >](#)



## TechRepublic

1. [Airports use LiDAR to make sure travelers stay six feet apart](#)
2. [18 companies now hiring remote workers](#)
3. [Over 3 in 5 entry-level jobs have been lost since COVID-19 pandemic](#)
4. [How to cultivate an inclusive workplace for LGBTQ employees \(free PDF\)](#)

[Read more >](#)

IN CASE YOU MISSED IT	
-----------------------	--

## iOS 14 kills the biggest iPhone annoyance

placeholder

This iOS annoyance has been plaguing users since the dawn of the iPhone.

[READ FULL STORY](#)

MORE SPONSORED RESEARCH

## Lunch and Learn: Microsoft Excel 2007 intermediate skills

Tools & Templates from [TechRepublic Premium](#)

DOWNLOAD NOW

## Lunch And Learn: Get Up To Speed On OpenOffice Impress

Tools & Templates from [TechRepublic Premium](#)

DOWNLOAD NOW

## IT leader's guide to the automated enterprise

eBooks from [TechRepublic Premium](#)

DOWNLOAD NOW

## Crash Course: Microsoft Word Basics

Tools & Templates from [TechRepublic Premium](#)

DOWNLOAD NOW



This newsletter is a service of ZDNet.com.  
To update your account, please visit our  
Subscription Center.

[Unsubscribe](#) | [Help](#) | [Privacy policy](#)

[Trouble viewing this?](#) [Read Online](#)

Copyright CBS Interactive, Inc.  
All rights reserved. ZDNet is a registered service  
mark of CBS Interactive, Inc.

ZDNet  
235 Second Street  
San Francisco, CA 94105  
U.S.A.

**From:** [HTCC on behalf of Rob Sherman v.a.HTCC](#)  
**To:** [High Tech Crime Consortium Listserv](#)  
**Cc:** [Rob Sherman](#)  
**Subject:** [HTCC] BlueLeaks  
**Date:** Tuesday, June 23, 2020 5:42:49 AM  
**Attachments:** [Untitled attachment.00317.txt](#)

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Listmates,

I ran across an article that is disturbing to say the least in regards to law enforcement data.

I just want to say that I appreciate the good job that each of you do.

So, Thank you.

Here is the article of interest

[https://www.zdnet.com/article/blueleaks-data-from-200-us-police-departments-fusion-centers-published-online/?utm\\_campaign=TECH-DSB-2020%20Global-M-CD-NL-AI&utm\\_medium=email&utm\\_source=Eloqua&member\\_token=UJCy5UoZwv2XtpRQe5VLIHsGI8gObuF4W3ixNw5YsuPes2z1BR5ivqIFUbyT8oY4qtXAGmlddwxH5chr%2FUFehJqaY4exxhRqHcPr%2Fc7k%3D&email\\_asset\\_id=80182&ref\\_GBSNewsletterEmail](https://www.zdnet.com/article/blueleaks-data-from-200-us-police-departments-fusion-centers-published-online/?utm_campaign=TECH-DSB-2020%20Global-M-CD-NL-AI&utm_medium=email&utm_source=Eloqua&member_token=UJCy5UoZwv2XtpRQe5VLIHsGI8gObuF4W3ixNw5YsuPes2z1BR5ivqIFUbyT8oY4qtXAGmlddwxH5chr%2FUFehJqaY4exxhRqHcPr%2Fc7k%3D&email_asset_id=80182&ref_GBSNewsletterEmail)

-Robert

**From:** [The IACP](#)  
**To:** [hchoi@sunnyvale.ca.gov](mailto:hchoi@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.  
**Date:** Tuesday, June 23, 2020 4:43:20 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings Hyun Choi

Tuesday, June 23, 2020





## POLICING & POLICY

Advertisement



### US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

[ABC News](#)  (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

[Newsday \(NY\)](#)  (6/22, Brune) reports that qualified immunity

"shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law — a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

### Senate Democrats Threaten To Block GOP Police Reform Bill

[Politico](#)  (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

**Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law.** [Reuters](#)  (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

## Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The [AP](#) (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

## Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The [New York Times](#) (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

## Massachusetts Governor Seeks Training Bonuses For Police Officers

[Boston](#) (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to \$5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

## San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The [San Diego Union-Tribune](#) (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."



Join the IACP on [June 24, 2020, at 1:00 p.m. EST for Part 2](#) and [July 16, 2020, at 1:00 p.m. EST for Part 3](#) of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

[Reserve your space.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Swedish Rape Conviction Rates Rise 75% After Change In Law

[Reuters](#) (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of



violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected.” According to Reuters, “Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms.”

### **New York City Raid Leads To Drug Seizures, Two Arrests**

The [New York Post](#) ☐ ☐ (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of “approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine.” Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face “charges of criminal possession of a controlled substance and criminally using drug paraphernalia.” The arrests were the result of joint operation conducted by “the city’s Special Narcotics Prosecutor,” the City of New York Police Department, and the DEA.

### **UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In**

The [Independent \(UK\)](#) ☐ ☐ (6/22, Gregory) reports, “Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police.” According to the Independent, “Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only ‘a number of people’ were said to take part in the blockade.” The Independent adds, “Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers.”

## **TECHNOLOGY**

---

### **“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers**

[The Blaze](#) ☐ ☐ (6/22, Taylor) reports hackers have “leaked highly sensitive police files from over 200 police departments across the country.” Activist group DDoSecrets “published what the outlet calls ‘hundreds of gigabytes’ worth of potentially sensitive files’ from police departments across the US.” The group has “called the information dump ‘BlueLeaks.’” The group “compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number.” Many of the files include “information such as memos, emails, and officers’ personal information”. The group “shared information on Twitter regarding the data dump.”

## **GLOBAL SECURITY**

---

### **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

The [New York Times](#) ☐ ☐ (6/22, Alba, Decker) examines how in recent weeks, “residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared.” On the local level, the analysis found that “the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks,” which “can fall under the radar of the tech companies and online fact checkers.”

**Black Lives Matter Protests Spread To White, Rural Areas.** The [Wall Street Journal](#) ☐ ☐ (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

## **MONDAY'S LEAD STORIES**

---

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal “Quarantine Raves”**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

### **Subscriber Tools**

- [Change Email Address](#)
- [Send Feedback](#)



- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to [hchoi@sunnyvale.ca.gov](mailto:hchoi@sunnyvale.ca.gov) as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

**From:** [The IACP](#)  
**To:** [hsyu@sunnyvale.ca.gov](mailto:hsyu@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.  
**Date:** Tuesday, June 23, 2020 4:43:20 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings Hank Syu

Tuesday, June 23, 2020



## POLICING & POLICY

Advertisement



### US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

[ABC News](#) (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

[Newsday \(NY\)](#) (6/22, Brune) reports that qualified immunity

"shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law — a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

### Senate Democrats Threaten To Block GOP Police Reform Bill

[Politico](#) (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

**Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law.** [Reuters](#) (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

## Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The [AP](#) (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

## Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The [New York Times](#) (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

## Massachusetts Governor Seeks Training Bonuses For Police Officers

[Boston](#) (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to \$5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

## San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The [San Diego Union-Tribune](#) (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."



Join the IACP on [June 24, 2020, at 1:00 p.m. EST for Part 2](#) and [July 16, 2020, at 1:00 p.m. EST for Part 3](#) of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

[Reserve your space.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Swedish Rape Conviction Rates Rise 75% After Change In Law

[Reuters](#) (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of



violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected.” According to Reuters, “Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms.”

### **New York City Raid Leads To Drug Seizures, Two Arrests**

The [New York Post](#) ☐ ☐ (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of “approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine.” Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face “charges of criminal possession of a controlled substance and criminally using drug paraphernalia.” The arrests were the result of joint operation conducted by “the city’s Special Narcotics Prosecutor,” the City of New York Police Department, and the DEA.

### **UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In**

The [Independent \(UK\)](#) ☐ ☐ (6/22, Gregory) reports, “Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police.” According to the Independent, “Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only ‘a number of people’ were said to take part in the blockade.” The Independent adds, “Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers.”

## **TECHNOLOGY**

---

### **“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers**

[The Blaze](#) ☐ ☐ (6/22, Taylor) reports hackers have “leaked highly sensitive police files from over 200 police departments across the country.” Activist group DDoSecrets “published what the outlet calls ‘hundreds of gigabytes’ worth of potentially sensitive files’ from police departments across the US.” The group has “called the information dump ‘BlueLeaks.’” The group “compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number.” Many of the files include “information such as memos, emails, and officers’ personal information”. The group “shared information on Twitter regarding the data dump.”

## **GLOBAL SECURITY**

---

### **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

The [New York Times](#) ☐ ☐ (6/22, Alba, Decker) examines how in recent weeks, “residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared.” On the local level, the analysis found that “the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks,” which “can fall under the radar of the tech companies and online fact checkers.”

**Black Lives Matter Protests Spread To White, Rural Areas.** The [Wall Street Journal](#) ☐ ☐ (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

## **MONDAY'S LEAD STORIES**

---

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal “Quarantine Raves”**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

### **Subscriber Tools**

- [Change Email Address](#)
- [Send Feedback](#)

- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to [hsyu@sunnyvale.ca.gov](mailto:hsyu@sunnyvale.ca.gov) as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191



**From:** [The IACP](#)  
**To:** [dsakurai@sunnyvale.ca.gov](mailto:dsakurai@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.  
**Date:** Tuesday, June 23, 2020 4:43:19 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings David Sakurai

Tuesday, June 23, 2020



## POLICING & POLICY

Advertisement



### US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

[ABC News](#) (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

[Newsday \(NY\)](#) (6/22, Brune) reports that qualified immunity

"shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law — a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

### Senate Democrats Threaten To Block GOP Police Reform Bill

[Politico](#) (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

**Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law.** [Reuters](#) (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

## Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The [AP](#) (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

## Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The [New York Times](#) (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

## Massachusetts Governor Seeks Training Bonuses For Police Officers

[Boston](#) (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to \$5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

## San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The [San Diego Union-Tribune](#) (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."



Join the IACP on [June 24, 2020, at 1:00 p.m. EST for Part 2](#) and [July 16, 2020, at 1:00 p.m. EST for Part 3](#) of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

[Reserve your space.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Swedish Rape Conviction Rates Rise 75% After Change In Law

[Reuters](#) (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of



violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected.” According to Reuters, “Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms.”

### **New York City Raid Leads To Drug Seizures, Two Arrests**

The [New York Post](#) ☐ ☐ (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of “approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine.” Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face “charges of criminal possession of a controlled substance and criminally using drug paraphernalia.” The arrests were the result of joint operation conducted by “the city’s Special Narcotics Prosecutor,” the City of New York Police Department, and the DEA.

### **UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In**

The [Independent \(UK\)](#) ☐ ☐ (6/22, Gregory) reports, “Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police.” According to the Independent, “Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only ‘a number of people’ were said to take part in the blockade.” The Independent adds, “Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers.”

## **TECHNOLOGY**

---

### **“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers**

[The Blaze](#) ☐ ☐ (6/22, Taylor) reports hackers have “leaked highly sensitive police files from over 200 police departments across the country.” Activist group DDoSecrets “published what the outlet calls ‘hundreds of gigabytes’ worth of potentially sensitive files’ from police departments across the US.” The group has “called the information dump ‘BlueLeaks.’” The group “compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number.” Many of the files include “information such as memos, emails, and officers’ personal information”. The group “shared information on Twitter regarding the data dump.”

## **GLOBAL SECURITY**

---

### **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

The [New York Times](#) ☐ ☐ (6/22, Alba, Decker) examines how in recent weeks, “residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared.” On the local level, the analysis found that “the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks,” which “can fall under the radar of the tech companies and online fact checkers.”

**Black Lives Matter Protests Spread To White, Rural Areas.** The [Wall Street Journal](#) ☐ ☐ (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

## **MONDAY'S LEAD STORIES**

---

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal “Quarantine Raves”**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

### **Subscriber Tools**

- [Change Email Address](#)
- [Send Feedback](#)

- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to dsakurai@sunnyvale.ca.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

**From:** [The IACP](#)  
**To:** [afanucchi@sunnyvale.ca.gov](mailto:afanucchi@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.  
**Date:** Tuesday, June 23, 2020 4:43:18 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings Ava Fanucchi

Tuesday, June 23, 2020



## POLICING & POLICY

Advertisement



### US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

[ABC News](#) (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

[Newsday \(NY\)](#) (6/22, Brune) reports that qualified immunity

"shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law — a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

### Senate Democrats Threaten To Block GOP Police Reform Bill

[Politico](#) (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

**Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law.** [Reuters](#) (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."



## Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The [AP](#) (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

## Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The [New York Times](#) (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

## Massachusetts Governor Seeks Training Bonuses For Police Officers

[Boston](#) (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to \$5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

## San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The [San Diego Union-Tribune](#) (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."



Join the IACP on [June 24, 2020, at 1:00 p.m. EST for Part 2](#) and [July 16, 2020, at 1:00 p.m. EST for Part 3](#) of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

[Reserve your space.](#)

Connect with the IACP online:



ICAP Event Calendar:



## CRIME & DRUGS

### Swedish Rape Conviction Rates Rise 75% After Change In Law

[Reuters](#) (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of

violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected.” According to Reuters, “Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms.”

### **New York City Raid Leads To Drug Seizures, Two Arrests**

The [New York Post](#) (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of “approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine.” Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face “charges of criminal possession of a controlled substance and criminally using drug paraphernalia.” The arrests were the result of joint operation conducted by “the city’s Special Narcotics Prosecutor,” the City of New York Police Department, and the DEA.

### **UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In**

The [Independent \(UK\)](#) (6/22, Gregory) reports, “Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police.” According to the Independent, “Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only ‘a number of people’ were said to take part in the blockade.” The Independent adds, “Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers.”

## **TECHNOLOGY**

---

### **“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers**

[The Blaze](#) (6/22, Taylor) reports hackers have “leaked highly sensitive police files from over 200 police departments across the country.” Activist group DDoSecrets “published what the outlet calls ‘hundreds of gigabytes’ worth of potentially sensitive files’ from police departments across the US.” The group has “called the information dump ‘BlueLeaks.’” The group “compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number.” Many of the files include “information such as memos, emails, and officers’ personal information”. The group “shared information on Twitter regarding the data dump.”

## **GLOBAL SECURITY**

---

### **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

The [New York Times](#) (6/22, Alba, Decker) examines how in recent weeks, “residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared.” On the local level, the analysis found that “the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks,” which “can fall under the radar of the tech companies and online fact checkers.”

**Black Lives Matter Protests Spread To White, Rural Areas.** The [Wall Street Journal](#) (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

## **MONDAY'S LEAD STORIES**

---

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal “Quarantine Raves”**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

### **Subscriber Tools**

- [Change Email Address](#)
- [Send Feedback](#)



- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to [afanucchi@sunnyvale.ca.gov](mailto:afanucchi@sunnyvale.ca.gov) as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

**From:** [The IACP](#)  
**To:** [jboone@sunnyvale.ca.gov](mailto:jboone@sunnyvale.ca.gov)  
**Subject:** IACP's The Lead: US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police.  
**Date:** Tuesday, June 23, 2020 4:43:11 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you are unable to see the message or images below, [click here to view](#)

Please add us to your address book



Greetings James Boone

Tuesday, June 23, 2020



## POLICING & POLICY

Advertisement



### US Supreme Court Will Not Revisit Challenge To Qualified Immunity For Police

[ABC News](#) (6/22, Dwyer) reports, "The U.S. Supreme Court on Monday officially took a pass on revisiting its 50-year-old doctrine of 'qualified immunity' for law enforcement officers, despite intense national outcry over police misconduct and legal protections that shield cops from liability. 'The Supreme Court has made clear that they are not prepared to reconsider qualified immunity at this moment,' said Joanna Schwartz, an expert on the doctrine at UCLA School of Law." ABC News adds, "While the Civil Rights Act of 1871 gives Americans the unambiguous ability to sue public officials over civil rights violations, the Supreme Court subsequently limited liability to only those rights that have become 'clearly established law.'"

[Newsday \(NY\)](#) (6/22, Brune) reports that qualified immunity

"shields police from being sued for money damages in federal court for constitutional violations such as excessive force unless the officers broke any 'clearly established' law — a high bar for plaintiffs to overcome." Newsday adds that police groups argue that ending qualified immunity "would have a chilling effect on police work, make them hesitant to act when they should be decisive in dicey situations, or lead to retirements and a smaller pool of applicants for police jobs. 'Qualified immunity is a foundational protection for the policing profession and any modification to this legal standard will have a devastating impact on the police's ability to fulfill its public safety mission,' the International Association of Chiefs of Police said in a statement."

### Senate Democrats Threaten To Block GOP Police Reform Bill

[Politico](#) (6/22, Everett, Levine) reports Senate Democrats are "strongly signaling they will filibuster Republicans' police reform bill later this week absent more concessions" from Senate Majority Leader McConnell, who "set the Senate on a path to consider the legislation on Wednesday." Sen. Jon Tester (D-MT) said, "If nothing changes, I'm voting no. I need some assurances that we're going to vote on amendments that will fix this bill. And it needs a lot of fixing." Senate Minority Leader Schumer called the GOP bill "deeply and fundamentally flawed."

**Reuters Analysis: Neither Senate Nor House Police Reform Bill Likely To Become Law.** [Reuters](#) (6/22, Morgan) reports that the Senate and the House "will vote this week on separate bills aimed at addressing police misconduct...but neither measure is likely to become law." The Senate "is expected to hold a procedural vote on a Republican bill by Wednesday, while the House is due to vote on more sweeping Democratic legislation on Thursday." However, Reuters says, "neither measure, as written, appears to have enough bipartisan support to win approval from both chambers and be signed into law."

## Studies Find Recreational Marijuana Laws May Boost Traffic Deaths

The [AP](#) (6/22, Tanner) reports, "Laws legalizing recreational marijuana may lead to more traffic deaths, two new studies suggest, although questions remain about how they might influence driving habits." According to the AP, "Previous research has had mixed results and the new studies, published Monday in JAMA Internal Medicine, can't prove that the traffic death increases they found were caused by marijuana use." The AP adds, "One study found an excess 75 traffic deaths per year after retail sales began in Colorado in January 2014, compared with states without similar laws," but "it found no similar change in Washington state." The other study "looked at those states plus two others that allow recreational pot sales, Oregon and Alaska. If every state legalized recreational marijuana sales, an extra 6,800 people would die each year in traffic accidents, the researchers calculated."

## Pandemic Has Increased New York City Criminal Court Backlog To More Than 39K Cases

The [New York Times](#) (6/22, A1, Feuer, Hong, Weiser, Ransom) has a 2,400-word report on what it calls New York City's "legal limbo," where "the backlog of pending cases in the city's criminal courts has risen by nearly a third" to 39,200 due to the coronavirus pandemic. The Times says "hundreds of jury trials in the city have been put on hold indefinitely," and "arraignments, pleas and evidentiary hearings are being held by video, with little public scrutiny."

## Massachusetts Governor Seeks Training Bonuses For Police Officers

[Boston](#) (6/22, Gavin) reports, "Police officers in Massachusetts could receive one-time bonuses of up to \$5,000 should they take on additional training under a bill filed last week by Gov. Charlie Baker centered on creating a police certification system." According to Boston, "The vision is to incentivize officers to go beyond the necessary minimum training laid out in the sweeping proposal, which comes amid the nationwide movement to reduce funding for law enforcement, and instead funnel resources into other initiatives such as anti-violence and public health programs." The bill, "which seeks to establish a system to uniformly certify, and de-certify, police officers," would "provide financial opportunity to officers to advance their training in key areas, including first aid, de-escalation tactics, and narcotics training."

## San Diego, California Ballot Measure Would Reform Police Oversight, Accountability

The [San Diego Union-Tribune](#) (6/22, Garrick) reports San Diego may "take a key step Tuesday toward more rigorous police oversight, transparency and accountability." The San Diego City Council "is scheduled to evaluate a proposed November ballot measure that would create a police review board with the power to launch independent misconduct investigations and subpoena witnesses. While the proposal has been in the works for several years, it gained momentum in the wake of recent local and national police protests that have sparked calls for fundamental law enforcement reforms." The city "completed negotiations May 21 with the labor union representing police officers on the proposed ballot measure, which would let officers appeal declarations by the commission that they are guilty of misconduct."



Join the IACP on [June 24, 2020, at 1:00 p.m. EST for Part 2](#) and [July 16, 2020, at 1:00 p.m. EST for Part 3](#) of *Mindfulness Strategies for Law Enforcement* webinar series. This webinar is part of the U.S. Department of Justice, Bureau of Justice Assistance's National Officer Safety Initiatives Program and will be hosted by Mindful Junkie Founder, Gina White. Police officers across every rank, dispatchers, victim services personnel, crime scene personnel, other law enforcement personnel and family members are encouraged to attend these 30-minute interactive mindfulness sessions.

[Reserve your space.](#)

Connect with the IACP online:



IACP Event Calendar:



## CRIME & DRUGS

### Swedish Rape Conviction Rates Rise 75% After Change In Law

[Reuters](#) (6/22, Batha) reports, "Rape conviction rates in Sweden have risen 75% in two years following a major change in the law, spurring calls on Monday for other countries to revamp their legislation." Reuters adds, "Sweden changed the legal definition of rape in 2018 to sex without consent. Unlike in many countries, prosecutors do not have to prove the use or threat of



violence or coercion. The National Council on Crime Prevention (Bra) said the rise in convictions – up from 190 in 2017 to 333 in 2019 – showed the change had had a greater impact than expected.” According to Reuters, “Britain, Belgium, Canada, Cyprus, Germany, Greece, Iceland, Ireland and Luxembourg already define rape as sex without consent, while Denmark, Finland, Spain and Portugal have promised similar reforms.”

### **New York City Raid Leads To Drug Seizures, Two Arrests**

The [New York Post](#) ☐ ☐ (6/22, Rosenberg) reports a recent raid of a suspected pill mill in New York City led to the seizure of “approximately 1.2 kilograms of heroin, 34 grams of fentanyl and 2.3 kilograms of methamphetamine.” Arrested in connection with the raid were Jeison Lebron and Alfredo Goris, who face “charges of criminal possession of a controlled substance and criminally using drug paraphernalia.” The arrests were the result of joint operation conducted by “the city’s Special Narcotics Prosecutor,” the City of New York Police Department, and the DEA.

### **UK Drinkers Barricade Themselves In Pub During Illegal Lockdown Lock-In**

The [Independent \(UK\)](#) ☐ ☐ (6/22, Gregory) reports, “Drinkers at an illegal lockdown-defying lock-in have barricaded themselves in a pub after police officers arrived to break up the session, according to police.” According to the Independent, “Merseyside Police officers were pelted with beer and other items as revellers took up their fortified position at the Britannia Hotel pub in Liverpool, the force said. There were reportedly more than 100 people gathered at the Vauxhall pub at around midnight on Sunday, playing loud music and disturbing residents nearby, although only ‘a number of people’ were said to take part in the blockade.” The Independent adds, “Seven men and one woman, aged between 21 and 33, were arrested for violent disorder and drugs offences. Pubs have been closed by law for the last three months to fight the spread of coronavirus, with Boris Johnson expected to allow them to re-open on 4 July, albeit with a range of new measures in place to protect customers.”

## **TECHNOLOGY**

---

### **“Blueleaks” Hackers Release “Hundreds Of Thousands” Of Private Records On Officers**

[The Blaze](#) ☐ ☐ (6/22, Taylor) reports hackers have “leaked highly sensitive police files from over 200 police departments across the country.” Activist group DDoSecrets “published what the outlet calls ‘hundreds of gigabytes’ worth of potentially sensitive files’ from police departments across the US.” The group has “called the information dump ‘BlueLeaks.’” The group “compiled the records, disseminating them into a searchable database that can pull up private information from a police badge number.” Many of the files include “information such as memos, emails, and officers’ personal information”. The group “shared information on Twitter regarding the data dump.”

## **GLOBAL SECURITY**

---

### **NYTimes Analysis: Antifa Rumors Show Ways Information Spreads Locally**

The [New York Times](#) ☐ ☐ (6/22, Alba, Decker) examines how in recent weeks, “residents in at least 41 U.S. cities and towns became alarmed by rumors that the loose collective of anti-fascist activists known as antifa was headed to their area, according to an analysis by The New York Times. In many cases, they contacted their local law enforcement for help. In each case, it was for a threat that never appeared.” On the local level, the analysis found that “the source of the false information has usually been more subtle, and shows the complexity of stunting misinformation online. The bad information often first appears in a Twitter or Facebook post, or a YouTube video there. It is then shared on online spaces like local Facebook groups, the neighborhood social networking app Nextdoor and community texting networks,” which “can fall under the radar of the tech companies and online fact checkers.”

**Black Lives Matter Protests Spread To White, Rural Areas.** The [Wall Street Journal](#) ☐ ☐ (6/22, Carlton, Subscription Publication) reports that the protests for racial justice have quickly spread from big cities to small, rural towns that are predominantly white.

## **MONDAY'S LEAD STORIES**

---

- **Former IACP President Addresses Police Reform**
- **UK Authorities Grapple With Illegal “Quarantine Raves”**
- **Libyan Refugee Arrested In UK Terrorist Attack That Left Three Dead**

### **Subscriber Tools**

- [Change Email Address](#)
- [Send Feedback](#)

- [Unsubscribe](#)
- [Email Help](#)
- [Archives](#)

*The Lead* is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to jboone@sunnyvale.ca.gov as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's [privacy policy](#).

For information about other member benefits, please contact the IACP at [membership@theiacp.org](mailto:membership@theiacp.org) or 1.800.THE IACP.

[International Association of Chiefs of Police](#) | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

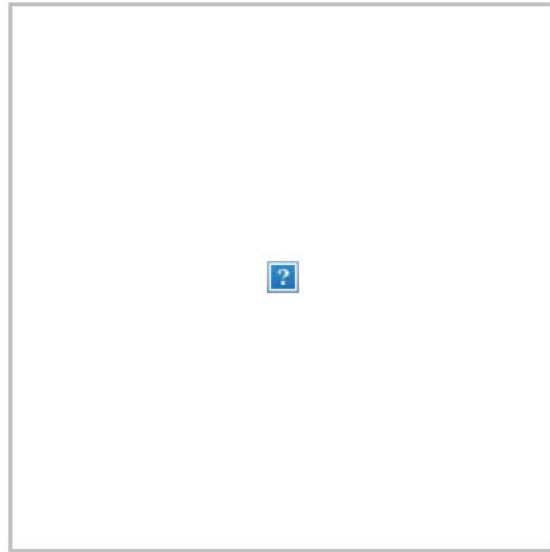
Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

**From:** [Jeffrey H. Snyder, Lead Anchor](#)  
**To:** [tsilva@sunnyvale.ca.gov](mailto:tsilva@sunnyvale.ca.gov)  
**Subject:** The Morning Pulse for Tuesday, June 23, 2020 - Technology boosts archeology and history  
**Date:** Tuesday, June 23, 2020 4:02:15 AM

---

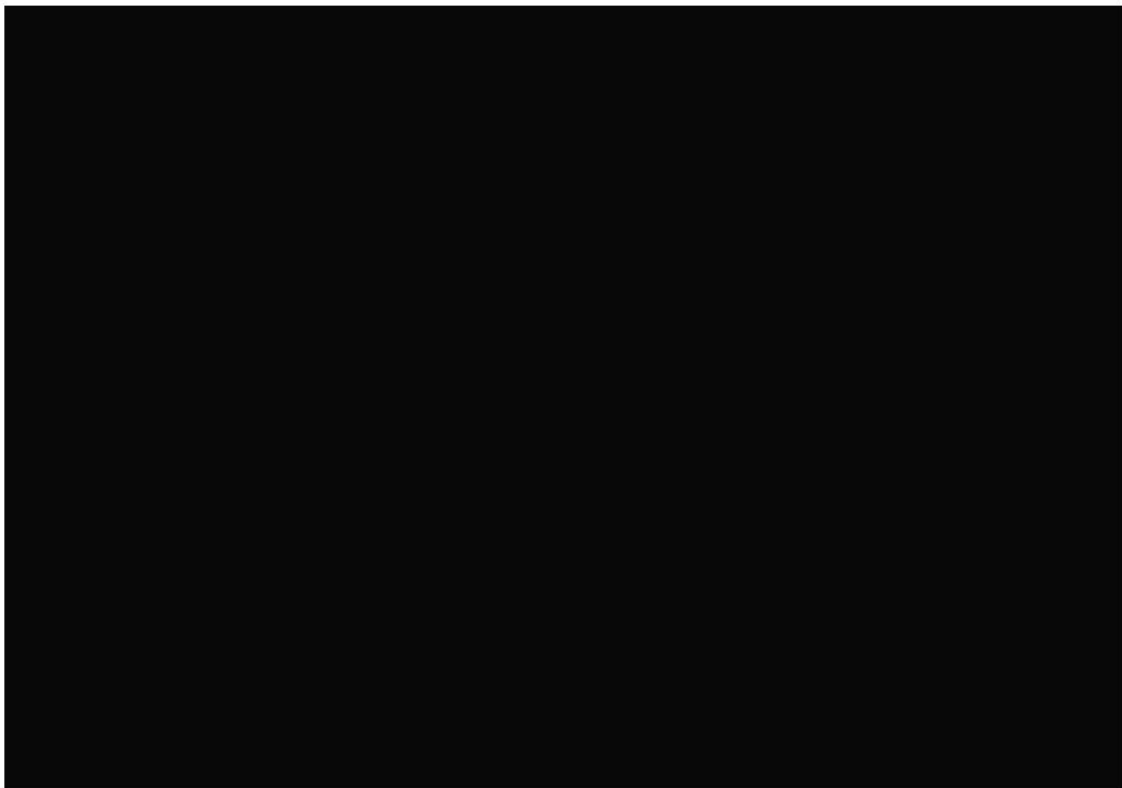
ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

---



# The Morning Pulse

*retirement news that matters.  
independent. unbiased. information for all.*



The Broadcast Retirement Network's #BRNAM for Tuesday, June 23, 2020 | Special guest: Daniel Kline, Senior Technology and Consumer Products Reporter, The Motley Fool | Top stories: The U.S. can get to 90% clean electricity in just 15 years and Technology boosts archeology and history | For more news and content each and every day subscribe and visit [www.broadcastretirementnetwork.com](http://www.broadcastretirementnetwork.com)

JUNE 23, 2020

[SUBSCRIBE](#)

#### PERSONAL FINANCE

- [TikTok is the new place to learn about managing your money ; CDs are popular option for safe return on savings ; A financial planner's strategy to cut spending during unemployment prioritizes your mental health ; Planning for loved ones with special needs](#)
- [Commission-free stock trades plus mobile phone apps equals risky speculation](#)
- [When times are good, charitable giving goes up ; Philanthropy steps up to help as crisis hits nonprofits hard](#)
- [Mortgage rates drop to another record low — here's why Americans may not want to wait too much longer](#)
- [This is what your next hotel stay will probably look like](#)

#### HEALTHY AGING

- [Covid-19 Reveals The Caregiving Mystique](#)
- [Mental health conditions are not a normal part of aging](#)
- [Combination of Lifestyle Traits Can Reduce Alzheimer: NIH Study](#)



- [With increasing longevity, boomers are the first 'older generation'](#)
- [Will smaller care homes prevail in the future?](#)

## HEALTHCARE

- [How to Prevent Medical Records From Being Hacked ; Healthcare cybersecurity market to hit \\$12 billion by 2027 – report](#)
- [Unemployed Struggle Without Healthcare](#)
- [WHO reports largest single-day surge in coronavirus cases yet](#)
- [Coronavirus will finally give artificial intelligence its moment](#)

## EDUCATION

- [The Higher Education Experience Coming Fall 2020 Is What You Make Of It](#)
- [University projects \\$100 million loss in revenue in upcoming fiscal year, after \\$44 million loss in current fiscal year](#)
- [What does the landscape of higher education look in the era of the coronavirus?](#)
- [Students Survey Consumer Sentiment Around Dining Out](#)
- [Higher education cuts could jeopardize research funding, freeze hiring](#)
- ['Extreme Economies' and Higher Ed in 2050](#)

## TECH

- [Lawsuit: Firm 'negligent' in unemployment data breach ; 'BlueLeaks' Exposes Files from Hundreds of Police Departments ; Companies Name One of the Biggest Cybersecurity Threats: Their Employees ; SEC Alleges Brothers' Digital Asset Fund Was a Scam](#)
- [Your Next Favorite Original Series May Be on Spotify](#)
- [Common misconceptions about smart homes and biometrics](#)

## RETIREMENT

- [These Are Baby Boomers' Top 3 Retirement Fears ; The Big Reason So Many Older Workers Risk Being Pushed Into Early Retirement Today ; Should You Keep Saving for Retirement When You're on Unemployment?](#)
- [Investment Losses in Your Retirement Account? How to Reset and Move Forward](#)
- [Social Security 'retirement test' gets a failing grade](#)
- [Analysis: Private equity isn't what retirement savers need](#)
- [IRS expands criteria to withdraw money from retirement plans for those affected by coronavirus](#)

## PENSIONS

- [Man Pleads Guilty to Stealing Over \\$400k in Pension Benefits](#)
- [The leaders of Pa.'s giant school pension plan are stumped by how to invest in this economy](#)
- [Before COVID-19, pension demands put San Rafael budget in vise](#)
- [CalPERS Now Looking to Borrow to Better Drive Returns ; CalPERS gambles on risky investment move ; Calpers board member objects to \\$80bn leverage gamble](#)

## INTERNATIONAL

- [Financial Literacy Is Everyone's Business](#)
- [Government caves in to pension concerns over insolvency changes](#)
- [Employees opting out of workplace pensions 'could be nudged back in sooner'](#)
- [Belarus to raise retirement pensions soon](#)
- [Workers allowed to suspend pension payments](#)

## MARKETS

- [The Stock Market Appears To Be Reaching Unsustainable Highs ; Global dollar crunch appears over as central banks rely less on Fed backstop](#)
- [Record Spending and Money-Printing Puts Markets in Uncharted Waters ; The Fed's Final Frontier - Negative Rates Or Yield Curve Control?](#)
- [US banks are 'swimming in money' as deposits increase by \\$2 trillion amid the coronavirus ; Investors dismiss prospect of 'V-shaped' recovery](#)
- [Oil Stockpiles Are Enormous ; The Oil Countries Suffering Most From The Oil Price Crash](#)
- [How To Align Investments To A Greater Purpose](#)
- [Private investment needed to rebuild the economy ; South Africa Sees Debt Topping 100% of GDP in 2025 ; UK debt is now higher than the country's entire GDP for the first time in 57 years](#)

## ALTERNATIVES

- [Hedge funds are starting to wind down ; SEC freezes Hvizdzak hedge fund, alleges fraud](#)
- [Bad Economy? Unleash Private Equity ; Financial wizardry breathes magic into private equity returns ; Private equity 'barbarians' weigh the risks of Covid-19 takeovers](#)
- [Experts react to bullish blockchain survey by Deloitte ; Is the Bitcoin ETF coming? Change of leadership at the SEC; Anthony Pompliano Continues Push for Pension Fund Crypto Allocation ; Gov't's move to tax cryptocurrency faces backlash ; SEC Issues Emergency Halt to Cryptocurrency Fund](#)
- [Is commercial real estate headed for a crash?](#)

## ABOUT THE BROADCAST RETIREMENT NETWORK



The Broadcast Retirement Network (BRN) is the first lifestyle media platform focused on helping Americans achieve financial independence and to make retirement and savings culturally relevant. The content is informative and engages the viewer. Most importantly - No agendas, no sales pitches, no product pushes.

Our morning show, BRN AM, provides an assessment of daily issues so that Americans can create a plan of action for themselves and their families. BRN AM focuses on delivering headline news via brief interviews with real Americans working toward their financial goals.

Unlike financial shows which prioritize institutional investment managers and public policy organizations, BRN AM is a lifestyle show that brings the stories and ideas of regular Americans to the forefront. We engage with a range of topics pertaining to retirement, focusing individual episodes on personal finance, healthcare, social security, home-ownership and so on to provide viewers with the full picture regarding the future of financial security in America.

*The hyperlinks above take you to internet site(s) sponsored and maintained by independent third parties that are unaffiliated with The Morning Pulse, Inc. The hyperlinks as provided are maintained to provide the author(s) and their respective organizations the proper attribution for developing the original content. The links and content provided in The Morning Pulse and The Weekly Pulse are for general reference and educational purposes only. Although we believe the content provider to be a reliable source of information, we do not guarantee the accuracy of the information or warranty the representations of such Websites. The information available through these Web sites has not been prepared by nor does The Morning Pulse, Inc. have an ability to alter the content, and content will not be monitored by The Morning Pulse, Inc. in the future. The Morning Pulse, Inc. assumes no responsibility for the use of or inability to use such site and recommends you review the terms, conditions, and privacy policy applying to your use of the site. Expression of opinions contained on these hyperlinks may or may not be consistent with the opinions of The Morning Pulse, Inc.*



[UNSUBSCRIBE](#)

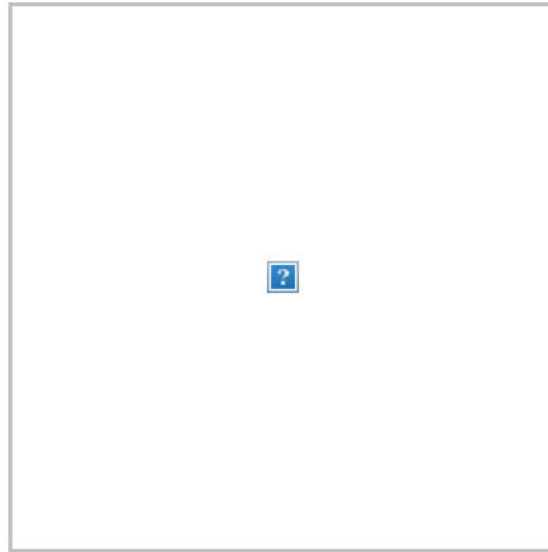
Copyright © 2020 The Morning Pulse, Inc., All rights reserved.

**From:** [Jeffrey H. Snyder, Lead Anchor](#)  
**To:** [dbaker@sunnyvale.ca.gov](mailto:dbaker@sunnyvale.ca.gov)  
**Subject:** The Morning Pulse for Tuesday, June 23, 2020 - Technology boosts archeology and history  
**Date:** Tuesday, June 23, 2020 4:01:17 AM

---

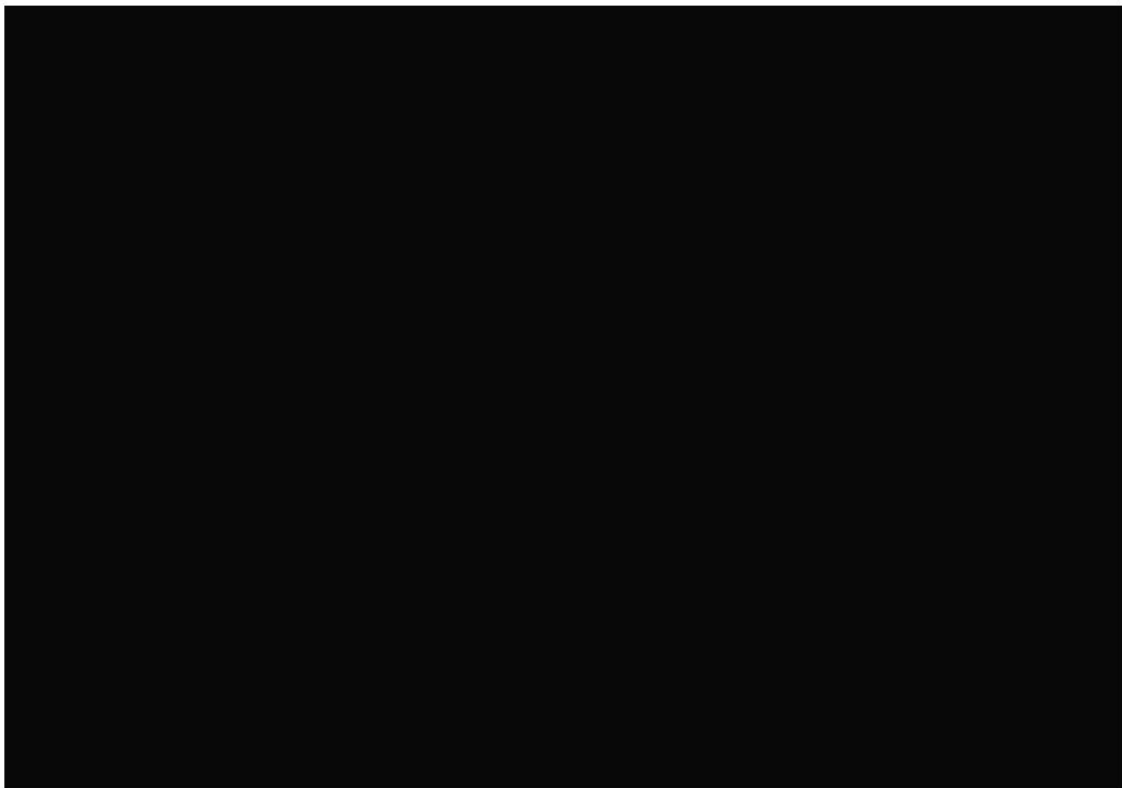
ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

---



# The Morning Pulse

*retirement news that matters.  
independent. unbiased. information for all.*



The Broadcast Retirement Network's #BRNAM for Tuesday, June 23, 2020 | Special guest: Daniel Kline, Senior Technology and Consumer Products Reporter, The Motley Fool | Top stories: The U.S. can get to 90% clean electricity in just 15 years and Technology boosts archeology and history | For more news and content each and every day subscribe and visit [www.broadcastretirementnetwork.com](http://www.broadcastretirementnetwork.com)

JUNE 23, 2020

[SUBSCRIBE](#)

#### PERSONAL FINANCE

- [TikTok is the new place to learn about managing your money ; CDs are popular option for safe return on savings ; A financial planner's strategy to cut spending during unemployment prioritizes your mental health ; Planning for loved ones with special needs](#)
- [Commission-free stock trades plus mobile phone apps equals risky speculation](#)
- [When times are good, charitable giving goes up ; Philanthropy steps up to help as crisis hits nonprofits hard](#)
- [Mortgage rates drop to another record low — here's why Americans may not want to wait too much longer](#)
- [This is what your next hotel stay will probably look like](#)

#### HEALTHY AGING

- [Covid-19 Reveals The Caregiving Mystique](#)
- [Mental health conditions are not a normal part of aging](#)
- [Combination of Lifestyle Traits Can Reduce Alzheimer: NIH Study](#)

- [With increasing longevity, boomers are the first 'older generation'](#)
- [Will smaller care homes prevail in the future?](#)

## HEALTHCARE

- [How to Prevent Medical Records From Being Hacked ; Healthcare cybersecurity market to hit \\$12 billion by 2027 – report](#)
- [Unemployed Struggle Without Healthcare](#)
- [WHO reports largest single-day surge in coronavirus cases yet](#)
- [Coronavirus will finally give artificial intelligence its moment](#)

## EDUCATION

- [The Higher Education Experience Coming Fall 2020 Is What You Make Of It](#)
- [University projects \\$100 million loss in revenue in upcoming fiscal year, after \\$44 million loss in current fiscal year](#)
- [What does the landscape of higher education look in the era of the coronavirus?](#)
- [Students Survey Consumer Sentiment Around Dining Out](#)
- [Higher education cuts could jeopardize research funding, freeze hiring](#)
- ['Extreme Economies' and Higher Ed in 2050](#)

## TECH

- [Lawsuit: Firm 'negligent' in unemployment data breach ; 'BlueLeaks' Exposes Files from Hundreds of Police Departments ; Companies Name One of the Biggest Cybersecurity Threats: Their Employees ; SEC Alleges Brothers' Digital Asset Fund Was a Scam](#)
- [Your Next Favorite Original Series May Be on Spotify](#)
- [Common misconceptions about smart homes and biometrics](#)

## RETIREMENT

- [These Are Baby Boomers' Top 3 Retirement Fears ; The Big Reason So Many Older Workers Risk Being Pushed Into Early Retirement Today ; Should You Keep Saving for Retirement When You're on Unemployment?](#)
- [Investment Losses in Your Retirement Account? How to Reset and Move Forward](#)
- [Social Security 'retirement test' gets a failing grade](#)
- [Analysis: Private equity isn't what retirement savers need](#)
- [IRS expands criteria to withdraw money from retirement plans for those affected by coronavirus](#)

## PENSIONS

- [Man Pleads Guilty to Stealing Over \\$400k in Pension Benefits](#)
- [The leaders of Pa.'s giant school pension plan are stumped by how to invest in this economy](#)
- [Before COVID-19, pension demands put San Rafael budget in vise](#)
- [CalPERS Now Looking to Borrow to Better Drive Returns ; CalPERS gambles on risky investment move ; Calpers board member objects to \\$80bn leverage gamble](#)

## INTERNATIONAL

- [Financial Literacy Is Everyone's Business](#)
- [Government caves in to pension concerns over insolvency changes](#)
- [Employees opting out of workplace pensions 'could be nudged back in sooner'](#)
- [Belarus to raise retirement pensions soon](#)
- [Workers allowed to suspend pension payments](#)

## MARKETS

- [The Stock Market Appears To Be Reaching Unsustainable Highs ; Global dollar crunch appears over as central banks rely less on Fed backstop](#)
- [Record Spending and Money-Printing Puts Markets in Uncharted Waters ; The Fed's Final Frontier - Negative Rates Or Yield Curve Control?](#)
- [US banks are 'swimming in money' as deposits increase by \\$2 trillion amid the coronavirus ; Investors dismiss prospect of 'V-shaped' recovery](#)
- [Oil Stockpiles Are Enormous ; The Oil Countries Suffering Most From The Oil Price Crash](#)
- [How To Align Investments To A Greater Purpose](#)
- [Private investment needed to rebuild the economy ; South Africa Sees Debt Topping 100% of GDP in 2025 ; UK debt is now higher than the country's entire GDP for the first time in 57 years](#)

## ALTERNATIVES

- [Hedge funds are starting to wind down ; SEC freezes Hvizdzak hedge fund, alleges fraud](#)
- [Bad Economy? Unleash Private Equity ; Financial wizardry breathes magic into private equity returns ; Private equity 'barbarians' weigh the risks of Covid-19 takeovers](#)
- [Experts react to bullish blockchain survey by Deloitte ; Is the Bitcoin ETF coming? Change of leadership at the SEC; Anthony Pompliano Continues Push for Pension Fund Crypto Allocation ; Gov't's move to tax cryptocurrency faces backlash ; SEC Issues Emergency Halt to Cryptocurrency Fund](#)
- [Is commercial real estate headed for a crash?](#)

## ABOUT THE BROADCAST RETIREMENT NETWORK



The Broadcast Retirement Network (BRN) is the first lifestyle media platform focused on helping Americans achieve financial independence and to make retirement and savings culturally relevant. The content is informative and engages the viewer. Most importantly - No agendas, no sales pitches, no product pushes.

Our morning show, BRN AM, provides an assessment of daily issues so that Americans can create a plan of action for themselves and their families. BRN AM focuses on delivering headline news via brief interviews with real Americans working toward their financial goals.

Unlike financial shows which prioritize institutional investment managers and public policy organizations, BRN AM is a lifestyle show that brings the stories and ideas of regular Americans to the forefront. We engage with a range of topics pertaining to retirement, focusing individual episodes on personal finance, healthcare, social security, home-ownership and so on to provide viewers with the full picture regarding the future of financial security in America.

*The hyperlinks above take you to internet site(s) sponsored and maintained by independent third parties that are unaffiliated with The Morning Pulse, Inc. The hyperlinks as provided are maintained to provide the author(s) and their respective organizations the proper attribution for developing the original content. The links and content provided in The Morning Pulse and The Weekly Pulse are for general reference and educational purposes only. Although we believe the content provider to be a reliable source of information, we do not guarantee the accuracy of the information or warranty the representations of such Websites. The information available through these Web sites has not been prepared by nor does The Morning Pulse, Inc. have an ability to alter the content, and content will not be monitored by The Morning Pulse, Inc. in the future. The Morning Pulse, Inc. assumes no responsibility for the use of or inability to use such site and recommends you review the terms, conditions, and privacy policy applying to your use of the site. Expression of opinions contained on these hyperlinks may or may not be consistent with the opinions of The Morning Pulse, Inc.*



[UNSUBSCRIBE](#)

Copyright © 2020 The Morning Pulse, Inc., All rights reserved.

---

This email was sent to [dbaker@sunnyvale.ca.gov](mailto:dbaker@sunnyvale.ca.gov)  
[why did I get this?](#) [unsubscribe from this list](#) [update subscription preferences](#)  
The Morning Pulse, Inc. · 4 Beacon Way · Jersey City, NJ 07304 · USA



**From:** [CyberScoop](#)  
**To:** [jleung@sunnyvale.ca.gov](mailto:jleung@sunnyvale.ca.gov)  
**Subject:** Here's what John Bolton wrote about U.S. cybersecurity policy  
**Date:** Monday, June 22, 2020 9:49:20 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

MONDAY, JUNE 22, 2020



*John Bolton dishes on cybersecurity policy in his new book. "Blue Leaks" looks to dump data on cops. A 'malware' attack hits a big health care provider outside Philly. This is CyberScoop for Monday, June 22.*



## Inside the cyber portions of John Bolton's book

In his new book, former national security adviser John Bolton says that squabbling amongst Trump administration officials hobbled the White House's efforts to issue new policies that shaped the U.S. government's offensive and defense cyber-operations. Although

Bolton eliminated the cybersecurity coordinator role, he portrays himself as being crucial to pushing updates to the U.S. government's cyber policies, while portraying other officials as impediments to progress. He also paints President Donald Trump as preoccupied and angered by cybersecurity-related issues, as well as all too willing to use hacking to prop up his political goals in negotiations with China and Ukraine. **Shannon Vavra has it all.**

#### **Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

### **Here's what 'Blue Leaks' is about**

The “Distributed Denial of Secrets” group marked Juneteenth, the June 19 holiday marking the end of slavery in the U.S., by publishing a searchable database containing 269 GB of data apparently stolen from more than 200 law enforcement agencies. The database, which the group has named “Blue Leaks,” appears to contain police training materials, police safety guidelines and protest containment strategies. The file appear to originate with a Texas web development firm that provides services to police information sharing centers. **Jeff Stone has the latest.**

---

SPONSORED BY SYNACK

### **How Oak Ridge National Lab DevSecOps team mobilized amid pandemic**

When the coronavirus pandemic required federal offices to start closing, Oak Ridge National Laboratory — the largest Department of Energy science and energy laboratory — all but 1,000 of the lab's 6,000 staff suddenly needed to conduct their work remotely. The lab's IT department was forced to quickly implement solutions to maintain continuity of operations while also supporting a newly mobile workforce. Oak Ridge National Laboratory's CISO shares

steps the research institute took to ensure security and integrity of its data.

**[Listen to more from Kevin Kerr.](#)**

**Define the Future of Government at Think Gov 2020, July 1**

Join IT leaders from across public sector at Think Gov 2020, a digital event experience, that will address how revolutionary technologies like supercomputing, artificial intelligence and IoT are driving rapid, high-performance solutions and services. Also hear perspectives from security leaders on the rapid shift to a remote workforce and the added need for cybersecurity.

[Register now to be a part of this conversation on July 1.](#)

## **Another health care organization needs a security prescription**

The computer systems of Crozer-Keystone Health System, which owns four hospitals in the Philadelphia suburbs, were hit with an attack, a spokesman for the organization confirmed Friday. Crozer-Keystone was mum on details on the attack, but did say they had “isolated the intrusion.” It was unclear what impact, if any, the incident had on the hospitals. A nascent ransomware gang known as NetWalker, which has had a habit of attacking health organizations, claimed responsibility. **[Sean Lyngaas has the details.](#)**

---

## **NSA tests a plan to secure web technology**

In an effort to protect the U.S. defense industrial base from hacking threats, the National Security Agency has launched a pilot program on securing Domain Name System use for contractors. The NSA’s secure DNS pilot is meant to provide secure services to small- and medium-sized companies working on Department of Defense weapons technologies, says Anne Neuberger, the chief of the NSA’s Cybersecurity Directorate. The pilot comes amid a broader push from the U.S. government to bolster government defenses against threat actors’ efforts to exploit DNS. **[Shannon walks through it.](#)**

---



## **This time, hackers are behind a Wells Fargo fraud campaign**

Hackers are aiming to infect Wells Fargo customers with malicious software by sending phishing emails that appear to be from members of the bank's security team. Some 15,000 people have received messages that contain malicious calendar invites which direct recipients to websites where visitors are prompted to enter their username, password, banking PINs and account data, according to Abnormal Security. In a statement to CyberScoop, Wells Fargo says it's aware of the effort. "We encourage our customers who receive suspicious emails to not respond, click on any links, or open any attachments in any format," the bank said. **[Find the full explanation here.](#)**

---

## **Web skimming is becoming even more annoying**

Web skimming — injecting commerce sites with code to steal data — is a well-worn tradition for cybercriminals. Kaspersky researchers just revealed a twist to the technique. Instead of redirecting stolen data to third-party sources, hackers are sending it to official Google Analytics accounts. It allows them to cover their tracks, in part because the Analytics accounts are something legitimate sites use to track users. Scammers used this technique to hit two dozen websites around the world, including stores selling food products and cosmetics in Europe and North and South America. **[Here's the blog.](#)**

---

## **Tweet of the Day**

Image

Technology solves another worldwide mystery.

---

*[Want more? Catch our events for all things cybersecurity!](#)*

Copyright (c) 2020 CyberScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)



**From:** StateScoop  
**To:** [jleung@sunnyvale.ca.gov](mailto:jleung@sunnyvale.ca.gov)  
**Subject:** Nonprofit groups push back on planned cuts to D.C.'s digital equity programs  
**Date:** Monday, June 22, 2020 9:23:46 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

MONDAY, JUNE 22, 2020



## Not so fast on the budget cuts, D.C.

Seventeen community organizations in Washington, D.C., are pushing back against a proposal from Mayor Muriel Bowser that would remove all funding for the city's primary digital inclusion programs from the city's budget in 2021. Bowser, forced by the pandemic to cut spending, proposed slashing \$678,000 from D.C.'s programs that help low-income communities access the internet. But a letter from the 17 groups warned that such a move would only set

back the city's residents even further. "Things will get worse," it read. **Ryan Johnston reports.**

**Governments can't stop, so Verizon won't stop.**

Getting vital information to the public is imperative. Having a reliable network is too. When you can rely on your network, you're ready.

[See how.](#)

## North Carolina CIO heads for the exit

North Carolina Chief Information Officer Tracy Doaks will step down July 31 to take over as president of the broadband advocacy nonprofit MCNC, Gov. Roy Cooper announced Wednesday. Doaks, who was appointed as the state's deputy CIO in 2015 and took over the North Carolina Department of Information Technology's top job in February, is the second statewide CIO to step down this month, following longtime Wisconsin IT chief David Cagigal, [who departed last week](#). Cooper's office plans to name Doaks' successor in the next few weeks. **Colin Wood reports.**

---

## Trove of police files leaked

An anonymous hacktivist group says it's published a trove of sensitive law enforcement data that originated with hundreds of police departments in an apparent effort to expose police abuses amid ongoing demonstrations through the U.S., CyberScoop's Jeff Stone reports. The "Distributed Denial of Secrets" group marked Juneteenth, which celebrates the end of slavery, by publishing a searchable database containing 269 GB of data apparently stolen from more than 200 law enforcement agencies. "Blue Leaks," as the group calls the the database, contains police training materials, police safety guidelines and protest containment strategies collected from state and local law enforcement agencies around the country. **Read more on CyberScoop.**

**Governments rely on Verizon to keep remote employees connected.**

We rely on governments to keep our country running. So having a reliable network is critical. When you can rely on your network, you're ready. [See how.](#)

---

SPONSORED BY CISCO

## Remote work could be here to stay

Governors across the country have made the call to reopen their states and lift stay-at-home orders put in place during the start of the coronavirus pandemic. State and local CIOs, who rushed into action to rapidly move government workforces to telework face new challenges now as the next normal begins. In this special report, StateScoop and EdScoop look into what's next for the remote workforce, how governments and universities are moving forward and what to expect next. **[See the full report.](#)**

---

*[Want more? Catch our events for all things state and local!](#)*

Copyright (c) 2020 StateScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

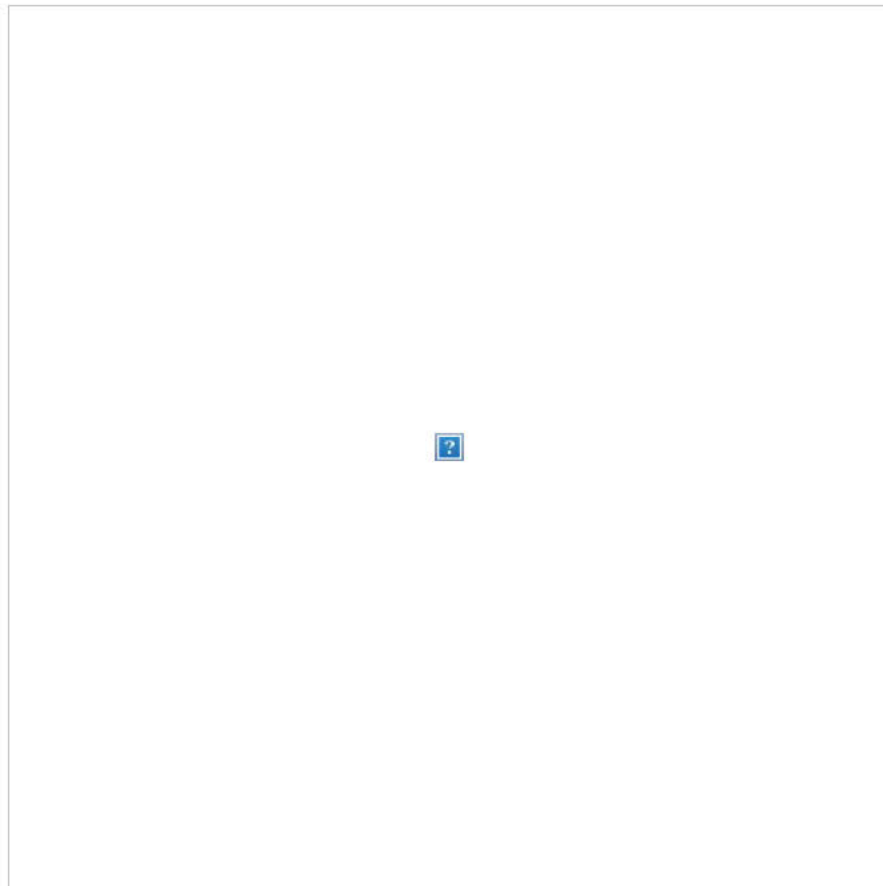
Update your [email preferences](#)  
[Unsubscribe](#)

**From:** [StateScoop](#)  
**To:** [smorton@ci.sunnyvale.ca.us](mailto:smorton@ci.sunnyvale.ca.us)  
**Subject:** Nonprofit groups push back on planned cuts to D.C.'s digital equity programs  
**Date:** Monday, June 22, 2020 9:22:41 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

MONDAY, JUNE 22, 2020



## Not so fast on the budget cuts, D.C.

Seventeen community organizations in Washington, D.C., are pushing back against a proposal from Mayor Muriel Bowser that would remove all funding for the city's primary digital inclusion programs from the city's budget in 2021. Bowser, forced by the pandemic to cut spending, proposed slashing \$678,000 from D.C.'s programs that help low-income communities access the internet. But a letter from the 17 groups warned that such a move would only set



back the city's residents even further. "Things will get worse," it read. **Ryan Johnston reports.**

**Governments can't stop, so Verizon won't stop.**

Getting vital information to the public is imperative. Having a reliable network is too. When you can rely on your network, you're ready.

[See how.](#)

## North Carolina CIO heads for the exit

North Carolina Chief Information Officer Tracy Doaks will step down July 31 to take over as president of the broadband advocacy nonprofit MCNC, Gov. Roy Cooper announced Wednesday. Doaks, who was appointed as the state's deputy CIO in 2015 and took over the North Carolina Department of Information Technology's top job in February, is the second statewide CIO to step down this month, following longtime Wisconsin IT chief David Cagigal, [who departed last week](#). Cooper's office plans to name Doaks' successor in the next few weeks. **Colin Wood reports.**

---

## Trove of police files leaked

An anonymous hacktivist group says it's published a trove of sensitive law enforcement data that originated with hundreds of police departments in an apparent effort to expose police abuses amid ongoing demonstrations through the U.S., CyberScoop's Jeff Stone reports. The "Distributed Denial of Secrets" group marked Juneteenth, which celebrates the end of slavery, by publishing a searchable database containing 269 GB of data apparently stolen from more than 200 law enforcement agencies. "Blue Leaks," as the group calls the the database, contains police training materials, police safety guidelines and protest containment strategies collected from state and local law enforcement agencies around the country.

**[Read more on CyberScoop.](#)**

**Governments rely on Verizon to keep remote employees connected.**

We rely on governments to keep our country running. So having a reliable network is critical. When you can rely on your network, you're ready. [See how.](#)



---

SPONSORED BY CISCO

## Remote work could be here to stay

Governors across the country have made the call to reopen their states and lift stay-at-home orders put in place during the start of the coronavirus pandemic. State and local CIOs, who rushed into action to rapidly move government workforces to telework face new challenges now as the next normal begins. In this special report, StateScoop and EdScoop look into what's next for the remote workforce, how governments and universities are moving forward and what to expect next. **See the full report.**

---

*[Want more? Catch our events for all things state and local!](#)*

Copyright (c) 2020 StateScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)

**From:** StateScoop  
**To:** [lvo@sunnyvale.ca.gov](mailto:lvo@sunnyvale.ca.gov)  
**Subject:** Nonprofit groups push back on planned cuts to D.C.'s digital equity programs  
**Date:** Monday, June 22, 2020 9:06:59 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

MONDAY, JUNE 22, 2020



## Not so fast on the budget cuts, D.C.

Seventeen community organizations in Washington, D.C., are pushing back against a proposal from Mayor Muriel Bowser that would remove all funding for the city's primary digital inclusion programs from the city's budget in 2021. Bowser, forced by the pandemic to cut spending, proposed slashing \$678,000 from D.C.'s programs that help low-income communities access the internet. But a letter from the 17 groups warned that such a move would only set

back the city's residents even further. "Things will get worse," it read. **Ryan Johnston reports.**

**Governments can't stop, so Verizon won't stop.**

Getting vital information to the public is imperative. Having a reliable network is too. When you can rely on your network, you're ready.

[See how.](#)

## North Carolina CIO heads for the exit

North Carolina Chief Information Officer Tracy Doaks will step down July 31 to take over as president of the broadband advocacy nonprofit MCNC, Gov. Roy Cooper announced Wednesday. Doaks, who was appointed as the state's deputy CIO in 2015 and took over the North Carolina Department of Information Technology's top job in February, is the second statewide CIO to step down this month, following longtime Wisconsin IT chief David Cagigal, [who departed last week](#). Cooper's office plans to name Doaks' successor in the next few weeks. **Colin Wood reports.**

---

## Trove of police files leaked

An anonymous hacktivist group says it's published a trove of sensitive law enforcement data that originated with hundreds of police departments in an apparent effort to expose police abuses amid ongoing demonstrations through the U.S., CyberScoop's Jeff Stone reports. The "Distributed Denial of Secrets" group marked Juneteenth, which celebrates the end of slavery, by publishing a searchable database containing 269 GB of data apparently stolen from more than 200 law enforcement agencies. "Blue Leaks," as the group calls the the database, contains police training materials, police safety guidelines and protest containment strategies collected from state and local law enforcement agencies around the country.

**Read more on CyberScoop.**

**Governments rely on Verizon to keep remote employees connected.**

We rely on governments to keep our country running. So having a reliable network is critical. When you can rely on your network, you're ready. [See how.](#)

---

SPONSORED BY CISCO

## Remote work could be here to stay

Governors across the country have made the call to reopen their states and lift stay-at-home orders put in place during the start of the coronavirus pandemic. State and local CIOs, who rushed into action to rapidly move government workforces to telework face new challenges now as the next normal begins. In this special report, StateScoop and EdScoop look into what's next for the remote workforce, how governments and universities are moving forward and what to expect next. **[See the full report.](#)**

---

*[Want more? Catch our events for all things state and local!](#)*

Copyright (c) 2020 StateScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)

**From:** [StateScoop](#)  
**To:** [kbfooster@sunnyvale.ca.gov](mailto:kbfooster@sunnyvale.ca.gov)  
**Subject:** Nonprofit groups push back on planned cuts to D.C.'s digital equity programs  
**Date:** Monday, June 22, 2020 8:46:26 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

READ IN BROWSER

MONDAY, JUNE 22, 2020



## Not so fast on the budget cuts, D.C.

Seventeen community organizations in Washington, D.C., are pushing back against a proposal from Mayor Muriel Bowser that would remove all funding for the city's primary digital inclusion programs from the city's budget in 2021. Bowser, forced by the pandemic to cut spending, proposed slashing \$678,000 from D.C.'s programs that help low-income communities access the internet. But a letter from the 17 groups warned that such a move would only set



back the city's residents even further. "Things will get worse," it read. **Ryan Johnston reports.**

**Governments can't stop, so Verizon won't stop.**

Getting vital information to the public is imperative. Having a reliable network is too. When you can rely on your network, you're ready.

[See how.](#)

## North Carolina CIO heads for the exit

North Carolina Chief Information Officer Tracy Doaks will step down July 31 to take over as president of the broadband advocacy nonprofit MCNC, Gov. Roy Cooper announced Wednesday. Doaks, who was appointed as the state's deputy CIO in 2015 and took over the North Carolina Department of Information Technology's top job in February, is the second statewide CIO to step down this month, following longtime Wisconsin IT chief David Cagigal, [who departed last week](#). Cooper's office plans to name Doaks' successor in the next few weeks. **Colin Wood reports.**

---

## Trove of police files leaked

An anonymous hacktivist group says it's published a trove of sensitive law enforcement data that originated with hundreds of police departments in an apparent effort to expose police abuses amid ongoing demonstrations through the U.S., CyberScoop's Jeff Stone reports. The "Distributed Denial of Secrets" group marked Juneteenth, which celebrates the end of slavery, by publishing a searchable database containing 269 GB of data apparently stolen from more than 200 law enforcement agencies. "Blue Leaks," as the group calls the the database, contains police training materials, police safety guidelines and protest containment strategies collected from state and local law enforcement agencies around the country.

**[Read more on CyberScoop.](#)**

**Governments rely on Verizon to keep remote employees connected.**

We rely on governments to keep our country running. So having a reliable network is critical. When you can rely on your network, you're ready. [See how.](#)

---

SPONSORED BY CISCO

## Remote work could be here to stay

Governors across the country have made the call to reopen their states and lift stay-at-home orders put in place during the start of the coronavirus pandemic. State and local CIOs, who rushed into action to rapidly move government workforces to telework face new challenges now as the next normal begins. In this special report, StateScoop and EdScoop look into what's next for the remote workforce, how governments and universities are moving forward and what to expect next. **[See the full report.](#)**

---

*[Want more? Catch our events for all things state and local!](#)*

Copyright (c) 2020 StateScoop, All rights reserved.

Scoop News Group  
2001 K Street NW  
Washington DC

Update your [email preferences](#)  
[Unsubscribe](#)

**From:** [ZDNet](#)  
**To:** [michael spath](#)  
**Subject:** Over a million police, FBI files leaked online  
**Date:** Monday, June 22, 2020 8:06:43 AM

---

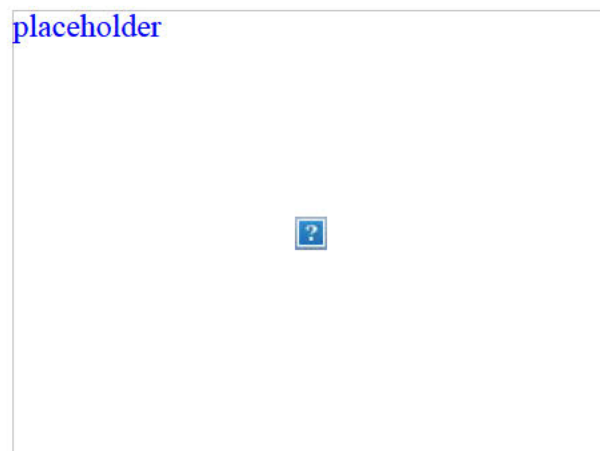
ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



## ZDNet Tech Today

June 22, 2020

placeholder



Apple's online-only WWDC 2020: What to expect and how to watch



Adobe wants users to uninstall Flash Player by the end of the year

## BlueLeaks: Data from 200 US police departments and fusion centers published online

[READ FULL STORY](#)



Programming languages: Julia touts its speed edge over Python and R



Samsung Blu-ray players are rebooting in a loop and nobody knows why

### RELATED

- [400 organizations sign open letter to save Open Technology Fund \(OTF\)](#)
- [There's been a huge spike in online shopping. Now scammers are cashing in, too](#)
- [Microsoft buys IoT security firm CyberX](#)



No, no one has secretly installed a COVID-19 tracker onto your smartphone

---

placeholder



How Salesforce plans to make virtual TrailheaDX 2020 a better, more meaningful tech conference

[READ FULL STORY](#)

placeholder



How tech is making justice virtual

[WATCH THE VIDEO](#)

placeholder



You want diversity, inclusion in tech? Embrace remote work

[READ FULL STORY](#)

placeholder



The best cheap web hosting services: How to find the right provider

[READ FULL STORY](#)

---

THIS WEEK ON ZD NET



## Security

1. Microsoft: These hackers got from a broken password to full control of a network -- in just days



2. [Academics studied DDoS takedowns and said they're ineffective, recommend patching vulnerable servers](#)
3. [AMD says it will fix new CPU bugs by the end of June 2020](#)
4. [CSIRO's Data61 develops voice detection technique to prevent voice spoofing attacks](#)

[See more >](#)



## TechRepublic

1. [GitHub's new "super linter" could make inconsistent code a thing of the past](#)
2. [Apple re-closing several stores in US due to COVID-19 spikes](#)
3. [CCPA: How to prepare for California's new privacy law before enforcement starts July 1](#)
4. [Why do we feel compelled to wave goodbye on Zoom?](#)

[Read more >](#)

IN CASE YOU MISSED IT	
-----------------------	--

**One in four enterprises will be all-cloud companies within a year**



placeholder

Cloud surges, and with it, interest in microservices and Site Reliability Engineering. However, serverless computing remains an open question.

[READ FULL STORY](#)

#### MORE SPONSORED RESEARCH

### Hardware decommissioning policy

Tools & Templates from [TechRepublic Premium](#)

[VIEW THIS NOW](#)

### Brute force and dictionary attacks: A guide for IT leaders

eBooks from [TechRepublic Premium](#)

[DOWNLOAD NOW](#)

### 2020 IT budget research report: Security, cloud services, and digitalization are top...

Research from [TechRepublic Premium](#)

[DOWNLOAD NOW](#)

### AWS re:Invent 2015: Highlights and analysis

eBooks from [TechRepublic Premium](#)

[DOWNLOAD NOW](#)

This newsletter is a service of ZDNet.com.  
To update your account, please visit our  
Subscription Center.

[Unsubscribe](#) | [Help](#) | [Privacy policy](#)

[Trouble viewing this?](#) [Read Online](#)

Copyright CBS Interactive, Inc.  
All rights reserved. ZDNet is a registered service  
mark of CBS Interactive, Inc.

ZDNet  
235 Second Street  
San Francisco, CA 94105  
U.S.A.

**From:** [HTCC](#) on behalf of [jeff.hall---](#) via [HTCC](#)  
**To:** [HTCC Listserv](#)  
**Cc:** [jeff.hall@wesbeyassoc.com](mailto:jeff.hall@wesbeyassoc.com)  
**Subject:** [HTCC] "BlueLeaks" Exposes Files from Hundreds of Police Departments  
**Date:** Monday, June 22, 2020 5:28:50 AM  
**Attachments:** [Untitled attachment 00288.txt](#)

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

<https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/>

Jeff Hall, senior consultant  
wesbey associates llc  
O: 952-934-6167 M: 612-719-4340  
[jeff.hall@wesbeyassoc.com](mailto:jeff.hall@wesbeyassoc.com)  
[www.wesbeyassoc.com](http://www.wesbeyassoc.com)

If you have received this email in error, please immediately notify the sender by return email and delete this email from your system. This email and any attachments may contain confidential or legally privileged information that is intended only for the individual(s) named in this email. If you are not the intended recipient, or an authorized representative of the intended recipient, you are hereby notified that any review, dissemination, disclosure, copying or reliance upon the contents of this email or its attachments is strictly prohibited.

**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of June 1, 2020  
**Date:** Monday, June 08, 2020 11:50:10 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of June 1, 2020](#)

06/08/2020 06:56 AM EDT

Original release date: June 8, 2020

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
asus -- aura_sync	Ene.sys in Asus Aura Sync through 1.07.71 does not properly validate input to IOCTL 0x80102044, 0x80102050, and 0x80102054, which allows local users to cause a denial of service (system crash) or gain privileges via IOCTL requests using crafted kernel addresses that trigger memory corruption.	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-17603</a> <a href="#">MISC</a>
cisco -- ios_xe_software	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute	2020-06-03	<a href="#">7.2</a>	<a href="#">CVE-2020-3207</a> <a href="#">CISCO</a>

	malicious code on an affected device with root-level privileges.			
cisco -- ios_xe_software	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	2020-06-03	<a href="#">7.2</a>	<a href="#">CVE-2020-3214</a> <a href="#">CISCO</a>
clearpass -- policy_manager	The ClearPass Policy Manager web interface is affected by a vulnerability that leads to authentication bypass. Upon successful bypass an attacker could then execute an exploit that would allow to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">10</a>	<a href="#">CVE-2020-7115</a> <a href="#">MISC</a>
clearpass -- policy_manager	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-7116</a> <a href="#">MISC</a>
clearpass -- policy_manager	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-7117</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices allow Command Injection.	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-13782</a> <a href="#">MISC</a>
docker -- engine	An issue was discovered in Docker Engine before 19.03.11. An attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service.	2020-06-02	<a href="#">7.5</a>	<a href="#">CVE-2020-13401</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows attackers to write arbitrary data	2020-06-	<a href="#">7.5</a>	<a href="#">CVE-2014-7175</a>



	to fsUI.xyz via fsSaveUIPersistence.php.	01		<a href="#">MISC</a>
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows command injection via shell metacharacters to sysSaveMonitorData.php, fsx25MonProxy.php, syseditdate.php, iframeupload.php, or sysRestoreX25Cplt.php.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2014-7173</a> <a href="#">MISC</a>
fortinet -- fortia- s/w2_and_fortiap-u	An improper input validation in FortiAP-S/W2 6.2.0 to 6.2.2, 6.0.5 and below, FortiAP-U 6.0.1 and below CLI admin console may allow unauthorized administrators to overwrite system files via specially crafted tcpdump commands in the CLI.	2020-06-01	<a href="#">8.5</a>	<a href="#">CVE-2019-15709</a> <a href="#">MISC</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has an out-of-bounds write when Internet Explorer is used.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2019-20830</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, an Integer Overflow to Buffer Overflow exists. When using /video redirection, a manipulated server can instruct the client to allocate a buffer with a smaller size than requested due to an integer overflow in size calculation. With later messages, the server can manipulate the client to write data out of bound to the previously allocated buffer. This has been patched in 2.1.0.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-11038</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, when using a manipulated server with USB redirection enabled (nearly) arbitrary memory can be read and written due to integer overflows in length checks. This has been patched in 2.1.0.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-11039</a> <a href="#">CONFIRM</a>
gesio -- erp	There is an improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in php files of GESIO ERP. GESIO ERP all versions prior to 11.2 allows malicious users to retrieve all database information.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2020-8967</a> <a href="#">CONFIRM</a>
github -- enterprise_server	An improper access control vulnerability was identified in the GitHub Enterprise Server API that allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.21 and was fixed in 2.20.9, 2.19.15, and 2.18.20. This	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-10516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	vulnerability was reported via the GitHub Bug Bounty program.			
ibm -- security_guardium	IBM Security Guardium 11.1 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 174735.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-4180</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174732.	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-4177</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
micro_focus -- service_management_authentication	There is an Incorrect Authorization vulnerability in Micro Focus Service Management Automation (SMA) product authentication version 2018.05 to 2020.02. The vulnerability could be exploited to provide unauthorized access to the Container Deployment Foundation.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-11844</a> <a href="#">CONFIRM</a>
piwigo -- lexiglot	admin.php?page=projects in Lexiglot through 2014-11-20 allows command injection via username and password fields.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2014-8945</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows SQL injection via an admin.php?page=users&from_id= or admin.php?page=history&limit= URI.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2014-8941</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Improper permissions in XBL_SEC region enable user to update XBL_SEC code and data and divert the RAM dump path to normal cold boot path in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM8150, SXR1130, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14054</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	2020-06-02	<a href="#">7.8</a>	<a href="#">CVE-2020-3645</a>

	Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130			<a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3618</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3625</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-06-02	<a href="#">7.5</a>	<a href="#">CVE-2020-3615</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow in calculating estimated output buffer size when getting a list of installed Feature IDs, Serial Numbers or checking Feature ID status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9205, MDM9607, Nicobar, QCS404, QCS405, Rennell, SA6155P, SC7180, SC8180X, SDX55, SM6150, SM7150, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14066</a> <a href="#">CONFIRM</a>
	Array out of bound may occur while playing mp3 file as no check is there on			

qualcomm -- multiple_snapdragon_products	offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	10	<a href="#">CVE-2020-3633</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	10	<a href="#">CVE-2020-3641</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150	2020-06-02	7.2	<a href="#">CVE-2020-3616</a> <a href="#">CONFIRM</a>
qualcomm --	Failure in buffer management while accessing handle for HDR blit when color			<a href="#">CVE-2019-</a>

multiple_snapdragon_products	modes not supported by display in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, QCS605	2020-06-02	<a href="#">7.2</a>	<a href="#">14087 CONFIRM</a>
qualcomm --sm8250_and_sxr2130	kernel failure due to load failures while devices v1 path directly via kernel in Snapdragon Mobile in SM8250, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3623 CONFIRM</a>
quickbox --quickbox_community_and_pro_editions	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user has sudo privileges and can execute commands as root without a password, which allows an attacker to obtain sensitive information via a grep of a /root/*.db or /etc/shadow file.	2020-06-01	<a href="#">9</a>	<a href="#">CVE-2020-13695 MISC</a>
quickbox --quickbox_community_and_pro_editions	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user can execute sudo and sql without a password, which means that the www-data user can execute arbitrary OS commands via the mysql -e option.	2020-06-01	<a href="#">9</a>	<a href="#">CVE-2020-13694 MISC</a>
quickbox --quickbox_community_and_pro_editions	QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8 allows <del>and authenticates</del> remote attacker to execute code on the server via command injection in the servicestart parameter.	2020-06-01	<a href="#">9</a>	<a href="#">CVE-2020-13448 MISC MISC</a>
rconfig -- rconfig	rConfig 3.9.4 and previous versions has unauthenticated devices.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-10548 MISC</a>
rconfig -- rconfig	rConfig 3.9.4 and previous versions has unauthenticated snippets.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-10549 MISC</a>
rconfig -- rconfig	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicies.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-10546 MISC</a>
	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicyelements.inc.php SQL			<a href="#">CVE-2020-</a>



rconfig -- rconfig	injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">10547 MISC</a>
sabberworm -- php_css_parser	Sabberworm PHP CSS Parser before 8.3.1 calls eval on uncontrolled data, possibly leading to remote code execution if the function allSelectors() or getSelectorsBySpecificity() is called with input from an attacker.	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-13756 MISC MISC MISC MISC</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with Q(10.0) (with TEEGRIS on Exynos chipsets) software. The Widevine Trustlet allows arbitrary code execution because of memory disclosure, The Samsung IDs are SVE-2020-17117, SVE-2020-17118, SVE-2020-17119, and SVE-2020-17161 (June 2020).	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-13832 CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software. The Trustonic Kinibi component allows arbitrary memory mapping. The Samsung ID is SVE-2019-16665 (June 2020).	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-13831 CONFIRM</a>
swarco -- cpu_ls4000_series	An open port used for debugging in SWARCOs CPU LS4000 Series with versions starting with G4... grants root access to the device without access control via network. A malicious user could use this vulnerability to get access to the device and disturb operations with connected devices.	2020-05-29	<a href="#">10</a>	<a href="#">CVE-2020-12493 CONFIRM</a>
systemd -- systemd	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-100082.	2020-06-03	<a href="#">10</a>	<a href="#">CVE-2020-13776 MISC</a>
verizon -- serialize-javascript	serialize-javascript prior to 3.1.0 allows remote attackers to inject arbitrary code via the function "deleteFunctions" within "index.js".	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2020-7660 MISC</a>
wordpress -- wordpress	An unauthenticated privilege-escalation issue exists in the bbPress plugin before 2.6.5 for WordPress when New User Registration is enabled.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-13693 MISC MISC MISC MISC</a>

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2pisoftware -- cmfive	system/classes/DbPDO.php in Cmfive through 2015-03-15, when database connectivity malfunctions, allows remote attackers to obtain sensitive information (username and password) via any request, such as a password reset request.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2014-9702</a> <a href="#">MISC</a>
apache -- ignite	Apache Ignite uses H2 database to build SQL distributed execution engine. H2 provides SQL functions which could be used by attacker to access to a filesystem.	2020-06-03	<a href="#">6.4</a>	<a href="#">CVE-2020-1963</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
atlassian -- companion_app	The file downloading functionality in the Atlassian Companion App before version 1.0.0 allows remote attackers, who control a Confluence Server instance that the Companion App is connected to, execute arbitrary .exe files via a Protection Mechanism Failure.	2020-06-01	<a href="#">6.5</a>	<a href="#">CVE-2020-4020</a> <a href="#">MISC</a>
atlassian -- companion_app	The file editing functionality in the Atlassian Companion App before version 1.0.0 allows local attackers to have the app run a different executable in place of the app's cmd.exe via a untrusted search path vulnerability.	2020-06-01	<a href="#">4.4</a>	<a href="#">CVE-2020-4019</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /plugins/servlet/jira-blockers/resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get the ID of configured Jira application links via an information disclosure vulnerability.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-4016</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /json/fe/activeUserFinder.do resource in Altassian Fisheye and Crucible before version 4.8.1 allows remote attackers to view user user email addresses via a information disclosure vulnerability.	2020-06-01	<a href="#">4</a>	<a href="#">CVE-2020-4015</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /rest/jira-ril/1.0/jira-rest/applinks resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-4017</a> <a href="#">MISC</a>

	get information about any configured Jira application links via an information disclosure vulnerability.			<a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /profile/deleteWatch.do resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to remove another user's watching settings for a repository via an improper authorization vulnerability.	2020-06-01	<a href="#">4</a>	<a href="#">CVE-2020-4014</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The review coverage resource in Atlassian Fisheye and Crucible before version 4.8.2 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the committerFilter parameter.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2020-4023</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The setup resources in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to complete the setup process via a cross-site request forgery (CSRF) vulnerability.	2020-06-01	<a href="#">6.8</a>	<a href="#">CVE-2020-4018</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- navigator_links	The CustomAppsRestResource list resource in Atlassian Navigator Links before version 3.3.23, from version 4.0.0 before version 4.3.7, from version 5.0.0 before 5.0.1, and from version 5.1.0 before 5.1.1 allows remote attackers to enumerate all linked applications, including those that are restricted or otherwise hidden, through an incorrect authorization check.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-4026</a> <a href="#">MISC</a> <a href="#">MISC</a>
bitrix -- bitrix24	modules/security/classes/general.post_filter.php/post_filter.php in the Web Application Firewall in Bitrix24 through 20.0.950 allows XSS by placing %00 before the payload.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2020-13758</a> <a href="#">MISC</a>
celluloid -- reel	reel through 0.6.1 allows Request Smuggling attacks due to incorrect Content-Length and Transfer encoding header parsing. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks. Note: This project is deprecated, and is not maintained any more.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-7659</a> <a href="#">MISC</a>
cisco -- multiple_products	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-10136</a> <a href="#">CERT-VN</a> <a href="#">MISC</a>

	exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors.			<a href="#">MISC</a>
cisco -- prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database.	2020-06-03	<a href="#">6.4</a>	<a href="#">CVE-2020-3339</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-3322</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-3321</a> <a href="#">CISCO</a>

	user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.			
compound -- finance_compound_price_oracle	The price oracle in PriceOracle.sol in Compound Finance Compound Price Oracle 1.0 through 2.0 allows a price oracle to set an invalid asset price via the setPrice function, and consequently violate the intended limits on price swings.	2020-06-03	5	<a href="#">CVE-2019-20809</a> <a href="#">MISC</a>
cybele -- thinfinity_virtualUI	Cybele Thinfinitiy VirtualUI 2.5.17.2 allows HTTP response splitting via the mimetype parameter within a PDF viewer request, as demonstrated by an example.pdf?mimetype= substring. The victim user must load an application request to view a PDF, containing the malicious payload. This results in a reflected XSS payload being executed.	2020-06-04	4.3	<a href="#">CVE-2019-16385</a> <a href="#">MISC</a>
cybele -- thinfinity_virtualui	Cybele Thinfinitiy VirtualUI 2.5.17.2 allows ../ path traversal that can be used for data exfiltration. This enables files outside of the web directory to be retrieved if the exact location is known and the user has permissions.	2020-06-04	4	<a href="#">CVE-2019-16384</a> <a href="#">MISC</a>
d-link -- dir- 856l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices allow CSRF.	2020-06-03	6.8	<a href="#">CVE-2020-13786</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Transmission of Sensitive Information.	2020-06-03	5	<a href="#">CVE-2020-13787</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Inadequate Encryption Strength.	2020-06-03	5	<a href="#">CVE-2020-13785</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have a predictable seed in a Pseudo-Random Number Generator.	2020-06-03	5	<a href="#">CVE-2020-13784</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Storage of Sensitive Information.	2020-06-03	5	<a href="#">CVE-2020-13783</a> <a href="#">MISC</a>
django-project -- django	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. Query parameters generated by the Django admin ForeignKeyRawIdWidget were not properly URL encoded, leading to a possibility of an XSS attack.	2020-06-03	4.3	<a href="#">CVE-2020-13596</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. In			<a href="#">CVE-2020-</a>



django_project -- django	cases where a memcached backend does not perform key validation, passing malformed cache keys could result in a key collision, and potential data leakage.	2020-06-03	5	<a href="#">13254</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
elastic -- elastic_app_search	Elastic App Search versions before 7.7.0 contain a cross site scripting (XSS) flaw when displaying document URLs in the Reference UI. If the Reference UI injects a URL into a result, that URL will be rendered by the web browser. If an attacker is able to control the contents of such a field, they could execute arbitrary JavaScript in the victim's web browser.	2020-06-03	4.3	<a href="#">CVE-2020-7011</a> <a href="#">N/A</a>
elastic -- elastic_cloud_on_kubernetes	Elastic Cloud on Kubernetes (ECK) versions prior to 1.1.0 generate passwords using a weak random number generator. If an attacker is able to determine when the current Elastic Stack cluster was deployed they may be able to more easily brute force the Elasticsearch credentials generated by ECK.	2020-06-03	5	<a href="#">CVE-2020-7010</a> <a href="#">N/A</a>
elastic -- kibana	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	2020-06-03	6.5	<a href="#">CVE-2020-7013</a> <a href="#">N/A</a>
elastic -- kibana	Kibana versions 6.7.0 to 6.8.8 and 7.0.0 to 7.6.2 contain a prototype pollution flaw in the Upgrade Assistant. An authenticated attacker with privileges to write to the Kibana index could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	2020-06-03	6.5	<a href="#">CVE-2020-7012</a> <a href="#">N/A</a>
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows directory traversal via the log-handling feature.	2020-06-01	5	<a href="#">CVE-2014-7174</a> <a href="#">MISC</a>
fastecdsa -- fastecdsa	An issue was discovered in fastecdsa before 2.1.2. When using the NIST P-256 curve in the ECDSA implementation, the point at infinity is mishandled. This means that for an extreme value in k and s <sup>-1</sup> , the signature verification fails even if the signature is correct. This behavior is not solely a usability problem. There are	2020-06-02	5	<a href="#">CVE-2020-12607</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	some threat models where an attacker can benefit by successfully guessing users for whom signature verification will fail.			<a href="#">CONFIRM</a>
fortiguard -- forticlient_for_windows	An Insecure Temporary File vulnerability in FortiClient for Windows 6.2.1 and below may allow a local user to gain elevated privileges via exhausting the pool of temporary file names combined with a symbolic link attack.	2020-06-01	<a href="#">4.6</a>	<a href="#">CVE-2020-9291</a> <a href="#">MISC</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20813</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows stack consumption via nested function calls for XML parsing.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20815</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20816</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows memory consumption because data is created for each page of an application level.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20814</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac_and_foxit_reader_for_mac	An issue was discovered in Foxit PhantomPDF Mac and Foxit Reader for Mac before 9.7. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13803</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows memory consumption because data is created for each page of an application level.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20818</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20837</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has homograph mishandling.	2020-06-04	<a href="#">4.3</a>	<a href="#">CVE-2019-20835</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20820</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has a use-after-free because of JavaScript execution after a deletion or close operation.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13806</a> <a href="#">CONFIRM</a>

foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has circular reference mishandling that causes a loop.	2020-06-04	5	<a href="#">CVE-2020-13807</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via crafted cross-reference stream data.	2020-06-04	5	<a href="#">CVE-2020-13808</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via long strings in the content stream.	2020-06-04	5	<a href="#">CVE-2020-13809</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference.	2020-06-04	5	<a href="#">CVE-2019-20817</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows stack consumption via nested function calls for XML parsing.	2020-06-04	5	<a href="#">CVE-2019-20819</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has brute-force attack mishandling because the CAS service lacks a limit on login failures.	2020-06-04	5	<a href="#">CVE-2020-13805</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	2020-06-04	5	<a href="#">CVE-2019-20828</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	2020-06-04	5	<a href="#">CVE-2019-20829</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has mishandling of cloud credentials, as demonstrated by Google Drive.	2020-06-04	5	<a href="#">CVE-2019-20836</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows information disclosure of a hardcoded username and password in the DocuSign plugin.	2020-06-04	6.8	<a href="#">CVE-2020-13804</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, when running with logger set to "WLOG_TRACE", a possible crash of application could occur due to a read of an invalid array index. Data could be printed as string to local terminal. This has been fixed in 2.1.0.	2020-05-29	5	<a href="#">CVE-2020-11019</a> <a href="#">CONFIRM</a>
	In FreeRDP before 2.1.0, there is an out-of-bounds read in			<a href="#">CVE-2020-</a>

freerdp -- freerdp	clipdr_read_format_list. Clipboard format data read (by client or server) might read data out-of-bounds. This has been fixed in 2.1.0.	2020-05-29	<a href="#">6.4</a>	<a href="#">11085</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_NegotiateMessage. This has been fixed in 2.1.0.	2020-05-29	<a href="#">5.5</a>	<a href="#">CVE-2020-11088</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_AuthenticateMessage. This has been fixed in 2.1.0.	2020-05-29	<a href="#">5.5</a>	<a href="#">CVE-2020-11087</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_ntlm_v2_client_challenge that reads up to 28 bytes out-of-bound to an internal structure. This has been fixed in 2.1.0.	2020-05-29	<a href="#">5.5</a>	<a href="#">CVE-2020-11086</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bounds read in rfx_process_message_tileset. Invalid data fed to RFX decoder results in garbage on screen (as colors). This has been patched in 2.1.0.	2020-05-29	<a href="#">5</a>	<a href="#">CVE-2020-11043</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound data read from memory in clear_decompress_subcode_rlex, visualized on screen as color. This has been patched in 2.1.0.	2020-05-29	<a href="#">4</a>	<a href="#">CVE-2020-11040</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, an outside controlled array index is used unchecked for data used as configuration for sound backend (alsa, oss, pulse, ...). The most likely outcome is a crash of the client instance followed by no or distorted sound or a session disconnect. If a user cannot upgrade to the patched version, a workaround is to disable sound for the session. This has been patched in 2.1.0.	2020-05-29	<a href="#">4</a>	<a href="#">CVE-2020-11041</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP before 2.1.0, there is an out-of-bound read in irp functions (parallel_process_irp_create, serial_process_irp_create, drive_process_irp_write, printer_process_irp_write, rdpei_rcv_pdu, serial_process_irp_write). This has been fixed in 2.1.0.	2020-05-29	<a href="#">6.5</a>	<a href="#">CVE-2020-11089</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- chrome	Incorrect implementation in permissions in Google Chrome prior to 80.0.3987.87	2020-06-	<a href="#">4.3</a>	<a href="#">CVE-2020-6502</a>

	allowed a remote attacker to spoof security UI via a crafted HTML page.	03		<a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.97 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6495</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass AppCache security restrictions via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6499</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in interstitials in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6500</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds write in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6419</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in CSP in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6501</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use after free in WebAuthentication in Google Chrome prior to 83.0.4103.97 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6493</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6453</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in V8 in Google Chrome prior to 14.0.0.0 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2011-2863</a> <a href="#">MISC</a>
google -- chrome	Bad cast in CSS in Google Chrome prior to 11.0.0.0 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2011-1805</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in notifications in Google Chrome prior to 74.0.3729.108 allowed a remote attacker	2020-06-	<a href="#">4.3</a>	<a href="#">CVE-2020-6504</a>



	to bypass notification restrictions via a crafted HTML page.	03		<a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_android	Incorrect security UI in payments in Google Chrome on Android prior to 83.0.4103.97 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6494</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_ios	Incorrect implementation in user interface in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6498</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_ios	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted URI.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6497</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_macos	Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6496</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana_labs -- grafana	The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-13379</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via a link on the "Dashboard > All Panels > General" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18625</a> <a href="#">MISC</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via the "Dashboard > Text Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18623</a> <a href="#">MISC</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via a column style on the "Dashboard > Table Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18624</a> <a href="#">MISC</a>
huawei -- cloudengine_12800_products	CloudEngine 12800 products with versions of V200R019C00, V200R019C10SPC800, V200R019C00SPC600, V200R019C10; and CloudEngine 6800 products with versions of V200R019C00SPC800 have potential of service vulnerability. Due to improper memory management, memory	2020-05-29	<a href="#">5</a>	<a href="#">CVE-2020-1870</a> <a href="#">CONFIRM</a>

	leakage may occur in some special cases. Attackers can perform a series of operations to exploit this vulnerability. Successful exploit may cause a denial of service.			
huawei -- e6878-370_products	E6878-370 products with versions of 10.0.3.1(H557SP27C233) and 10.0.3.1(H563SP1C00) have a stack buffer overflow vulnerability. The program copies an input buffer to an output buffer without verification. An attacker in the adjacent network could send a crafted message, successful exploit could lead to stack buffer overflow which may cause malicious code execution.	2020-05-29	5.8	<a href="#">CVE-2020-1832</a> <a href="#">CONFIRM</a>
huawei -- multiple_products	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario. Affected product versions include: AR120-S versions V200R007C00SPC900, V200R007C00SPCa00	2020-06-01	4	<a href="#">MISC</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178965.	2020-06-02	4.3	<a href="#">CVE-2020-4366</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 179001.	2020-06-02	5	<a href="#">CVE-2020-4367</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182283.	2020-06-02	4.3	<a href="#">CVE-2020-4503</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- qradar_siem	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit	2020-06-04	5.5	<a href="#">CVE-2020-4509</a> <a href="#">XF</a>

	this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182364.			<a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174738.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-4182</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10.6, 11.0, and 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174851.	2020-06-03	<a href="#">4.6</a>	<a href="#">CVE-2020-4190</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 174857.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-4193</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 could disclose sensitive information on the login page that could aid in further attacks against the system. IBM X-Force ID: 174805.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-4187</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174739.	2020-06-04	<a href="#">4.3</a>	<a href="#">CVE-2020-4183</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
istio -- istio	Istio 1.4.x before 1.4.9 and Istio 1.5.x before 1.5.4 contain the following vulnerability when telemetry v2 is enabled: by sending a specially crafted packet, an attacker could trigger a Null Pointer Exception resulting in a Denial of Service. This could be sent to the ingress gateway or a sidecar, triggering a null pointer exception which results in a denial of service. This also affects servicemesh-proxy where a null pointer exception flaw was found in servicemesh-proxy. When running Telemetry v2 (not on by default in version 1.4.x), an attacker could send a specially crafted packet to the ingress gateway or proxy sidecar, triggering a	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-10739</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	denial of service.			
jenkins -- jenkins	Jenkins Play Framework Plugin 1.0.2 and earlier lets users specify the path to the `play` command on the Jenkins master for a form validation endpoint, resulting in an OS command injection vulnerability exploitable by users able to store such a file on the Jenkins master.	2020-06-03	<a href="#">6.5</a>	<a href="#">CVE-2020-2200</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Subversion Partial Release Manager Plugin 1.0.1 and earlier does not escape the error message for the repository URL field form validation, resulting in a reflected cross-site scripting vulnerability.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-2199</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier allows attackers to add or remove agent labels.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-2192</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier does not check permissions on API endpoints that allow adding and removing agent labels.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2191</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not redact encrypted secrets in the 'getConfigAsXML' API URL when transmitting job config.xml data to users without Job/Configure.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2198</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not require users to have Job/ExtendedRead permission to access Inheritance Project job configurations in XML format.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2197</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Selenium Plugin 3.141.59 and earlier has no CSRF protection for its HTTP endpoints, allowing attackers to perform all administrative actions provided by the plugin.	2020-06-03	<a href="#">6</a>	<a href="#">CVE-2020-2196</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	In Joomla! before 3.9.19, lack of input validation in the heading tag option of the "Articles - Newsflash" and "Articles - Categories" modules allows XSS.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13761</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, the default settings of the global textfilter configuration do not block HTML inputs for Guest users.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13763</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, missing token checks in com_postinstall lead to CSRF.	2020-06-02	<a href="#">6.8</a>	<a href="#">CVE-2020-13760</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, incorrect input validation of the module tag option in	2020-06-	<a href="#">4.3</a>	<a href="#">CVE-2020-13762</a>

	com_modules allows XSS.	02		<a href="#">MISC</a>
kubernetes -- containernetworking/plugins	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious containers in Kubernetes clusters to perform man-in-the-middle (MitM) attacks. A malicious container can exploit this flaw by sending rogue IPv6 router advertisements to the host or other containers, to redirect traffic to the malicious container.	2020-06-03	<a href="#">6</a>	<a href="#">CVE-2020-10749</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libjpeg-turbo -- libjpeg-turbo	libjpeg-turbo 2.0.4, and mozjpeg 4.0.0, has a heap-based buffer over-read in get_rgb_row() in rdppm.c via a malformed PPM input file.	2020-06-03	<a href="#">5.8</a>	<a href="#">CVE-2020-13790</a> <a href="#">MISC</a> <a href="#">MISC</a>
libvirt -- libvirt	A NULL pointer dereference was found in the libvirt API responsible introduced in upstream version 3.10.0, and fixed in libvirt 6.0.0, for fetching a storage pool based on its target path. In more detail, this flaw affects storage pools created without a target path such as network-based pools like gluster and RBD. Unprivileged users with a read-only connection could abuse this flaw to crash the libvirt daemon, resulting in a potential denial of service.	2020-06-02	<a href="#">4</a>	<a href="#">CVE-2020-10703</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	go7007_snd_init in drivers/media/usb/go7007/snd-go7007.c in the Linux kernel before 5.6 does not call snd_card_free for a failure path, which causes a memory leak, aka CID-9453264ef586.	2020-06-03	<a href="#">4.9</a>	<a href="#">CVE-2019-20810</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.4.7. The prb_calc_retire_blk_tmo() function in net/packet/af_packet.c can result in a denial of service (CPU consumption and soft lockup) in a certain failure case involving TPACKET_V3, aka CID-b43d1f9f7067.	2020-06-03	<a href="#">4.9</a>	<a href="#">CVE-2019-20812</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki -- mediawiki	resources/src/mediawiki.page.ready/ready.js in MediaWiki before 1.35 allows remote attackers to force a logout and external redirection via HTML content in a MediaWiki page.	2020-06-02	<a href="#">5.8</a>	<a href="#">CVE-2020-10959</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mulesoft -- mulesoft_ce/ee	A Denial of Service vulnerability in MuleSoft Mule CE/EE 3.8.x, 3.9.x, and 4.x released before April 7, 2020, could allow remote attackers to submit data which can lead to resource exhaustion.	2020-05-29	<a href="#">5</a>	<a href="#">CVE-2020-6937</a> <a href="#">CONFIRM</a>



naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/feeds/feed.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13798</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/structure/structure.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13796</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/websites/website.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13797</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows Directory Traversal because lib/packages/templates/template.class.php mishandles ../ and ../ substrings.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-13795</a> <a href="#">MISC</a> <a href="#">MISC</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to delete arbitrary local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5296</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to upload jpg, jpeg, bmp, png, webp, gif, ico, css, js, woff, woff2, svg, ttf, eot, json, md, less, sass, scss, xml files to any directory of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5297</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to read local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5295</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phplist -- phplist	phplist before 3.5.4 allows XSS via /lists/admin/user.php and /lists/admin/users.php.	2020-06-04	<a href="#">4.3</a>	<a href="#">CVE-2020-13827</a> <a href="#">MISC</a>

pi-hole -- pi-hole_web	Pi-hole Web v4.3.2 (aka AdminLTE) allows Remote Code Execution by privileged dashboard users via a crafted DHCP static lease.	2020-05-29	6.5	<a href="#">CVE-2020-8816</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows CSRF.	2020-06-01	6.8	<a href="#">CVE-2014-8942</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows denial of service because api/update.php launches svn update operations that use a great deal of resources.	2020-06-01	5	<a href="#">CVE-2014-8937</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (full path) via an include/smarty/plugins/modifier.date_format.php request if PHP has a non-recommended configuration that produces warning messages.	2020-06-01	4.3	<a href="#">CVE-2014-8939</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (names and details of projects) by visiting the /update.log URI.	2020-06-01	5	<a href="#">CVE-2014-8940</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows SSRF via the admin.php?page=projects svn_url parameter.	2020-06-01	6.5	<a href="#">CVE-2014-8943</a> <a href="#">MISC</a>
playtube -- playtube	PlayTube 1.8 allows disclosure of user details via ajax.php?type=../admin-panel/autoload&page=manage-users directory traversal, aka local file inclusion.	2020-06-03	4	<a href="#">CVE-2020-13792</a> <a href="#">MISC</a>
python-rsa -- python-rsa	Python-RSA 4.0 ignores leading ' ' bytes during decryption of ciphertext. This could conceivably have a security-relevant impact, e.g., by helping an attacker to infer that an application uses Python-RSA, or if the length of accepted ciphertext affects application behavior (such as by causing excessive memory allocation).	2020-06-01	5	<a href="#">CVE-2020-13757</a> <a href="#">MISC</a>
qemu -- qemu	address_space_map in exec.c in QEMU 4.2.0 can trigger a NULL pointer dereference related to BounceBuffer.	2020-06-02	5	<a href="#">CVE-2020-13659</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
qemu -- qemu	hw/pci/msix.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access via a crafted address in an msi-x mmio operation.	2020-06-02	4.6	<a href="#">CVE-2020-13754</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
	A race condition can occur when using			

qualcomm -- multiple_snapdragon_products	the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130	2020-06-02	<a href="#">6.9</a>	<a href="#">CVE-2020-3680</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2020-3630</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2020-3610</a> <a href="#">CONFIRM</a>
	Out of bound memory access while processing qpay due to not validating			

qualcomm -- multiple_snapdragon_processors	length of the response buffer provided by User. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, MSM8909, MSM8998, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845	2020-06-02	4.6	<a href="#">CVE-2019-14078</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_processors	Out of bound memory access while processing ese transmit command due to passing Response buffer received from user in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9607, MDM9650, MSM8909, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	4.6	<a href="#">CVE-2019-14077</a> <a href="#">CONFIRM</a>
rust-vmm -- vm-memory	rust-vmm vm-memory before 0.1.1 and 0.2.x before 0.2.1 allows attackers to cause a denial of service (loss of IP networking) because read_obj and write_obj do not properly access memory. This affects aarch64 (with musl or glibc) and x86_64 (with musl).	2020-06-02	5	<a href="#">CVE-2020-13759</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) software. One UI HOME logging can leak information. The Samsung ID is SVE-2019-16382 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13830</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x) (with TEEGRIS) software. The Gatekeeper Trustlet allows a brute-force attack on user credentials. The Samsung ID is SVE-2020-16908 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13835</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The system area allows arbitrary file overwrites via a symlink attack. The Samsung ID is SVE-2020-17183 (June 2020).	2020-06-04	6.4	<a href="#">CVE-2020-13833</a> <a href="#">CONFIRM</a>

samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. HWRResProvider allows path traversal for data exposure. The Samsung ID is SVE-2020-16954 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13836</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (with TEEGRIS) software. SecureFolder does not properly restrict use of Android Debug Bridge (adb) for arbitrary installations. The Samsung ID is SVE-2020-17369 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13834</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can disable the SEAndroid protection mechanism in the RKP. The Samsung ID is SVE-2019-15998 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13829</a> <a href="#">CONFIRM</a>
synk -- broker	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network by creating symlinks to match whitelisted paths.	2020-05-29	4	<a href="#">CVE-2020-7653</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.73.1 are vulnerable to Information Exposure. It logs private keys if logging level is set to DEBUG.	2020-05-29	4.3	<a href="#">CVE-2020-7654</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.72.2 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users who have access to Snyk's internal network by appending the URL with a fragment identifier and a whitelisted path e.g. `#package.json`	2020-05-29	4	<a href="#">CVE-2020-7648</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network via directory traversal.	2020-05-29	4	<a href="#">CVE-2020-7652</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker after 4.72.0 including and before 4.73.1 are vulnerable to Arbitrary File Read. It allows arbitrary file reads to users with access to Snyk's internal network of any files ending in the following extensions: yaml, yml or json.	2020-05-29	4	<a href="#">CVE-2020-7650</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.79.0 are vulnerable to Arbitrary File Read. It allows partial file reads for users who	2020-05-	4	<a href="#">CVE-2020-7651</a>



	have access to Snyk's internal network via patch history from GitHub Commits API.	29		<a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. An attacker can determine the username (under which the web server is running) by triggering an invalid path permission error. This bypasses the fakepath protection mechanism.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13227</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. There is reflected XSS via the /scgi sid parameter.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13228</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. A session can be hijacked if one observes the sid value in any /scgi URI, because it is an authentication token.	2020-06-02	<a href="#">6.8</a>	<a href="#">CVE-2020-13229</a> <a href="#">MISC</a> <a href="#">MISC</a>
upx -- upx	p_lx_elf.cpp in UPX before 3.96 has an integer overflow during unpacking via crafted values in a PT_DYNAMIC segment.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2019-20805</a> <a href="#">MISC</a> <a href="#">MISC</a>
vmware -- multiple_products	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior) and VMware Horizon Client for Mac (5.x and prior) contain a local privilege escalation vulnerability due to a Time-of-check Time-of-use (TOCTOU) issue in the service opener. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC and Horizon Client are installed.	2020-05-29	<a href="#">6.9</a>	<a href="#">CVE-2020-3957</a> <a href="#">CONFIRM</a>
vmware -- spring_cloud_config	Spring Cloud Config, versions 2.2.x prior to 2.2.3, versions 2.1.x prior to 2.1.9, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-5410</a> <a href="#">CONFIRM</a>
websocket-extensions -- websocket-extensions	websocket-extensions ruby module prior to 0.1.5 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-7663</a> <a href="#">MISC</a> <a href="#">MISC</a>

	could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.			<a href="#">MISC</a> <a href="#">MISC</a>
websocket-extensions -- websocket-extensions	websocket-extensions npm module prior to 1.0.4 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-7662</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	common.php in the Gravity Forms plugin before 2.4.9 for WordPress can leak hashed passwords because user_pass is not considered a special case for a \$current_user->get(\$property) call.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13764</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The MailPoet plugin before 3.23.2 for WordPress allows remote attackers to inject arbitrary web script or HTML using extra parameters in the URL (Reflective Server-Side XSS).	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2019-11843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zimbra -- zimbra	Zimbra before 8.8.15 Patch 10 and 9.x before 9.0.0 Patch 3 allows remote code execution via an avatar file. There is potential abuse of /service/upload servlet in the webmail subsystem. A user can upload executable files (exe,sh,bat,jar) in the Contact section of the mailbox as an avatar image for a contact. A user will receive a "Corrupt File" error, but the file is still uploaded and stored locally in /opt/zimbra/data/tmp/upload/, leaving it open to possible remote execution.	2020-06-03	<a href="#">6</a>	<a href="#">CVE-2020-12846</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
znc -- znc	ZNC 1.8.0 up to 1.8.1-rc1 allows attackers to trigger an application crash (with a NULL pointer dereference) if echo-message is not enabled and there is no network.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13775</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zoho -- manageengine_opmanager	In Zoho ManageEngine OpManager before 125144, when <cachestart> is used, directory traversal validation can be bypassed.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13818</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- device_library_wizard	Insecure storage of sensitive information in ABB Device Library Wizard versions 6.0.X, 6.0.3.1 and 6.0.3.2 allows unauthenticated low privilege user to read file that contains confidential data	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-8482</a> <a href="#">CONFIRM</a>
atlassian -- fisheye_and_crucible	The review resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the review objectives.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2020-4013</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira_server_and_data_center	Affected versions are: Before 8.5.5, and from 8.6.0 before 8.8.1 of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the XML export view.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2020-4021</a> <a href="#">MISC</a>
avaya -- ip_office	A sensitive information disclosure vulnerability was discovered in the web interface component of IP Office that may potentially allow a local user to gain unauthorized access to the component. Affected versions of IP Office include: 9.x, 10.0 through 10.1.0.7 and 11.0 though 11.0.4.3.	2020-06-04	<a href="#">2.1</a>	<a href="#">CVE-2020-7030</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
elastic -- kibana	Kibana versions before 6.8.9 and 7.7.0 contains a stored XSS flaw in the TSVB visualization. An attacker who is able to edit or create a TSVB visualization could allow the attacker to obtain sensitive information from, or perform destructive actions, on behalf of Kibana users who edit the TSVB visualization.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-7015</a> <a href="#">N/A</a>
fortiguard -- fortianalyzer	An improper neutralization of input vulnerability in the Admin Profile of FortiAnalyzer may allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the Description Area.	2020-06-04	<a href="#">3.5</a>	<a href="#">CVE-2020-6640</a> <a href="#">MISC</a>
huawei -- honor_9x_smartphones	Honor 9X smartphones with versions earlier than 9.1.1.172(C00E170R8P1) have an improper authentication vulnerability. A logic error occurs when handling clock function, an attacker should do a series of crafted operations	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1833</a>

	quickly before the phone is unlocked, successful exploit could allow the attacker to access clock information without unlock the phone.			<a href="#">CONFIRM</a>
huawei -- mate_10_smartphones	HUAWEI Mate 10 smartphones with versions earlier than 10.0.0.143(C00E143R2P4) have an information disclosure vulnerability. The attacker could wake up voice assistant then do a series of crafted voice operation, successful exploit could allow the attacker read certain files without unlock the phone leading to information disclosure.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1809</a> <a href="#">CONFIRM</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.185(C00E74R3P8) have an improper authorization vulnerability. The system does not properly restrict certain operation in ADB mode, successful exploit could allow certain user break the limit of digital balance function.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1797</a> <a href="#">CONFIRM</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.195(SP31C00E74R3P8) have an improper authorization vulnerability. The digital balance function does not sufficiently restrict the using time of certain user, successful exploit could allow the user break the limit of digital balance function after a series of operations with a PC.	2020-05-29	<a href="#">1.9</a>	<a href="#">CVE-2020-1831</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178765.	2020-06-02	<a href="#">3.5</a>	<a href="#">CVE-2020-4360</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 180761.	2020-06-02	<a href="#">3.5</a>	<a href="#">CVE-2020-4431</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 could allow an attacker on the same network to gain access to the Solr dashboard and cause a denial of service attack. IBM X-Force	2020-06-03	<a href="#">3.3</a>	<a href="#">CVE-2020-4307</a> <a href="#">XF</a>

	ID: 176997.			<a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174852.	2020-06-04	<a href="#">2.1</a>	<a href="#">CVE-2020-4191</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Compact Columns Plugin 1.11 and earlier displays the unprocessed job description in tooltips, resulting in a stored cross-site scripting vulnerability that can be exploited by users with Job/Configure permission.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2195</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Script Security Plugin 1.72 and earlier does not correctly escape pending or approved classpath entries on the In-process Script Approval page, resulting in a stored cross-site scripting vulnerability.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2190</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the display name of the builds in the trend chart, resulting in a stored cross-site scripting vulnerability.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2194</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the parser identifier when rendering charts, resulting in a stored cross-site scripting vulnerability.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2193</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.6. In rx_queue_add_kobject() and netdev_queue_add_kobject() in net/core/net-sysfs.c, a reference count is mishandled, aka CID-a3e23f719f5c.	2020-06-03	<a href="#">2.1</a>	<a href="#">CVE-2019-20811</a> <a href="#">MISC</a> <a href="#">MISC</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, a user with the ability to use the import functionality of the `ImportExportController` behavior can be socially engineered by an attacker to upload a maliciously crafted CSV file which could result in a reflected XSS attack on the user in question Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-5298</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows XSS (Reflected) via the username, or XSS (Stored) via the admin.php?page=config install_name, intro_message, or new_file_content parameter.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2014-8944</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows local users to obtain sensitive information by listing a process because the username and password are on the command line.	2020-06-01	<a href="#">2.1</a>	<a href="#">CVE-2014-8938</a> <a href="#">MISC</a>



qualcomm -- multiple_snapdragon_products	When attempting to create a new XFRM policy, a stack out-of-bounds read will occur if the user provides a template where the mode is set to a value that does not resolve to a valid XFRM mode in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCA4531, QCN7605, QCS605, QM215, SA415M, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	3.6	<a href="#">CVE-2019-14053</a> CONFIRM
qualcomm -- multiple_snapdragon_products	Buffer over-read in ADSP parse function due to lack of check for availability of sufficient data payload received in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710, SDM845, SDX20, SDX24	2020-06-02	3.6	<a href="#">CVE-2019-14038</a> CONFIRM
qualcomm -- multiple_snapdragon_products	Out of bound read in adm call back function due to incorrect boundary check for payload in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710,	2020-06-02	3.6	<a href="#">CVE-2019-14039</a> CONFIRM

	SDM845, SDX20, SDX24			
qualcomm -- multiple_snapdragon_products	Using non-time-constant functions like memcmp to compare sensitive data can lead to information leakage through timing side channel issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	2020-06-02	2.1	<a href="#">CVE-2019-14067</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound read in Fingerprint application due to requested data is being used without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9150, MDM9205, MDM9650, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	3.6	<a href="#">CVE-2019-14043</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound read in in fingerprint application due to requested data assigned to a local buffer without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in	2020-06-02	3.6	<a href="#">CVE-2019-14042</a> <a href="#">CONFIRM</a>

	Kamorta, MDM9205, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with Q(10.0) software. The Lockscreen feature does not block Quick Panel access to Music Share. The Samsung ID is SVE-2020-17145 (June 2020).	2020-06-04	<a href="#">3.6</a>	<a href="#">CVE-2020-13837</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. The DeX Lockscreen feature does not block access to Quick Panel and notifications. The Samsung ID is SVE-2020-17187 (June 2020).	2020-06-04	<a href="#">3.6</a>	<a href="#">CVE-2020-13838</a> <a href="#">CONFIRM</a>
sane -- backends	A NULL pointer dereference in sanei_epson_net_read in SANE Backends through 1.0.29 allows a malicious device connected to the same local network as the victim to cause a denial of service, aka GHSL-2020-075.	2020-06-01	<a href="#">2.1</a>	<a href="#">CVE-2020-12867</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.5.2) and VMware Fusion (11.x before 11.5.2) contain a denial-of-service vulnerability in the shader functionality. Successful exploitation of this issue may allow attackers with non-administrative access to a virtual machine to crash the virtual machine's vmx process leading to a denial of service condition.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-3958</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.1.0) and VMware Fusion (11.x before 11.1.0) contain a memory leak vulnerability in the VMCI module. A malicious actor with local non-administrative access to a virtual machine may be able to crash the virtual machine's vmx process leading to a partial denial of service.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-3959</a> <a href="#">CONFIRM</a>
zte -- ft680_router	ZTE's PON terminal product is impacted by the access control vulnerability. Due to the system not performing correct access control on some program interfaces, an attacker could use this vulnerability to	2020-06-01	<a href="#">3.3</a>	<a href="#">CVE-2020-6868</a>

	tamper with the program interface parameters to perform unauthenticated operations. This affects: <ZTE F680> <V9.0.10P1N6>			<a href="#">MISC</a>
--	--	--	--	----------------------

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- unomi	Apache Unomi allows conditions to use OGNL scripting which offers the possibility to call static Java classes from the JDK that could execute code with the permission level of the running Java process.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11975</a> <a href="#">MISC</a>
apple -- multiple_products	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges.	2020-06-05	not yet calculated	<a href="#">CVE-2020-9859</a> <a href="#">MISC</a>
athom -- homey_and_homey_products	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks.	2020-06-04	not yet calculated	<a href="#">CVE-2020-9462</a> <a href="#">MISC</a>
bitdefender -- antivirus_free	A vulnerability in the improper handling of symbolic links in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects Bitdefender Antivirus Free versions prior to 1.0.17.178.	2020-06-05	not yet calculated	<a href="#">CVE-2020-8103</a> <a href="#">CONFIRM</a>
bludit -- bludit	showAlert() in the administration panel in Bludit 3.12.0 allows XSS.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13889</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to privilege escalation through the Adminstrator/Users/Edit/:UserId functionality. Adminstrator/Users/Edit/:UserId fails to check that the request was submitted by	2020-06-04	not yet calculated	<a href="#">CVE-2020-11679</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>

	an Administrator. This allows a normal user to escalate their privileges by adding additional roles to their account.			<a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to CSRF in all state-changing request. A __RequestVerificationToken is set by the web interface, and included in requests sent by web interface. However, this token is not verified by the application: the token can be removed from all requests and the request will succeed.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11682</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 stores and displays credentials for the associated SMTP server in cleartext. Low privileged users can exploit this to create an administrator user and obtain the SMTP credentials.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11681</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to authorization bypass on all administrator functionality. The application fails to check that a request was submitted by an administrator. Consequently, a normal user can perform actions including, but not limited to, creating/modifying the file store, creating/modifying alerts, creating/modifying users, etc.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11680</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
cisco -- 4300_series_integrated_services_routers_and_catalyst_9800-l_wireless_controllers	A vulnerability in the hardware crypto driver of Cisco IOS XE Software for Cisco 4300 Series Integrated Services Routers and Cisco Catalyst 9800-L Wireless Controllers could allow an unauthenticated, remote attacker to disconnect legitimate IPsec VPN sessions to an affected device. The vulnerability is due to insufficient verification of authenticity of received Encapsulating Security Payload (ESP) packets. An attacker could exploit this vulnerability by tampering with ESP cleartext values as a man-in-the-middle.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3220</a> <a href="#">CISCO</a>
cisco -- 809_and_829_industrial_services_routers	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first	2020-06-	not yet	<a href="#">CVE-2020-3208</a>



	<p>authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the attacker must have valid user credentials at privilege level 15.</p>	03	calculated	<a href="#">CISCO</a>
cisco -- application_services_engine_software	<p>A vulnerability in the key store of Cisco Application Services Engine Software could allow an authenticated, local attacker to read sensitive information of other users on an affected device. The vulnerability is due to insufficient authentication limitations. An attacker could exploit this vulnerability by logging in to an affected device locally with valid credentials. A successful exploit could allow the attacker to read the sensitive information of other users on the affected device.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3335</a> <a href="#">CISCO</a>
cisco -- application_services_engine_software	<p>A vulnerability in the API of Cisco Application Services Engine Software could allow an unauthenticated, remote attacker to update event policies on an affected device. The vulnerability is due to insufficient authentication of users who modify policies on an affected device. An attacker could exploit this vulnerability by crafting a malicious HTTP request to contact an affected device. A successful exploit could allow the attacker to update event policies on the affected device.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3333</a> <a href="#">CISCO</a>
cisco -- asr_920_series_aggregation_services	<p>A vulnerability in the Simple Network Management Protocol (SNMP) implementation in Cisco ASR 920 Series Aggregation Services Router model ASR920-12SZ-IM could allow an authenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect handling of data that is returned from Cisco Discovery Protocol queries to SNMP. An attacker could exploit this vulnerability by sending a request for Cisco Discovery Protocol information by using SNMP. An exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3232</a> <a href="#">CISCO</a>
	A vulnerability in the 802.1X feature of			

cisco -- catalyst-2960-l_series_switches_and_catalyst_cdb-8p_switches	<p>Cisco Catalyst 2960-L Series Switches and Cisco Catalyst CDB-8P Switches could allow an unauthenticated, adjacent attacker to forward broadcast traffic before being authenticated on the port. The vulnerability exists because broadcast traffic that is received on the 802.1X-enabled port is mishandled. An attacker could exploit this vulnerability by sending broadcast traffic on the port before being authenticated. A successful exploit could allow the attacker to send and receive broadcast traffic on the 802.1X-enabled port before authentication.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3231</a> <a href="#">CISCO</a>
cisco -- catalyst_4500_series_switches	<p>A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3235</a> <a href="#">CISCO</a>
cisco -- catalyst_9800_series_wireless_controllers	<p>A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3221</a> <a href="#">CISCO</a>

	to trigger an infinite loop, resulting in a process crash that would cause a reload of the device.			
cisco -- catalyst_9800_series_wireless_controllers	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3203</a> <a href="#">CISCO</a>
cisco -- catalyst_9800_series_wireless_controllers	A vulnerability in the handling of IEEE 802.11w Protected Management Frames (PMFs) of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to terminate a valid user connection to an affected device. The vulnerability exists because the affected software does not properly validate IEEE 802.11w disassociation and deauthentication PMFs that it receives. An attacker could exploit this vulnerability by sending a spoofed 802.11w PMF from a valid, authenticated client on a network adjacent to an affected device. A successful exploit could allow the attacker to terminate a single valid user connection to the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3206</a> <a href="#">CISCO</a>
cisco -- digital_network_architecture_center	A vulnerability in the audit logging component of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage	2020-06-03	not yet calculated	<a href="#">CVE-2020-3281</a> <a href="#">CISCO</a>

	network devices.			
cisco -- identity_services_engine	A vulnerability in the syslog processing engine of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a race condition that may occur when syslog messages are processed. An attacker could exploit this vulnerability by sending a high rate of syslog messages to an affected device. A successful exploit could allow the attacker to cause the Application Server process to crash, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3353</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by executing crafted Tcl arguments on an affected device. An exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3201</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to execute arbitrary code on the underlying operating system (OS) with root privileges. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to cause memory corruption or execute the code with root privileges on the underlying OS of the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3204</a> <a href="#">CISCO</a>
	A vulnerability in the Secure Shell (SSH) server code of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. The vulnerability is due to an internal state not being represented correctly in the SSH			

cisco -- ios_and_ios_xe_software	state machine, which leads to an unexpected behavior. An attacker could exploit this vulnerability by creating an SSH connection to an affected device and using a specific traffic pattern that causes an error condition within that connection. A successful exploit could allow an attacker to cause the device to reload, resulting in a denial of service (DoS) condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3200</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent IKEv2 from establishing new security associations. The vulnerability is due to incorrect handling of crafted IKEv2 SA-Init packets. An attacker could exploit this vulnerability by sending crafted IKEv2 SA-Init packets to the affected device. An exploit could allow the attacker to cause the affected device to reach the maximum incoming negotiation limits and prevent further IKEv2 security associations from being formed.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3230</a> <a href="#">CISCO</a>
cisco -- ios_xe_sd- wan_software	A vulnerability in Cisco IOS XE SD-WAN Software could allow an unauthenticated, physical attacker to bypass authentication and gain unrestricted access to the root shell of an affected device. The vulnerability exists because the affected software has insufficient authentication mechanisms for certain commands. An attacker could exploit this vulnerability by stopping the boot initialization of an affected device. A successful exploit could allow the attacker to bypass authentication and gain unrestricted access to the root shell of the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3216</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to insufficient input processing of CIP traffic. An attacker could exploit these vulnerabilities by sending crafted CIP traffic to be processed by an affected	2020-06-03	not yet calculated	<a href="#">CVE-2020-3225</a> <a href="#">CISCO</a>



	device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.			
cisco -- ios_xe_software	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to read arbitrary files on the underlying filesystem of the device. The vulnerability is due to insufficient file scope limiting. An attacker could exploit this vulnerability by creating a specific file reference on the filesystem and then accessing it through the web UI. An exploit could allow the attacker to read arbitrary files from the underlying operating system's filesystem.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3223</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker could exploit this vulnerability by uploading a crafted file to the web UI of an affected device. A successful exploit could allow the attacker to inject and execute arbitrary commands with root privileges on the device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3212</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with administrative privileges on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input to the web UI. A successful exploit could allow an attacker to execute arbitrary commands with administrative privileges on an affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3219</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the Session Initiation Protocol (SIP) library of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on received SIP messages. An attacker could exploit	2020-06-03	not yet calculated	<a href="#">CVE-2020-3226</a> <a href="#">CISCO</a>

	<p>this vulnerability by sending crafted SIP messages to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service condition.</p>			
cisco -- ios_xe_software	<p>A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with read-only privileges to inject IOS commands to an affected device. The injected commands should require a higher privilege level in order to be executed. The vulnerability is due to insufficient input validation of specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a specific web UI endpoint on an affected device. A successful exploit could allow the attacker to inject IOS commands to the affected device, which could allow the attacker to alter the configuration of the device or cause a denial of service (DoS) condition.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3224</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	<p>A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to bypass access control restrictions on an affected device. The vulnerability is due to the presence of a proxy service at a specific endpoint of the web UI. An attacker could exploit this vulnerability by connecting to the proxy service. An exploit could allow the attacker to bypass access restrictions on the network by proxying their access request through the management network of the affected device. As the proxy is reached over the management virtual routing and forwarding (VRF), this could reduce the effectiveness of the bypass.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3222</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	<p>A vulnerability in software image verification in Cisco IOS XE Software could allow an unauthenticated, physical attacker to install and boot a malicious software image or execute unsigned binaries on an affected device. The vulnerability is due to an improper check on the area of code that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3209</a> <a href="#">CISCO</a>

	exploit could allow the attacker to install and boot a malicious software image or execute unsigned binaries on the targeted device.			
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker who has valid administrative access to an affected device could exploit this vulnerability by supplying a crafted input parameter on a form in the web UI and then submitting that form. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device, which could lead to complete system compromise.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3211</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the Virtual Services Container of Cisco IOS XE Software could allow an authenticated, local attacker to gain root-level privileges on an affected device. The vulnerability is due to insufficient validation of a user-supplied open virtual appliance (OVA). An attacker could exploit this vulnerability by installing a malicious OVA on an affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3215</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the ROMMON of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to those of the root user of the underlying operating system. The vulnerability is due to the ROMMON allowing for special parameters to be passed to the device at initial boot up. An attacker could exploit this vulnerability by sending parameters to the device at initial boot up. An exploit could allow the attacker to elevate from a Priv15 user to the root user and execute arbitrary commands with the privileges of the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3213</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software could allow an unauthenticated, remote attacker to execute Cisco IOx API commands without proper authorization. The vulnerability is due to incorrect handling of requests for authorization tokens. An attacker could exploit this	2020-06-03	not yet calculated	<a href="#">CVE-2020-3227</a> <a href="#">CISCO</a>

	vulnerability by using a crafted API call to request such a token. An exploit could allow the attacker to obtain an authorization token and execute any of the IOx API commands on an affected device.			
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code with root privileges on the underlying Linux shell. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by first creating a malicious file on the affected device itself and then uploading a second malicious file to the device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or bypass licensing requirements on the device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3218</a> <a href="#">CISCO</a>
cisco -- ios_xe_web_management	A vulnerability in Role Based Access Control (RBAC) functionality of Cisco IOS XE Web Management Software could allow a Read-Only authenticated, remote attacker to execute commands or configuration changes as an Admin user. The vulnerability is due to incorrect handling of RBAC for the administration GUI. An attacker could exploit this vulnerability by sending a modified HTTP request to the affected device. An exploit could allow the attacker as a Read-Only user to execute CLI commands or configuration changes as if they were an Admin user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3229</a> <a href="#">CISCO</a>
cisco -- iox_application	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, remote attacker to write or modify arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient input validation of user-supplied application packages. An attacker who can upload a malicious package within Cisco IOx could exploit the vulnerability to modify arbitrary files. The impacts of a successful exploit are limited to the scope of the virtual instance and do not affect the device that is hosting Cisco IOx.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3238</a> <a href="#">CISCO</a>
	A vulnerability in the Cisco Application			

cisco -- iox_application	Framework component of the Cisco IOx application environment could allow an authenticated, local attacker to overwrite arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient path restriction enforcement. An attacker could exploit this vulnerability by including a crafted file in an application package. An exploit could allow the attacker to overwrite files.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3237</a> <a href="#">CISCO</a>
cisco -- iox_application_framework	A vulnerability in the web-based Local Manager interface of the Cisco IOx Application Framework could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based Local Manager interface of an affected device. The attacker must have valid Local Manager credentials. The vulnerability is due to insufficient validation of user-supplied input by the web-based Local Manager interface of the affected software. An attacker could exploit this vulnerability by injecting malicious code into a system settings tab. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3233</a> <a href="#">CISCO</a>
cisco -- multiple_products	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3217</a> <a href="#">CISCO</a>



cisco -- multiple_products	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3228</a> <a href="#">CISCO</a>
cisco -- multiple_routers	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3199</a> <a href="#">CISCO</a>
cisco -- multiple_routers	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device's virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3234</a> <a href="#">CISCO</a>
	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell			

cisco -- multiple_routers	commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3210</a> <a href="#">CISCO</a>
cisco -- multiple_routers	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3198</a> <a href="#">CISCO</a>
cisco -- multiple_routers	A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3205</a> <a href="#">CISCO</a>
	Multiple vulnerabilities in the Cisco IOx			

cisco -- multiple_routers	application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3257</a> <a href="#">CISCO</a>
cisco -- multiple_routers	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3258</a> <a href="#">CISCO</a>
cisco -- unified_contact_center_express	A vulnerability in the API subsystem of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to change the availability state of any agent. The vulnerability is due to insufficient authorization enforcement on an affected system. An attacker could exploit this vulnerability by authenticating to an affected system with valid agent credentials and performing a specific API call with crafted input. A successful exploit could allow the attacker to change the availability state of an agent, potentially causing a denial of service condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3267</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_and_webex_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link	2020-06-03	not yet calculated	<a href="#">CVE-2020-3319</a> <a href="#">CISCO</a>

	or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3.			
combodo -- itop	In Combodo iTop, dashboard ids can be exploited with a reflective XSS payload. This is fixed in all iTop packages (community, essential, professional) for version 2.7.0 and in iTop essential and iTop professional packages for version 2.6.4.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11697</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
combodo -- itop	In Combodo iTop a menu shortcut name can be exploited with a stored XSS payload. This is fixed in all iTop packages (community, essential, professional) in version 2.7.0 and iTop essential and iTop professional in version 2.6.4.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11696</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.6 for Craft CMS. There is stored XSS via a guest name.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13869</a> <a href="#">MISC</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. There is stored XSS via an asset volume name.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13870</a> <a href="#">MISC</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. CSRF affects comment integrity.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13868</a> <a href="#">MISC</a>
docker -- desktop	An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11492</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- elasticsearch	The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to 7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an	2020-06-03	not yet calculated	<a href="#">CVE-2020-7014</a> <a href="#">N/A</a>

	authentication token being generated with elevated privileges.			
elliptic -- elliptic	The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading to bytes, or integer overflows. This could conceivably have a security-relevant impact if an application relied on a single canonical signature.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13822</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fortiguard -- forticlient_for_windows	Use of a hard-coded cryptographic key to encrypt security sensitive data in local storage and configuration in FortiClient for Windows prior to 6.4.0 may allow an attacker with access to the local storage or the configuration backup file to decrypt the sensitive data via knowledge of the hard-coded key.	2020-06-04	not yet calculated	<a href="#">CVE-2019-16150</a> <a href="#">MISC</a>
fortiguard -- fortisiem_windows_agent	An unquoted service path vulnerability in the FortiSIEM Windows Agent component may allow an attacker to gain elevated privileges via the AoWinAgt executable service path.	2020-06-04	not yet calculated	<a href="#">CVE-2020-9292</a> <a href="#">MISC</a>
foxit -- e-mail_advertising_system	An issue was discovered in Foxit E-mail advertising system before September 2018. It allows authentication bypass and information disclosure, related to Interspire Email Marketer.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21235</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has an out-of-bounds write when Internet Explorer is used.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20825</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has homograph mishandling.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20832</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows NTLM credential theft via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21237</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It allows Remote Code Execution via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21242</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20824</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has an untrusted search path that allows a DLL to execute remote code.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21241</a> <a href="#">CONFIRM</a>
	An issue was discovered in Foxit			



foxit -- phantompdf	PhantomPDF before 8.3.6. It allows arbitrary application execution via an embedded executable file in a PDF portfolio, aka FG-VD-18-029.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21244</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20834</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20823</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has COM object mishandling when Microsoft Word is used.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21243</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows memory consumption via an <code>ArrayBuffer(0xffffffff)</code> call.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21238</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has mishandling of cloud credentials, as demonstrated by Google Drive.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20833</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac	An issue was discovered in Foxit PhantomPDF Mac before 3.4. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20821</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20826</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac_and_reader_for_mac	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It allows stack consumption because of interaction between ICC-Based color space and Alternate color space.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20827</a> <a href="#">CONFIRM</a>
foxit -- reader	An issue was discovered in Foxit Reader before 2.4.4. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21236</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.7.0.29430. It has an out-of-bounds write via incorrect image data.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20822</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.2. It allows NTLM credential theft via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21239</a> <a href="#">CONFIRM</a>
foxit --	An issue was discovered in Foxit Reader			<a href="#">CVE-2018-</a>

reader_and_phantompdf	and PhantomPDF before 9.2. It allows memory consumption via an <code>ArrayBuffer(0xffffffff)</code> call.	2020-06-04	not yet calculated	<a href="#">21240 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It has a use-after-free via a document that lacks a dictionary.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13814 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13810 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It allows stack consumption via a loop of an indirect object reference.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13815 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.5.0.20733. It has void data mishandling, causing a crash.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20831 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13812 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory when <code>FoxitStudioPhoto366_3.6.6.916.exe</code> is used.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13813 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It has an out-of-bounds write via a crafted TIFF file.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13811 CONFIRM</a>
ge -- multiple_grid_solutions	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the	2020-06-02	not yet calculated	<a href="#">CVE-2020-12017 MISC</a>

	device and reboot the system.			
gnutls -- gnutls	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13777</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">DEBIAN</a>
google -- chrome	Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-06-03	not yet calculated	<a href="#">CVE-2020-6503</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- multiple_products	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause service abnormal.	2020-06-05	not yet calculated	<a href="#">CVE-2020-1883</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones.	2020-06-05	not yet calculated	<a href="#">CVE-2020-9074</a> <a href="#">MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181230.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4449</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181231.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4450</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- websphere_application_server_network_deployment	IBM WebSphere Application Server Network Deployment 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 181228.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4448</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

ibm -- worklight/mobilefoundation	IBM Worklight/MobileFoundation 8.0.0.0 does not properly invalidate session cookies when a user logs out of a session, which could allow another user to gain unauthorized access to a user's session. IBM X-Force ID: 175211.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4229</a> <a href="#">CONFIRM</a>
kubernetes -- kube-controller-manager	The Kubernetes kube-controller-manager in versions v1.0-1.14, versions prior to v1.15.12, v1.16.9, v1.17.5, and version v1.18.0 are vulnerable to a Server Side Request Forgery (SSRF) that allows certain authorized users to leak up to 500 bytes of arbitrary information from unprotected endpoints within the master's host network (such as link-local or loopback services).	2020-06-05	not yet calculated	<a href="#">CVE-2020-8555</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13841</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS software before 2020-06-01. Local users can cause a denial of service because checking of the userdata partition is mishandled. The LG ID is LVE-SMP-200014 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13843</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13839</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13842</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13840</a> <a href="#">CONFIRM</a>
minishare -- minishare	In MiniShare before 1.4.2, there is a stack-based buffer overflow via an HTTP PUT request, which allows an attacker to achieve arbitrary code execution, a similar issue to CVE-2018-19861, CVE-2018-19862, and CVE-2019-17601.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13768</a> <a href="#">MISC</a>

	NOTE: this product is discontinued.			
mqtt -- mqtt	The MQTT protocol 3.1.1 requires a server to set a timeout value of 1.5 times the Keep-Alive value specified by a client, which allows remote attackers to cause a denial of service (loss of the ability to establish new connections), as demonstrated by SlowITe.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13849</a> <a href="#">MISC</a> <a href="#">MISC</a>
neon -- neon	The Neon theme 2.0 before 2020-06-03 for Bootstrap allows XSS via an Add Task Input operation in a dashboard.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13890</a> <a href="#">MISC</a>
network_time_foundation -- network_time_protocol	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13817</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_rcv_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection.	2020-06-03	not yet calculated	<a href="#">CVE-2020-11080</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
	In WatermelonDB (NPM package "@nozbe/watermelondb") before versions 0.15.1 and 0.16.2, a maliciously crafted record ID can exploit a SQL Injection vulnerability in iOS adapter implementation and cause the app to delete all or selected records from the database, generally causing the app to become unusable. This may happen in apps that don't validate IDs (valid IDs are /^[a-zA-Z0-9_-.]+\$/') and use Watermelon Sync or low-level `database.adapter.destroyDeletedRecords` method. The integrity risk is low due to the fact that maliciously deleted records			



nozbe -- watermelondb	won't synchronize, so logout-login will restore all data, although some local changes may be lost if the malicious deletion causes the sync process to fail to proceed to push stage. No way to breach confidentiality with this vulnerability is known. Full exploitation of SQL Injection is mitigated, because it's not possible to nest an insert/update query inside a delete query in SQLite, and it's not possible to pass a semicolon-separated second query. There's also no known practicable way to breach confidentiality by selectively deleting records, because those records will not be synchronized. It's theoretically possible that selective record deletion could cause an app to behave insecurely if lack of a record is used to make security decisions by the app. This is patched in versions 0.15.1, 0.16.2, and 0.16.1-fix	2020-06-03	not yet calculated	<a href="#">CVE-2020-4035</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, any users with the ability to modify any data that could eventually be exported as a CSV file from the `ImportExportController` could potentially introduce a CSV injection into the data to cause the generated CSV export file to be malicious. This requires attackers to achieve the following before a successful attack can be completed: 1. Have found a vulnerability in the victims spreadsheet software of choice. 2. Control data that would potentially be exported through the `ImportExportController` by a theoretical victim. 3. Convince the victim to export above data as a CSV and run it in vulnerable spreadsheet software while also bypassing any sanity checks by said software. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	not yet calculated	<a href="#">CVE-2020-5299</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	The October CMS debugbar plugin before version 3.1.0 contains a feature where it will log all requests (and all information pertaining to each request including session data) whenever it is enabled. This presents a problem if the plugin is ever enabled on a system that is open to untrusted users as the potential exists for them to use this feature to view all requests being made to the application			

october -- october_cms	and obtain sensitive information from those requests. There even exists the potential for account takeovers of authenticated users by non-authenticated public users, which would then lead to a number of other potential issues as an attacker could theoretically get full access to the system if the required conditions existed. Issue has been patched in v3.1.0 by locking down access to the debugbar to all users; it now requires an authenticated backend user with a specifically enabled permission before it is even usable, and the feature that allows access to stored request information is restricted behind a different permission that's more restrictive.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11094</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open-iscsi -- targetcli-fb	Open-iSCSI targetcli-fb through 2.1.52 has weak permissions for /etc/target (and for the backup directory and backup files).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13867</a> <a href="#">MISC</a>
pam_tacplus -- pam_tacplus	In support.c in pam_tacplus 1.3.8 through 1.5.1, the TACACS+ shared secret gets logged via syslog if the DEBUG loglevel and journald are used.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13881</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12723</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10878</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
perl -- perl	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10543</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
postgresql -- jdbc_driver	PostgreSQL JDBC Driver (aka PgJDBC) before 42.2.13 allows XXE.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13692</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
pupnp -- pupnp	Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and	2020-06-04	not yet calculated	<a href="#">CVE-2020-13848</a> <a href="#">MISC</a> <a href="#">MISC</a>

	FindServiceEventURLPath in genlib/service_table/service_table.c.			
pydio -- cells	Pydio Cells 2.0.4 allows XSS. A malicious user can either upload or create a new file that contains potentially malicious HTML and JavaScript code to personal folders or accessible cells.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12853</a> MISC
pydio -- cells	Pydio Cells 2.0.4 allows an authenticated user to write or overwrite existing files in another user's personal and cells folders (repositories) by uploading a custom generated ZIP file and leveraging the file extraction feature present in the web application. The extracted files will be placed in the targeted user folders.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12851</a> MISC MISC
pydio -- cells	The update feature for Pydio Cells 2.0.4 allows an administrator user to set a custom update URL and the public RSA key used to validate the downloaded update package. The update process involves downloading the updated binary file from a URL indicated in the update server response, validating its checksum and signature with the provided public key and finally replacing the current application binary. To complete the update process, the application's service or appliance needs to be restarted. An attacker with administrator access can leverage the software update feature to force the application to download a custom binary that will replace current Pydio Cells binary. When the server or service is eventually restarted the attacker will be able to execute code under the privileges of the user running the application. In the Pydio Cells enterprise appliance this is with the privileges of the user named "pydio".	2020-06-04	not yet calculated	<a href="#">CVE-2020-12852</a> MISC MISC
pydio -- cells	In Pydio Cells 2.0.4, once an authenticated user shares a file selecting the create a public link option, a hidden shared user account is created in the backend with a random username. An anonymous user that obtains a valid public link can get the associated hidden account username and password and proceed to login to the web application. Once logged into the web application with the hidden user account, some actions that were not available with the public share link can now be performed.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12848</a> MISC MISC

pydio -- cells	Pydio Cells 2.0.4 allows any user to upload a profile image to the web application, including standard and shared user roles. These profile pictures can later be accessed directly with the generated URL by any unauthenticated or authenticated user.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12849</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	Pydio Cells 2.0.4 web application offers an administrative console named "Cells Console" that is available to users with an administrator role. This console provides an administrator user with the possibility of changing several settings, including the application's mailer configuration. It is possible to configure a few engines to be used by the mailer application to send emails. If the user selects the "sendmail" option as the default one, the web application offers to edit the full path where the sendmail binary is hosted. Since there is no restriction in place while editing this value, an attacker authenticated as an administrator user could force the web application into executing any arbitrary binary.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12847</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	A flaw was found in QEMU in the implementation of the Pointer Authentication (PAuth) support for ARM introduced in version 4.0 and fixed in version 5.0.0. A general failure of the signature generation process caused every PAuth-enforced pointer to be signed with the same signature. A local attacker could obtain the signature of a protected pointer and abuse this flaw to bypass PAuth protection for all programs running on QEMU.	2020-06-04	not yet calculated	<a href="#">CVE-2020-10702</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
qemu -- qemu	ati-vga in hw/display/ati.c in QEMU 4.2.0 allows guest OS users to trigger infinite recursion via a crafted mm_index value during an ati_mm_read or ati_mm_write call.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13800</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
qemu -- qemu	rom_copy() in hw/core/loader.c in QEMU 4.1.0 does not validate the relationship between two addresses, which allows attackers to trigger an invalid memory copy operation.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13765</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
qemu -- qemu	hw/pci/pci.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access by providing an address near the end of the PCI configuration space.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13791</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	SQLite 3.32.2 has a use-after-free in			<a href="#">CVE-2020-</a>

sqlite -- sqlite	resetAccumulator in select.c because the parse tree rewrite for window functions is too late.	2020-06-06	not yet calculated	<a href="#">13871</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
swift_networks -- red_cheetah	In the cheetah free wifi 5.1 driver file liebaonat.sys, local users are allowed to cause a denial of service (BSOD) or other unknown impact due to failure to verify the value of a specific IOCTL.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13646</a> <a href="#">MISC</a>
tigera -- calico_and_calico_enterprise	Clusters using Calico (version 3.14.0 and below), Calico Enterprise (version 2.8.2 and below), may be vulnerable to information disclosure if IPv6 is enabled but unused. A compromised pod with sufficient privilege is able to reconfigure the node's IPv6 interface due to the node accepting route advertisement by default, allowing the attacker to redirect full or partial network traffic from the node to the compromised pod.	2020-06-03	not yet calculated	<a href="#">CVE-2020-13597</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
url-regex -- url-regex	all versions of url-regex are vulnerable to Regular Expression Denial of Service. An attacker providing a very long string in String.test can cause a Denial of Service.	2020-06-04	not yet calculated	<a href="#">CVE-2020-7661</a> <a href="#">MISC</a> <a href="#">MISC</a>
weaveworks -- weave_net	In Weave Net before version 2.6.3, an attacker able to run a process as root in a container is able to respond to DNS requests from the host and thereby insert themselves as a fake service. In a cluster with an IPv4 internal network, if IPv6 is not totally disabled on the host (via ipv6.disable=1 on the kernel cmdline), it will be either unconfigured or configured on some interfaces, but it's pretty likely that ipv6 forwarding is disabled, ie /proc/sys/net/ipv6/conf//forwarding == 0. Also by default, /proc/sys/net/ipv6/conf//accept_ra == 1. The combination of these 2 sysctls means that the host accepts router advertisements and configure the IPv6 stack using them. By sending rogue router advertisements, an attacker can reconfigure the host to redirect part or all of the IPv6 traffic of the host to the attacker controlled container. Even if there was no IPv6 traffic before, if the DNS returns A (IPv4) and AAAA (IPv6) records, many HTTP libraries will try to connect via IPv6 first then fallback to IPv4, giving an opportunity to the attacker to respond. If by chance you also have on the host a vulnerability like last year's	2020-06-03	not yet calculated	<a href="#">CVE-2020-11091</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



	RCE in apt (CVE-2019-3462), you can now escalate to the host. Weave Net version 2.6.3 disables the accept_ra option on the veth devices that it creates.			
wordpress -- wordpress	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from a stored XSS vulnerability. An author user can create posts that result in a stored XSS by using a crafted payload in custom links.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13864</a> <a href="#">MISC</a>
wordpress -- wordpress	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from multiple stored XSS vulnerabilities. An author user can create posts that result in stored XSS vulnerabilities, by using a crafted link in the custom URL or by applying custom attributes.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13865</a> <a href="#">MISC</a>
wso2 -- multiple_products	In WSO2 API Manager 3.0.0 and earlier, WSO2 API Microgateway 2.2.0, and WSO2 IS as Key Manager 5.9.0 and earlier, Management Console allows XXE during addition or update of a Lifecycle.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13883</a> <a href="#">MISC</a>
xack -- dns	XACK DNS 1.11.0 to 1.11.4, 1.10.0 to 1.10.8, 1.8.0 to 1.8.23, 1.7.0 to 1.7.18, and versions before 1.7.0 allow remote attackers to cause a denial of service condition resulting in degradation of the recursive resolver's performance or compromising the recursive resolver as a reflector in a reflection attack.	2020-06-05	not yet calculated	<a href="#">CVE-2020-5591</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	A remote adversary with the ability to send arbitrary CoAP packets to be parsed by Zephyr is able to cause a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10063</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	An off-by-one error in the Zephyr project MQTT packet length decoder can result in memory corruption and possible remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	The Zephyr MQTT parsing code performs insufficient checking of the length field on publish messages, allowing a buffer overflow and potentially remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

zephyrproject -- zephyr	In the Zephyr Project MQTT code, improper bounds checking can result in memory corruption and possibly remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	Improper handling of the full-buffer case in the Zephyr Bluetooth implementation can result in memory corruption. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10061</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	In the Zephyr project Bluetooth subsystem, certain duplicate and back-to-back packets can cause incorrect behavior, resulting in a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10068</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [edigiovanna@sunnyvale.ca.gov](mailto:edigiovanna@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of June 1, 2020  
**Date:** Monday, June 08, 2020 11:49:05 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of June 1, 2020](#)

06/08/2020 06:56 AM EDT

Original release date: June 8, 2020

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
asus -- aura_sync	Ene.sys in Asus Aura Sync through 1.07.71 does not properly validate input to IOCTL 0x80102044, 0x80102050, and 0x80102054, which allows local users to cause a denial of service (system crash) or gain privileges via IOCTL requests using crafted kernel addresses that trigger memory corruption.	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-17603</a> <a href="#">MISC</a>
cisco -- ios_xe_software	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute	2020-06-03	<a href="#">7.2</a>	<a href="#">CVE-2020-3207</a> <a href="#">CISCO</a>

	malicious code on an affected device with root-level privileges.			
cisco -- ios_xe_software	A vulnerability in Cisco IOS XE Software could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	2020-06-03	<a href="#">7.2</a>	<a href="#">CVE-2020-3214</a> <a href="#">CISCO</a>
clearpass -- policy_manager	The ClearPass Policy Manager web interface is affected by a vulnerability that leads to authentication bypass. Upon successful bypass an attacker could then execute an exploit that would allow to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">10</a>	<a href="#">CVE-2020-7115</a> <a href="#">MISC</a>
clearpass -- policy_manager	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-7116</a> <a href="#">MISC</a>
clearpass -- policy_manager	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-7117</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices allow Command Injection.	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-13782</a> <a href="#">MISC</a>
docker -- engine	An issue was discovered in Docker Engine before 19.03.11. An attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service.	2020-06-02	<a href="#">7.5</a>	<a href="#">CVE-2020-13401</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows attackers to write arbitrary data	2020-06-	<a href="#">7.5</a>	<a href="#">CVE-2014-7175</a>

	to fsUI.xyz via fsSaveUIPersistence.php.	01		<a href="#">MISC</a>
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows command injection via shell metacharacters to sysSaveMonitorData.php, fsx25MonProxy.php, syseditdate.php, iframeupload.php, or sysRestoreX25Cplt.php.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2014-7173</a> <a href="#">MISC</a>
fortinet -- fortia- s/w2_and_fortiap-u	An improper input validation in FortiAP-S/W2 6.2.0 to 6.2.2, 6.0.5 and below, FortiAP-U 6.0.1 and below CLI admin console may allow unauthorized administrators to overwrite system files via specially crafted tcpdump commands in the CLI.	2020-06-01	<a href="#">8.5</a>	<a href="#">CVE-2019-15709</a> <a href="#">MISC</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has an out-of-bounds write when Internet Explorer is used.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2019-20830</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, an Integer Overflow to Buffer Overflow exists. When using /video redirection, a manipulated server can instruct the client to allocate a buffer with a smaller size than requested due to an integer overflow in size calculation. With later messages, the server can manipulate the client to write data out of bound to the previously allocated buffer. This has been patched in 2.1.0.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-11038</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, when using a manipulated server with USB redirection enabled (nearly) arbitrary memory can be read and written due to integer overflows in length checks. This has been patched in 2.1.0.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-11039</a> <a href="#">CONFIRM</a>
gesio -- erp	There is an improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in php files of GESIO ERP. GESIO ERP all versions prior to 11.2 allows malicious users to retrieve all database information.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2020-8967</a> <a href="#">CONFIRM</a>
github -- enterprise_server	An improper access control vulnerability was identified in the GitHub Enterprise Server API that allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.21 and was fixed in 2.20.9, 2.19.15, and 2.18.20. This	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-10516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	vulnerability was reported via the GitHub Bug Bounty program.			
ibm -- security_guardium	IBM Security Guardium 11.1 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 174735.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-4180</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174732.	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-4177</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
micro_focus -- service_management_authentication	There is an Incorrect Authorization vulnerability in Micro Focus Service Management Automation (SMA) product authentication version 2018.05 to 2020.02. The vulnerability could be exploited to provide unauthorized access to the Container Deployment Foundation.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-11844</a> <a href="#">CONFIRM</a>
piwigo -- lexiglot	admin.php?page=projects in Lexiglot through 2014-11-20 allows command injection via username and password fields.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2014-8945</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows SQL injection via an admin.php?page=users&from_id= or admin.php?page=history&limit= URI.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2014-8941</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Improper permissions in XBL_SEC region enable user to update XBL_SEC code and data and divert the RAM dump path to normal cold boot path in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM8150, SXR1130, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14054</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired	2020-06-02	<a href="#">7.8</a>	<a href="#">CVE-2020-3645</a>

	Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell, SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130			<a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3618</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3625</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-06-02	<a href="#">7.5</a>	<a href="#">CVE-2020-3615</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow in calculating estimated output buffer size when getting a list of installed Feature IDs, Serial Numbers or checking Feature ID status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9205, MDM9607, Nicobar, QCS404, QCS405, Rennell, SA6155P, SC7180, SC8180X, SDX55, SM6150, SM7150, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14066</a> <a href="#">CONFIRM</a>
	Array out of bound may occur while playing mp3 file as no check is there on			

qualcomm -- multiple_snapdragon_products	offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	10	<a href="#">CVE-2020-3633</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	10	<a href="#">CVE-2020-3641</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150	2020-06-02	7.2	<a href="#">CVE-2020-3616</a> <a href="#">CONFIRM</a>
qualcomm --	Failure in buffer management while accessing handle for HDR blit when color			<a href="#">CVE-2019-</a>

multiple_snapdragon_products	modes not supported by display in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, QCS605	2020-06-02	<a href="#">7.2</a>	<a href="#">14087 CONFIRM</a>
qualcomm --sm8250_and_sxr2130	kernel failure due to load failures while devices v1 path directly via kernel in Snapdragon Mobile in SM8250, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3623 CONFIRM</a>
quickbox --quickbox_community_and_quickbox_pro	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user has sudo privileges and can execute commands as root without a password, which allows an attacker to obtain sensitive information via a grep of a /root/*.db or /etc/shadow file.	2020-06-01	<a href="#">9</a>	<a href="#">CVE-2020-13695 MISC</a>
quickbox --quickbox_community_and_quickbox_pro	In QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8, the local www-data user can execute sudo and sql without a password, which means that the www-data user can execute arbitrary OS commands via the mysql -e option.	2020-06-01	<a href="#">9</a>	<a href="#">CVE-2020-13694 MISC</a>
quickbox --quickbox_community_and_quickbox_pro	QuickBox Community Edition through 2.5.5 and Pro Edition through 2.1.8 allows <del>and authenticates</del> remote attacker to execute code on the server via command injection in the servicestart parameter.	2020-06-01	<a href="#">9</a>	<a href="#">CVE-2020-13448 MISC MISC</a>
rconfig -- rconfig	rConfig 3.9.4 and previous versions has unauthenticated devices.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-10548 MISC</a>
rconfig -- rconfig	rConfig 3.9.4 and previous versions has unauthenticated snippets.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-10549 MISC</a>
rconfig -- rconfig	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicies.inc.php SQL injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-10546 MISC</a>
	rConfig 3.9.4 and previous versions has unauthenticated compliancepolicyelements.inc.php SQL			<a href="#">CVE-2020-</a>

rconfig -- rconfig	injection. Because, by default, nodes' passwords are stored in cleartext, this vulnerability leads to lateral movement, granting an attacker access to monitored network devices.	2020-06-04	<a href="#">7.5</a>	<a href="#">10547 MISC</a>
sabberworm -- php_css_parser	Sabberworm PHP CSS Parser before 8.3.1 calls eval on uncontrolled data, possibly leading to remote code execution if the function allSelectors() or getSelectorsBySpecificity() is called with input from an attacker.	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-13756 MISC MISC MISC MISC</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with Q(10.0) (with TEEGRIS on Exynos chipsets) software. The Widevine Trustlet allows arbitrary code execution because of memory disclosure, The Samsung IDs are SVE-2020-17117, SVE-2020-17118, SVE-2020-17119, and SVE-2020-17161 (June 2020).	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-13832 CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software. The Trustonic Kinibi component allows arbitrary memory mapping. The Samsung ID is SVE-2019-16665 (June 2020).	2020-06-04	<a href="#">7.5</a>	<a href="#">CVE-2020-13831 CONFIRM</a>
swarco -- cpu_ls4000_series	An open port used for debugging in SWARCOs CPU LS4000 Series with versions starting with G4... grants root access to the device without access control via network. A malicious user could use this vulnerability to get access to the device and disturb operations with connected devices.	2020-05-29	<a href="#">10</a>	<a href="#">CVE-2020-12493 CONFIRM</a>
systemd -- systemd	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-100082.	2020-06-03	<a href="#">10</a>	<a href="#">CVE-2020-13776 MISC</a>
verizon -- serialize-javascript	serialize-javascript prior to 3.1.0 allows remote attackers to inject arbitrary code via the function "deleteFunctions" within "index.js".	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2020-7660 MISC</a>
wordpress -- wordpress	An unauthenticated privilege-escalation issue exists in the bbPress plugin before 2.6.5 for WordPress when New User Registration is enabled.	2020-05-29	<a href="#">7.5</a>	<a href="#">CVE-2020-13693 MISC MISC MISC MISC</a>



## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2pisoftware -- cmfive	system/classes/DbPDO.php in Cmfive through 2015-03-15, when database connectivity malfunctions, allows remote attackers to obtain sensitive information (username and password) via any request, such as a password reset request.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2014-9702</a> <a href="#">MISC</a>
apache -- ignite	Apache Ignite uses H2 database to build SQL distributed execution engine. H2 provides SQL functions which could be used by attacker to access to a filesystem.	2020-06-03	<a href="#">6.4</a>	<a href="#">CVE-2020-1963</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
atlassian -- companion_app	The file downloading functionality in the Atlassian Companion App before version 1.0.0 allows remote attackers, who control a Confluence Server instance that the Companion App is connected to, execute arbitrary .exe files via a Protection Mechanism Failure.	2020-06-01	<a href="#">6.5</a>	<a href="#">CVE-2020-4020</a> <a href="#">MISC</a>
atlassian -- companion_app	The file editing functionality in the Atlassian Companion App before version 1.0.0 allows local attackers to have the app run a different executable in place of the app's cmd.exe via a untrusted search path vulnerability.	2020-06-01	<a href="#">4.4</a>	<a href="#">CVE-2020-4019</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /plugins/servlet/jira-blockers/resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get the ID of configured Jira application links via an information disclosure vulnerability.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-4016</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /json/fe/activeUserFinder.do resource in Altassian Fisheye and Crucible before version 4.8.1 allows remote attackers to view user user email addresses via a information disclosure vulnerability.	2020-06-01	<a href="#">4</a>	<a href="#">CVE-2020-4015</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /rest/jira-ril/1.0/jira-rest/applinks resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-4017</a> <a href="#">MISC</a>

	get information about any configured Jira application links via an information disclosure vulnerability.			<a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /profile/deleteWatch.do resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to remove another user's watching settings for a repository via an improper authorization vulnerability.	2020-06-01	<a href="#">4</a>	<a href="#">CVE-2020-4014</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The review coverage resource in Atlassian Fisheye and Crucible before version 4.8.2 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the committerFilter parameter.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2020-4023</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The setup resources in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to complete the setup process via a cross-site request forgery (CSRF) vulnerability.	2020-06-01	<a href="#">6.8</a>	<a href="#">CVE-2020-4018</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- navigator_links	The CustomAppsRestResource list resource in Atlassian Navigator Links before version 3.3.23, from version 4.0.0 before version 4.3.7, from version 5.0.0 before 5.0.1, and from version 5.1.0 before 5.1.1 allows remote attackers to enumerate all linked applications, including those that are restricted or otherwise hidden, through an incorrect authorization check.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-4026</a> <a href="#">MISC</a> <a href="#">MISC</a>
bitrix -- bitrix24	modules/security/classes/general.post_filter.php/post_filter.php in the Web Application Firewall in Bitrix24 through 20.0.950 allows XSS by placing %00 before the payload.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2020-13758</a> <a href="#">MISC</a>
celluloid -- reel	reel through 0.6.1 allows Request Smuggling attacks due to incorrect Content-Length and Transfer encoding header parsing. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks. Note: This project is deprecated, and is not maintained any more.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-7659</a> <a href="#">MISC</a>
cisco -- multiple_products	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-10136</a> <a href="#">CERT-VN</a> <a href="#">MISC</a>

	exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors.			<a href="#">MISC</a>
cisco -- prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database.	2020-06-03	<a href="#">6.4</a>	<a href="#">CVE-2020-3339</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-3322</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-3321</a> <a href="#">CISCO</a>

	user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.			
compound -- finance_compound_price_oracle	The price oracle in PriceOracle.sol in Compound Finance Compound Price Oracle 1.0 through 2.0 allows a price oracle to set an invalid asset price via the setPrice function, and consequently violate the intended limits on price swings.	2020-06-03	5	<a href="#">CVE-2019-20809</a> <a href="#">MISC</a>
cybele -- thinfinity_virtualUI	Cybele Thinfinitiy VirtualUI 2.5.17.2 allows HTTP response splitting via the mimetype parameter within a PDF viewer request, as demonstrated by an example.pdf?mimetype= substring. The victim user must load an application request to view a PDF, containing the malicious payload. This results in a reflected XSS payload being executed.	2020-06-04	4.3	<a href="#">CVE-2019-16385</a> <a href="#">MISC</a>
cybele -- thinfinity_virtualui	Cybele Thinfinitiy VirtualUI 2.5.17.2 allows ../ path traversal that can be used for data exfiltration. This enables files outside of the web directory to be retrieved if the exact location is known and the user has permissions.	2020-06-04	4	<a href="#">CVE-2019-16384</a> <a href="#">MISC</a>
d-link -- dir- 856l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices allow CSRF.	2020-06-03	6.8	<a href="#">CVE-2020-13786</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Transmission of Sensitive Information.	2020-06-03	5	<a href="#">CVE-2020-13787</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Inadequate Encryption Strength.	2020-06-03	5	<a href="#">CVE-2020-13785</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have a predictable seed in a Pseudo-Random Number Generator.	2020-06-03	5	<a href="#">CVE-2020-13784</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Storage of Sensitive Information.	2020-06-03	5	<a href="#">CVE-2020-13783</a> <a href="#">MISC</a>
django-project -- django	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. Query parameters generated by the Django admin ForeignKeyRawIdWidget were not properly URL encoded, leading to a possibility of an XSS attack.	2020-06-03	4.3	<a href="#">CVE-2020-13596</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. In			<a href="#">CVE-2020-</a>

django_project -- django	cases where a memcached backend does not perform key validation, passing malformed cache keys could result in a key collision, and potential data leakage.	2020-06-03	5	<a href="#">13254</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
elastic -- elastic_app_search	Elastic App Search versions before 7.7.0 contain a cross site scripting (XSS) flaw when displaying document URLs in the Reference UI. If the Reference UI injects a URL into a result, that URL will be rendered by the web browser. If an attacker is able to control the contents of such a field, they could execute arbitrary JavaScript in the victim's web browser.	2020-06-03	4.3	<a href="#">CVE-2020-7011</a> <a href="#">N/A</a>
elastic -- elastic_cloud_on_kubernetes	Elastic Cloud on Kubernetes (ECK) versions prior to 1.1.0 generate passwords using a weak random number generator. If an attacker is able to determine when the current Elastic Stack cluster was deployed they may be able to more easily brute force the Elasticsearch credentials generated by ECK.	2020-06-03	5	<a href="#">CVE-2020-7010</a> <a href="#">N/A</a>
elastic -- kibana	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	2020-06-03	6.5	<a href="#">CVE-2020-7013</a> <a href="#">N/A</a>
elastic -- kibana	Kibana versions 6.7.0 to 6.8.8 and 7.0.0 to 7.6.2 contain a prototype pollution flaw in the Upgrade Assistant. An authenticated attacker with privileges to write to the Kibana index could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	2020-06-03	6.5	<a href="#">CVE-2020-7012</a> <a href="#">N/A</a>
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows directory traversal via the log-handling feature.	2020-06-01	5	<a href="#">CVE-2014-7174</a> <a href="#">MISC</a>
fastecdsa -- fastecdsa	An issue was discovered in fastecdsa before 2.1.2. When using the NIST P-256 curve in the ECDSA implementation, the point at infinity is mishandled. This means that for an extreme value in k and s <sup>-1</sup> , the signature verification fails even if the signature is correct. This behavior is not solely a usability problem. There are	2020-06-02	5	<a href="#">CVE-2020-12607</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>



	some threat models where an attacker can benefit by successfully guessing users for whom signature verification will fail.			<a href="#">CONFIRM</a>
fortiguard -- forticlient_for_windows	An Insecure Temporary File vulnerability in FortiClient for Windows 6.2.1 and below may allow a local user to gain elevated privileges via exhausting the pool of temporary file names combined with a symbolic link attack.	2020-06-01	<a href="#">4.6</a>	<a href="#">CVE-2020-9291</a> <a href="#">MISC</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20813</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows stack consumption via nested function calls for XML parsing.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20815</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20816</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows memory consumption because data is created for each page of an application level.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20814</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac_and_foxit_reader_for_mac	An issue was discovered in Foxit PhantomPDF Mac and Foxit Reader for Mac before 9.7. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13803</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows memory consumption because data is created for each page of an application level.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20818</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20837</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has homograph mishandling.	2020-06-04	<a href="#">4.3</a>	<a href="#">CVE-2019-20835</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2019-20820</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has a use-after-free because of JavaScript execution after a deletion or close operation.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13806</a> <a href="#">CONFIRM</a>

foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has circular reference mishandling that causes a loop.	2020-06-04	5	<a href="#">CVE-2020-13807</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via crafted cross-reference stream data.	2020-06-04	5	<a href="#">CVE-2020-13808</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via long strings in the content stream.	2020-06-04	5	<a href="#">CVE-2020-13809</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference.	2020-06-04	5	<a href="#">CVE-2019-20817</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows stack consumption via nested function calls for XML parsing.	2020-06-04	5	<a href="#">CVE-2019-20819</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has brute-force attack mishandling because the CAS service lacks a limit on login failures.	2020-06-04	5	<a href="#">CVE-2020-13805</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	2020-06-04	5	<a href="#">CVE-2019-20828</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	2020-06-04	5	<a href="#">CVE-2019-20829</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has mishandling of cloud credentials, as demonstrated by Google Drive.	2020-06-04	5	<a href="#">CVE-2019-20836</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows information disclosure of a hardcoded username and password in the DocuSign plugin.	2020-06-04	6.8	<a href="#">CVE-2020-13804</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, when running with logger set to "WLOG_TRACE", a possible crash of application could occur due to a read of an invalid array index. Data could be printed as string to local terminal. This has been fixed in 2.1.0.	2020-05-29	5	<a href="#">CVE-2020-11019</a> <a href="#">CONFIRM</a>
	In FreeRDP before 2.1.0, there is an out-of-bounds read in			<a href="#">CVE-2020-</a>

freerdp -- freerdp	clipdr_read_format_list. Clipboard format data read (by client or server) might read data out-of-bounds. This has been fixed in 2.1.0.	2020-05-29	<a href="#">6.4</a>	<a href="#">11085</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_NegotiateMessage. This has been fixed in 2.1.0.	2020-05-29	<a href="#">5.5</a>	<a href="#">CVE-2020-11088</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_AuthenticateMessage. This has been fixed in 2.1.0.	2020-05-29	<a href="#">5.5</a>	<a href="#">CVE-2020-11087</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_ntlm_v2_client_challenge that reads up to 28 bytes out-of-bound to an internal structure. This has been fixed in 2.1.0.	2020-05-29	<a href="#">5.5</a>	<a href="#">CVE-2020-11086</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bounds read in rfx_process_message_tileset. Invalid data fed to RFX decoder results in garbage on screen (as colors). This has been patched in 2.1.0.	2020-05-29	<a href="#">5</a>	<a href="#">CVE-2020-11043</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound data read from memory in clear_decompress_subcode_rlex, visualized on screen as color. This has been patched in 2.1.0.	2020-05-29	<a href="#">4</a>	<a href="#">CVE-2020-11040</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, an outside controlled array index is used unchecked for data used as configuration for sound backend (alsa, oss, pulse, ...). The most likely outcome is a crash of the client instance followed by no or distorted sound or a session disconnect. If a user cannot upgrade to the patched version, a workaround is to disable sound for the session. This has been patched in 2.1.0.	2020-05-29	<a href="#">4</a>	<a href="#">CVE-2020-11041</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP before 2.1.0, there is an out-of-bound read in irp functions (parallel_process_irp_create, serial_process_irp_create, drive_process_irp_write, printer_process_irp_write, rdpei_rcv_pdu, serial_process_irp_write). This has been fixed in 2.1.0.	2020-05-29	<a href="#">6.5</a>	<a href="#">CVE-2020-11089</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- chrome	Incorrect implementation in permissions in Google Chrome prior to 80.0.3987.87	2020-06-	<a href="#">4.3</a>	<a href="#">CVE-2020-6502</a>

	allowed a remote attacker to spoof security UI via a crafted HTML page.	03		<a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.97 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6495</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass AppCache security restrictions via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6499</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in interstitials in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6500</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds write in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6419</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in CSP in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6501</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use after free in WebAuthentication in Google Chrome prior to 83.0.4103.97 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6493</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6453</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in V8 in Google Chrome prior to 14.0.0.0 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2011-2863</a> <a href="#">MISC</a>
google -- chrome	Bad cast in CSS in Google Chrome prior to 11.0.0.0 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2011-1805</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in notifications in Google Chrome prior to 74.0.3729.108 allowed a remote attacker	2020-06-	<a href="#">4.3</a>	<a href="#">CVE-2020-6504</a>

	to bypass notification restrictions via a crafted HTML page.	03		<a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_android	Incorrect security UI in payments in Google Chrome on Android prior to 83.0.4103.97 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6494</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_ios	Incorrect implementation in user interface in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6498</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_ios	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted URI.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6497</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_macos	Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6496</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana_labs -- grafana	The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-13379</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via a link on the "Dashboard > All Panels > General" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18625</a> <a href="#">MISC</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via the "Dashboard > Text Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18623</a> <a href="#">MISC</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via a column style on the "Dashboard > Table Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18624</a> <a href="#">MISC</a>
huawei -- cloudengine_12800_products	CloudEngine 12800 products with versions of V200R019C00, V200R019C10SPC800, V200R019C00SPC600, V200R019C10; and CloudEngine 6800 products with versions of V200R019C00SPC800 have potential of service vulnerability. Due to improper memory management, memory	2020-05-29	<a href="#">5</a>	<a href="#">CVE-2020-1870</a> <a href="#">CONFIRM</a>



	leakage may occur in some special cases. Attackers can perform a series of operations to exploit this vulnerability. Successful exploit may cause a denial of service.			
huawei -- e6878-370_products	E6878-370 products with versions of 10.0.3.1(H557SP27C233) and 10.0.3.1(H563SP1C00) have a stack buffer overflow vulnerability. The program copies an input buffer to an output buffer without verification. An attacker in the adjacent network could send a crafted message, successful exploit could lead to stack buffer overflow which may cause malicious code execution.	2020-05-29	5.8	<a href="#">CVE-2020-1832</a> <a href="#">CONFIRM</a>
huawei -- multiple_products	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario. Affected product versions include: AR120-S versions V200R007C00SPC900, V200R007C00SPCa00	2020-06-01	4	<a href="#">MISC</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178965.	2020-06-02	4.3	<a href="#">CVE-2020-4366</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 179001.	2020-06-02	5	<a href="#">CVE-2020-4367</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182283.	2020-06-02	4.3	<a href="#">CVE-2020-4503</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- qradar_siem	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit	2020-06-04	5.5	<a href="#">CVE-2020-4509</a> <a href="#">XF</a>

	this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182364.			<a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174738.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-4182</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10.6, 11.0, and 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174851.	2020-06-03	<a href="#">4.6</a>	<a href="#">CVE-2020-4190</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 174857.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-4193</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 could disclose sensitive information on the login page that could aid in further attacks against the system. IBM X-Force ID: 174805.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-4187</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174739.	2020-06-04	<a href="#">4.3</a>	<a href="#">CVE-2020-4183</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
istio -- istio	Istio 1.4.x before 1.4.9 and Istio 1.5.x before 1.5.4 contain the following vulnerability when telemetry v2 is enabled: by sending a specially crafted packet, an attacker could trigger a Null Pointer Exception resulting in a Denial of Service. This could be sent to the ingress gateway or a sidecar, triggering a null pointer exception which results in a denial of service. This also affects servicemesh-proxy where a null pointer exception flaw was found in servicemesh-proxy. When running Telemetry v2 (not on by default in version 1.4.x), an attacker could send a specially crafted packet to the ingress gateway or proxy sidecar, triggering a	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-10739</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	denial of service.			
jenkins -- jenkins	Jenkins Play Framework Plugin 1.0.2 and earlier lets users specify the path to the `play` command on the Jenkins master for a form validation endpoint, resulting in an OS command injection vulnerability exploitable by users able to store such a file on the Jenkins master.	2020-06-03	<a href="#">6.5</a>	<a href="#">CVE-2020-2200</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Subversion Partial Release Manager Plugin 1.0.1 and earlier does not escape the error message for the repository URL field form validation, resulting in a reflected cross-site scripting vulnerability.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-2199</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier allows attackers to add or remove agent labels.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-2192</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier does not check permissions on API endpoints that allow adding and removing agent labels.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2191</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not redact encrypted secrets in the 'getConfigAsXML' API URL when transmitting job config.xml data to users without Job/Configure.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2198</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not require users to have Job/ExtendedRead permission to access Inheritance Project job configurations in XML format.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2197</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Selenium Plugin 3.141.59 and earlier has no CSRF protection for its HTTP endpoints, allowing attackers to perform all administrative actions provided by the plugin.	2020-06-03	<a href="#">6</a>	<a href="#">CVE-2020-2196</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	In Joomla! before 3.9.19, lack of input validation in the heading tag option of the "Articles - Newsflash" and "Articles - Categories" modules allows XSS.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13761</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, the default settings of the global textfilter configuration do not block HTML inputs for Guest users.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13763</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, missing token checks in com_postinstall lead to CSRF.	2020-06-02	<a href="#">6.8</a>	<a href="#">CVE-2020-13760</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, incorrect input validation of the module tag option in	2020-06-	<a href="#">4.3</a>	<a href="#">CVE-2020-13762</a>

	com_modules allows XSS.	02		<a href="#">MISC</a>
kubernetes -- containernetworking/plugins	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious containers in Kubernetes clusters to perform man-in-the-middle (MitM) attacks. A malicious container can exploit this flaw by sending rogue IPv6 router advertisements to the host or other containers, to redirect traffic to the malicious container.	2020-06-03	<a href="#">6</a>	<a href="#">CVE-2020-10749</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libjpeg-turbo -- libjpeg-turbo	libjpeg-turbo 2.0.4, and mozjpeg 4.0.0, has a heap-based buffer over-read in get_rgb_row() in rdppm.c via a malformed PPM input file.	2020-06-03	<a href="#">5.8</a>	<a href="#">CVE-2020-13790</a> <a href="#">MISC</a> <a href="#">MISC</a>
libvirt -- libvirt	A NULL pointer dereference was found in the libvirt API responsible introduced in upstream version 3.10.0, and fixed in libvirt 6.0.0, for fetching a storage pool based on its target path. In more detail, this flaw affects storage pools created without a target path such as network-based pools like gluster and RBD. Unprivileged users with a read-only connection could abuse this flaw to crash the libvirt daemon, resulting in a potential denial of service.	2020-06-02	<a href="#">4</a>	<a href="#">CVE-2020-10703</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	go7007_snd_init in drivers/media/usb/go7007/snd-go7007.c in the Linux kernel before 5.6 does not call snd_card_free for a failure path, which causes a memory leak, aka CID-9453264ef586.	2020-06-03	<a href="#">4.9</a>	<a href="#">CVE-2019-20810</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.4.7. The prb_calc_retire_blk_tmo() function in net/packet/af_packet.c can result in a denial of service (CPU consumption and soft lockup) in a certain failure case involving TPACKET_V3, aka CID-b43d1f9f7067.	2020-06-03	<a href="#">4.9</a>	<a href="#">CVE-2019-20812</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki -- mediawiki	resources/src/mediawiki.page.ready/ready.js in MediaWiki before 1.35 allows remote attackers to force a logout and external redirection via HTML content in a MediaWiki page.	2020-06-02	<a href="#">5.8</a>	<a href="#">CVE-2020-10959</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mulesoft -- mulesoft_ce/ee	A Denial of Service vulnerability in MuleSoft Mule CE/EE 3.8.x, 3.9.x, and 4.x released before April 7, 2020, could allow remote attackers to submit data which can lead to resource exhaustion.	2020-05-29	<a href="#">5</a>	<a href="#">CVE-2020-6937</a> <a href="#">CONFIRM</a>

naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/feeds/feed.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13798</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/structure/structure.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13796</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/websites/website.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13797</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows Directory Traversal because lib/packages/templates/template.class.php mishandles ../ and ../ substrings.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-13795</a> <a href="#">MISC</a> <a href="#">MISC</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to delete arbitrary local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5296</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to upload jpg, jpeg, bmp, png, webp, gif, ico, css, js, woff, woff2, svg, ttf, eot, json, md, less, sass, scss, xml files to any directory of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5297</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to read local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5295</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phplist -- phplist	phplist before 3.5.4 allows XSS via /lists/admin/user.php and /lists/admin/users.php.	2020-06-04	<a href="#">4.3</a>	<a href="#">CVE-2020-13827</a> <a href="#">MISC</a>



pi-hole -- pi-hole_web	Pi-hole Web v4.3.2 (aka AdminLTE) allows Remote Code Execution by privileged dashboard users via a crafted DHCP static lease.	2020-05-29	6.5	<a href="#">CVE-2020-8816</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows CSRF.	2020-06-01	6.8	<a href="#">CVE-2014-8942</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows denial of service because api/update.php launches svn update operations that use a great deal of resources.	2020-06-01	5	<a href="#">CVE-2014-8937</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (full path) via an include/smarty/plugins/modifier.date_format.php request if PHP has a non-recommended configuration that produces warning messages.	2020-06-01	4.3	<a href="#">CVE-2014-8939</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (names and details of projects) by visiting the /update.log URI.	2020-06-01	5	<a href="#">CVE-2014-8940</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows SSRF via the admin.php?page=projects svn_url parameter.	2020-06-01	6.5	<a href="#">CVE-2014-8943</a> <a href="#">MISC</a>
playtube -- playtube	PlayTube 1.8 allows disclosure of user details via ajax.php?type=../admin-panel/autoload&page=manage-users directory traversal, aka local file inclusion.	2020-06-03	4	<a href="#">CVE-2020-13792</a> <a href="#">MISC</a>
python-rsa -- python-rsa	Python-RSA 4.0 ignores leading ' ' bytes during decryption of ciphertext. This could conceivably have a security-relevant impact, e.g., by helping an attacker to infer that an application uses Python-RSA, or if the length of accepted ciphertext affects application behavior (such as by causing excessive memory allocation).	2020-06-01	5	<a href="#">CVE-2020-13757</a> <a href="#">MISC</a>
qemu -- qemu	address_space_map in exec.c in QEMU 4.2.0 can trigger a NULL pointer dereference related to BounceBuffer.	2020-06-02	5	<a href="#">CVE-2020-13659</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
qemu -- qemu	hw/pci/msix.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access via a crafted address in an msi-x mmio operation.	2020-06-02	4.6	<a href="#">CVE-2020-13754</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
	A race condition can occur when using			

qualcomm -- multiple_snapdragon_products	the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130	2020-06-02	<a href="#">6.9</a>	<a href="#">CVE-2020-3680</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2020-3630</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2020-3610</a> <a href="#">CONFIRM</a>
	Out of bound memory access while processing qpay due to not validating			

qualcomm -- multiple_snapdragon_processors	length of the response buffer provided by User. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, MSM8909, MSM8998, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845	2020-06-02	4.6	<a href="#">CVE-2019-14078</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_processors	Out of bound memory access while processing ese transmit command due to passing Response buffer received from user in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9607, MDM9650, MSM8909, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	4.6	<a href="#">CVE-2019-14077</a> <a href="#">CONFIRM</a>
rust-vmm -- vm-memory	rust-vmm vm-memory before 0.1.1 and 0.2.x before 0.2.1 allows attackers to cause a denial of service (loss of IP networking) because read_obj and write_obj do not properly access memory. This affects aarch64 (with musl or glibc) and x86_64 (with musl).	2020-06-02	5	<a href="#">CVE-2020-13759</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) software. One UI HOME logging can leak information. The Samsung ID is SVE-2019-16382 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13830</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x) (with TEEGRIS) software. The Gatekeeper Trustlet allows a brute-force attack on user credentials. The Samsung ID is SVE-2020-16908 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13835</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The system area allows arbitrary file overwrites via a symlink attack. The Samsung ID is SVE-2020-17183 (June 2020).	2020-06-04	6.4	<a href="#">CVE-2020-13833</a> <a href="#">CONFIRM</a>

samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. HWRResProvider allows path traversal for data exposure. The Samsung ID is SVE-2020-16954 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13836</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (with TEEGRIS) software. SecureFolder does not properly restrict use of Android Debug Bridge (adb) for arbitrary installations. The Samsung ID is SVE-2020-17369 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13834</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can disable the SEAndroid protection mechanism in the RKP. The Samsung ID is SVE-2019-15998 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13829</a> <a href="#">CONFIRM</a>
synk -- broker	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network by creating symlinks to match whitelisted paths.	2020-05-29	4	<a href="#">CVE-2020-7653</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.73.1 are vulnerable to Information Exposure. It logs private keys if logging level is set to DEBUG.	2020-05-29	4.3	<a href="#">CVE-2020-7654</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.72.2 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users who have access to Snyk's internal network by appending the URL with a fragment identifier and a whitelisted path e.g. `#package.json`	2020-05-29	4	<a href="#">CVE-2020-7648</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network via directory traversal.	2020-05-29	4	<a href="#">CVE-2020-7652</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker after 4.72.0 including and before 4.73.1 are vulnerable to Arbitrary File Read. It allows arbitrary file reads to users with access to Snyk's internal network of any files ending in the following extensions: yaml, yml or json.	2020-05-29	4	<a href="#">CVE-2020-7650</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.79.0 are vulnerable to Arbitrary File Read. It allows partial file reads for users who	2020-05-	4	<a href="#">CVE-2020-7651</a>

	have access to Snyk's internal network via patch history from GitHub Commits API.	29		<a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. An attacker can determine the username (under which the web server is running) by triggering an invalid path permission error. This bypasses the fakepath protection mechanism.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13227</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. There is reflected XSS via the /scgi sid parameter.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13228</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. A session can be hijacked if one observes the sid value in any /scgi URI, because it is an authentication token.	2020-06-02	<a href="#">6.8</a>	<a href="#">CVE-2020-13229</a> <a href="#">MISC</a> <a href="#">MISC</a>
upx -- upx	p_lx_elf.cpp in UPX before 3.96 has an integer overflow during unpacking via crafted values in a PT_DYNAMIC segment.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2019-20805</a> <a href="#">MISC</a> <a href="#">MISC</a>
vmware -- multiple_products	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior) and VMware Horizon Client for Mac (5.x and prior) contain a local privilege escalation vulnerability due to a Time-of-check Time-of-use (TOCTOU) issue in the service opener. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC and Horizon Client are installed.	2020-05-29	<a href="#">6.9</a>	<a href="#">CVE-2020-3957</a> <a href="#">CONFIRM</a>
vmware -- spring_cloud_config	Spring Cloud Config, versions 2.2.x prior to 2.2.3, versions 2.1.x prior to 2.1.9, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-5410</a> <a href="#">CONFIRM</a>
websocket-extensions -- websocket-extensions	websocket-extensions ruby module prior to 0.1.5 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-7663</a> <a href="#">MISC</a> <a href="#">MISC</a>



	could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.			<a href="#">MISC</a> <a href="#">MISC</a>
websocket-extensions -- websocket-extensions	websocket-extensions npm module prior to 1.0.4 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-7662</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	common.php in the Gravity Forms plugin before 2.4.9 for WordPress can leak hashed passwords because user_pass is not considered a special case for a \$current_user->get(\$property) call.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13764</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The MailPoet plugin before 3.23.2 for WordPress allows remote attackers to inject arbitrary web script or HTML using extra parameters in the URL (Reflective Server-Side XSS).	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2019-11843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zimbra -- zimbra	Zimbra before 8.8.15 Patch 10 and 9.x before 9.0.0 Patch 3 allows remote code execution via an avatar file. There is potential abuse of /service/upload servlet in the webmail subsystem. A user can upload executable files (exe,sh,bat,jar) in the Contact section of the mailbox as an avatar image for a contact. A user will receive a "Corrupt File" error, but the file is still uploaded and stored locally in /opt/zimbra/data/tmp/upload/, leaving it open to possible remote execution.	2020-06-03	<a href="#">6</a>	<a href="#">CVE-2020-12846</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
znc -- znc	ZNC 1.8.0 up to 1.8.1-rc1 allows attackers to trigger an application crash (with a NULL pointer dereference) if echo-message is not enabled and there is no network.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13775</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zoho -- manageengine_opmanager	In Zoho ManageEngine OpManager before 125144, when <cachestart> is used, directory traversal validation can be bypassed.	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13818</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- device_library_wizard	Insecure storage of sensitive information in ABB Device Library Wizard versions 6.0.X, 6.0.3.1 and 6.0.3.2 allows unauthenticated low privilege user to read file that contains confidential data	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-8482</a> <a href="#">CONFIRM</a>
atlassian -- fisheye_and_crucible	The review resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the review objectives.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2020-4013</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira_server_and_data_center	Affected versions are: Before 8.5.5, and from 8.6.0 before 8.8.1 of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the XML export view.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2020-4021</a> <a href="#">MISC</a>
avaya -- ip_office	A sensitive information disclosure vulnerability was discovered in the web interface component of IP Office that may potentially allow a local user to gain unauthorized access to the component. Affected versions of IP Office include: 9.x, 10.0 through 10.1.0.7 and 11.0 though 11.0.4.3.	2020-06-04	<a href="#">2.1</a>	<a href="#">CVE-2020-7030</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
elastic -- kibana	Kibana versions before 6.8.9 and 7.7.0 contains a stored XSS flaw in the TSVB visualization. An attacker who is able to edit or create a TSVB visualization could allow the attacker to obtain sensitive information from, or perform destructive actions, on behalf of Kibana users who edit the TSVB visualization.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-7015</a> <a href="#">N/A</a>
fortiguard -- fortianalyzer	An improper neutralization of input vulnerability in the Admin Profile of FortiAnalyzer may allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the Description Area.	2020-06-04	<a href="#">3.5</a>	<a href="#">CVE-2020-6640</a> <a href="#">MISC</a>
huawei -- honor_9x_smartphones	Honor 9X smartphones with versions earlier than 9.1.1.172(C00E170R8P1) have an improper authentication vulnerability. A logic error occurs when handling clock function, an attacker should do a series of crafted operations	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1833</a>

	quickly before the phone is unlocked, successful exploit could allow the attacker to access clock information without unlock the phone.			<a href="#">CONFIRM</a>
huawei -- mate_10_smartphones	HUAWEI Mate 10 smartphones with versions earlier than 10.0.0.143(C00E143R2P4) have an information disclosure vulnerability. The attacker could wake up voice assistant then do a series of crafted voice operation, successful exploit could allow the attacker read certain files without unlock the phone leading to information disclosure.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1809</a> <a href="#">CONFIRM</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.185(C00E74R3P8) have an improper authorization vulnerability. The system does not properly restrict certain operation in ADB mode, successful exploit could allow certain user break the limit of digital balance function.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1797</a> <a href="#">CONFIRM</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.195(SP31C00E74R3P8) have an improper authorization vulnerability. The digital balance function does not sufficiently restrict the using time of certain user, successful exploit could allow the user break the limit of digital balance function after a series of operations with a PC.	2020-05-29	<a href="#">1.9</a>	<a href="#">CVE-2020-1831</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178765.	2020-06-02	<a href="#">3.5</a>	<a href="#">CVE-2020-4360</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 180761.	2020-06-02	<a href="#">3.5</a>	<a href="#">CVE-2020-4431</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 could allow an attacker on the same network to gain access to the Solr dashboard and cause a denial of service attack. IBM X-Force	2020-06-03	<a href="#">3.3</a>	<a href="#">CVE-2020-4307</a> <a href="#">XF</a>

	ID: 176997.			<a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174852.	2020-06-04	<a href="#">2.1</a>	<a href="#">CVE-2020-4191</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Compact Columns Plugin 1.11 and earlier displays the unprocessed job description in tooltips, resulting in a stored cross-site scripting vulnerability that can be exploited by users with Job/Configure permission.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2195</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Script Security Plugin 1.72 and earlier does not correctly escape pending or approved classpath entries on the In-process Script Approval page, resulting in a stored cross-site scripting vulnerability.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2190</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the display name of the builds in the trend chart, resulting in a stored cross-site scripting vulnerability.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2194</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the parser identifier when rendering charts, resulting in a stored cross-site scripting vulnerability.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-2193</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.6. In rx_queue_add_kobject() and netdev_queue_add_kobject() in net/core/net-sysfs.c, a reference count is mishandled, aka CID-a3e23f719f5c.	2020-06-03	<a href="#">2.1</a>	<a href="#">CVE-2019-20811</a> <a href="#">MISC</a> <a href="#">MISC</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, a user with the ability to use the import functionality of the `ImportExportController` behavior can be socially engineered by an attacker to upload a maliciously crafted CSV file which could result in a reflected XSS attack on the user in question Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-5298</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows XSS (Reflected) via the username, or XSS (Stored) via the admin.php?page=config install_name, intro_message, or new_file_content parameter.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2014-8944</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows local users to obtain sensitive information by listing a process because the username and password are on the command line.	2020-06-01	<a href="#">2.1</a>	<a href="#">CVE-2014-8938</a> <a href="#">MISC</a>

qualcomm -- multiple_snapdragon_products	When attempting to create a new XFRM policy, a stack out-of-bounds read will occur if the user provides a template where the mode is set to a value that does not resolve to a valid XFRM mode in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCA4531, QCN7605, QCS605, QM215, SA415M, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	3.6	<a href="#">CVE-2019-14053</a> CONFIRM
qualcomm -- multiple_snapdragon_products	Buffer over-read in ADSP parse function due to lack of check for availability of sufficient data payload received in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710, SDM845, SDX20, SDX24	2020-06-02	3.6	<a href="#">CVE-2019-14038</a> CONFIRM
qualcomm -- multiple_snapdragon_products	Out of bound read in adm call back function due to incorrect boundary check for payload in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710,	2020-06-02	3.6	<a href="#">CVE-2019-14039</a> CONFIRM



	SDM845, SDX20, SDX24			
qualcomm -- multiple_snapdragon_products	Using non-time-constant functions like memcmp to compare sensitive data can lead to information leakage through timing side channel issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	2020-06-02	2.1	<a href="#">CVE-2019-14067</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound read in Fingerprint application due to requested data is being used without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9150, MDM9205, MDM9650, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	3.6	<a href="#">CVE-2019-14043</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound read in in fingerprint application due to requested data assigned to a local buffer without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in	2020-06-02	3.6	<a href="#">CVE-2019-14042</a> <a href="#">CONFIRM</a>

	Kamorta, MDM9205, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with Q(10.0) software. The Lockscreen feature does not block Quick Panel access to Music Share. The Samsung ID is SVE-2020-17145 (June 2020).	2020-06-04	<a href="#">3.6</a>	<a href="#">CVE-2020-13837</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. The DeX Lockscreen feature does not block access to Quick Panel and notifications. The Samsung ID is SVE-2020-17187 (June 2020).	2020-06-04	<a href="#">3.6</a>	<a href="#">CVE-2020-13838</a> <a href="#">CONFIRM</a>
sane -- backends	A NULL pointer dereference in sanei_epson_net_read in SANE Backends through 1.0.29 allows a malicious device connected to the same local network as the victim to cause a denial of service, aka GHSL-2020-075.	2020-06-01	<a href="#">2.1</a>	<a href="#">CVE-2020-12867</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.5.2) and VMware Fusion (11.x before 11.5.2) contain a denial-of-service vulnerability in the shader functionality. Successful exploitation of this issue may allow attackers with non-administrative access to a virtual machine to crash the virtual machine's vmx process leading to a denial of service condition.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-3958</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.1.0) and VMware Fusion (11.x before 11.1.0) contain a memory leak vulnerability in the VMCI module. A malicious actor with local non-administrative access to a virtual machine may be able to crash the virtual machine's vmx process leading to a partial denial of service.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-3959</a> <a href="#">CONFIRM</a>
zte -- ft680_router	ZTE's PON terminal product is impacted by the access control vulnerability. Due to the system not performing correct access control on some program interfaces, an attacker could use this vulnerability to	2020-06-01	<a href="#">3.3</a>	<a href="#">CVE-2020-6868</a>

	tamper with the program interface parameters to perform unauthenticated operations. This affects: <ZTE F680> <V9.0.10P1N6>			<a href="#">MISC</a>
--	--	--	--	----------------------

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- unomi	Apache Unomi allows conditions to use OGNL scripting which offers the possibility to call static Java classes from the JDK that could execute code with the permission level of the running Java process.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11975</a> <a href="#">MISC</a>
apple -- multiple_products	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges.	2020-06-05	not yet calculated	<a href="#">CVE-2020-9859</a> <a href="#">MISC</a>
athom -- homey_and_homey_pro_devices	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks.	2020-06-04	not yet calculated	<a href="#">CVE-2020-9462</a> <a href="#">MISC</a>
bitdefender -- antivirus_free	A vulnerability in the improper handling of symbolic links in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects Bitdefender Antivirus Free versions prior to 1.0.17.178.	2020-06-05	not yet calculated	<a href="#">CVE-2020-8103</a> <a href="#">CONFIRM</a>
bludit -- bludit	showAlert() in the administration panel in Bludit 3.12.0 allows XSS.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13889</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to privilege escalation through the Adminstrator/Users/Edit/:UserId functionality. Adminstrator/Users/Edit/:UserId fails to check that the request was submitted by	2020-06-04	not yet calculated	<a href="#">CVE-2020-11679</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>

	an Administrator. This allows a normal user to escalate their privileges by adding additional roles to their account.			<a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to CSRF in all state-changing request. A __RequestVerificationToken is set by the web interface, and included in requests sent by web interface. However, this token is not verified by the application: the token can be removed from all requests and the request will succeed.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11682</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 stores and displays credentials for the associated SMTP server in cleartext. Low privileged users can exploit this to create an administrator user and obtain the SMTP credentials.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11681</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to authorization bypass on all administrator functionality. The application fails to check that a request was submitted by an administrator. Consequently, a normal user can perform actions including, but not limited to, creating/modifying the file store, creating/modifying alerts, creating/modifying users, etc.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11680</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
cisco -- 4300_series_integrated_services_routers_and_catalyst_9800-l_wireless_controllers	A vulnerability in the hardware crypto driver of Cisco IOS XE Software for Cisco 4300 Series Integrated Services Routers and Cisco Catalyst 9800-L Wireless Controllers could allow an unauthenticated, remote attacker to disconnect legitimate IPsec VPN sessions to an affected device. The vulnerability is due to insufficient verification of authenticity of received Encapsulating Security Payload (ESP) packets. An attacker could exploit this vulnerability by tampering with ESP cleartext values as a man-in-the-middle.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3220</a> <a href="#">CISCO</a>
cisco -- 809_and_829_industrial_services_routers	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first	2020-06-	not yet	<a href="#">CVE-2020-3208</a>

	<p>authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the attacker must have valid user credentials at privilege level 15.</p>	03	calculated	<a href="#">CISCO</a>
cisco -- application_services_engine_software	<p>A vulnerability in the key store of Cisco Application Services Engine Software could allow an authenticated, local attacker to read sensitive information of other users on an affected device. The vulnerability is due to insufficient authentication limitations. An attacker could exploit this vulnerability by logging in to an affected device locally with valid credentials. A successful exploit could allow the attacker to read the sensitive information of other users on the affected device.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3335</a> <a href="#">CISCO</a>
cisco -- application_services_engine_software	<p>A vulnerability in the API of Cisco Application Services Engine Software could allow an unauthenticated, remote attacker to update event policies on an affected device. The vulnerability is due to insufficient authentication of users who modify policies on an affected device. An attacker could exploit this vulnerability by crafting a malicious HTTP request to contact an affected device. A successful exploit could allow the attacker to update event policies on the affected device.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3333</a> <a href="#">CISCO</a>
cisco -- asr_920_series_aggregation_services	<p>A vulnerability in the Simple Network Management Protocol (SNMP) implementation in Cisco ASR 920 Series Aggregation Services Router model ASR920-12SZ-IM could allow an authenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect handling of data that is returned from Cisco Discovery Protocol queries to SNMP. An attacker could exploit this vulnerability by sending a request for Cisco Discovery Protocol information by using SNMP. An exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3232</a> <a href="#">CISCO</a>
	<p>A vulnerability in the 802.1X feature of</p>			



cisco -- catalyst-2960-l_series_switches_and_catalyst_cdb-8p_switches	<p>Cisco Catalyst 2960-L Series Switches and Cisco Catalyst CDB-8P Switches could allow an unauthenticated, adjacent attacker to forward broadcast traffic before being authenticated on the port. The vulnerability exists because broadcast traffic that is received on the 802.1X-enabled port is mishandled. An attacker could exploit this vulnerability by sending broadcast traffic on the port before being authenticated. A successful exploit could allow the attacker to send and receive broadcast traffic on the 802.1X-enabled port before authentication.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3231</a> <a href="#">CISCO</a>
cisco -- catalyst_4500_series_switches	<p>A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3235</a> <a href="#">CISCO</a>
cisco -- catalyst_9800_series_wireless_controllers	<p>A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3221</a> <a href="#">CISCO</a>

	to trigger an infinite loop, resulting in a process crash that would cause a reload of the device.			
cisco -- catalyst_9800_series_wireless_controllers	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3203</a> <a href="#">CISCO</a>
cisco -- catalyst_9800_series_wireless_controllers	A vulnerability in the handling of IEEE 802.11w Protected Management Frames (PMFs) of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to terminate a valid user connection to an affected device. The vulnerability exists because the affected software does not properly validate IEEE 802.11w disassociation and deauthentication PMFs that it receives. An attacker could exploit this vulnerability by sending a spoofed 802.11w PMF from a valid, authenticated client on a network adjacent to an affected device. A successful exploit could allow the attacker to terminate a single valid user connection to the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3206</a> <a href="#">CISCO</a>
cisco -- digital_network_architecture_center	A vulnerability in the audit logging component of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage	2020-06-03	not yet calculated	<a href="#">CVE-2020-3281</a> <a href="#">CISCO</a>

	network devices.			
cisco -- identity_services_engine	A vulnerability in the syslog processing engine of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a race condition that may occur when syslog messages are processed. An attacker could exploit this vulnerability by sending a high rate of syslog messages to an affected device. A successful exploit could allow the attacker to cause the Application Server process to crash, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3353</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by executing crafted Tcl arguments on an affected device. An exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3201</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to execute arbitrary code on the underlying operating system (OS) with root privileges. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to cause memory corruption or execute the code with root privileges on the underlying OS of the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3204</a> <a href="#">CISCO</a>
	A vulnerability in the Secure Shell (SSH) server code of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. The vulnerability is due to an internal state not being represented correctly in the SSH			

cisco -- ios_and_ios_xe_software	state machine, which leads to an unexpected behavior. An attacker could exploit this vulnerability by creating an SSH connection to an affected device and using a specific traffic pattern that causes an error condition within that connection. A successful exploit could allow an attacker to cause the device to reload, resulting in a denial of service (DoS) condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3200</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent IKEv2 from establishing new security associations. The vulnerability is due to incorrect handling of crafted IKEv2 SA-Init packets. An attacker could exploit this vulnerability by sending crafted IKEv2 SA-Init packets to the affected device. An exploit could allow the attacker to cause the affected device to reach the maximum incoming negotiation limits and prevent further IKEv2 security associations from being formed.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3230</a> <a href="#">CISCO</a>
cisco -- ios_xe_sd- wan_software	A vulnerability in Cisco IOS XE SD-WAN Software could allow an unauthenticated, physical attacker to bypass authentication and gain unrestricted access to the root shell of an affected device. The vulnerability exists because the affected software has insufficient authentication mechanisms for certain commands. An attacker could exploit this vulnerability by stopping the boot initialization of an affected device. A successful exploit could allow the attacker to bypass authentication and gain unrestricted access to the root shell of the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3216</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to insufficient input processing of CIP traffic. An attacker could exploit these vulnerabilities by sending crafted CIP traffic to be processed by an affected	2020-06-03	not yet calculated	<a href="#">CVE-2020-3225</a> <a href="#">CISCO</a>

	device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.			
cisco -- ios_xe_software	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to read arbitrary files on the underlying filesystem of the device. The vulnerability is due to insufficient file scope limiting. An attacker could exploit this vulnerability by creating a specific file reference on the filesystem and then accessing it through the web UI. An exploit could allow the attacker to read arbitrary files from the underlying operating system's filesystem.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3223</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker could exploit this vulnerability by uploading a crafted file to the web UI of an affected device. A successful exploit could allow the attacker to inject and execute arbitrary commands with root privileges on the device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3212</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with administrative privileges on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input to the web UI. A successful exploit could allow an attacker to execute arbitrary commands with administrative privileges on an affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3219</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the Session Initiation Protocol (SIP) library of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on received SIP messages. An attacker could exploit	2020-06-03	not yet calculated	<a href="#">CVE-2020-3226</a> <a href="#">CISCO</a>



	<p>this vulnerability by sending crafted SIP messages to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service condition.</p>			
cisco -- ios_xe_software	<p>A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with read-only privileges to inject IOS commands to an affected device. The injected commands should require a higher privilege level in order to be executed. The vulnerability is due to insufficient input validation of specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a specific web UI endpoint on an affected device. A successful exploit could allow the attacker to inject IOS commands to the affected device, which could allow the attacker to alter the configuration of the device or cause a denial of service (DoS) condition.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3224</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	<p>A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to bypass access control restrictions on an affected device. The vulnerability is due to the presence of a proxy service at a specific endpoint of the web UI. An attacker could exploit this vulnerability by connecting to the proxy service. An exploit could allow the attacker to bypass access restrictions on the network by proxying their access request through the management network of the affected device. As the proxy is reached over the management virtual routing and forwarding (VRF), this could reduce the effectiveness of the bypass.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3222</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	<p>A vulnerability in software image verification in Cisco IOS XE Software could allow an unauthenticated, physical attacker to install and boot a malicious software image or execute unsigned binaries on an affected device. The vulnerability is due to an improper check on the area of code that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3209</a> <a href="#">CISCO</a>

	exploit could allow the attacker to install and boot a malicious software image or execute unsigned binaries on the targeted device.			
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker who has valid administrative access to an affected device could exploit this vulnerability by supplying a crafted input parameter on a form in the web UI and then submitting that form. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device, which could lead to complete system compromise.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3211</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the Virtual Services Container of Cisco IOS XE Software could allow an authenticated, local attacker to gain root-level privileges on an affected device. The vulnerability is due to insufficient validation of a user-supplied open virtual appliance (OVA). An attacker could exploit this vulnerability by installing a malicious OVA on an affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3215</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the ROMMON of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to those of the root user of the underlying operating system. The vulnerability is due to the ROMMON allowing for special parameters to be passed to the device at initial boot up. An attacker could exploit this vulnerability by sending parameters to the device at initial boot up. An exploit could allow the attacker to elevate from a Priv15 user to the root user and execute arbitrary commands with the privileges of the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3213</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software could allow an unauthenticated, remote attacker to execute Cisco IOx API commands without proper authorization. The vulnerability is due to incorrect handling of requests for authorization tokens. An attacker could exploit this	2020-06-03	not yet calculated	<a href="#">CVE-2020-3227</a> <a href="#">CISCO</a>

	vulnerability by using a crafted API call to request such a token. An exploit could allow the attacker to obtain an authorization token and execute any of the IOx API commands on an affected device.			
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code with root privileges on the underlying Linux shell. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by first creating a malicious file on the affected device itself and then uploading a second malicious file to the device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or bypass licensing requirements on the device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3218</a> <a href="#">CISCO</a>
cisco -- ios_xe_web_management	A vulnerability in Role Based Access Control (RBAC) functionality of Cisco IOS XE Web Management Software could allow a Read-Only authenticated, remote attacker to execute commands or configuration changes as an Admin user. The vulnerability is due to incorrect handling of RBAC for the administration GUI. An attacker could exploit this vulnerability by sending a modified HTTP request to the affected device. An exploit could allow the attacker as a Read-Only user to execute CLI commands or configuration changes as if they were an Admin user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3229</a> <a href="#">CISCO</a>
cisco -- iox_application	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, remote attacker to write or modify arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient input validation of user-supplied application packages. An attacker who can upload a malicious package within Cisco IOx could exploit the vulnerability to modify arbitrary files. The impacts of a successful exploit are limited to the scope of the virtual instance and do not affect the device that is hosting Cisco IOx.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3238</a> <a href="#">CISCO</a>
	A vulnerability in the Cisco Application			

cisco -- iox_application	Framework component of the Cisco IOx application environment could allow an authenticated, local attacker to overwrite arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient path restriction enforcement. An attacker could exploit this vulnerability by including a crafted file in an application package. An exploit could allow the attacker to overwrite files.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3237</a> <a href="#">CISCO</a>
cisco -- iox_application_framework	A vulnerability in the web-based Local Manager interface of the Cisco IOx Application Framework could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based Local Manager interface of an affected device. The attacker must have valid Local Manager credentials. The vulnerability is due to insufficient validation of user-supplied input by the web-based Local Manager interface of the affected software. An attacker could exploit this vulnerability by injecting malicious code into a system settings tab. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3233</a> <a href="#">CISCO</a>
cisco -- multiple_products	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3217</a> <a href="#">CISCO</a>

cisco -- multiple_products	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3228</a> <a href="#">CISCO</a>
cisco -- multiple_routers	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3199</a> <a href="#">CISCO</a>
cisco -- multiple_routers	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device's virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3234</a> <a href="#">CISCO</a>
	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell			



cisco -- multiple_routers	commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3210</a> <a href="#">CISCO</a>
cisco -- multiple_routers	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3198</a> <a href="#">CISCO</a>
cisco -- multiple_routers	A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3205</a> <a href="#">CISCO</a>
	Multiple vulnerabilities in the Cisco IOx			

cisco -- multiple_routers	application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3257</a> <a href="#">CISCO</a>
cisco -- multiple_routers	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3258</a> <a href="#">CISCO</a>
cisco -- unified_contact_center_express	A vulnerability in the API subsystem of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to change the availability state of any agent. The vulnerability is due to insufficient authorization enforcement on an affected system. An attacker could exploit this vulnerability by authenticating to an affected system with valid agent credentials and performing a specific API call with crafted input. A successful exploit could allow the attacker to change the availability state of an agent, potentially causing a denial of service condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3267</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_and_webex_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link	2020-06-03	not yet calculated	<a href="#">CVE-2020-3319</a> <a href="#">CISCO</a>

	or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3.			
combodo -- itop	In Combodo iTop, dashboard ids can be exploited with a reflective XSS payload. This is fixed in all iTop packages (community, essential, professional) for version 2.7.0 and in iTop essential and iTop professional packages for version 2.6.4.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11697</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
combodo -- itop	In Combodo iTop a menu shortcut name can be exploited with a stored XSS payload. This is fixed in all iTop packages (community, essential, professional) in version 2.7.0 and iTop essential and iTop professional in version 2.6.4.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11696</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.6 for Craft CMS. There is stored XSS via a guest name.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13869</a> <a href="#">MISC</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. There is stored XSS via an asset volume name.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13870</a> <a href="#">MISC</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. CSRF affects comment integrity.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13868</a> <a href="#">MISC</a>
docker -- desktop	An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11492</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- elasticsearch	The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to 7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an	2020-06-03	not yet calculated	<a href="#">CVE-2020-7014</a> <a href="#">N/A</a>

	authentication token being generated with elevated privileges.			
elliptic -- elliptic	The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading to bytes, or integer overflows. This could conceivably have a security-relevant impact if an application relied on a single canonical signature.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13822</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fortiguard -- forticlient_for_windows	Use of a hard-coded cryptographic key to encrypt security sensitive data in local storage and configuration in FortiClient for Windows prior to 6.4.0 may allow an attacker with access to the local storage or the configuration backup file to decrypt the sensitive data via knowledge of the hard-coded key.	2020-06-04	not yet calculated	<a href="#">CVE-2019-16150</a> <a href="#">MISC</a>
fortiguard -- fortisiem_windows_agent	An unquoted service path vulnerability in the FortiSIEM Windows Agent component may allow an attacker to gain elevated privileges via the AoWinAgt executable service path.	2020-06-04	not yet calculated	<a href="#">CVE-2020-9292</a> <a href="#">MISC</a>
foxit -- e-mail_advertising_system	An issue was discovered in Foxit E-mail advertising system before September 2018. It allows authentication bypass and information disclosure, related to Interspire Email Marketer.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21235</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has an out-of-bounds write when Internet Explorer is used.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20825</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has homograph mishandling.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20832</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows NTLM credential theft via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21237</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It allows Remote Code Execution via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21242</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20824</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has an untrusted search path that allows a DLL to execute remote code.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21241</a> <a href="#">CONFIRM</a>
	An issue was discovered in Foxit			

foxit -- phantompdf	PhantomPDF before 8.3.6. It allows arbitrary application execution via an embedded executable file in a PDF portfolio, aka FG-VD-18-029.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21244</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20834</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20823</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has COM object mishandling when Microsoft Word is used.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21243</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows memory consumption via an <code>ArrayBuffer(0xffffffff)</code> call.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21238</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has mishandling of cloud credentials, as demonstrated by Google Drive.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20833</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac	An issue was discovered in Foxit PhantomPDF Mac before 3.4. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20821</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20826</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac_and_reader_for_mac	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It allows stack consumption because of interaction between ICC-Based color space and Alternate color space.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20827</a> <a href="#">CONFIRM</a>
foxit -- reader	An issue was discovered in Foxit Reader before 2.4.4. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21236</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.7.0.29430. It has an out-of-bounds write via incorrect image data.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20822</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.2. It allows NTLM credential theft via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21239</a> <a href="#">CONFIRM</a>
foxit --	An issue was discovered in Foxit Reader			<a href="#">CVE-2018-</a>



reader_and_phantompdf	and PhantomPDF before 9.2. It allows memory consumption via an <code>ArrayBuffer(0xffffffff)</code> call.	2020-06-04	not yet calculated	<a href="#">21240 CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It has a use-after-free via a document that lacks a dictionary.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13814 CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13810 CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It allows stack consumption via a loop of an indirect object reference.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13815 CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.5.0.20733. It has void data mishandling, causing a crash.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20831 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13812 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory when <code>FoxitStudioPhoto366_3.6.6.916.exe</code> is used.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13813 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It has an out-of-bounds write via a crafted TIFF file.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13811 CONFIRM</a>
ge --multiple_grid_solutions	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the	2020-06-02	not yet calculated	<a href="#">CVE-2020-12017 MISC</a>

	device and reboot the system.			
gnutls -- gnutls	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13777</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">DEBIAN</a>
google -- chrome	Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-06-03	not yet calculated	<a href="#">CVE-2020-6503</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- multiple_products	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause service abnormal.	2020-06-05	not yet calculated	<a href="#">CVE-2020-1883</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones.	2020-06-05	not yet calculated	<a href="#">CVE-2020-9074</a> <a href="#">MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181230.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4449</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181231.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4450</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- websphere_application_server_network_deployment	IBM WebSphere Application Server Network Deployment 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 181228.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4448</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

ibm -- worklight/mobilefoundation	IBM Worklight/MobileFoundation 8.0.0.0 does not properly invalidate session cookies when a user logs out of a session, which could allow another user to gain unauthorized access to a user's session. IBM X-Force ID: 175211.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4229</a> <a href="#">CONFIRM</a>
kubernetes -- kube-controller-manager	The Kubernetes kube-controller-manager in versions v1.0-1.14, versions prior to v1.15.12, v1.16.9, v1.17.5, and version v1.18.0 are vulnerable to a Server Side Request Forgery (SSRF) that allows certain authorized users to leak up to 500 bytes of arbitrary information from unprotected endpoints within the master's host network (such as link-local or loopback services).	2020-06-05	not yet calculated	<a href="#">CVE-2020-8555</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13841</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS software before 2020-06-01. Local users can cause a denial of service because checking of the userdata partition is mishandled. The LG ID is LVE-SMP-200014 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13843</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13839</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13842</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13840</a> <a href="#">CONFIRM</a>
minishare -- minishare	In MiniShare before 1.4.2, there is a stack-based buffer overflow via an HTTP PUT request, which allows an attacker to achieve arbitrary code execution, a similar issue to CVE-2018-19861, CVE-2018-19862, and CVE-2019-17601.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13768</a> <a href="#">MISC</a>

	NOTE: this product is discontinued.			
mqtt -- mqtt	The MQTT protocol 3.1.1 requires a server to set a timeout value of 1.5 times the Keep-Alive value specified by a client, which allows remote attackers to cause a denial of service (loss of the ability to establish new connections), as demonstrated by SlowITe.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13849</a> <a href="#">MISC</a> <a href="#">MISC</a>
neon -- neon	The Neon theme 2.0 before 2020-06-03 for Bootstrap allows XSS via an Add Task Input operation in a dashboard.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13890</a> <a href="#">MISC</a>
network_time_foundation -- network_time_protocol	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13817</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_rcv_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection.	2020-06-03	not yet calculated	<a href="#">CVE-2020-11080</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
	In WatermelonDB (NPM package "@nozbe/watermelondb") before versions 0.15.1 and 0.16.2, a maliciously crafted record ID can exploit a SQL Injection vulnerability in iOS adapter implementation and cause the app to delete all or selected records from the database, generally causing the app to become unusable. This may happen in apps that don't validate IDs (valid IDs are /^[a-zA-Z0-9_-.]+\$/') and use Watermelon Sync or low-level `database.adapter.destroyDeletedRecords` method. The integrity risk is low due to the fact that maliciously deleted records			

nozbe -- watermelondb	won't synchronize, so logout-login will restore all data, although some local changes may be lost if the malicious deletion causes the sync process to fail to proceed to push stage. No way to breach confidentiality with this vulnerability is known. Full exploitation of SQL Injection is mitigated, because it's not possible to nest an insert/update query inside a delete query in SQLite, and it's not possible to pass a semicolon-separated second query. There's also no known practicable way to breach confidentiality by selectively deleting records, because those records will not be synchronized. It's theoretically possible that selective record deletion could cause an app to behave insecurely if lack of a record is used to make security decisions by the app. This is patched in versions 0.15.1, 0.16.2, and 0.16.1-fix	2020-06-03	not yet calculated	<a href="#">CVE-2020-4035</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, any users with the ability to modify any data that could eventually be exported as a CSV file from the `ImportExportController` could potentially introduce a CSV injection into the data to cause the generated CSV export file to be malicious. This requires attackers to achieve the following before a successful attack can be completed: 1. Have found a vulnerability in the victims spreadsheet software of choice. 2. Control data that would potentially be exported through the `ImportExportController` by a theoretical victim. 3. Convince the victim to export above data as a CSV and run it in vulnerable spreadsheet software while also bypassing any sanity checks by said software. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	not yet calculated	<a href="#">CVE-2020-5299</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	The October CMS debugbar plugin before version 3.1.0 contains a feature where it will log all requests (and all information pertaining to each request including session data) whenever it is enabled. This presents a problem if the plugin is ever enabled on a system that is open to untrusted users as the potential exists for them to use this feature to view all requests being made to the application			



october -- october_cms	and obtain sensitive information from those requests. There even exists the potential for account takeovers of authenticated users by non-authenticated public users, which would then lead to a number of other potential issues as an attacker could theoretically get full access to the system if the required conditions existed. Issue has been patched in v3.1.0 by locking down access to the debugbar to all users; it now requires an authenticated backend user with a specifically enabled permission before it is even usable, and the feature that allows access to stored request information is restricted behind a different permission that's more restrictive.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11094</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open-iscsi -- targetcli-fb	Open-iSCSI targetcli-fb through 2.1.52 has weak permissions for /etc/target (and for the backup directory and backup files).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13867</a> <a href="#">MISC</a>
pam_tacplus -- pam_tacplus	In support.c in pam_tacplus 1.3.8 through 1.5.1, the TACACS+ shared secret gets logged via syslog if the DEBUG loglevel and journald are used.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13881</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12723</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10878</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
perl -- perl	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10543</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
postgresql -- jdbc_driver	PostgreSQL JDBC Driver (aka PgJDBC) before 42.2.13 allows XXE.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13692</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
pupnp -- pupnp	Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and	2020-06-04	not yet calculated	<a href="#">CVE-2020-13848</a> <a href="#">MISC</a> <a href="#">MISC</a>

	FindServiceEventURLPath in genlib/service_table/service_table.c.			
pydio -- cells	Pydio Cells 2.0.4 allows XSS. A malicious user can either upload or create a new file that contains potentially malicious HTML and JavaScript code to personal folders or accessible cells.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12853</a> <a href="#">MISC</a>
pydio -- cells	Pydio Cells 2.0.4 allows an authenticated user to write or overwrite existing files in another user's personal and cells folders (repositories) by uploading a custom generated ZIP file and leveraging the file extraction feature present in the web application. The extracted files will be placed in the targeted user folders.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12851</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	The update feature for Pydio Cells 2.0.4 allows an administrator user to set a custom update URL and the public RSA key used to validate the downloaded update package. The update process involves downloading the updated binary file from a URL indicated in the update server response, validating its checksum and signature with the provided public key and finally replacing the current application binary. To complete the update process, the application's service or appliance needs to be restarted. An attacker with administrator access can leverage the software update feature to force the application to download a custom binary that will replace current Pydio Cells binary. When the server or service is eventually restarted the attacker will be able to execute code under the privileges of the user running the application. In the Pydio Cells enterprise appliance this is with the privileges of the user named "pydio".	2020-06-04	not yet calculated	<a href="#">CVE-2020-12852</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	In Pydio Cells 2.0.4, once an authenticated user shares a file selecting the create a public link option, a hidden shared user account is created in the backend with a random username. An anonymous user that obtains a valid public link can get the associated hidden account username and password and proceed to login to the web application. Once logged into the web application with the hidden user account, some actions that were not available with the public share link can now be performed.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12848</a> <a href="#">MISC</a> <a href="#">MISC</a>

pydio -- cells	Pydio Cells 2.0.4 allows any user to upload a profile image to the web application, including standard and shared user roles. These profile pictures can later be accessed directly with the generated URL by any unauthenticated or authenticated user.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12849</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	Pydio Cells 2.0.4 web application offers an administrative console named "Cells Console" that is available to users with an administrator role. This console provides an administrator user with the possibility of changing several settings, including the application's mailer configuration. It is possible to configure a few engines to be used by the mailer application to send emails. If the user selects the "sendmail" option as the default one, the web application offers to edit the full path where the sendmail binary is hosted. Since there is no restriction in place while editing this value, an attacker authenticated as an administrator user could force the web application into executing any arbitrary binary.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12847</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	A flaw was found in QEMU in the implementation of the Pointer Authentication (PAuth) support for ARM introduced in version 4.0 and fixed in version 5.0.0. A general failure of the signature generation process caused every PAuth-enforced pointer to be signed with the same signature. A local attacker could obtain the signature of a protected pointer and abuse this flaw to bypass PAuth protection for all programs running on QEMU.	2020-06-04	not yet calculated	<a href="#">CVE-2020-10702</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
qemu -- qemu	ati-vga in hw/display/ati.c in QEMU 4.2.0 allows guest OS users to trigger infinite recursion via a crafted mm_index value during an ati_mm_read or ati_mm_write call.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13800</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
qemu -- qemu	rom_copy() in hw/core/loader.c in QEMU 4.1.0 does not validate the relationship between two addresses, which allows attackers to trigger an invalid memory copy operation.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13765</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
qemu -- qemu	hw/pci/pci.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access by providing an address near the end of the PCI configuration space.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13791</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	SQLite 3.32.2 has a use-after-free in			<a href="#">CVE-2020-</a>

sqlite -- sqlite	resetAccumulator in select.c because the parse tree rewrite for window functions is too late.	2020-06-06	not yet calculated	<a href="#">13871</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
swift_networks -- red_cheetah	In the cheetah free wifi 5.1 driver file liebaonat.sys, local users are allowed to cause a denial of service (BSOD) or other unknown impact due to failure to verify the value of a specific IOCTL.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13646</a> <a href="#">MISC</a>
tigera -- calico_and_calico_enterprise	Clusters using Calico (version 3.14.0 and below), Calico Enterprise (version 2.8.2 and below), may be vulnerable to information disclosure if IPv6 is enabled but unused. A compromised pod with sufficient privilege is able to reconfigure the node's IPv6 interface due to the node accepting route advertisement by default, allowing the attacker to redirect full or partial network traffic from the node to the compromised pod.	2020-06-03	not yet calculated	<a href="#">CVE-2020-13597</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
url-regex -- url-regex	all versions of url-regex are vulnerable to Regular Expression Denial of Service. An attacker providing a very long string in String.test can cause a Denial of Service.	2020-06-04	not yet calculated	<a href="#">CVE-2020-7661</a> <a href="#">MISC</a> <a href="#">MISC</a>
weaveworks -- weave_net	In Weave Net before version 2.6.3, an attacker able to run a process as root in a container is able to respond to DNS requests from the host and thereby insert themselves as a fake service. In a cluster with an IPv4 internal network, if IPv6 is not totally disabled on the host (via ipv6.disable=1 on the kernel cmdline), it will be either unconfigured or configured on some interfaces, but it's pretty likely that ipv6 forwarding is disabled, ie /proc/sys/net/ipv6/conf//forwarding == 0. Also by default, /proc/sys/net/ipv6/conf//accept_ra == 1. The combination of these 2 sysctls means that the host accepts router advertisements and configure the IPv6 stack using them. By sending rogue router advertisements, an attacker can reconfigure the host to redirect part or all of the IPv6 traffic of the host to the attacker controlled container. Even if there was no IPv6 traffic before, if the DNS returns A (IPv4) and AAAA (IPv6) records, many HTTP libraries will try to connect via IPv6 first then fallback to IPv4, giving an opportunity to the attacker to respond. If by chance you also have on the host a vulnerability like last year's	2020-06-03	not yet calculated	<a href="#">CVE-2020-11091</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	RCE in apt (CVE-2019-3462), you can now escalate to the host. Weave Net version 2.6.3 disables the accept_ra option on the veth devices that it creates.			
wordpress -- wordpress	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from a stored XSS vulnerability. An author user can create posts that result in a stored XSS by using a crafted payload in custom links.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13864</a> <a href="#">MISC</a>
wordpress -- wordpress	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from multiple stored XSS vulnerabilities. An author user can create posts that result in stored XSS vulnerabilities, by using a crafted link in the custom URL or by applying custom attributes.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13865</a> <a href="#">MISC</a>
wso2 -- multiple_products	In WSO2 API Manager 3.0.0 and earlier, WSO2 API Microgateway 2.2.0, and WSO2 IS as Key Manager 5.9.0 and earlier, Management Console allows XXE during addition or update of a Lifecycle.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13883</a> <a href="#">MISC</a>
xack -- dns	XACK DNS 1.11.0 to 1.11.4, 1.10.0 to 1.10.8, 1.8.0 to 1.8.23, 1.7.0 to 1.7.18, and versions before 1.7.0 allow remote attackers to cause a denial of service condition resulting in degradation of the recursive resolver's performance or compromising the recursive resolver as a reflector in a reflection attack.	2020-06-05	not yet calculated	<a href="#">CVE-2020-5591</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	A remote adversary with the ability to send arbitrary CoAP packets to be parsed by Zephyr is able to cause a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10063</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	An off-by-one error in the Zephyr project MQTT packet length decoder can result in memory corruption and possible remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	The Zephyr MQTT parsing code performs insufficient checking of the length field on publish messages, allowing a buffer overflow and potentially remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



zephyrproject -- zephyr	In the Zephyr Project MQTT code, improper bounds checking can result in memory corruption and possibly remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	Improper handling of the full-buffer case in the Zephyr Bluetooth implementation can result in memory corruption. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10061</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	In the Zephyr project Bluetooth subsystem, certain duplicate and back-to-back packets can cause incorrect behavior, resulting in a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10068</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of June 1, 2020  
**Date:** Monday, June 08, 2020 11:44:53 AM

---



National Cyber Awareness System:

## **Vulnerability Summary for the Week of June 1, 2020**

06/08/2020 06:56 AM EDT

Original release date: June 8, 2020

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
asus -- aura_sync	Ene.sys in Asus Aura Sync through 1.07.71 does not properly validate input to IOCTL 0x80102044, 0x80102050, and 0x80102054, which allows local users to cause a denial of service (system crash) or gain privileges via IOCTL requests using crafted kernel addresses that trigger memory corruption.	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-17603</a> <a href="#">MISC</a>
cisco -- ios_xe_software	A vulnerability in the processing of boot options of specific Cisco IOS XE Software switches could allow an authenticated, local attacker with root shell access to the underlying operating system (OS) to conduct a command injection attack during device boot. This vulnerability is due to insufficient input validation checks while processing boot options. An attacker could exploit this vulnerability by modifying device boot options to execute attacker-provided code. A successful exploit may allow an attacker to bypass the Secure Boot process and execute malicious code on an affected device with root-level privileges.	2020-06-03	<a href="#">7.2</a>	<a href="#">CVE-2020-3207</a> <a href="#">CISCO</a>
	A vulnerability in Cisco IOS XE Software			

cisco -- ios_xe_software	could allow an authenticated, local attacker to escalate their privileges to a user with root-level privileges. The vulnerability is due to insufficient validation of user-supplied content. This vulnerability could allow an attacker to load malicious software onto an affected device.	2020-06-03	<a href="#">7.2</a>	<a href="#">CVE-2020-3214</a> <a href="#">CISCO</a>
clearpass -- policy_manager	The ClearPass Policy Manager web interface is affected by a vulnerability that leads to authentication bypass. Upon successful bypass an attacker could then execute an exploit that would allow to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">10</a>	<a href="#">CVE-2020-7115</a> <a href="#">MISC</a>
clearpass -- policy_manager	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-7116</a> <a href="#">MISC</a>
clearpass -- policy_manager	The ClearPass Policy Manager WebUI administrative interface has an authenticated command remote execution. When the attacker is already authenticated to the administrative interface, they could then exploit the system, leading to remote command execution in the underlying operating system. Resolution: Fixed in 6.7.13-HF, 6.8.5-HF, 6.8.6, 6.9.1 and higher.	2020-06-03	<a href="#">9</a>	<a href="#">CVE-2020-7117</a> <a href="#">MISC</a>
d-link -- dir-865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices allow Command Injection.	2020-06-03	<a href="#">7.5</a>	<a href="#">CVE-2020-13782</a> <a href="#">MISC</a>
docker -- engine	An issue was discovered in Docker Engine before 19.03.11. An attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service.	2020-06-02	<a href="#">7.5</a>	<a href="#">CVE-2020-13401</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows attackers to write arbitrary data to fsUI.xyz via fsSaveUIPersistence.php.	2020-06-01	<a href="#">7.5</a>	<a href="#">CVE-2014-7175</a> <a href="#">MISC</a>
	FarLinX X25 Gateway through 2014-09-25 allows command injection via shell			

farsite -- farlinx_x25_gateway	metacharacters to sysSaveMonitorData.php, fsx25MonProxy.php, syseditdate.php, iframeupload.php, or sysRestoreX25Cplt.php.	2020-06-01	7.5	<a href="#">CVE-2014-7173</a> <a href="#">MISC</a>
fortinet -- fortitap- s/w2_and_fortiap-u	An improper input validation in FortiAP-S/W2 6.2.0 to 6.2.2, 6.0.5 and below, FortiAP-U 6.0.1 and below CLI admin console may allow unauthorized administrators to overwrite system files via specially crafted tcpdump commands in the CLI.	2020-06-01	8.5	<a href="#">CVE-2019-15709</a> <a href="#">MISC</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has an out-of-bounds write when Internet Explorer is used.	2020-06-04	7.5	<a href="#">CVE-2019-20830</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, an Integer Overflow to Buffer Overflow exists. When using /video redirection, a manipulated server can instruct the client to allocate a buffer with a smaller size than requested due to an integer overflow in size calculation. With later messages, the server can manipulate the client to write data out of bound to the previously allocated buffer. This has been patched in 2.1.0.	2020-05-29	7.5	<a href="#">CVE-2020-11038</a> <a href="#">CONFIRM</a>
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, when using a manipulated server with USB redirection enabled (nearly) arbitrary memory can be read and written due to integer overflows in length checks. This has been patched in 2.1.0.	2020-05-29	7.5	<a href="#">CVE-2020-11039</a> <a href="#">CONFIRM</a>
gesio -- erp	There is an improper Neutralization of Special Elements used in an SQL Command (SQL Injection) vulnerability in php files of GESIO ERP. GESIO ERP all versions prior to 11.2 allows malicious users to retrieve all database information.	2020-06-01	7.5	<a href="#">CVE-2020-8967</a> <a href="#">CONFIRM</a>
github -- enterprise_server	An improper access control vulnerability was identified in the GitHub Enterprise Server API that allowed an organization member to escalate permissions and gain access to unauthorized repositories within an organization. This vulnerability affected all versions of GitHub Enterprise Server prior to 2.21 and was fixed in 2.20.9, 2.19.15, and 2.18.20. This vulnerability was reported via the GitHub Bug Bounty program.	2020-06-03	7.5	<a href="#">CVE-2020-10516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	IBM Security Guardium 11.1 could allow a remote authenticated attacker to execute			

ibm -- security_guardium	arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 174735.	2020-06-03	9	<a href="#">CVE-2020-4180</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174732.	2020-06-03	7.5	<a href="#">CVE-2020-4177</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
micro_focus -- service_management_authentication	There is an Incorrect Authorization vulnerability in Micro Focus Service Management Automation (SMA) product authentication version 2018.05 to 2020.02. The vulnerability could be exploited to provide unauthorized access to the Container Deployment Foundation.	2020-05-29	7.5	<a href="#">CVE-2020-11844</a> <a href="#">CONFIRM</a>
piwigo -- lexiglot	admin.php?page=projects in Lexiglot through 2014-11-20 allows command injection via username and password fields.	2020-06-01	7.5	<a href="#">CVE-2014-8945</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows SQL injection via an admin.php?page=users&from_id= or admin.php?page=history&limit= URI.	2020-06-01	7.5	<a href="#">CVE-2014-8941</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Improper permissions in XBL_SEC region enable user to update XBL_SEC code and data and divert the RAM dump path to normal cold boot path in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in Kamorta, MSM8998, QCS404, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SM8150, SXR1130, SXR2130	2020-06-02	7.2	<a href="#">CVE-2019-14054</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Firmware will hit assert in WLAN firmware If encrypted data length in FILS IE of reassoc response is more than 528 bytes in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, Kamorta, Nicobar, QCA6390, QCA8081, QCN7605, QCS404, QCS405, QCS605, Rennell,	2020-06-02	7.8	<a href="#">CVE-2020-3645</a> <a href="#">CONFIRM</a>



	SC7180, SC8180X, SDA845, SDM670, SDM710, SDM845, SDM850, SM6150, SM7150, SM8150, SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	NULL exception due to accessing bad pointer while posting events on RT FIFO in Snapdragon Compute, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking in IPQ6018, IPQ8074, QCA8081, SC8180X, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3618</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	When making query to DSP capabilities, Stack out of bounds occurs due to wrong buffer length configured for DSP attributes in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile in SM8250, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3625</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Valid deauth/disassoc frames is dropped in case if RMF is enabled and some rouge peer keep on sending rogue deauth/disassoc frames due to improper enum values used to check the frame subtype in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8009, APQ8053, APQ8096AU, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SC8180X, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-06-02	<a href="#">7.5</a>	<a href="#">CVE-2020-3615</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow in calculating estimated output buffer size when getting a list of installed Feature IDs, Serial Numbers or checking Feature ID status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9205, MDM9607, Nicobar, QCS404, QCS405, Rennell, SA6155P, SC7180, SC8180X, SDX55, SM6150, SM7150, SXR2130	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14066</a> <a href="#">CONFIRM</a>
	Array out of bound may occur while playing mp3 file as no check is there on offset if it is greater than the buffer allocated or not in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial			

qualcomm -- multiple_snapdragon_products	IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	<a href="#">10</a>	<a href="#">CVE-2020-3633</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow may occur if atom size is less than atom offset as there is improper validation of atom size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	<a href="#">10</a>	<a href="#">CVE-2020-3641</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer overflow in display function due to memory copy without checking length of size using strcpy function in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2020-3616</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Failure in buffer management while accessing handle for HDR blit when color modes not supported by display in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables in MSM8909W, QCS605	2020-06-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14087</a> <a href="#">CONFIRM</a>



sabberworm -- php_css_parser	Sabberworm PHP CSS Parser before 8.3.1 calls eval on uncontrolled data, possibly leading to remote code execution if the function allSelectors() or getSelectorsBySpecificity() is called with input from an attacker.	2020-06-03	7.5	<a href="#">CVE-2020-13756</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with Q(10.0) (with TEEGRIS on Exynos chipsets) software. The Widevine Trustlet allows arbitrary code execution because of memory disclosure, The Samsung IDs are SVE-2020-17117, SVE-2020-17118, SVE-2020-17119, and SVE-2020-17161 (June 2020).	2020-06-04	7.5	<a href="#">CVE-2020-13832</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x) and P(9.0) (Exynos 7570 chipsets) software. The Trustonic Kinibi component allows arbitrary memory mapping. The Samsung ID is SVE-2019-16665 (June 2020).	2020-06-04	7.5	<a href="#">CVE-2020-13831</a> <a href="#">CONFIRM</a>
swarco -- cpu_ls4000_series	An open port used for debugging in SWARCOs CPU LS4000 Series with versions starting with G4... grants root access to the device without access control via network. A malicious user could use this vulnerability to get access to the device and disturb operations with connected devices.	2020-05-29	10	<a href="#">CVE-2020-12493</a> <a href="#">CONFIRM</a>
systemd -- systemd	systemd through v245 mishandles numerical usernames such as ones composed of decimal digits or 0x followed by hex digits, as demonstrated by use of root privileges when privileges of the 0x0 user account were intended. NOTE: this issue exists because of an incomplete fix for CVE-2017-1000082.	2020-06-03	10	<a href="#">CVE-2020-13776</a> <a href="#">MISC</a>
verizon -- serialize-javascript	serialize-javascript prior to 3.1.0 allows remote attackers to inject arbitrary code via the function "deleteFunctions" within "index.js".	2020-06-01	7.5	<a href="#">CVE-2020-7660</a> <a href="#">MISC</a>
wordpress -- wordpress	An unauthenticated privilege-escalation issue exists in the bbPress plugin before 2.6.5 for WordPress when New User Registration is enabled.	2020-05-29	7.5	<a href="#">CVE-2020-13693</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2pisoftware -- cmfive	system/classes/DbPDO.php in Cmfive through 2015-03-15, when database connectivity malfunctions, allows remote attackers to obtain sensitive information (username and password) via any request, such as a password reset request.	2020-06-01	5	<a href="#">CVE-2014-9702</a> <a href="#">MISC</a>
apache -- ignite	Apache Ignite uses H2 database to build SQL distributed execution engine. H2 provides SQL functions which could be used by attacker to access to a filesystem.	2020-06-03	6.4	<a href="#">CVE-2020-1963</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
atlassian -- companion_app	The file downloading functionality in the Atlassian Companion App before version 1.0.0 allows remote attackers, who control a Confluence Server instance that the Companion App is connected to, execute arbitrary .exe files via a Protection Mechanism Failure.	2020-06-01	6.5	<a href="#">CVE-2020-4020</a> <a href="#">MISC</a>
atlassian -- companion_app	The file editing functionality in the Atlassian Companion App before version 1.0.0 allows local attackers to have the app run a different executable in place of the app's cmd.exe via a untrusted search path vulnerability.	2020-06-01	4.4	<a href="#">CVE-2020-4019</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /plugins/servlet/jira-blockers/resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get the ID of configured Jira application links via an information disclosure vulnerability.	2020-06-01	5	<a href="#">CVE-2020-4016</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /json/fe/activeUserFinder.do resource in Altassian Fisheye and Crucible before version 4.8.1 allows remote attackers to view user email addresses via a information disclosure vulnerability.	2020-06-01	4	<a href="#">CVE-2020-4015</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The /rest/jira-ril/1.0/jira-rest/applinks resource in the crucible-jira-ril plugin in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to get information about any configured Jira application links via an information disclosure vulnerability.	2020-06-01	5	<a href="#">CVE-2020-4017</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The /profile/deleteWatch.do resource in			



atlassian -- fisheye_and_crucible	Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to remove another user's watching settings for a repository via an improper authorization vulnerability.	2020-06-01	<a href="#">4</a>	<a href="#">CVE-2020-4014</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The review coverage resource in Atlassian Fisheye and Crucible before version 4.8.2 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the committerFilter parameter.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2020-4023</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- fisheye_and_crucible	The setup resources in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to complete the setup process via a cross-site request forgery (CSRF) vulnerability.	2020-06-01	<a href="#">6.8</a>	<a href="#">CVE-2020-4018</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- navigator_links	The CustomAppsRestResource list resource in Atlassian Navigator Links before version 3.3.23, from version 4.0.0 before version 4.3.7, from version 5.0.0 before 5.0.1, and from version 5.1.0 before 5.1.1 allows remote attackers to enumerate all linked applications, including those that are restricted or otherwise hidden, through an incorrect authorization check.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-4026</a> <a href="#">MISC</a> <a href="#">MISC</a>
bitrix -- bitrix24	modules/security/classes/general.post_filter.php/post_filter.php in the Web Application Firewall in Bitrix24 through 20.0.950 allows XSS by placing %00 before the payload.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2020-13758</a> <a href="#">MISC</a>
celluloid -- reel	reel through 0.6.1 allows Request Smuggling attacks due to incorrect Content-Length and Transfer encoding header parsing. It is possible to conduct HTTP request smuggling attacks by sending the Content-Length header twice. Furthermore, invalid Transfer Encoding headers were found to be parsed as valid which could be leveraged for TE:CL smuggling attacks. Note: This project is deprecated, and is not maintained any more.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-7659</a> <a href="#">MISC</a>
cisco -- multiple_products	Multiple products that implement the IP Encapsulation within IP standard (RFC 2003, STD 1) decapsulate and route IP-in-IP traffic without any validation, which could allow an unauthenticated remote attacker to route arbitrary traffic via an exposed network interface and lead to spoofing, access control bypass, and other unexpected network behaviors.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-10136</a> <a href="#">CERT-VN</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A vulnerability in the web-based			

cisco -- prime_infrastructure	management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database.	2020-06-03	6.4	<a href="#">CVE-2020-3339</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_and_webex_recording_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious file.	2020-06-03	4.3	<a href="#">CVE-2020-3322</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_and_webex_recording_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to	2020-06-03	4.3	<a href="#">CVE-2020-3321</a> <a href="#">CISCO</a>

	crash when trying to view the malicious file.			
compound -- finance_compound_price_oracle	The price oracle in PriceOracle.sol in Compound Finance Compound Price Oracle 1.0 through 2.0 allows a price oracle to set an invalid asset price via the setPrice function, and consequently violate the intended limits on price swings.	2020-06-03	5	<a href="#">CVE-2019-20809</a> <a href="#">MISC</a>
cybele -- thinfinity_virtualui	Cybele Thinfinity VirtualUI 2.5.17.2 allows HTTP response splitting via the mimetype parameter within a PDF viewer request, as demonstrated by an example.pdf?mimetype= substring. The victim user must load an application request to view a PDF, containing the malicious payload. This results in a reflected XSS payload being executed.	2020-06-04	4.3	<a href="#">CVE-2019-16385</a> <a href="#">MISC</a>
cybele -- thinfinity_virtualui	Cybele Thinfinity VirtualUI 2.5.17.2 allows ../ path traversal that can be used for data exfiltration. This enables files outside of the web directory to be retrieved if the exact location is known and the user has permissions.	2020-06-04	4	<a href="#">CVE-2019-16384</a> <a href="#">MISC</a>
d-link -- dir- 856l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices allow CSRF.	2020-06-03	6.8	<a href="#">CVE-2020-13786</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Transmission of Sensitive Information.	2020-06-03	5	<a href="#">CVE-2020-13787</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Inadequate Encryption Strength.	2020-06-03	5	<a href="#">CVE-2020-13785</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have a predictable seed in a Pseudo-Random Number Generator.	2020-06-03	5	<a href="#">CVE-2020-13784</a> <a href="#">MISC</a>
d-link -- dir- 865l_devices	D-Link DIR-865L Ax 1.20B01 Beta devices have Cleartext Storage of Sensitive Information.	2020-06-03	5	<a href="#">CVE-2020-13783</a> <a href="#">MISC</a>
django-project -- django	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. Query parameters generated by the Django admin ForeignKeyRawIdWidget were not properly URL encoded, leading to a possibility of an XSS attack.	2020-06-03	4.3	<a href="#">CVE-2020-13596</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
django_project -- django	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. In cases where a memcached backend does not perform key validation, passing malformed cache keys could result in a key collision, and potential data leakage.	2020-06-03	5	<a href="#">CVE-2020-13254</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

elastic -- elastic_app_search	Elastic App Search versions before 7.7.0 contain a cross site scripting (XSS) flaw when displaying document URLs in the Reference UI. If the Reference UI injects a URL into a result, that URL will be rendered by the web browser. If an attacker is able to control the contents of such a field, they could execute arbitrary JavaScript in the victim's web browser.	2020-06-03	4.3	<a href="#">CVE-2020-7011</a> N/A
elastic -- elastic_cloud_on_kubernetes	Elastic Cloud on Kubernetes (ECK) versions prior to 1.1.0 generate passwords using a weak random number generator. If an attacker is able to determine when the current Elastic Stack cluster was deployed they may be able to more easily brute force the Elasticsearch credentials generated by ECK.	2020-06-03	5	<a href="#">CVE-2020-7010</a> N/A
elastic -- kibana	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	2020-06-03	6.5	<a href="#">CVE-2020-7013</a> N/A
elastic -- kibana	Kibana versions 6.7.0 to 6.8.8 and 7.0.0 to 7.6.2 contain a prototype pollution flaw in the Upgrade Assistant. An authenticated attacker with privileges to write to the Kibana index could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.	2020-06-03	6.5	<a href="#">CVE-2020-7012</a> N/A
farsite -- farlinx_x25_gateway	FarLinX X25 Gateway through 2014-09-25 allows directory traversal via the log-handling feature.	2020-06-01	5	<a href="#">CVE-2014-7174</a> MISC
fastecdsa -- fastecdsa	An issue was discovered in fastecdsa before 2.1.2. When using the NIST P-256 curve in the ECDSA implementation, the point at infinity is mishandled. This means that for an extreme value in k and s <sup>-1</sup> , the signature verification fails even if the signature is correct. This behavior is not solely a usability problem. There are some threat models where an attacker can benefit by successfully guessing users for whom signature verification will fail.	2020-06-02	5	<a href="#">CVE-2020-12607</a> CONFIRM CONFIRM CONFIRM CONFIRM

fortiguard -- forticlient_for_windows	An Insecure Temporary File vulnerability in FortiClient for Windows 6.2.1 and below may allow a local user to gain elevated privileges via exhausting the pool of temporary file names combined with a symbolic link attack.	2020-06-01	4.6	<a href="#">CVE-2020-9291</a> <a href="#">MISC</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference.	2020-06-04	5	<a href="#">CVE-2019-20813</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows stack consumption via nested function calls for XML parsing.	2020-06-04	5	<a href="#">CVE-2019-20815</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It has a NULL pointer dereference.	2020-06-04	5	<a href="#">CVE-2019-20816</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.12. It allows memory consumption because data is created for each page of an application level.	2020-06-04	5	<a href="#">CVE-2019-20814</a> <a href="#">CONFIRM</a>
foxit -- phantompdf_mac_and_foxit_reader_for_mac	An issue was discovered in Foxit PhantomPDF Mac and Foxit Reader for Mac before 9.7. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	5	<a href="#">CVE-2020-13803</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows memory consumption because data is created for each page of an application level.	2020-06-04	5	<a href="#">CVE-2019-20818</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	5	<a href="#">CVE-2019-20837</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has homograph mishandling.	2020-06-04	4.3	<a href="#">CVE-2019-20835</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference.	2020-06-04	5	<a href="#">CVE-2019-20820</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has a use-after-free because of JavaScript execution after a deletion or close operation.	2020-06-04	5	<a href="#">CVE-2020-13806</a> <a href="#">CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has circular reference mishandling that causes a loop.	2020-06-04	5	<a href="#">CVE-2020-13807</a> <a href="#">CONFIRM</a>



foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via crafted cross-reference stream data.	2020-06-04	5	<a href="#">CVE-2020-13808</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows resource consumption via long strings in the content stream.	2020-06-04	5	<a href="#">CVE-2020-13809</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It has a NULL pointer dereference.	2020-06-04	5	<a href="#">CVE-2019-20817</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7. It allows stack consumption via nested function calls for XML parsing.	2020-06-04	5	<a href="#">CVE-2019-20819</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It has a brute-force attack mishandling because the CAS service lacks a limit on login failures.	2020-06-04	5	<a href="#">CVE-2020-13805</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	2020-06-04	5	<a href="#">CVE-2019-20828</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.6. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	2020-06-04	5	<a href="#">CVE-2019-20829</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.5. It has mishandling of cloud credentials, as demonstrated by Google Drive.	2020-06-04	5	<a href="#">CVE-2019-20836</a> <a href="#">CONFIRM</a>
foxit --reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows information disclosure of a hardcoded username and password in the DocuSign plugin.	2020-06-04	6.8	<a href="#">CVE-2020-13804</a> <a href="#">CONFIRM</a>
freerdp --freerdp	In FreeRDP less than or equal to 2.0.0, when running with logger set to "WLOG_TRACE", a possible crash of application could occur due to a read of an invalid array index. Data could be printed as string to local terminal. This has been fixed in 2.1.0.	2020-05-29	5	<a href="#">CVE-2020-11019</a> <a href="#">CONFIRM</a>
freerdp --freerdp	In FreeRDP before 2.1.0, there is an out-of-bounds read in cliprdr_read_format_list. Clipboard format data read (by client or server) might read data out-of-bounds. This has been fixed in 2.1.0.	2020-05-29	6.4	<a href="#">CVE-2020-11085</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_NegotiateMessage. This has been fixed in 2.1.0.	2020-05-29	5.5	<a href="#">CVE-2020-11088</a> MISC CONFIRM
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_AuthenticateMessage. This has been fixed in 2.1.0.	2020-05-29	5.5	<a href="#">CVE-2020-11087</a> MISC CONFIRM
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_ntlm_v2_client_challenge that reads up to 28 bytes out-of-bound to an internal structure. This has been fixed in 2.1.0.	2020-05-29	5.5	<a href="#">CVE-2020-11086</a> MISC CONFIRM
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bounds read in rfx_process_message_tileset. Invalid data fed to RFX decoder results in garbage on screen (as colors). This has been patched in 2.1.0.	2020-05-29	5	<a href="#">CVE-2020-11043</a> CONFIRM
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound data read from memory in clear_decompress_subcode_rlex, visualized on screen as color. This has been patched in 2.1.0.	2020-05-29	4	<a href="#">CVE-2020-11040</a> CONFIRM
freerdp -- freerdp	In FreeRDP less than or equal to 2.0.0, an outside controlled array index is used unchecked for data used as configuration for sound backend (alsa, oss, pulse, ...). The most likely outcome is a crash of the client instance followed by no or distorted sound or a session disconnect. If a user cannot upgrade to the patched version, a workaround is to disable sound for the session. This has been patched in 2.1.0.	2020-05-29	4	<a href="#">CVE-2020-11041</a> CONFIRM
freerdp -- freerdp	In FreeRDP before 2.1.0, there is an out-of-bound read in irp functions (parallel_process_irp_create, serial_process_irp_create, drive_process_irp_write, printer_process_irp_write, rdpei_recv_pdu, serial_process_irp_write). This has been fixed in 2.1.0.	2020-05-29	6.5	<a href="#">CVE-2020-11089</a> MISC MISC CONFIRM
google -- chrome	Incorrect implementation in permissions in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.	2020-06-03	4.3	<a href="#">CVE-2020-6502</a> MISC MISC
	Insufficient policy enforcement in developer tools in Google Chrome prior to			<a href="#">CVE-2020-</a>

google -- chrome	83.0.4103.97 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.	2020-06-03	<a href="#">4.3</a>	<a href="#">6495</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass AppCache security restrictions via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6499</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in interstitials in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6500</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds write in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6419</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in CSP in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6501</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use after free in WebAuthentication in Google Chrome prior to 83.0.4103.97 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6493</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6453</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in V8 in Google Chrome prior to 14.0.0.0 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2011-2863</a> <a href="#">MISC</a>
google -- chrome	Bad cast in CSS in Google Chrome prior to 11.0.0.0 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2011-1805</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in notifications in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass notification restrictions via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6504</a> <a href="#">MISC</a> <a href="#">MISC</a>
google --	Incorrect security UI in payments in Google Chrome on Android prior to			<a href="#">CVE-2020-</a>

chrome_on_android	83.0.4103.97 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">6494</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_ios	Incorrect implementation in user interface in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6498</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_ios	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 83.0.4103.88 allowed a remote attacker to perform domain spoofing via a crafted URI.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-6497</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome_on_macos	Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2020-06-03	<a href="#">6.8</a>	<a href="#">CVE-2020-6496</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana_labs -- grafana	The avatar feature in Grafana 3.0.1 through 7.0.1 has an SSRF Incorrect Access Control issue. This vulnerability allows any unauthenticated user/client to make Grafana send HTTP requests to any URL and return its result to the user/client. This can be used to gain information about the network that Grafana is running on.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-13379</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via a link on the "Dashboard > All Panels > General" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18625</a> <a href="#">MISC</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via the "Dashboard > Text Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18623</a> <a href="#">MISC</a>
grafana_labs -- grafana	Grafana 5.3.1 has XSS via a column style on the "Dashboard > Table Panel" screen. NOTE: this issue exists because of an incomplete fix for CVE-2018-12099.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2018-18624</a> <a href="#">MISC</a>
huawei -- cloudengine_12800_products	CloudEngine 12800 products with versions of V200R019C00, V200R019C10SPC800, V200R019C00SPC600, V200R019C10; and CloudEngine 6800 products with versions of V200R019C00SPC800 have a denial of service vulnerability. Due to improper memory management, memory leakage may occur in some special cases. Attackers can perform a series of operations to exploit this vulnerability. Successful exploit may cause a denial of	2020-05-29	<a href="#">5</a>	<a href="#">CVE-2020-1870</a> <a href="#">CONFIRM</a>

	service.			
huawei -- e6878-370_products	E6878-370 products with versions of 10.0.3.1(H557SP27C233) and 10.0.3.1(H563SP1C00) have a stack buffer overflow vulnerability. The program copies an input buffer to an output buffer without verification. An attacker in the adjacent network could send a crafted message, successful exploit could lead to stack buffer overflow which may cause malicious code execution.	2020-05-29	<a href="#">5.8</a>	<a href="#">CVE-2020-1832</a> <a href="#">CONFIRM</a>
huawei -- multiple_products	There is a few bytes out-of-bounds read vulnerability in some Huawei products. The software reads data past the end of the intended buffer when parsing certain message, an authenticated attacker could exploit this vulnerability by sending crafted messages to the device. Successful exploit may cause service abnormal in specific scenario. Affected product versions include: AR120-S versions V200R007C00SPC900, V200R007C00SPCa00	2020-06-01	<a href="#">4</a>	<a href="#">MISC</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178965.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-4366</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 179001.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-4367</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182283.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-4503</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- qradar_siem	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 182364.	2020-06-04	<a href="#">5.5</a>	<a href="#">CVE-2020-4509</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
	IBM Security Guardium 11.1 is vulnerable			



ibm -- security_guardium	to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174738.	2020-06-03	4.3	<a href="#">CVE-2020-4182</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10.6, 11.0, and 11.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174851.	2020-06-03	4.6	<a href="#">CVE-2020-4190</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 174857.	2020-06-04	5	<a href="#">CVE-2020-4193</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 could disclose sensitive information on the login page that could aid in further attacks against the system. IBM X-Force ID: 174805.	2020-06-03	5	<a href="#">CVE-2020-4187</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 174739.	2020-06-04	4.3	<a href="#">CVE-2020-4183</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
istio -- istio	Istio 1.4.x before 1.4.9 and Istio 1.5.x before 1.5.4 contain the following vulnerability when telemetry v2 is enabled: by sending a specially crafted packet, an attacker could trigger a Null Pointer Exception resulting in a Denial of Service. This could be sent to the ingress gateway or a sidecar, triggering a null pointer exception which results in a denial of service. This also affects servicemesh-proxy where a null pointer exception flaw was found in servicemesh-proxy. When running Telemetry v2 (not on by default in version 1.4.x), an attacker could send a specially crafted packet to the ingress gateway or proxy sidecar, triggering a denial of service.	2020-06-02	5	<a href="#">CVE-2020-10739</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Jenkins Play Framework Plugin 1.0.2 and earlier lets users specify the path to the `play` command on the Jenkins master	2020-06-		<a href="#">CVE-2020-2200</a>

jenkins -- jenkins	for a form validation endpoint, resulting in an OS command injection vulnerability exploitable by users able to store such a file on the Jenkins master.	03	<a href="#">6.5</a>	<a href="#">MLIST CONFIRM</a>
jenkins -- jenkins	Jenkins Subversion Partial Release Manager Plugin 1.0.1 and earlier does not escape the error message for the repository URL field form validation, resulting in a reflected cross-site scripting vulnerability.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-2199</a> <a href="#">MLIST CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier allows attackers to add or remove agent labels.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-2192</a> <a href="#">MLIST CONFIRM</a>
jenkins -- jenkins	Jenkins Self-Organizing Swarm Plug-in Modules Plugin 3.20 and earlier does not check permissions on API endpoints that allow adding and removing agent labels.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2191</a> <a href="#">MLIST CONFIRM</a>
jenkins -- jenkins	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not redact encrypted secrets in the 'getConfigAsXML' API URL when transmitting job config.xml data to users without Job/Configure.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2198</a> <a href="#">MLIST CONFIRM</a>
jenkins -- jenkins	Jenkins Project Inheritance Plugin 19.08.02 and earlier does not require users to have Job/ExtendedRead permission to access Inheritance Project job configurations in XML format.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-2197</a> <a href="#">MLIST CONFIRM</a>
jenkins -- jenkins	Jenkins Selenium Plugin 3.141.59 and earlier has no CSRF protection for its HTTP endpoints, allowing attackers to perform all administrative actions provided by the plugin.	2020-06-03	<a href="#">6</a>	<a href="#">CVE-2020-2196</a> <a href="#">MLIST CONFIRM</a>
joomla! -- joomla!	In Joomla! before 3.9.19, lack of input validation in the heading tag option of the "Articles - Newsflash" and "Articles - Categories" modules allows XSS.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13761</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, the default settings of the global textfilter configuration do not block HTML inputs for Guest users.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13763</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, missing token checks in com_postinstall lead to CSRF.	2020-06-02	<a href="#">6.8</a>	<a href="#">CVE-2020-13760</a> <a href="#">MISC</a>
joomla! -- joomla!	In Joomla! before 3.9.19, incorrect input validation of the module tag option in com_modules allows XSS.	2020-06-02	<a href="#">4.3</a>	<a href="#">CVE-2020-13762</a> <a href="#">MISC</a>
	A vulnerability was found in all versions of containernetworking/plugins before version 0.8.6, that allows malicious			

kubernetes -- containernetworking/plugins	containers in Kubernetes clusters to perform man-in-the-middle (MitM) attacks. A malicious container can exploit this flaw by sending rogue IPv6 router advertisements to the host or other containers, to redirect traffic to the malicious container.	2020-06-03	6	<a href="#">CVE-2020-10749</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libjpeg-turbo -- libjpeg-turbo	libjpeg-turbo 2.0.4, and mozjpeg 4.0.0, has a heap-based buffer over-read in get_rgb_row() in rdppm.c via a malformed PPM input file.	2020-06-03	5.8	<a href="#">CVE-2020-13790</a> <a href="#">MISC</a> <a href="#">MISC</a>
libvirt -- libvirt	A NULL pointer dereference was found in the libvirt API responsible introduced in upstream version 3.10.0, and fixed in libvirt 6.0.0, for fetching a storage pool based on its target path. In more detail, this flaw affects storage pools created without a target path such as network-based pools like gluster and RBD. Unprivileged users with a read-only connection could abuse this flaw to crash the libvirt daemon, resulting in a potential denial of service.	2020-06-02	4	<a href="#">CVE-2020-10703</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	go7007_snd_init in drivers/media/usb/go7007/snd-go7007.c in the Linux kernel before 5.6 does not call snd_card_free for a failure path, which causes a memory leak, aka CID-9453264ef586.	2020-06-03	4.9	<a href="#">CVE-2019-20810</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.4.7. The prb_calc_retire_blk_tmo() function in net/packet/af_packet.c can result in a denial of service (CPU consumption and soft lockup) in a certain failure case involving TPACKET_V3, aka CID-b43d1f9f7067.	2020-06-03	4.9	<a href="#">CVE-2019-20812</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki -- mediawiki	resources/src/mediawiki.page.ready/ready.js in MediaWiki before 1.35 allows remote attackers to force a logout and external redirection via HTML content in a MediaWiki page.	2020-06-02	5.8	<a href="#">CVE-2020-10959</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mulesoft -- mulesoft_ce/ee	A Denial of Service vulnerability in MuleSoft Mule CE/EE 3.8.x, 3.9.x, and 4.x released before April 7, 2020, could allow remote attackers to submit data which can lead to resource exhaustion.	2020-05-29	5	<a href="#">CVE-2020-6937</a> <a href="#">CONFIRM</a>
naviwebs -- navigate cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/feeds/feed.class.php.	2020-06-03	4.3	<a href="#">CVE-2020-13798</a> <a href="#">MISC</a>

naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/structure/structure.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13796</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows XSS because of a lack of purify calls in lib/packages/websites/website.class.php.	2020-06-03	<a href="#">4.3</a>	<a href="#">CVE-2020-13797</a> <a href="#">MISC</a>
naviwebs -- navigate_cms	An issue was discovered in Navigate CMS through 2.8.7. It allows Directory Traversal because lib/packages/templates/template.class.php mishandles ../ and ../ substrings.	2020-06-03	<a href="#">5</a>	<a href="#">CVE-2020-13795</a> <a href="#">MISC</a> <a href="#">MISC</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to delete arbitrary local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5296</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to upload jpg, jpeg, bmp, png, webp, gif, ico, css, js, woff, woff2, svg, ttf, eot, json, md, less, sass, scss, xml files to any directory of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5297</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, an attacker can exploit this vulnerability to read local files of an October CMS server. The vulnerability is only exploitable by an authenticated backend user with the `cms.manage_assets` permission. Issue has been patched in Build 466 (v1.0.466).	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-5295</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phplist -- phplist	phplist before 3.5.4 allows XSS via /lists/admin/user.php and /lists/admin/users.php.	2020-06-04	<a href="#">4.3</a>	<a href="#">CVE-2020-13827</a> <a href="#">MISC</a>
pi-hole -- pi-hole_web	Pi-hole Web v4.3.2 (aka AdminLTE) allows Remote Code Execution by privileged dashboard users via a crafted	2020-05-29	<a href="#">6.5</a>	<a href="#">CVE-2020-8816</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>

	DHCP static lease.			<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows CSRF.	2020-06-01	<a href="#">6.8</a>	<a href="#">CVE-2014-8942</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows denial of service because api/update.php launches svn update operations that use a great deal of resources.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2014-8937</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (full path) via an include/smarty/plugins/modifier.date_format.php request if PHP has a non-recommended configuration that produces warning messages.	2020-06-01	<a href="#">4.3</a>	<a href="#">CVE-2014-8939</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows remote attackers to obtain sensitive information (names and details of projects) by visiting the /update.log URI.	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2014-8940</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows SSRF via the admin.php?page=projects svn_url parameter.	2020-06-01	<a href="#">6.5</a>	<a href="#">CVE-2014-8943</a> <a href="#">MISC</a>
playtube -- playtube	PlayTube 1.8 allows disclosure of user details via ajax.php?type=../admin-panel/autoload&page=manage-users directory traversal, aka local file inclusion.	2020-06-03	<a href="#">4</a>	<a href="#">CVE-2020-13792</a> <a href="#">MISC</a>
python-rsa -- python-rsa	Python-RSA 4.0 ignores leading ' ' bytes during decryption of ciphertext. This could conceivably have a security-relevant impact, e.g., by helping an attacker to infer that an application uses Python-RSA, or if the length of accepted ciphertext affects application behavior (such as by causing excessive memory allocation).	2020-06-01	<a href="#">5</a>	<a href="#">CVE-2020-13757</a> <a href="#">MISC</a>
qemu -- qemu	address_space_map in exec.c in QEMU 4.2.0 can trigger a NULL pointer dereference related to BounceBuffer.	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13659</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
qemu -- qemu	hw/pci/msix.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access via a crafted address in an msi-x mmio operation.	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2020-13754</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_processors	A race condition can occur when using the fastrpc memory mapping API. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8009, Snapdragon	2020-06-	<a href="#">6.9</a>	<a href="#">CVE-2020-3680</a>



	APQ8053, MSM8909W, MSM8917, MSM8953, QCS605, QM215, SA415M, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SXR1130	02		<a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Possibility of out of bound access while processing the responses from video firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, Saipan, SC8180X, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2020-3630</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Possibility of double free of the drawobj that is added to the drawqueue array of the context during IOCTL commands as there is no refcount taken for this object in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCS405, QCS605, QM215, Rennell, SA415M, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2020-3610</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound memory access while processing qpay due to not validating length of the response buffer provided by User. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2019-14078</a> <a href="#">CONFIRM</a>

	Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, MSM8909, MSM8998, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845			
qualcomm -- multiple_snapdragon_processors	Out of bound memory access while processing ese transmit command due to passing Response buffer received from user in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8098, IPQ6018, Kamorta, MDM9150, MDM9205, MDM9607, MDM9650, MSM8909, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	<a href="#">4.6</a>	<a href="#">CVE-2019-14077</a> <a href="#">CONFIRM</a>
rust-vmm -- vm-memory	rust-vmm vm-memory before 0.1.1 and 0.2.x before 0.2.1 allows attackers to cause a denial of service (loss of IP networking) because read_obj and write_obj do not properly access memory. This affects aarch64 (with musl or glibc) and x86_64 (with musl).	2020-06-02	<a href="#">5</a>	<a href="#">CVE-2020-13759</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) software. One UI HOME logging can leak information. The Samsung ID is SVE-2019-16382 (June 2020).	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13830</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x) (with TEEGRIS) software. The Gatekeeper Trustlet allows a brute-force attack on user credentials. The Samsung ID is SVE-2020-16908 (June 2020).	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13835</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. The system area allows arbitrary file overwrites via a symlink attack. The Samsung ID is SVE-2020-17183 (June 2020).	2020-06-04	<a href="#">6.4</a>	<a href="#">CVE-2020-13833</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. HWRResProvider allows path traversal for data exposure. The Samsung ID is SVE-2020-16954	2020-06-04	<a href="#">5</a>	<a href="#">CVE-2020-13836</a> <a href="#">CONFIRM</a>

	(June 2020).			
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (with TEEGRIS) software. Secure Folder does not properly restrict use of Android Debug Bridge (adb) for arbitrary installations. The Samsung ID is SVE-2020-17369 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13834</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. Attackers can disable the SEAndroid protection mechanism in the RKP. The Samsung ID is SVE-2019-15998 (June 2020).	2020-06-04	5	<a href="#">CVE-2020-13829</a> <a href="#">CONFIRM</a>
synk -- broker	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network by creating symlinks to match whitelisted paths.	2020-05-29	4	<a href="#">CVE-2020-7653</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.73.1 are vulnerable to Information Exposure. It logs private keys if logging level is set to DEBUG.	2020-05-29	4.3	<a href="#">CVE-2020-7654</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.72.2 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users who have access to Snyk's internal network by appending the URL with a fragment identifier and a whitelisted path e.g. `#package.json`	2020-05-29	4	<a href="#">CVE-2020-7648</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.80.0 are vulnerable to Arbitrary File Read. It allows arbitrary file reads for users with access to Snyk's internal network via directory traversal.	2020-05-29	4	<a href="#">CVE-2020-7652</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker after 4.72.0 including and before 4.73.1 are vulnerable to Arbitrary File Read. It allows arbitrary file reads to users with access to Snyk's internal network of any files ending in the following extensions: yaml, yml or json.	2020-05-29	4	<a href="#">CVE-2020-7650</a> <a href="#">MISC</a> <a href="#">MISC</a>
synk -- broker	All versions of snyk-broker before 4.79.0 are vulnerable to Arbitrary File Read. It allows partial file reads for users who have access to Snyk's internal network via patch history from GitHub Commits API.	2020-05-29	4	<a href="#">CVE-2020-7651</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in Sysax Multi Server 6.90. An attacker can determine			<a href="#">CVE-2020-13227</a>

sysax -- multi_server	the username (under which the web server is running) by triggering an invalid path permission error. This bypasses the fakepath protection mechanism.	2020-06-02	5	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. There is reflected XSS via the /scgi sid parameter.	2020-06-02	4.3	<a href="#">CVE-2020-13228</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sysax -- multi_server	An issue was discovered in Sysax Multi Server 6.90. A session can be hijacked if one observes the sid value in any /scgi URI, because it is an authentication token.	2020-06-02	6.8	<a href="#">CVE-2020-13229</a> <a href="#">MISC</a> <a href="#">MISC</a>
upx -- upx	p_lx_elf.cpp in UPX before 3.96 has an integer overflow during unpacking via crafted values in a PT_DYNAMIC segment.	2020-06-01	4.3	<a href="#">CVE-2019-20805</a> <a href="#">MISC</a> <a href="#">MISC</a>
vmware -- multiple_products	VMware Fusion (11.x before 11.5.5), VMware Remote Console for Mac (11.x and prior) and VMware Horizon Client for Mac (5.x and prior) contain a local privilege escalation vulnerability due to a Time-of-check Time-of-use (TOCTOU) issue in the service opener. Successful exploitation of this issue may allow attackers with normal user privileges to escalate their privileges to root on the system where Fusion, VMRC and Horizon Client are installed.	2020-05-29	6.9	<a href="#">CVE-2020-3957</a> <a href="#">CONFIRM</a>
vmware -- spring_cloud_config	Spring Cloud Config, versions 2.2.x prior to 2.2.3, versions 2.1.x prior to 2.1.9, and older unsupported versions allow applications to serve arbitrary configuration files through the spring-cloud-config-server module. A malicious user, or attacker, can send a request using a specially crafted URL that can lead to a directory traversal attack.	2020-06-02	5	<a href="#">CVE-2020-5410</a> <a href="#">CONFIRM</a>
websocket-extensions -- websocket-extensions	websocket-extensions ruby module prior to 0.1.5 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.	2020-06-02	5	<a href="#">CVE-2020-7663</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

websocket-extensions -- websocket-extensions	websocket-extensions npm module prior to 1.0.4 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.	2020-06-02	5	<a href="#">CVE-2020-7662</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	common.php in the Gravity Forms plugin before 2.4.9 for WordPress can leak hashed passwords because user_pass is not considered a special case for a \$current_user->get(\$property) call.	2020-06-02	5	<a href="#">CVE-2020-13764</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The MailPoet plugin before 3.23.2 for WordPress allows remote attackers to inject arbitrary web script or HTML using extra parameters in the URL (Reflective Server-Side XSS).	2020-06-02	4.3	<a href="#">CVE-2019-11843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zimbra -- zimbra	Zimbra before 8.8.15 Patch 10 and 9.x before 9.0.0 Patch 3 allows remote code execution via an avatar file. There is potential abuse of /service/upload servlet in the webmail subsystem. A user can upload executable files (exe,sh,bat,jar) in the Contact section of the mailbox as an avatar image for a contact. A user will receive a "Corrupt File" error, but the file is still uploaded and stored locally in /opt/zimbra/data/tmp/upload/, leaving it open to possible remote execution.	2020-06-03	6	<a href="#">CVE-2020-12846</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
znc -- znc	ZNC 1.8.0 up to 1.8.1-rc1 allows attackers to trigger an application crash (with a NULL pointer dereference) if echo-message is not enabled and there is no network.	2020-06-02	4.3	<a href="#">CVE-2020-13775</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zoho -- manageengine_opmanager	In Zoho ManageEngine OpManager before 125144, when <cachestart> is used, directory traversal validation can be bypassed.	2020-06-04	5	<a href="#">CVE-2020-13818</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
------------------------------	-------------	-----------	---------------	------------------------



abb -- device_library_wizard	Insecure storage of sensitive information in ABB Device Library Wizard versions 6.0.X, 6.0.3.1 and 6.0.3.2 allows unauthenticated low privilege user to read file that contains confidential data	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-8482</a> <a href="#">CONFIRM</a>
atlassian -- fisheye_and_crucible	The review resource in Atlassian Fisheye and Crucible before version 4.8.1 allows remote attackers to inject arbitrary HTML or Javascript via a cross site scripting (XSS) vulnerability through the review objectives.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2020-4013</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira_server_and_data_center	Affected versions are: Before 8.5.5, and from 8.6.0 before 8.8.1 of Atlassian Jira Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the XML export view.	2020-06-01	<a href="#">3.5</a>	<a href="#">CVE-2020-4021</a> <a href="#">MISC</a>
avaya -- ip_office	A sensitive information disclosure vulnerability was discovered in the web interface component of IP Office that may potentially allow a local user to gain unauthorized access to the component. Affected versions of IP Office include: 9.x, 10.0 through 10.1.0.7 and 11.0 though 11.0.4.3.	2020-06-04	<a href="#">2.1</a>	<a href="#">CVE-2020-7030</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
elastic -- kibana	Kibana versions before 6.8.9 and 7.7.0 contains a stored XSS flaw in the TSVB visualization. An attacker who is able to edit or create a TSVB visualization could allow the attacker to obtain sensitive information from, or perform destructive actions, on behalf of Kibana users who edit the TSVB visualization.	2020-06-03	<a href="#">3.5</a>	<a href="#">CVE-2020-7015</a> <a href="#">N/A</a>
fortiguard -- fortianalyzer	An improper neutralization of input vulnerability in the Admin Profile of FortiAnalyzer may allow a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the Description Area.	2020-06-04	<a href="#">3.5</a>	<a href="#">CVE-2020-6640</a> <a href="#">MISC</a>
huawei -- honor_9x_smartphones	Honor 9X smartphones with versions earlier than 9.1.1.172(C00E170R8P1) have an improper authentication vulnerability. A logic error occurs when handling clock function, an attacker should do a series of crafted operations quickly before the phone is unlocked, successful exploit could allow the attacker to access clock information without unlock the phone.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1833</a> <a href="#">CONFIRM</a>
	HUAWEI Mate 10 smartphones with versions earlier than			

huawei -- mate_10_smartphones	10.0.0.143(C00E143R2P4) have an information disclosure vulnerability. The attacker could wake up voice assistant then do a series of crafted voice operation, successful exploit could allow the attacker read certain files without unlock the phone leading to information disclosure.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1809</a> <a href="#">CONFIRM</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.185(C00E74R3P8) have an improper authorization vulnerability. The system does not properly restrict certain operation in ADB mode, successful exploit could allow certain user break the limit of digital balance function.	2020-05-29	<a href="#">2.1</a>	<a href="#">CVE-2020-1797</a> <a href="#">CONFIRM</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.195(SP31C00E74R3P8) have an improper authorization vulnerability. The digital balance function does not sufficiently restrict the using time of certain user, successful exploit could allow the user break the limit of digital balance function after a series of operations with a PC.	2020-05-29	<a href="#">1.9</a>	<a href="#">CVE-2020-1831</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 178765.	2020-06-02	<a href="#">3.5</a>	<a href="#">CVE-2020-4360</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics_local	IBM Planning Analytics Local 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 180761.	2020-06-02	<a href="#">3.5</a>	<a href="#">CVE-2020-4431</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 could allow an attacker on the same network to gain access to the Solr dashboard and cause a denial of service attack. IBM X-Force ID: 176997.	2020-06-03	<a href="#">3.3</a>	<a href="#">CVE-2020-4307</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174852.	2020-06-04	<a href="#">2.1</a>	<a href="#">CVE-2020-4191</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

jenkins -- jenkins	Jenkins Compact Columns Plugin 1.11 and earlier displays the unprocessed job description in tooltips, resulting in a stored cross-site scripting vulnerability that can be exploited by users with Job/Configure permission.	2020-06-03	3.5	<a href="#">CVE-2020-2195</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Script Security Plugin 1.72 and earlier does not correctly escape pending or approved classpath entries on the In-process Script Approval page, resulting in a stored cross-site scripting vulnerability.	2020-06-03	3.5	<a href="#">CVE-2020-2190</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the display name of the builds in the trend chart, resulting in a stored cross-site scripting vulnerability.	2020-06-03	3.5	<a href="#">CVE-2020-2194</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins ECharts API Plugin 4.7.0-3 and earlier does not escape the parser identifier when rendering charts, resulting in a stored cross-site scripting vulnerability.	2020-06-03	3.5	<a href="#">CVE-2020-2193</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.6. In rx_queue_add_kobject() and netdev_queue_add_kobject() in net/core/net-sysfs.c, a reference count is mishandled, aka CID-a3e23f719f5c.	2020-06-03	2.1	<a href="#">CVE-2019-20811</a> <a href="#">MISC</a> <a href="#">MISC</a>
october -- october_cms	In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, a user with the ability to use the import functionality of the `ImportExportController` behavior can be socially engineered by an attacker to upload a maliciously crafted CSV file which could result in a reflected XSS attack on the user in question Issue has been patched in Build 466 (v1.0.466).	2020-06-03	3.5	<a href="#">CVE-2020-5298</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows XSS (Reflected) via the username, or XSS (Stored) via the admin.php?page=config install_name, intro_message, or new_file_content parameter.	2020-06-01	3.5	<a href="#">CVE-2014-8944</a> <a href="#">MISC</a>
piwigo -- lexiglot	Lexiglot through 2014-11-20 allows local users to obtain sensitive information by listing a process because the username and password are on the command line.	2020-06-01	2.1	<a href="#">CVE-2014-8938</a> <a href="#">MISC</a>
	When attempting to create a new XFRM policy, a stack out-of-bounds read will occur if the user provides a template where the mode is set to a value that does not resolve to a valid XFRM mode in Snapdragon Auto, Snapdragon Compute,			

qualcomm -- multiple_snapdragon_products	Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, QCA4531, QCN7605, QCS605, QM215, SA415M, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-06-02	3.6	<a href="#">CVE-2019-14053</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer over-read in ADSP parse function due to lack of check for availability of sufficient data payload received in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710, SDM845, SDX20, SDX24	2020-06-02	3.6	<a href="#">CVE-2019-14038</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound read in adm call back function due to incorrect boundary check for payload in command response in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8053, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, QCS605, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM670, SDM710, SDM845, SDX20, SDX24	2020-06-02	3.6	<a href="#">CVE-2019-14039</a> <a href="#">CONFIRM</a>
	Using non-time-constant functions like memcmp to compare sensitive data can lead to information leakage through timing side channel issue. in Snapdragon Auto, Snapdragon Compute, Snapdragon			

qualcomm -- multiple_snapdragon_products	Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, Kamorta, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS404, QCS405, QCS605, QM215, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130	2020-06-02	2.1	<a href="#">CVE-2019-14067</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound read in Fingerprint application due to requested data is being used without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9150, MDM9205, MDM9650, MSM8998, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDA660, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	3.6	<a href="#">CVE-2019-14043</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound read in in fingerprint application due to requested data assigned to a local buffer without length check in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in Kamorta, MDM9205, Nicobar, QCS404, QCS405, QCS605, Rennell, SA415M, SA6155P, SC7180, SC8180X, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-06-02	3.6	<a href="#">CVE-2019-14042</a> <a href="#">CONFIRM</a>



samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with Q(10.0) software. The Lockscreen feature does not block Quick Panel access to Music Share. The Samsung ID is SVE-2020-17145 (June 2020).	2020-06-04	3.6	<a href="#">CVE-2020-13837</a> <a href="#">CONFIRM</a>
samsung -- multiple_mobile_devices	An issue was discovered on Samsung mobile devices with P(9.0) and Q(10.0) software. The DeX Lockscreen feature does not block access to Quick Panel and notifications. The Samsung ID is SVE-2020-17187 (June 2020).	2020-06-04	3.6	<a href="#">CVE-2020-13838</a> <a href="#">CONFIRM</a>
sane -- backends	A NULL pointer dereference in sane_epson_net_read in SANE Backends through 1.0.29 allows a malicious device connected to the same local network as the victim to cause a denial of service, aka GHSL-2020-075.	2020-06-01	2.1	<a href="#">CVE-2020-12867</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.5.2) and VMware Fusion (11.x before 11.5.2) contain a denial-of-service vulnerability in the shader functionality. Successful exploitation of this issue may allow attackers with non-administrative access to a virtual machine to crash the virtual machine's vmx process leading to a denial of service condition.	2020-05-29	2.1	<a href="#">CVE-2020-3958</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), VMware Workstation (15.x before 15.1.0) and VMware Fusion (11.x before 11.1.0) contain a memory leak vulnerability in the VMCI module. A malicious actor with local non-administrative access to a virtual machine may be able to crash the virtual machine's vmx process leading to a partial denial of service.	2020-05-29	2.1	<a href="#">CVE-2020-3959</a> <a href="#">CONFIRM</a>
zte -- ft680_router	ZTE's PON terminal product is impacted by the access control vulnerability. Due to the system not performing correct access control on some program interfaces, an attacker could use this vulnerability to tamper with the program interface parameters to perform unauthenticated operations. This affects: <ZTE F680> <V9.0.10P1N6>	2020-06-01	3.3	<a href="#">CVE-2020-6868</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- unomi	Apache Unomi allows conditions to use OGNL scripting which offers the possibility to call static Java classes from the JDK that could execute code with the permission level of the running Java process.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11975</a> <a href="#">MISC</a>
apple -- multiple_products	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5.1 and iPadOS 13.5.1, macOS Catalina 10.15.5 Supplemental Update, tvOS 13.4.6, watchOS 6.2.6. An application may be able to execute arbitrary code with kernel privileges.	2020-06-05	not yet calculated	<a href="#">CVE-2020-9859</a> <a href="#">MISC</a>
athom -- homey_and_homey_products	An issue was discovered in all Athom Homey and Homey Pro devices up to the current version 4.2.0. An attacker within RF range can obtain a cleartext copy of the network configuration of the device, including the Wi-Fi PSK, during device setup. Upon success, the attacker is able to further infiltrate the target's Wi-Fi networks.	2020-06-04	not yet calculated	<a href="#">CVE-2020-9462</a> <a href="#">MISC</a>
bitdefender -- antivirus_free	A vulnerability in the improper handling of symbolic links in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects Bitdefender Antivirus Free versions prior to 1.0.17.178.	2020-06-05	not yet calculated	<a href="#">CVE-2020-8103</a> <a href="#">CONFIRM</a>
bludit -- bludit	showAlert() in the administration panel in Bludit 3.12.0 allows XSS.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13889</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to privilege escalation through the Adminstrator/Users/Edit/:UserId functionality. Adminstrator/Users/Edit/:UserId fails to check that the request was submitted by an Administrator. This allows a normal user to escalate their privileges by adding additional roles to their account.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11679</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
	Castel NextGen DVR v1.0.0 is vulnerable to CSRF in all state-changing request. A __RequestVerificationToken is set by the			<a href="#">CVE-2020-</a>

castel -- nextgen_dvr	web interface, and included in requests sent by web interface. However, this token is not verified by the application: the token can be removed from all requests and the request will succeed.	2020-06-04	not yet calculated	<a href="#">11682</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 stores and displays credentials for the associated SMTP server in cleartext. Low privileged users can exploit this to create an administrator user and obtain the SMTP credentials.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11681</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
castel -- nextgen_dvr	Castel NextGen DVR v1.0.0 is vulnerable to authorization bypass on all administrator functionality. The application fails to check that a request was submitted by an administrator. Consequently, a normal user can perform actions including, but not limited to, creating/modifying the file store, creating/modifying alerts, creating/modifying users, etc.	2020-06-04	not yet calculated	<a href="#">CVE-2020-11680</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
cisco -- 4300_series_integrated_services_routers_and_catalyst_9800-l_wireless_controllers	A vulnerability in the hardware crypto driver of Cisco IOS XE Software for Cisco 4300 Series Integrated Services Routers and Cisco Catalyst 9800-L Wireless Controllers could allow an unauthenticated, remote attacker to disconnect legitimate IPsec VPN sessions to an affected device. The vulnerability is due to insufficient verification of authenticity of received Encapsulating Security Payload (ESP) packets. An attacker could exploit this vulnerability by tampering with ESP cleartext values as a man-in-the-middle.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3220</a> <a href="#">CISCO</a>
cisco -- 809_and_829_industrial_services_routers	A vulnerability in the image verification feature of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) could allow an authenticated, local attacker to boot a malicious software image on an affected device. The vulnerability is due to insufficient access restrictions on the area of code that manages the image verification feature. An attacker could exploit this vulnerability by first authenticating to the targeted device and then logging in to the Virtual Device Server (VDS) of an affected device. The attacker could then, from the VDS shell, disable Cisco IOS Software integrity (image) verification. A successful exploit	2020-06-03	not yet calculated	<a href="#">CVE-2020-3208</a> <a href="#">CISCO</a>

	could allow the attacker to boot a malicious Cisco IOS Software image on the targeted device. To exploit this vulnerability, the attacker must have valid user credentials at privilege level 15.			
cisco -- application_services_engine_software	A vulnerability in the key store of Cisco Application Services Engine Software could allow an authenticated, local attacker to read sensitive information of other users on an affected device. The vulnerability is due to insufficient authentication limitations. An attacker could exploit this vulnerability by logging in to an affected device locally with valid credentials. A successful exploit could allow the attacker to read the sensitive information of other users on the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3335</a> <a href="#">CISCO</a>
cisco -- application_services_engine_software	A vulnerability in the API of Cisco Application Services Engine Software could allow an unauthenticated, remote attacker to update event policies on an affected device. The vulnerability is due to insufficient authentication of users who modify policies on an affected device. An attacker could exploit this vulnerability by crafting a malicious HTTP request to contact an affected device. A successful exploit could allow the attacker to update event policies on the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3333</a> <a href="#">CISCO</a>
cisco -- asr_920_series_aggregation_services_router	A vulnerability in the Simple Network Management Protocol (SNMP) implementation in Cisco ASR 920 Series Aggregation Services Router model ASR920-12SZ-IM could allow an authenticated, remote attacker to cause the device to reload. The vulnerability is due to incorrect handling of data that is returned from Cisco Discovery Protocol queries to SNMP. An attacker could exploit this vulnerability by sending a request for Cisco Discovery Protocol information by using SNMP. An exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3232</a> <a href="#">CISCO</a>
	A vulnerability in the 802.1X feature of Cisco Catalyst 2960-L Series Switches and Cisco Catalyst CDB-8P Switches could allow an unauthenticated, adjacent attacker to forward broadcast traffic before being authenticated on the port. The vulnerability exists because			

cisco -- catalyst-2960-l_series_switches_and-8p_switches	broadcast traffic that is received on the catalyst cdp-802.1X-enabled port is mishandled. An attacker could exploit this vulnerability by sending broadcast traffic on the port before being authenticated. A successful exploit could allow the attacker to send and receive broadcast traffic on the 802.1X-enabled port before authentication.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3231</a> <a href="#">CISCO</a>
cisco -- catalyst_4500_series_switches	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS Software and Cisco IOS XE Software on Catalyst 4500 Series Switches could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient input validation when the software processes specific SNMP object identifiers. An attacker could exploit this vulnerability by sending a crafted SNMP packet to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition. Note: To exploit this vulnerability by using SNMPv2c or earlier, the attacker must know the SNMP read-only community string for an affected system. To exploit this vulnerability by using SNMPv3, the attacker must know the user credentials for the affected system.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3235</a> <a href="#">CISCO</a>
cisco -- catalyst_9800_series_wireless_controllers	A vulnerability in the Flexible NetFlow Version 9 packet processor of Cisco IOS XE Software for Cisco Catalyst 9800 Series Wireless Controllers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of parameters in a Flexible NetFlow Version 9 record. An attacker could exploit this vulnerability by sending a malformed Flexible NetFlow Version 9 packet to the Control and Provisioning of Wireless Access Points (CAPWAP) data port of an affected device. An exploit could allow the attacker to trigger an infinite loop, resulting in a process crash that would cause a reload of the device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3221</a> <a href="#">CISCO</a>
	A vulnerability in the locally significant certificate (LSC) provisioning feature of Cisco Catalyst 9800 Series Wireless			



cisco -- catalyst_9800_series_wireless_controllers	<p>Controllers that are running Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a memory leak that could lead to a denial of service (DoS) condition. The vulnerability is due to incorrect processing of certain public key infrastructure (PKI) packets. An attacker could exploit this vulnerability by sending crafted Secure Sockets Layer (SSL) packets to an affected device. A successful exploit could cause an affected device to continuously consume memory, which could result in a memory allocation failure that leads to a crash and causes a DoS condition.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3203</a> <a href="#">CISCO</a>
cisco -- catalyst_9800_series_wireless_controllers	<p>A vulnerability in the handling of IEEE 802.11w Protected Management Frames (PMFs) of Cisco Catalyst 9800 Series Wireless Controllers that are running Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to terminate a valid user connection to an affected device. The vulnerability exists because the affected software does not properly validate IEEE 802.11w disassociation and deauthentication PMFs that it receives. An attacker could exploit this vulnerability by sending a spoofed 802.11w PMF from a valid, authenticated client on a network adjacent to an affected device. A successful exploit could allow the attacker to terminate a single valid user connection to the affected device.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3206</a> <a href="#">CISCO</a>
cisco -- digital_network_architecture_center	<p>A vulnerability in the audit logging component of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to view sensitive information in clear text. The vulnerability is due to the storage of certain unencrypted credentials. An attacker could exploit this vulnerability by accessing the audit logs and obtaining credentials that they may not normally have access to. A successful exploit could allow the attacker to use those credentials to discover and manage network devices.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3281</a> <a href="#">CISCO</a>
	<p>A vulnerability in the syslog processing engine of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected</p>			

cisco -- identity_services_engine	device. The vulnerability is due to a race condition that may occur when syslog messages are processed. An attacker could exploit this vulnerability by sending a high rate of syslog messages to an affected device. A successful exploit could allow the attacker to cause the Application Server process to crash, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3353</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by executing crafted Tcl arguments on an affected device. An exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3201</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Tool Command Language (Tcl) interpreter of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, local attacker with privileged EXEC credentials to execute arbitrary code on the underlying operating system (OS) with root privileges. The vulnerability is due to insufficient input validation of data passed to the Tcl interpreter. An attacker could exploit this vulnerability by loading malicious Tcl code on an affected device. A successful exploit could allow the attacker to cause memory corruption or execute the code with root privileges on the underlying OS of the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3204</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the Secure Shell (SSH) server code of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to cause an affected device to reload. The vulnerability is due to an internal state not being represented correctly in the SSH state machine, which leads to an unexpected behavior. An attacker could exploit this vulnerability by creating an SSH connection to an affected device and using a specific traffic pattern that causes an error condition within that connection.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3200</a> <a href="#">CISCO</a>

	A successful exploit could allow an attacker to cause the device to reload, resulting in a denial of service (DoS) condition.			
cisco -- ios_and_ios_xe_software	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) implementation in Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to prevent IKEv2 from establishing new security associations. The vulnerability is due to incorrect handling of crafted IKEv2 SA-Init packets. An attacker could exploit this vulnerability by sending crafted IKEv2 SA-Init packets to the affected device. An exploit could allow the attacker to cause the affected device to reach the maximum incoming negotiation limits and prevent further IKEv2 security associations from being formed.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3230</a> <a href="#">CISCO</a>
cisco -- ios_xe_sd-wan_software	A vulnerability in Cisco IOS XE SD-WAN Software could allow an unauthenticated, physical attacker to bypass authentication and gain unrestricted access to the root shell of an affected device. The vulnerability exists because the affected software has insufficient authentication mechanisms for certain commands. An attacker could exploit this vulnerability by stopping the boot initialization of an affected device. A successful exploit could allow the attacker to bypass authentication and gain unrestricted access to the root shell of the affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3216</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	Multiple vulnerabilities in the implementation of the Common Industrial Protocol (CIP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to insufficient input processing of CIP traffic. An attacker could exploit these vulnerabilities by sending crafted CIP traffic to be processed by an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3225</a> <a href="#">CISCO</a>
	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an authenticated,			

cisco -- ios_xe_software	remote attacker with administrative privileges to read arbitrary files on the underlying filesystem of the device. The vulnerability is due to insufficient file scope limiting. An attacker could exploit this vulnerability by creating a specific file reference on the filesystem and then accessing it through the web UI. An exploit could allow the attacker to read arbitrary files from the underlying operating system's filesystem.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3223</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker could exploit this vulnerability by uploading a crafted file to the web UI of an affected device. A successful exploit could allow the attacker to inject and execute arbitrary commands with root privileges on the device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3212</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to inject and execute arbitrary commands with administrative privileges on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of user-supplied input to the web UI. An attacker could exploit this vulnerability by submitting crafted input to the web UI. A successful exploit could allow an attacker to execute arbitrary commands with administrative privileges on an affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3219</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the Session Initiation Protocol (SIP) library of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to trigger a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient sanity checks on received SIP messages. An attacker could exploit this vulnerability by sending crafted SIP messages to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3226</a> <a href="#">CISCO</a>
	A vulnerability in the web-based user			

cisco -- ios_xe_software	interface (web UI) of Cisco IOS XE Software could allow an authenticated, remote attacker with read-only privileges to inject IOS commands to an affected device. The injected commands should require a higher privilege level in order to be executed. The vulnerability is due to insufficient input validation of specific HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to a specific web UI endpoint on an affected device. A successful exploit could allow the attacker to inject IOS commands to the affected device, which could allow the attacker to alter the configuration of the device or cause a denial of service (DoS) condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3224</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to bypass access control restrictions on an affected device. The vulnerability is due to the presence of a proxy service at a specific endpoint of the web UI. An attacker could exploit this vulnerability by connecting to the proxy service. An exploit could allow the attacker to bypass access restrictions on the network by proxying their access request through the management network of the affected device. As the proxy is reached over the management virtual routing and forwarding (VRF), this could reduce the effectiveness of the bypass.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3222</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in software image verification in Cisco IOS XE Software could allow an unauthenticated, physical attacker to install and boot a malicious software image or execute unsigned binaries on an affected device. The vulnerability is due to an improper check on the area of code that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to install and boot a malicious software image or execute unsigned binaries on the targeted device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3209</a> <a href="#">CISCO</a>
	A vulnerability in the web UI of Cisco IOS XE Software could allow an			



cisco -- ios_xe_software	authenticated, remote attacker to execute arbitrary commands with root privileges on the underlying operating system of an affected device. The vulnerability is due to improper input sanitization. An attacker who has valid administrative access to an affected device could exploit this vulnerability by supplying a crafted input parameter on a form in the web UI and then submitting that form. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the device, which could lead to complete system compromise.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3211</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the Virtual Services Container of Cisco IOS XE Software could allow an authenticated, local attacker to gain root-level privileges on an affected device. The vulnerability is due to insufficient validation of a user-supplied open virtual appliance (OVA). An attacker could exploit this vulnerability by installing a malicious OVA on an affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3215</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the ROMMON of Cisco IOS XE Software could allow an authenticated, local attacker to elevate privileges to those of the root user of the underlying operating system. The vulnerability is due to the ROMMON allowing for special parameters to be passed to the device at initial boot up. An attacker could exploit this vulnerability by sending parameters to the device at initial boot up. An exploit could allow the attacker to elevate from a Priv15 user to the root user and execute arbitrary commands with the privileges of the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3213</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the authorization controls for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software could allow an unauthenticated, remote attacker to execute Cisco IOx API commands without proper authorization. The vulnerability is due to incorrect handling of requests for authorization tokens. An attacker could exploit this vulnerability by using a crafted API call to request such a token. An exploit could allow the attacker to obtain an authorization token and execute any of the IOx API commands on an affected device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3227</a> <a href="#">CISCO</a>

cisco -- ios_xe_software	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code with root privileges on the underlying Linux shell. The vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by first creating a malicious file on the affected device itself and then uploading a second malicious file to the device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or bypass licensing requirements on the device.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3218</a> <a href="#">CISCO</a>
cisco -- ios_xe_web_management	A vulnerability in Role Based Access Control (RBAC) functionality of Cisco IOS XE Web Management Software could allow a Read-Only authenticated, remote attacker to execute commands or configuration changes as an Admin user. The vulnerability is due to incorrect handling of RBAC for the administration GUI. An attacker could exploit this vulnerability by sending a modified HTTP request to the affected device. An exploit could allow the attacker as a Read-Only user to execute CLI commands or configuration changes as if they were an Admin user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3229</a> <a href="#">CISCO</a>
cisco -- iox_application	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, remote attacker to write or modify arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient input validation of user-supplied application packages. An attacker who can upload a malicious package within Cisco IOx could exploit the vulnerability to modify arbitrary files. The impacts of a successful exploit are limited to the scope of the virtual instance and do not affect the device that is hosting Cisco IOx.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3238</a> <a href="#">CISCO</a>
cisco -- iox_application	A vulnerability in the Cisco Application Framework component of the Cisco IOx application environment could allow an authenticated, local attacker to overwrite arbitrary files in the virtual instance that is running on the affected device. The vulnerability is due to insufficient path	2020-06-03	not yet calculated	<a href="#">CVE-2020-3237</a> <a href="#">CISCO</a>

	restriction enforcement. An attacker could exploit this vulnerability by including a crafted file in an application package. An exploit could allow the attacker to overwrite files.			
cisco -- iox_application_framework	A vulnerability in the web-based Local Manager interface of the Cisco IOx Application Framework could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based Local Manager interface of an affected device. The attacker must have valid Local Manager credentials. The vulnerability is due to insufficient validation of user-supplied input by the web-based Local Manager interface of the affected software. An attacker could exploit this vulnerability by injecting malicious code into a system settings tab. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3233</a> <a href="#">CISCO</a>
cisco -- multiple_products	A vulnerability in the Topology Discovery Service of Cisco One Platform Kit (onePK) in Cisco IOS Software, Cisco IOS XE Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient length restrictions when the onePK Topology Discovery Service parses Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol message to an affected device. An exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges, or to cause a process crash, which could result in a reload of the device and cause a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3217</a> <a href="#">CISCO</a>
	A vulnerability in Security Group Tag Exchange Protocol (SXP) in Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause the affected device to reload,			

cisco -- multiple_products	resulting in a denial of service (DoS) condition. The vulnerability exists because crafted SXP packets are mishandled. An attacker could exploit this vulnerability by sending specifically crafted SXP packets to the affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3228</a> <a href="#">CISCO</a>
cisco -- multiple_routers	Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3199</a> <a href="#">CISCO</a>
cisco -- multiple_routers	A vulnerability in the virtual console authentication of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated but low-privileged, local attacker to log in to the Virtual Device Server (VDS) of an affected device by using a set of default credentials. The vulnerability is due to the presence of weak, hard-coded credentials. An attacker could exploit this vulnerability by authenticating to the targeted device and then connecting to VDS through the device's virtual console by using the static credentials. A successful exploit could allow the attacker to access the Linux shell of VDS as the root user.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3234</a> <a href="#">CISCO</a>
cisco -- multiple_routers	A vulnerability in the CLI parsers of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an authenticated, local attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The attacker must have valid user credentials at privilege level 15. The vulnerability is due to insufficient validation of arguments that are passed to specific VDS-related CLI	2020-06-03	not yet calculated	<a href="#">CVE-2020-3210</a> <a href="#">CISCO</a>

	<p>commands. An attacker could exploit this vulnerability by authenticating to the targeted device and including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user.</p>			
cisco -- multiple_routers	<p>Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3198</a> <a href="#">CISCO</a>
cisco -- multiple_routers	<p>A vulnerability in the implementation of the inter-VM channel of Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, adjacent attacker to execute arbitrary shell commands on the Virtual Device Server (VDS) of an affected device. The vulnerability is due to insufficient validation of signaling packets that are destined to VDS. An attacker could exploit this vulnerability by sending malicious packets to an affected device. A successful exploit could allow the attacker to execute arbitrary commands in the context of the Linux shell of VDS with the privileges of the root user. Because the device is designed on a hypervisor architecture, exploitation of a vulnerability that affects the inter-VM channel may lead to a complete system compromise. For more information about this vulnerability, see the Details section of this advisory.</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3205</a> <a href="#">CISCO</a>
cisco -- multiple_routers	<p>Multiple vulnerabilities in the Cisco IOx application environment of Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) that are running Cisco IOS Software could allow an attacker to cause</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-3257</a> <a href="#">CISCO</a>



	a denial of service (DoS) condition or execute arbitrary code with elevated privileges on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.			
cisco -- multiple_routers	Multiple vulnerabilities in Cisco IOS Software for Cisco 809 and 829 Industrial Integrated Services Routers (Industrial ISRs) and Cisco 1000 Series Connected Grid Routers (CGR1000) could allow an unauthenticated, remote attacker or an authenticated, local attacker to execute arbitrary code on an affected system or cause an affected system to crash and reload. For more information about these vulnerabilities, see the Details section of this advisory.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3258</a> <a href="#">CISCO</a>
cisco -- unified_contact_center_express	A vulnerability in the API subsystem of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to change the availability state of any agent. The vulnerability is due to insufficient authorization enforcement on an affected system. An attacker could exploit this vulnerability by authenticating to an affected system with valid agent credentials and performing a specific API call with crafted input. A successful exploit could allow the attacker to change the availability state of an agent, potentially causing a denial of service condition.	2020-06-03	not yet calculated	<a href="#">CVE-2020-3267</a> <a href="#">CISCO</a>
cisco -- webex_network_recording_player_and_webex_player_for_microsoft_windows	A vulnerability in Cisco Webex Network Recording Player and Cisco Webex Player for Microsoft Windows could allow an attacker to cause a process crash resulting in a Denial of service (DoS) condition for the player application on an affected system. The vulnerability exists due to insufficient validation of certain elements with a Webex recording stored in either the Advanced Recording Format (ARF) or the Webex Recording Format (WRF). An attacker could exploit this vulnerability by sending a user a malicious ARF or WRF file through a link or email attachment and persuading the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to cause the Webex player application to crash when trying to view the malicious	2020-06-03	not yet calculated	<a href="#">CVE-2020-3319</a> <a href="#">CISCO</a>

	file. This vulnerability affects Cisco Webex Network Recording Player and Webex Player releases earlier than Release 3.0 MR3 Security Patch 2 and 4.0 MR3.			
combodo -- itop	In Combodo iTop, dashboard ids can be exploited with a reflective XSS payload. This is fixed in all iTop packages (community, essential, professional) for version 2.7.0 and in iTop essential and iTop professional packages for version 2.6.4.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11697</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
combodo -- itop	In Combodo iTop a menu shortcut name can be exploited with a stored XSS payload. This is fixed in all iTop packages (community, essential, professional) in version 2.7.0 and iTop essential and iTop professional in version 2.6.4.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11696</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.6 for Craft CMS. There is stored XSS via a guest name.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13869</a> <a href="#">MISC</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. There is stored XSS via an asset volume name.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13870</a> <a href="#">MISC</a>
craft -- craft_cms	An issue was discovered in the Comments plugin before 1.5.5 for Craft CMS. CSRF affects comment integrity.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13868</a> <a href="#">MISC</a>
docker -- desktop	An issue was discovered in Docker Desktop through 2.2.0.5 on Windows. If a local attacker sets up their own named pipe prior to starting Docker with the same name, this attacker can intercept a connection attempt from Docker Service (which runs as SYSTEM), and then impersonate their privileges.	2020-06-05	not yet calculated	<a href="#">CVE-2020-11492</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- elasticsearch	The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to 7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an authentication token being generated with elevated privileges.	2020-06-03	not yet calculated	<a href="#">CVE-2020-7014</a> <a href="#">N/A</a>
elliptic -- elliptic	The Elliptic package 6.5.2 for Node.js allows ECDSA signature malleability via variations in encoding, leading '' bytes, or	2020-06-	not yet	<a href="#">CVE-2020-13822</a> <a href="#">MISC</a>

	integer overflows. This could conceivably have a security-relevant impact if an application relied on a single canonical signature.	04	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fortiguard -- forticlient_for_windows	Use of a hard-coded cryptographic key to encrypt security sensitive data in local storage and configuration in FortiClient for Windows prior to 6.4.0 may allow an attacker with access to the local storage or the configuration backup file to decrypt the sensitive data via knowledge of the hard-coded key.	2020-06-04	not yet calculated	<a href="#">CVE-2019-16150</a> <a href="#">MISC</a>
fortiguard -- fortisiem_windows_agent	An unquoted service path vulnerability in the FortiSIEM Windows Agent component may allow an attacker to gain elevated privileges via the AoWinAgt executable service path.	2020-06-04	not yet calculated	<a href="#">CVE-2020-9292</a> <a href="#">MISC</a>
foxit -- e-mail_advertising_system	An issue was discovered in Foxit E-mail advertising system before September 2018. It allows authentication bypass and information disclosure, related to Interspire Email Marketer.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21235</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has an out-of-bounds write when Internet Explorer is used.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20825</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has homograph mishandling.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20832</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows NTLM credential theft via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21237</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It allows Remote Code Execution via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21242</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a NULL pointer dereference via FXSYS_wcslen in an Epub file.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20824</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has an untrusted search path that allows a DLL to execute remote code.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21241</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It allows arbitrary application execution via an embedded executable file in a PDF portfolio, aka FG-VD-18-029.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21244</a> <a href="#">CONFIRM</a>
	An issue was discovered in Foxit			

foxit -- phantompdf	PhantomPDF before 8.3.10. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20834 CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.11. It has a buffer overflow because a looping correction does not occur after JavaScript updates Field APs.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20823 CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.6. It has COM object mishandling when Microsoft Word is used.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21243 CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.7. It allows memory consumption via an <code>ArrayBuffer(0xffffffff)</code> call.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21238 CONFIRM</a>
foxit -- phantompdf	An issue was discovered in Foxit PhantomPDF before 8.3.10. It has mishandling of cloud credentials, as demonstrated by Google Drive.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20833 CONFIRM</a>
foxit -- phantompdf_mac	An issue was discovered in Foxit PhantomPDF Mac before 3.4. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20821 CONFIRM</a>
foxit -- phantompdf_mac	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20826 CONFIRM</a>
foxit -- phantompdf_mac_and_reader_for_mac	An issue was discovered in Foxit PhantomPDF Mac 3.3 and Foxit Reader for Mac before 3.3. It allows stack consumption because of interaction between ICC-Based color space and Alternate color space.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20827 CONFIRM</a>
foxit -- reader	An issue was discovered in Foxit Reader before 2.4.4. It has a NULL pointer dereference.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21236 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.7.0.29430. It has an out-of-bounds write via incorrect image data.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20822 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.2. It allows NTLM credential theft via a GoToE or GoToR action.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21239 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.2. It allows memory consumption via an <code>ArrayBuffer(0xffffffff)</code> call.	2020-06-04	not yet calculated	<a href="#">CVE-2018-21240 CONFIRM</a>
foxit --	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It has a	2020-06-	not yet	<a href="#">CVE-2020-</a>

reader_and_phantompdf	use-after-free via a document that lacks a dictionary.	04	calculated	<a href="#">13814 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.2. It allows signature validation bypass via a modified file or a file with non-standard signatures.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13810 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.7.1. It allows stack consumption via a loop of an indirect object reference.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13815 CONFIRM</a>
foxit -- reader_and_phantompdf	An issue was discovered in the 3D Plugin Beta for Foxit Reader and PhantomPDF before 9.5.0.20733. It has void data mishandling, causing a crash.	2020-06-04	not yet calculated	<a href="#">CVE-2019-20831 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13812 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It allows local users to gain privileges via a crafted DLL in the current working directory when FoxitStudioPhoto366_3.6.6.916.exe is used.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13813 CONFIRM</a>
foxit -- studio_photo	An issue was discovered in Foxit Studio Photo before 3.6.6.922. It has an out-of-bounds write via a crafted TIFF file.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13811 CONFIRM</a>
ge -- multiple_grid_solutions-reason_rt_clocks	GE Grid Solutions Reason RT Clocks, RT430, RT431, and RT434, all firmware versions prior to 08A05. The device's vulnerability in the web application could allow multiple unauthenticated attacks that could cause serious impact. The vulnerability may allow an unauthenticated attacker to execute arbitrary commands and send a request to a specific URL that could cause the device to become unresponsive. The unauthenticated attacker may change the password of the 'configuration' user account, allowing the attacker to modify the configuration of the device via the web interface using the new password. This vulnerability may also allow an unauthenticated attacker to bypass the authentication required to configure the device and reboot the system.	2020-06-02	not yet calculated	<a href="#">CVE-2020-12017 MISC</a>
	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in			<a href="#">CVE-2020-</a>



gnutls -- gnutls	TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application.	2020-06-04	not yet calculated	<a href="#">13777</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">DEBIAN</a>
google -- chrome	Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-06-03	not yet calculated	<a href="#">CVE-2020-6503</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- multiple_products	Huawei products NIP6800;Secospace USG6600;USG9500 have a memory leak vulnerability. An attacker with high privileges exploits this vulnerability by continuously performing specific operations. Successful exploitation of this vulnerability can cause service abnormal.	2020-06-05	not yet calculated	<a href="#">CVE-2020-1883</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	Huawei Smartphones HONOR 20 PRO;Honor View 20;HONOR 20 have an improper handling of exceptional condition Vulnerability. A component cannot deal with an exception correctly. Attackers can exploit this vulnerability by sending malformed message. This could compromise normal service of affected phones.	2020-06-05	not yet calculated	<a href="#">CVE-2020-9074</a> <a href="#">MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181230.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4449</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181231.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4450</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- websphere_application_server_network_deployment	IBM WebSphere Application Server Network Deployment 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 181228.	2020-06-05	not yet calculated	<a href="#">CVE-2020-4448</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- worklight/mobilefoundation	IBM Worklight/MobileFoundation 8.0.0.0 does not properly invalidate session cookies when a user logs out of a session, which could allow another user	2020-06-05	not yet calculated	<a href="#">CVE-2020-4229</a> <a href="#">XF</a>

	to gain unauthorized access to a user's session. IBM X-Force ID: 175211.			<a href="#">CONFIRM</a>
kubernetes -- kube-controller-manager	The Kubernetes kube-controller-manager in versions v1.0-1.14, versions prior to v1.15.12, v1.16.9, v1.17.5, and version v1.18.0 are vulnerable to a Server Side Request Forgery (SSRF) that allows certain authorized users to leak up to 500 bytes of arbitrary information from unprotected endpoints within the master's host network (such as link-local or loopback services).	2020-06-05	not yet calculated	<a href="#">CVE-2020-8555</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9 and 10 (MTK chipsets). An AT command handler allows attackers to bypass intended access restrictions. The LG ID is LVE-SMP-200009 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13841</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS software before 2020-06-01. Local users can cause a denial of service because checking of the userdata partition is mishandled. The LG ID is LVE-SMP-200014 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13843</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via a custom AT command handler buffer overflow. The LG ID is LVE-SMP-200007 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13839</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). A dangerous AT command was made available even though it is unused. The LG ID is LVE-SMP-200010 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13842</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 (MTK chipsets). Code execution can occur via an MTK AT command handler buffer overflow. The LG ID is LVE-SMP-200008 (June 2020).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13840</a> <a href="#">CONFIRM</a>
minishare -- minishare	In MiniShare before 1.4.2, there is a stack-based buffer overflow via an HTTP PUT request, which allows an attacker to achieve arbitrary code execution, a similar issue to CVE-2018-19861, CVE-2018-19862, and CVE-2019-17601. NOTE: this product is discontinued.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13768</a> <a href="#">MISC</a>
	The MQTT protocol 3.1.1 requires a server to set a timeout value of 1.5 times			<a href="#">CVE-2020-</a>

mqtt -- mqtt	the Keep-Alive value specified by a client, which allows remote attackers to cause a denial of service (loss of the ability to establish new connections), as demonstrated by SlowITe.	2020-06-04	not yet calculated	<a href="#">13849</a> <a href="#">MISC</a> <a href="#">MISC</a>
neon -- neon	The Neon theme 2.0 before 2020-06-03 for Bootstrap allows XSS via an Add Task Input operation in a dashboard.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13890</a> <a href="#">MISC</a>
network_time_foundation -- network_time_protocol	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13817</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	In nghttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. nghttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement nghttp2_on_frame_recv_callback callback, and if received frame is SETTINGS frame and the number of settings entries are large (e.g., > 32), then drop the connection.	2020-06-03	not yet calculated	<a href="#">CVE-2020-11080</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
nozbe -- watermelondb	In WatermelonDB (NPM package "@nozbe/watermelondb") before versions 0.15.1 and 0.16.2, a maliciously crafted record ID can exploit a SQL Injection vulnerability in iOS adapter implementation and cause the app to delete all or selected records from the database, generally causing the app to become unusable. This may happen in apps that don't validate IDs (valid IDs are <code> /^[a-zA-Z0-9_-.]+\$/ </code> ) and use <code>Watermelon Sync</code> or low-level <code> `database.adapter.destroyDeletedRecords` </code> method. The integrity risk is low due to the fact that maliciously deleted records won't synchronize, so logout-login will restore all data, although some local changes may be lost if the malicious deletion causes the sync process to fail to	2020-06-03	not yet calculated	<a href="#">CVE-2020-4035</a> <a href="#">MISC</a>

	<p>proceed to push stage. No way to breach confidentiality with this vulnerability is known. Full exploitation of SQL Injection is mitigated, because it's not possible to nest an insert/update query inside a delete query in SQLite, and it's not possible to pass a semicolon-separated second query. There's also no known practicable way to breach confidentiality by selectively deleting records, because those records will not be synchronized. It's theoretically possible that selective record deletion could cause an app to behave insecurely if lack of a record is used to make security decisions by the app. This is patched in versions 0.15.1, 0.16.2, and 0.16.1-fix</p>			<a href="#">CONFIRM</a>
october -- october_cms	<p>In OctoberCMS (october/october composer package) versions from 1.0.319 and before 1.0.466, any users with the ability to modify any data that could eventually be exported as a CSV file from the `ImportExportController` could potentially introduce a CSV injection into the data to cause the generated CSV export file to be malicious. This requires attackers to achieve the following before a successful attack can be completed: 1. Have found a vulnerability in the victims spreadsheet software of choice. 2. Control data that would potentially be exported through the `ImportExportController` by a theoretical victim. 3. Convince the victim to export above data as a CSV and run it in vulnerable spreadsheet software while also bypassing any sanity checks by said software. Issue has been patched in Build 466 (v1.0.466).</p>	2020-06-03	not yet calculated	<a href="#">CVE-2020-5299</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
october -- october_cms	<p>The October CMS debugbar plugin before version 3.1.0 contains a feature where it will log all requests (and all information pertaining to each request including session data) whenever it is enabled. This presents a problem if the plugin is ever enabled on a system that is open to untrusted users as the potential exists for them to use this feature to view all requests being made to the application and obtain sensitive information from those requests. There even exists the potential for account takeovers of authenticated users by non-authenticated</p>	2020-06-	not yet	<a href="#">CVE-2020-11094</a>

	public users, which would then lead to a number of other potential issues as an attacker could theoretically get full access to the system if the required conditions existed. Issue has been patched in v3.1.0 by locking down access to the debugbar to all users; it now requires an authenticated backend user with a specifically enabled permission before it is even usable, and the feature that allows access to stored request information is restricted behind a different permission that's more restrictive.	04	calculated	<a href="#">MISC</a> <a href="#">CONFIRM</a>
open-iscsi -- targetcli-fb	Open-iSCSI targetcli-fb through 2.1.52 has weak permissions for /etc/target (and for the backup directory and backup files).	2020-06-05	not yet calculated	<a href="#">CVE-2020-13867</a> <a href="#">MISC</a>
pam_tacplus -- pam_tacplus	In support.c in pam_tacplus 1.3.8 through 1.5.1, the TACACS+ shared secret gets logged via syslog if the DEBUG loglevel and journald are used.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13881</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12723</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10878</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
perl -- perl	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10543</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
postgresql -- jdbc_driver	PostgreSQL JDBC Driver (aka PgJDBC) before 42.2.13 allows XXE.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13692</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
pupnp -- pupnp	Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and FindServiceEventURLPath in genlib/service_table/service_table.c.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13848</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Pydio Cells 2.0.4 allows XSS. A malicious			



pydio -- cells	user can either upload or create a new file that contains potentially malicious HTML and JavaScript code to personal folders or accessible cells.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12853</a> <a href="#">MISC</a>
pydio -- cells	Pydio Cells 2.0.4 allows an authenticated user to write or overwrite existing files in another user's personal and cells folders (repositories) by uploading a custom generated ZIP file and leveraging the file extraction feature present in the web application. The extracted files will be placed in the targeted user folders.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12851</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	The update feature for Pydio Cells 2.0.4 allows an administrator user to set a custom update URL and the public RSA key used to validate the downloaded update package. The update process involves downloading the updated binary file from a URL indicated in the update server response, validating its checksum and signature with the provided public key and finally replacing the current application binary. To complete the update process, the application's service or appliance needs to be restarted. An attacker with administrator access can leverage the software update feature to force the application to download a custom binary that will replace current Pydio Cells binary. When the server or service is eventually restarted the attacker will be able to execute code under the privileges of the user running the application. In the Pydio Cells enterprise appliance this is with the privileges of the user named "pydio".	2020-06-04	not yet calculated	<a href="#">CVE-2020-12852</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	In Pydio Cells 2.0.4, once an authenticated user shares a file selecting the create a public link option, a hidden shared user account is created in the backend with a random username. An anonymous user that obtains a valid public link can get the associated hidden account username and password and proceed to login to the web application. Once logged into the web application with the hidden user account, some actions that were not available with the public share link can now be performed.	2020-06-05	not yet calculated	<a href="#">CVE-2020-12848</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	Pydio Cells 2.0.4 allows any user to upload a profile image to the web application, including standard and shared user roles. These profile pictures	2020-06-	not yet	<a href="#">CVE-2020-12849</a>

	can later be accessed directly with the generated URL by any unauthenticated or authenticated user.	05	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
pydio -- cells	Pydio Cells 2.0.4 web application offers an administrative console named “Cells Console” that is available to users with an administrator role. This console provides an administrator user with the possibility of changing several settings, including the application’s mailer configuration. It is possible to configure a few engines to be used by the mailer application to send emails. If the user selects the “sendmail” option as the default one, the web application offers to edit the full path where the sendmail binary is hosted. Since there is no restriction in place while editing this value, an attacker authenticated as an administrator user could force the web application into executing any arbitrary binary.	2020-06-04	not yet calculated	<a href="#">CVE-2020-12847</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	A flaw was found in QEMU in the implementation of the Pointer Authentication (PAuth) support for ARM introduced in version 4.0 and fixed in version 5.0.0. A general failure of the signature generation process caused every PAuth-enforced pointer to be signed with the same signature. A local attacker could obtain the signature of a protected pointer and abuse this flaw to bypass PAuth protection for all programs running on QEMU.	2020-06-04	not yet calculated	<a href="#">CVE-2020-10702</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
qemu -- qemu	ati-vga in hw/display/ati.c in QEMU 4.2.0 allows guest OS users to trigger infinite recursion via a crafted mm_index value during an ati_mm_read or ati_mm_write call.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13800</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
qemu -- qemu	rom_copy() in hw/core/loader.c in QEMU 4.1.0 does not validate the relationship between two addresses, which allows attackers to trigger an invalid memory copy operation.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13765</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
qemu -- qemu	hw/pci/pci.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access by providing an address near the end of the PCI configuration space.	2020-06-04	not yet calculated	<a href="#">CVE-2020-13791</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sqlite -- sqlite	SQLite 3.32.2 has a use-after-free in resetAccumulator in select.c because the parse tree rewrite for window functions is too late.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13871</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

swift_networks -- red_cheetah	In the cheetah free wifi 5.1 driver file liebaonat.sys, local users are allowed to cause a denial of service (BSOD) or other unknown impact due to failure to verify the value of a specific IOCTL.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13646</a> <a href="#">MISC</a>
tigera -- calico_and_calico_enterprise	Clusters using Calico (version 3.14.0 and below), Calico Enterprise (version 2.8.2 and below), may be vulnerable to information disclosure if IPv6 is enabled but unused. A compromised pod with sufficient privilege is able to reconfigure the node's IPv6 interface due to the node accepting route advertisement by default, allowing the attacker to redirect full or partial network traffic from the node to the compromised pod.	2020-06-03	not yet calculated	<a href="#">CVE-2020-13597</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
url-regex -- url-regex	all versions of url-regex are vulnerable to Regular Expression Denial of Service. An attacker providing a very long string in String.test can cause a Denial of Service.	2020-06-04	not yet calculated	<a href="#">CVE-2020-7661</a> <a href="#">MISC</a> <a href="#">MISC</a>
weaveworks -- weave_net	In Weave Net before version 2.6.3, an attacker able to run a process as root in a container is able to respond to DNS requests from the host and thereby insert themselves as a fake service. In a cluster with an IPv4 internal network, if IPv6 is not totally disabled on the host (via ipv6.disable=1 on the kernel cmdline), it will be either unconfigured or configured on some interfaces, but it's pretty likely that ipv6 forwarding is disabled, ie /proc/sys/net/ipv6/conf//forwarding == 0. Also by default, /proc/sys/net/ipv6/conf//accept_ra == 1. The combination of these 2 sysctls means that the host accepts router advertisements and configure the IPv6 stack using them. By sending rogue router advertisements, an attacker can reconfigure the host to redirect part or all of the IPv6 traffic of the host to the attacker controlled container. Even if there was no IPv6 traffic before, if the DNS returns A (IPv4) and AAAA (IPv6) records, many HTTP libraries will try to connect via IPv6 first then fallback to IPv4, giving an opportunity to the attacker to respond. If by chance you also have on the host a vulnerability like last year's RCE in apt (CVE-2019-3462), you can now escalate to the host. Weave Net version 2.6.3 disables the accept_ra option on the veth devices that it creates.	2020-06-03	not yet calculated	<a href="#">CVE-2020-11091</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

wordpress -- wordpress	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from a stored XSS vulnerability. An author user can create posts that result in a stored XSS by using a crafted payload in custom links.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13864</a> <a href="#">MISC</a>
wordpress -- wordpress	The Elementor Page Builder plugin before 2.9.9 for WordPress suffers from multiple stored XSS vulnerabilities. An author user can create posts that result in stored XSS vulnerabilities, by using a crafted link in the custom URL or by applying custom attributes.	2020-06-05	not yet calculated	<a href="#">CVE-2020-13865</a> <a href="#">MISC</a>
wso2 -- multiple_products	In WSO2 API Manager 3.0.0 and earlier, WSO2 API Microgateway 2.2.0, and WSO2 IS as Key Manager 5.9.0 and earlier, Management Console allows XXE during addition or update of a Lifecycle.	2020-06-06	not yet calculated	<a href="#">CVE-2020-13883</a> <a href="#">MISC</a>
xack -- dns	XACK DNS 1.11.0 to 1.11.4, 1.10.0 to 1.10.8, 1.8.0 to 1.8.23, 1.7.0 to 1.7.18, and versions before 1.7.0 allow remote attackers to cause a denial of service condition resulting in degradation of the recursive resolver's performance or compromising the recursive resolver as a reflector in a reflection attack.	2020-06-05	not yet calculated	<a href="#">CVE-2020-5591</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	A remote adversary with the ability to send arbitrary CoAP packets to be parsed by Zephyr is able to cause a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10063</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	An off-by-one error in the Zephyr project MQTT packet length decoder can result in memory corruption and possible remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	The Zephyr MQTT parsing code performs insufficient checking of the length field on publish messages, allowing a buffer overflow and potentially remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	In the Zephyr Project MQTT code, improper bounds checking can result in memory corruption and possibly remote code execution. NCC-ZEP-031 This issue affects: zephyrproject-rtos zephyr version	2020-06-05	not yet calculated	<a href="#">CVE-2020-10070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	2.2.0 and later versions.			<a href="#">MISC</a>
zephyrproject -- zephyr	Improper handling of the full-buffer case in the Zephyr Bluetooth implementation can result in memory corruption. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10061</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zephyrproject -- zephyr	In the Zephyr project Bluetooth subsystem, certain duplicate and back-to-back packets can cause incorrect behavior, resulting in a denial of service. This issue affects: zephyrproject-rtos zephyr version 2.2.0 and later versions, and version 1.14.0 and later versions.	2020-06-05	not yet calculated	<a href="#">CVE-2020-10068</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870





From: [Homeland Security News Wire](#)  
To: [info@hcn.sunnyvale.ca.us](mailto:info@hcn.sunnyvale.ca.us)  
Subject: Week in Review  
Date: Saturday, June 06, 2020 7:30:37 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)

?

?

## Week in Review

BIOMETRICS BORDER/IMMIG. BUSINESS CYBERSECURITY DETECTION DISASTERS GOVERNMENT INFRASTRUCTURE  
PUBLIC HEALTH PUBLIC SAFETY REGIONAL SCI-TECH SURVEILLANCE TERRORISM TRANSPORTATION WATER

Saturday 6 June 2020 vol. 3 no. 111

### Overlapping disasters

#### Heightened Risks When Pandemic and Hurricane Season Overlap

Researchers studying the ability of coastal communities to respond to disasters say that combined disasters may make community recovery vastly more difficult. What they have found serves as a stark warning to policymakers preparing for hurricane season during a pandemic. One of the main worries is that there will be significant delays in recovery efforts if front-line workers are not kept healthy.

[Read more](#)

#### COVID-19 Highlights the Need to Plan for Joint Disasters

By Renee Cho

June 1 is the official start of hurricane season in the U.S., and scientists are predicting a particularly active season, including more major hurricanes. We have also entered the time of year when floods, heat waves and wildfires occur more often. Over the longer term, climate change is causing more frequent extreme weather events. Rising temperatures also exacerbate the spread of disease and could make pandemics more difficult to control in the future. Considering that most risk studies in the past have been focused on single events, is the U.S. prepared to deal with the possibility of extreme weather events as well as a pandemic?

[Read more](#)

### Floyd protests

#### Sorting out Claims of Extremist Involvement in U.S. Protests is Challenging

By Masood Farivar

The series of nationwide protests the past nine days over the death of African American George Floyd while in the custody of Minneapolis police have drawn a hodgepodge of outside agitators. They range from anarchists to anti-fascists, radical environmentalists, white supremacists, anti-government militiamen and just straight-up opportunists. All have been seen in numbers small and large at mass gatherings across the country. But sorting out their precise involvement in the demonstrations — and the related violence, burning and looting — has presented a challenge to law enforcement officials and researchers.

[Read more](#)

### Extremism

#### Trump's "Antifa" Accusations Spark Debate in Germany, the Movement's Birthplace

By Mark Hallam

After Donald Trump claimed most protesters in the U.S. were "antifa," Germany's Social Democrats rushed to declare solidarity with the

movement. But which movement? And why did other politicians object? What the word means is simple enough in German. Antifa is short for *antifaschistisch*, or anti-Fascist. In the most literal sense, one might hope this label could apply to almost all modern German people and politicians. But does antifa refer to all those opposed to fascism, or does it refer only to black-clad anarchists and leftists staring down German police in the streets?

[Read more](#)

## **German, Swedish, Finnish Neo-Nazis Receive Military Training at Russian Camps**

Militant far-right extremists from Germany, Sweden, and Finland are receiving combat training in Russia. The training camps are run by the right-wing extremist Russian Imperial Movement (RIM), which, in April, was designated by the United States as a terrorist organization – the first white supremacist group to be so designated. Russia deployed the foreign nationals to Russian militias operating in eastern Ukraine. Sources in German intelligence said they were worried that when the Germans come home from their stint in Ukraine, they would add military know-how and experience to the rising tide of far-right terrorism in Germany.

[Read more](#)

## **Germany Gets Tougher on Soldiers Engaged in Extremist Activities**

The German government on Wednesday approved a change to the Military Law which would make it easier to dismiss career soldiers who engage in extremist activities. The proposed changes must be approved by the Bundestag. The move comes after a series of incidents in which career soldiers were found to belong to extremist cells and shadowy far-right organizations. In a series of raids in the past few months, the police found these cells to stash arms caches and develop detailed plans for attacking Muslim immigrants and law enforcement personnel.

[Read more](#)

**Truth decay**

## **Virality Project (US): Marketing Meets Misinformation**

Pseudoscience and government conspiracy theories swirl on social media, though most of them stay largely confined to niche communities. In the case of COVID-19, however, a combination of anger at what some see as overly restrictive government policies, conflicting information about treatments and disease spread, and anxiety about the future has many people searching for facts...and finding misinformation. This dynamic creates an opportunity for determined people and skilled marketers to fill the void - to create content and produce messages designed to be shared widely.

[Read more](#)

**Bioweapons**

## **The Future Bioweapons Threat: Lessons from the COVID-19 Pandemic**

By Yong-Bee Lim

Experts discussing the lessons of the coronavirus epidemic for preparations for a bioweapon attack, are worried that the failures to detect, mitigate, and respond to COVID-19 may make a future biological weapon attack more likely. These experts agree that the U.S. has a long way to go in addressing biological threats from natural and man-made sources. Further, the U.S. needs to adapt to new realities – a time where citizens' trust of government is significantly lower, where citizens actively protest experts and their recommendations, and where misinformation is one tap on a smartphone away.

[Read more](#)

**Surveillance**

## **IoT: Which Devices Are Spying on You?**

When hungry consumers want to know how many calories are in a bag of

chips, they can check the nutrition label on the bag. When those same consumers want to check the security and privacy practices of a new IoT device, they aren't able to find even the most basic facts. Not yet, at least.

[Read more](#)

#### Cybersecurity

### Thwarting DDoS Technique that Threatened Large-Scale Cyberattack

Researchers have developed a technique that could allow a relatively small number of computers to carry out DDoS (distributed denial of service) attacks on a massive scale, overwhelming targets with false requests for information until they were thrown offline. The attack exploits vulnerabilities in the Domain Name System or DNS. The researchers alerted a broad collection of companies responsible for the internet's infrastructure to their findings.

[Read more](#)

### Users Rarely Change Passwords after a Breach – or They Choose a Weaker Password

Have you been pwned? In other words, have any of your username / password combinations been stolen during any of the many data breaches in recent years? Chances are, they probably have, and it's also likely you didn't take the proper precaution of changing your password to a more secure one. That's not necessarily your fault.

[Read more](#)

#### Forensics

### Slime Scene: Unusual Forensic Investigation Technique Put to the Test

Could household slime become a tool to help solve crimes? This is the question researchers sought to answer in a recent study that tested a popular children's "slime" recipe as a technique to enhance the appearance of hard-to-see fingerprints in forensic investigations.

[Read more](#)

#### Critical infrastructure

### Cybercriminals Are Now Targeting Critical Electricity Infrastructure

By Henri van Soest

Amid the constant stream of news on the coronavirus pandemic, one event passed relatively unnoticed. On the afternoon of May 14, a company named Elexon was hacked. You probably haven't heard of it, but Elexon plays a key role in the UK's electricity market, and though the attack did not affect the electricity supply itself, as an academic who researches cybersecurity in the electricity system, I am worried. This near miss reveals just how vulnerable our critical infrastructure is to such attacks – especially during a pandemic.

[Read more](#)

#### Supply chains

### During Global Crises, Strategic Redundancy Can Prevent Collapse of Supply Chains

When the novel coronavirus began spreading during the early months of 2020, it put kinks in multinational production chains — first in China and then around the globe. But it didn't have to happen that way. Experts suggest companies use redundancy as a way to fortify their operations against unforeseeable events such as pandemics.

[Read more](#)

#### Earthquakes

### A Step Closer to Being Able to Forecast Earthquakes

Scientists identify specific conditions that cause tectonic plates to slowly creep underneath one another rather than generate potentially catastrophic earthquakes. This could potentially contribute to solving one of the greatest challenges that faces seismologists, which is to be able to forecast earthquakes with enough precision to save lives and reduce the economic damage that is caused.

[Read more](#)

[Search-and-rescue](#)

## **Search-and-Rescue Algorithm Identifies Hidden “Traps” in Ocean Waters**

When an object or person goes missing at sea, the complex, constantly changing conditions of the ocean can confound and delay critical search-and-rescue operations. Now researchers have developed a technique they hope will help first responders quickly zero in on regions of the sea where missing objects or people are likely to be.

[Read more](#)

[Argument](#)

## **Riots, White Supremacy and Accelerationism**

White supremacists are gleeful as police violence and the resulting rioting tear apart cities, Dan Byman writes. “Even if the unrest ends in the weeks to come, they may look back at the violence as a win for their side,” he writes. “Even if the violence declines, it may bolster an increasingly important white supremacist concept—’accelerationism.’”

[Read more](#)

[Perspective](#)

## **Invoking “Terrorism” Against Police Protestors**

President Trump on Sunday tweeted that the United States should designate Antifa, a movement of leftists radicals prone to violence, as a “terrorist” organization. Shirin Sinnar writes that leaving aside the fact that current law does not grant the president the authority to designate the movement a terrorist organization, the deeper issue is this: “The sad irony in all this is that, over the past two years, some on the left have vocally supported an expansion of domestic terrorism frameworks” – calls which neglected the many concerns that civil rights groups.

[Read more](#)

## **Department of Homeland Security Law Enforcement Agencies Require Expanded Oversight**

Hundreds of Department of Homeland Security officers have been called up to serve along with other federal law enforcement officers and the National Guard to provide security within the District of Columbia. The question is whether the deployed officers are adequately trained and prepared for the current tense environment. “Repurposing law enforcement officers to work in a tense civic moment is not as easy as it might sound,” Carrie Cordero writes. If they are not well prepared, “the consequences can range from the embarrassing to the dangerous.”

[Read more](#)

## **“Domestic Terrorist Actors” Could Exploit Floyd Protests, DHS Memo Warns**

The DHS intelligence unit has sent out a memo to law enforcement officials around the country warning of the mobilization of far-right domestic terrorists and violent extremists in the context of a national crisis. Betsy Woodruff Swan and Natasha Bertrand write that this is at least the fifth DHS has sent out to law enforcement officials in the last two months warning of the growing danger of far-right violent extremists.

[Read more](#)

[Our picks this week](#)

## **Doomsday Planners | Are Incels Terrorists? | Police as Paramilitaries, and more**

- [Here's What Deployed Federal Agencies Say They Are Doing During Protests](#)
- [DOJ Accelerates Federal Crackdown on Looting and Vandalism](#)
- [Lawmakers, Tech Companies Struggle to Curb Coronavirus Disinformation](#)
- [U.S. Considers Adding More Chinese Media Outlets to Foreign-Mission List](#) (

- Lawmakers Seek Answers From FBI, DHS on Protest Involvement
- How Police Became Paramilitaries
- Top DHS Official Says to Expect “Every Intelligence Service” to Target COVID-19 Research
- Chaos in Primary Elections Offers Troubling Signs for November
- Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks
- Rare NSA Advisory About Russia-Based Cyberattacks Unlikely to Stop Them
- Israel Believes Assad's Syria Is Restarting Its Chemical Weapons Programs
- Why a Vaccine May Not Be Enough to End the Pandemic
- Small Military Nuclear Reactors: In Need of Global Safeguards
- How to Protest Safely in the Age of Surveillance
- 'Nonlethal' Anti-Protest Weapons Can Cause Serious Harm
- 'Uncomfortable Mission': Pentagon Tries to Retreat from Trump's Call to 'Dominate' Protests
- Coronavirus Is the Day of Reckoning for the Anti-Vaccine Movement
- Incels Are Radicalized and Dangerous. But Are They Terrorists?
- Antifa's Complex Origins: 'Terrorism' or Anti-Fascism?
- George Floyd Protests: Misleading Footage and Conspiracy Theories Spread Online
- Iran Is Working Hard to Revive Anti-U.S. Operations in Latin America
- Police Officers Accused of Brutal Violence Often Have a History of Complaints by Citizens
- Is the Conflict in Libya a Preview of the Future of Warfare?
- The Governor's Office Says the NSA Isn't Involved in the Response to Minnesota's Protests. But Here's How It Could Be.
- Rod Rosenstein Is Working with NSO Group, the Israeli Firm Accused of Spying on Dissidents
- Coronavirus: Most Disruption for Universities Since World War II
- Cops on the Hot Seat as Protests Turn to Uncontrolled Looting
- It's Time to Listen to the Doomsday Planners
- Britain Pushing U.S. to Form 5G Club of Nations to Cut Out Huawei
- Battered Caribbean Prepares for Hurricanes amid Pandemic
- NSA Exposes Software Flaw Used by Russian Hacking Groups
- Germany Wants E.U. to Sanction Head of Russian Military Intelligence
- Case files Discredit Gov. Brian Kemp's Accusation that Democrats Tried to Hack Georgia Election
- The DHS Is Working to Access 300 Million More Facial Recognition Photos
- Fixing a Critical Vulnerability in Our Critical Infrastructure
- The DHS Inspector General Claimed to Have a Philosophy Ph.D. He Doesn't.
- The U.K. Government May Have to Give Up on Reforming Some Terrorists, Says Watchdog, As Attempts to Deradicalize Flounder
- Here's What Deployed Federal Agencies Say They Are Doing During Protests
- DOJ Accelerates Federal Crackdown on Looting and Vandalism
- Lawmakers, Tech Companies Struggle to Curb Coronavirus Disinformation
- U.S. Considers Adding More Chinese Media Outlets to Foreign-Mission List (
- Lawmakers Seek Answers From FBI, DHS on Protest Involvement
- How Police Became Paramilitaries
- Top DHS Official Says to Expect “Every Intelligence Service” to Target COVID-19 Research
- Chaos in Primary Elections Offers Troubling Signs for November
- Israel and Iran Just Showed Us the Future of Cyberwar with Their



Unusual Attacks

[Read more](#)

## Also noted this week

- Attack on NYPD officers being investigated as possible act of terrorism, source says
- The long journey to herd immunity
- Doctor who advised Homeland Security testifies against COVID-19 protocols in immigration detention
- Fewer Security Incidents Affected US Federal Government in 2019
- Facebook labels state-controlled media posts, will block ads
- EU espionage panic: Brussels on 'very high alert' over state-sponsored hacking attacks
- Hackers steal secrets from US nuclear missile contractor
- Has COVID-19 increased the threat of bioterrorism in Europe?
- Facebook shuts down far-right group planning to bring weapons to protests
- Lack of cyber talent remains a national security threat
- Hurricane Season Collides With Coronavirus, As Communities Plan For Dual Emergencies
- The Army Is Funding Research Into A Structural Cloak Of Invisibility To Protect Soldiers, Vehicles And More
- NSA's cyber wing looks to safeguard COVID research and expand outreach
- The Internet vs. Trump: Should Travelers Be Forced To Disclose Social Media History?
- Customs and Border Protection drone flew over Minneapolis to provide live video to law enforcement
- Trump vows to designate antifa a terrorist group. Here's why DOJ officials call that 'highly problematic'
- The Cyber Budget Shows What the U.S. Values—And It Isn't Defense
- DHS Has Made Significant Progress in Implementing Leading Practices, but Needs to Take Additional Actions
- State Department announces \$3M reward for info on senior ISIS leader
- Florida Prepares for Hurricane Season amid Pandemic

[Read more](#)

---

BIOMETRICS | BORDER/IMMIG. | BUSINESS | CYBERSECURITY | DETECTION | DISASTERS | GOVERNMENT | INFRASTRUCTURE  
PUBLIC HEALTH | PUBLIC SAFETY | REGIONAL | SCI-TECH | SURVEILLANCE | TERRORISM | TRANSPORTATION | WATER

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



Advertising & Marketing [advertise@newswirepubs.com](mailto:advertise@newswirepubs.com)

Editorial [editor@newswirepubs.com](mailto:editor@newswirepubs.com)

General [info@newswirepubs.com](mailto:info@newswirepubs.com)

2010-2011 © News Wire Publications, LLC News Wire Publications, LLC

220 Old Country Road | Suite 200 | Mineola | New York | 11501

[Permissions and Policies](#)

Homeland Security News Wire, 220 Old Country Road, Suite 200, Mineola, NY 11501

SafeUnsubscribe™ [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)

[Forward email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [hsnewswire@newswirepubs.com](mailto:hsnewswire@newswirepubs.com)

From: [Homeland Security News Wire](#)  
To: [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)  
Subject: Extremists & Violence | Thwarting DDoS Attacks | Underwater Rescue  
Date: Thursday, June 04, 2020 7:58 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



## DAILY REPORT

BIOMETRICS BORDER/IMMIG. BUSINESS CYBERSECURITY DETECTION DISASTERS GOVERNMENT INFRASTRUCTURE  
PUBLIC HEALTH PUBLIC SAFETY REGIONAL SCI-TECH SURVEILLANCE TERRORISM TRANSPORTATION WATER

Thursday 4 June 2020 vol. 14 no. 109

### Floyd protests

## Sorting out Claims of Extremist Involvement in U.S. Protests is Challenging

By Masood Farivar

The series of nationwide protests the past nine days over the death of African American George Floyd while in the custody of Minneapolis police have drawn a hodgepodge of outside agitators. They range from anarchists to anti-fascists, radical environmentalists, white supremacists, anti-government militiamen and just straight-up opportunists. All have been seen in numbers small and large at mass gatherings across the country. But sorting out their precise involvement in the demonstrations — and the related violence, burning and looting — has presented a challenge to law enforcement officials and researchers.

[Read more](#)

### Extremism

## Trump's "Antifa" Accusations Spark Debate in Germany, the Movement's Birthplace

By Mark Hallam

After Donald Trump claimed most protesters in the U.S. were "antifa," Germany's Social Democrats rushed to declare solidarity with the movement. But which movement? And why did other politicians object? What the word means is simple enough in German. Antifa is short for *antifaschistisch*, or anti-Fascist. In the most literal sense, one might hope this label could apply to almost all modern German people and politicians. But does antifa refer to all those opposed to fascism, or does it refer only to black-clad anarchists and leftists staring down German police in the streets?

[Read more](#)

## Germany Gets Tougher on Soldiers Engaged in Extremist Activities

The German government on Wednesday approved a change to the Military Law which would make it easier to dismiss career soldiers who engage in extremist activities. The proposed changes must be approved by the Bundestag. The move comes after a series of incidents in which career soldiers were found to belong to extremist cells and shadowy far-right organizations. In a series of raids in the past few months, the police found these cells to stash arms caches and develop detailed plans for attacking Muslim immigrants and law enforcement personnel.

[Read more](#)

### Policing

## Militarization Has Fostered a Policing Culture that Sets up Protesters as "The Enemy"

By Tom Nolan

The militarization of police departments has been a feature of U.S. domestic law enforcement since the 9/11 attacks. What is clear from the latest round of protest and response, is that despite efforts to promote de-escalation as a policy, police culture appears to be stuck in an “us vs. them” mentality.

[Read more](#)

#### Cybersecurity

### Thwarting DDoS Technique that Threatened Large-Scale Cyberattack

Researchers have developed a technique that could allow a relatively small number of computers to carry out DDoS (distributed denial of service) attacks on a massive scale, overwhelming targets with false requests for information until they were thrown offline. The attack exploits vulnerabilities in the Domain Name System or DNS. The researchers alerted a broad collection of companies responsible for the internet's infrastructure to their findings.

[Read more](#)

#### Overlapping disasters

### Heightened Risks When Pandemic and Hurricane Season Overlap

Researchers studying the ability of coastal communities to respond to disasters say that combined disasters may make community recovery vastly more difficult. What they have found serves as a stark warning to policymakers preparing for hurricane season during a pandemic. One of the main worries is that there will be significant delays in recovery efforts if front-line workers are not kept healthy.

[Read more](#)

#### Earthquakes

### A Step Closer to Being Able to Forecast Earthquakes

Scientists identify specific conditions that cause tectonic plates to slowly creep underneath one another rather than generate potentially catastrophic earthquakes. This could potentially contribute to solving one of the greatest challenges that faces seismologists, which is to be able to forecast earthquakes with enough precision to save lives and reduce the economic damage that is caused.

[Read more](#)

#### Search-and-rescue

### Search-and-Rescue Algorithm Identifies Hidden “Traps” in Ocean Waters

When an object or person goes missing at sea, the complex, constantly changing conditions of the ocean can confound and delay critical search-and-rescue operations. Now researchers have developed a technique they hope will help first responders quickly zero in on regions of the sea where missing objects or people are likely to be.

[Read more](#)

#### Our picks

### Syria Restarts Chem Weapons Program | Are Incels Terrorists? | Protesting Safely, and more

- Rare NSA Advisory About Russia-Based Cyberattacks Unlikely to Stop Them
- Israel Believes Assad's Syria Is Restarting Its Chemical Weapons Programs
- Why a Vaccine May Not Be Enough to End the Pandemic
- Small Military Nuclear Reactors: In Need of Global Safeguards
- How to Protest Safely in the Age of Surveillance
- 'Nonlethal' Anti-Protest Weapons Can Cause Serious Harm
- 'Uncomfortable Mission': Pentagon Tries to Retreat from Trump's Call to 'Dominate' Protests
- Coronavirus Is the Day of Reckoning for the Anti-Vaccine Movement
- Incels Are Radicalized and Dangerous. But Are They Terrorists?

- Antifa's Complex Origins: 'Terrorism' or Anti-Fascism?

[Read more](#)

## Also noted

- EU espionage panic: Brussels on 'very high alert' over state-sponsored hacking attacks
- Hackers steal secrets from US nuclear missile contractor
- Has COVID-19 increased the threat of bioterrorism in Europe?
- Facebook shuts down far-right group planning to bring weapons to protests
- Lack of cyber talent remains a national security threat

[Read more](#)

---

BIOMETRICS | BORDER/IMMIG. | BUSINESS | CYBERSECURITY | DETECTION | DISASTERS | GOVERNMENT | INFRASTRUCTURE  
PUBLIC HEALTH | PUBLIC SAFETY | REGIONAL | SCI-TECH | SURVEILLANCE | TERRORISM | TRANSPORTATION | WATER

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



Advertising & Marketing [advertise@newswirepubs.com](mailto:advertise@newswirepubs.com)

Editorial [editor@newswirepubs.com](mailto:editor@newswirepubs.com)

General [info@newswirepubs.com](mailto:info@newswirepubs.com)

2010-2011 © News Wire Publications, LLC News Wire Publications, LLC  
220 Old Country Road | Suite 200 | Mineola | New York | 11501

[Permissions and Policies](#)

Homeland Security News Wire, 220 Old Country Road, Suite 200, Mineola, NY 11501

SafeUnsubscribe™ [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)

[Forward email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [hsnewswire@newswirepubs.com](mailto:hsnewswire@newswirepubs.com)

**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of April 27, 2020  
**Date:** Monday, May 04, 2020 10:26:57 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of April 27, 2020](#)

05/04/2020 06:45 AM EDT

Original release date: May 4, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atrifex -- jbig2dec	jbig2_image_compose in jbig2_image.c in Artifex jbig2dec before 0.18 has a heap-based buffer overflow.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12268</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Overlayfs in the Linux kernel and shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points. On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patches change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount	2020-04-24	<a href="#">7.2</a>	<a href="#">CVE-2019-15794</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	underflow.			
f5 -- big-iq	In BIG-IQ 6.0.0-7.0.0, a remote access vulnerability has been discovered that may allow a remote user to execute shell commands on affected systems using HTTP requests to the BIG-IQ user interface.	2020-04-24	10	<a href="#">CVE-2020-5868</a> <a href="#">MISC</a>
google -- openthread	OpenThread before 2019-12-13 has a stack-based buffer overflow in MeshCoP::Commissioner::GeneratePskc.	2020-04-28	7.5	<a href="#">CVE-2019-20791</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- ar3200_products	Huawei AR3200 products with versions of V200R007C00SPC900, V200R007C00SPCa00, V200R007C00SPCb00, V200R007C00SPCc00, V200R009C00SPC500 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device.	2020-04-27	7.5	<a href="#">CVE-2020-9068</a> <a href="#">CONFIRM</a>
ivanti -- avalanche	Ivanti Avalanche 6.3 allows a SQL injection that is vaguely associated with the Apache HTTP Server, aka Bug 683250.	2020-04-28	7.5	<a href="#">CVE-2020-12442</a> <a href="#">MISC</a>
mozilla -- firefox	A malicious extension could have called <code>browser.identity.launchWebAuthFlow</code> , controlling the <code>redirect_uri</code> , and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. This vulnerability affects Firefox < 75.	2020-04-24	7.5	<a href="#">CVE-2020-6823</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 75.	2020-04-24	7.5	<a href="#">CVE-2020-6826</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects	2020-04-24	7.5	<a href="#">CVE-2020-6825</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.			
netgear -- wnr854t_devices	NETGEAR WNR854T devices before 1.5.2 are affected by command execution.	2020-04-29	<a href="#">8.3</a>	<a href="#">CVE-2017-18855</a> <a href="#">CONFIRM</a>
node-rules -- node-rules	node-rules including 3.0.0 and prior to 5.0.0 allows injection of arbitrary commands. The argument rules of function "fromJSON()" can be controlled by users without any sanitization.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-7609</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
pixlcore -- pixl-class	pixl-class prior to 1.0.3 allows execution of arbitrary commands. The members argument of the create function can be controlled by users without any sanitization.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-7640</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qt -- qt	setMarkdown in Qt before 5.14.2 has a use-after-free related to QTextMarkdownImporter::insertBlock.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12267</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
shareit -- shareit	SHAREit through 4.0.6.177 does not check the body length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation.	2020-04-27	<a href="#">7.8</a>	<a href="#">CVE-2019-14941</a> <a href="#">MISC</a> <a href="#">MISC</a>
shareit -- shareit	SHAREit through 4.0.6.177 does not check the full message length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation. This is different from CVE-2019-14941.	2020-04-27	<a href="#">7.8</a>	<a href="#">CVE-2019-15234</a> <a href="#">MISC</a> <a href="#">MISC</a>
sophos -- xg_firewall_devices	A SQL injection issue was found in SFOS 17.0, 17.1, 17.5, and 18.0 before 2020-04-25 on Sophos XG Firewall devices, as exploited in the wild in April 2020. This affected devices configured with either the administration (HTTPS) service or the User Portal exposed on the WAN zone. A successful attack may have caused remote code execution that exfiltrated usernames and hashed passwords for the local device admin(s), portal admins, and user accounts used for remote access (but not external Active Directory or LDAP passwords)	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12271</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abbs -- software_audio_media_player	ABBS Software Audio Media Player version 3.1 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	6.8	<a href="#">CVE-2019-5621</a> <a href="#">MISC</a>
admidio -- admidio	SQL Injection was discovered in Admidio before version 3.3.13. The main cookie parameter is concatenated into a SQL query without any input validation/sanitization, thus an attacker without logging in, can send a GET request with arbitrary SQL queries appended to the cookie parameter and execute SQL queries. The vulnerability impacts the confidentiality of the system. This has been patched in version 3.3.13.	2020-04-24	5	<a href="#">CVE-2020-11004</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
apache -- ats	Apache ATS 6.0.0 to 6.2.3, 7.0.0 to 7.1.9, and 8.0.0 to 8.0.6 is vulnerable to a HTTP/2 slow read attack.	2020-04-27	5	<a href="#">CVE-2020-9481</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
apache -- log4j	Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.	2020-04-27	4.3	<a href="#">CVE-2020-9488</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
apache -- ofbiz	Apache OFBiz 17.12.01 is vulnerable to Host header injection by accepting arbitrary host	2020-04-30	5	<a href="#">CVE-2019-12425</a> <a href="#">CONFIRM</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	2020-04-24	4.3	<a href="#">CVE-2020-12130</a> <a href="#">MISC</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	2020-04-24	4.3	<a href="#">CVE-2020-12129</a> <a href="#">MISC</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	2020-04-24	4.3	<a href="#">CVE-2020-12131</a> <a href="#">MISC</a>
avira -- antivirus	Avira Antivirus before 5.0.2003.1821 on Windows allows privilege escalation or a denial of service via abuse of a symlink.	2020-04-26	4.6	<a href="#">CVE-2020-12254</a> <a href="#">MISC</a>
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shiftfs_btrfs_ioctl_fd_replace() installs an fd referencing a file from the lower filesystem without taking an additional	2020-04-24	4.6	<a href="#">CVE-2019-15791</a> <a href="#">MISC</a> <a href="#">MISC</a>

	reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a refcount underflow.			<a href="#">MISC</a>
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shiftfs_btrfs_ioctl_fd_replace() calls fdget(oldfd), then without further checks passes the resulting file* into shiftfs_real_fdget(), which casts file->private_data, a void* that points to a filesystem-dependent type, to a "struct shiftfs_file_info *". As the private_data is not required to be a pointer, an attacker can use this to cause a denial of service or possibly execute arbitrary code.	2020-04-24	<a href="#">4.6</a>	<a href="#">CVE-2019-15792</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into init_user_ns, whereas they should have been translated into the s_user_ns for the lower filesystem. This resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts s_user_ns. A local attacker could use this to possibly bypass discretionary access control permissions.	2020-04-24	<a href="#">4.6</a>	<a href="#">CVE-2019-15793</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Improper authorization vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote authenticated attackers to alter the application's data via the applications 'E-mail' and 'Messages'.	2020-04-28	<a href="#">4</a>	<a href="#">CVE-2020-5566</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Improper input validation vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows a remote authenticated attacker to alter the application's data via the applications 'Workflow' and 'MultiReport'.	2020-04-28	<a href="#">4</a>	<a href="#">CVE-2020-5565</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Server-side request forgery (SSRF) vulnerability in Cybozu Garoon 4.6.0 to 4.6.3 allows a remote attacker with an administrative privilege to issue arbitrary HTTP requests to other web servers via V-CUBE Meeting function.	2020-04-28	<a href="#">4</a>	<a href="#">CVE-2020-5562</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Improper authentication vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in Application Menu.	2020-04-28	<a href="#">5</a>	<a href="#">CVE-2020-5567</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Improper authentication vulnerability in			<a href="#">CVE-2020-</a>

cybozu -- garoon	Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in the affected product via the API.	2020-04-28	<a href="#">5</a>	<a href="#">5563</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to inject arbitrary web script or HTML via the application 'E-mail'.	2020-04-28	<a href="#">4.3</a>	<a href="#">CVE-2020-5564</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.6.0 to 5.0.0 allows remote attackers to inject arbitrary web script or HTML via the applications 'Messages' and 'Bulletin Board'.	2020-04-28	<a href="#">4.3</a>	<a href="#">CVE-2020-5568</a> <a href="#">MISC</a> <a href="#">MISC</a>
dong_joo_cho -- file_transfer_ifamily	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the ./etc/ path.	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2020-12128</a> <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer.	2020-04-24	<a href="#">4.8</a>	<a href="#">CVE-2020-5870</a> <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit.	2020-04-24	<a href="#">6.4</a>	<a href="#">CVE-2020-5869</a> <a href="#">MISC</a>
gnu -- mailman	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12137</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12245</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	Grafana version < 6.7.3 is vulnerable for annotation popup XSS.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-12052</a> <a href="#">CONFIRM</a>
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 2	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1805</a> <a href="#">CONFIRM</a>



	out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1806.			
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 1 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1805 and CVE-2020-1806.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1804</a> <a href="#">CONFIRM</a>
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 3 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1805.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1806</a> <a href="#">CONFIRM</a>
huawei -- lion- al00c_devices	Huawei smartphone Lion-AL00C with versions earlier than 10.0.0.205(C00E202R7P2) have a denial of service vulnerability. An attacker crafted specially file to the affected device. Due to insufficient input validation of the value when executing the file, successful exploit may cause device abnormal.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-1880</a> <a href="#">CONFIRM</a>
huawei -- pcmanager	Huawei PCManager product with versions earlier than 10.0.5.53 have a local privilege escalation vulnerability. An authenticated, local attacker can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	2020-04-27	<a href="#">4.6</a>	<a href="#">CVE-2020-1845</a> <a href="#">CONFIRM</a>
ibm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 173310.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2019-4750</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
	IBM Cloud App Management 2019.3.0			

ibm -- cloud_app_management	and 2019.4.0 reveals a stack trace on certain API requests which can allow an attacker further information about the implementation of the offering. IBM X-Force ID: 173311.	2020-04-24	5	<a href="#">CVE-2019-4751</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 172519.	2020-04-27	4	<a href="#">CVE-2019-4729</a> <a href="#">XE</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- mq_appliance	IBM MQ and MQ Appliance 8.0, 9.1 LTS, and 9.1 CD could allow an authenticated user cause a denial of service due to a memory leak. IBM X-Force ID: 175840.	2020-04-24	4	<a href="#">CVE-2020-4267</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server_and_liberty	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 20.0.0.4 could allow a remote, authenticated attacker to obtain sensitive information, caused by improper parameter checking. This could be exploited to conduct spoofing attacks. IBM X-Force ID: 177841.	2020-04-28	4	<a href="#">CVE-2020-4329</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows session fixation via an alphanumeric value in a session cookie.	2020-04-29	6.4	<a href="#">CVE-2020-12467</a> <a href="#">MISC</a>
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows CSV injection via a phrase value within a language. This is related to phrases/add/ and languages/download/.	2020-04-29	6.8	<a href="#">CVE-2020-12468</a> <a href="#">MISC</a>
mailbeez -- mailbeez	Cross-site scripting (XSS) vulnerability in mailhive/cloudbeez/cloudloader.php and mailhive/cloudbeez/cloudloader_core.php in the MailBeez plugin for ZenCart before 3.9.22 allows remote attackers to inject arbitrary web script or HTML via the cloudloader_mode parameter.	2020-04-30	4.3	<a href="#">CVE-2020-6579</a> <a href="#">MISC</a>
mozilla -- firefox_esr	When following a link that opened an intent://-schemed URL, causing a custom tab to be opened, Firefox for Android could be tricked into displaying the incorrect URI.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	2020-04-24	4.3	<a href="#">CVE-2020-6827</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A malicious Android application could craft an Intent that would have been processed by Firefox for Android and potentially result in a file overwrite in the user's profile directory. One exploitation			

mozilla -- firefox_esr	vector for this would be to supply a user.js file providing arbitrary malicious preference values. Control of arbitrary preferences can lead to sufficient compromise such that it is generally equivalent to arbitrary code execution.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	2020-04-24	6.4	<a href="#">CVE-2020-6828</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	When reading from areas partially or fully outside the source resource with WebGL's <code>copyTexSubImage</code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	5	<a href="#">CVE-2020-6821</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	6.8	<a href="#">CVE-2020-6820</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	6.8	<a href="#">CVE-2020-6819</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code>GMPDecodeData</code> . It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	6.8	<a href="#">CVE-2020-6822</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgate -- pfsense	An XSS vulnerability resides in the hostname field of the diag_ping.php page in pfsense before 2.4.5 version. After passing inputs to the command and executing this command, the \$result variable is not sanitized before it is printed.	2020-04-29	4.3	<a href="#">CVE-2020-10797</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear --	Certain NETGEAR devices are affected by a stack-based buffer overflow by an	2020-04-		<a href="#">CVE-2017-</a>

multiple_devices	authenticated user. This affects R6100 before 1.0.1.20, R7800 before 1.0.2.40, and R9000 before 1.0.2.52.	24	<a href="#">5.2</a>	<a href="#">18698 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21213 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21194 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21193 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects EX3700 before 1.0.0.66, EX3800 before 1.0.0.66, EX6100 before 1.0.2.20, EX6120 before 1.0.0.34, EX6150 before 1.0.0.36, EX6200 before 1.0.3.84, and EX7000 before 1.0.0.60.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2017-18715 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, EX6100v2 before 1.0.1.50, EX6150v2 before 1.0.1.50, EX6200v2 before 1.0.1.44, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60,	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2018-21228 CONFIRM</a>

	R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.2.30, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18723</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1., JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98,	2020-04-24	<a href="#">4.8</a>	<a href="#">CVE-2018-21230</a> <a href="#">CONFIRM</a>



	WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.			
netgear -- multiple_devices	<p>Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1.78, JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.</p>	2020-04-24	4.8	<a href="#">CVE-2018-21231</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6400 before 1.0.0.60, D7000 before 1.0.1.50, D8500 before 1.0.3.29, EX6200 before 1.0.3.84, EX7000 before 1.0.0.60, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R9000 before 1.0.2.52, WNDR3400v3 before 1.0.1.16, WNR3500Lv2 before 1.2.0.46, and WNDR3700v5 before 1.1.0.48.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2017-18700</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D1500 before 1.0.0.25, D500 before 1.0.0.25, D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, EX6100v2 before 1.0.1.60, EX6150v2 before 1.0.1.60, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.16, JWNDR2010v5 before 1.1.0.46, PR2000 before 1.0.0.18, R6020 before 1.0.0.26, R6050 before 1.0.1.16, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6220 before 1.1.0.60, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3700v5 before 1.1.0.48, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.46, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2017-18703</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18727</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92,	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21189</a>

	WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21191</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18722</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21187</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18729</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18728</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18726</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18725</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18724</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21192</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R6400v2 before 1.0.2.34, R6700 before 1.0.1.30, R6900 before 1.0.1.30, R6900P before 1.0.0.62, R7000 before 1.0.9.12, R7000P before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2018-21227</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21173</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18721</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21216</a> <a href="#">CONFIRM</a>

	1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.			
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18718</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18717</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18716</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18730</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18705</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.28, EX2700 before 1.0.1.32, EX6200v2 before 1.0.1.56, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.52, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and	2020-04-28	<a href="#">6.5</a>	<a href="#">CVE-2018-21181</a> <a href="#">CONFIRM</a>



	WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">6.5</a>	<a href="#">CVE-2018-21177</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, and WNR2000v5 before 1.0.0.58.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18731</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX2700 before 1.0.1.28, R7800 before 1.0.2.40, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2018-21170</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21190</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.98.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21171</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21180</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21179</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21178</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21172</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.94.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21182</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, and R9000 before 1.0.2.52.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21221</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21217</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18720</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected			

netgear -- multiple_devices	by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.1.00.26, R6080 before 1.1.00.26; R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18719</a> <a href="#">CONFIRM</a>
netgear -- r6220_devices	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	2020-04-24	<a href="#">4.8</a>	<a href="#">CVE-2017-18702</a> <a href="#">CONFIRM</a>
netgear -- r6700_and_r6900_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2017-18701</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2017-18699</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.3.6.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21200</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2017-18697</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21099</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21098</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.46 are affected by incorrect configuration of security settings.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2018-21158</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21100</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020-04-24	<a href="#">4.6</a>	<a href="#">CVE-2017-18709</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2017-18707</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by CSRF. This affects R8300 before	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2017-18708</a>

	1.0.2.94 and R8500 before 1.0.2.94.			<a href="#">CONFIRM</a>
pegasystems -- pega_platform	Pega Platform before version 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability in the comment tags.	2020-04-29	<a href="#">6</a>	<a href="#">CVE-2020-8775</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
pegasystems -- pega_platform	The Richtext Editor in Pega Platform before 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability.	2020-04-29	<a href="#">6</a>	<a href="#">CVE-2020-8773</a> <a href="#">CONFIRM</a>
pegasystems -- pega_platform	Pega Platform before version 8.2.6 is affected by a Reflected Cross-Site Scripting vulnerability in the "ActionStringID" function.	2020-04-29	<a href="#">6.8</a>	<a href="#">CVE-2020-8774</a> <a href="#">CONFIRM</a>
red_hat -- openshift_container_platform	A flaw was found in openshift-ansible. OpenShift Container Platform (OCP) 3.11 is too permissive in the way it specified CORS allowed origins during installation. An attacker, able to man-in-the-middle the connection between the user's browser and the openshift console, could use this flaw to perform a phishing attack. The main threat from this vulnerability is data confidentiality.	2020-04-24	<a href="#">4</a>	<a href="#">CVE-2020-1741</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	An issue was discovered in Sonatype Nexus Repository Manager 2.x before 2.14.17 and 3.x before 3.22.1. Admin users can retrieve the LDAP server system username/password (as configured in nxrm) in cleartext.	2020-04-27	<a href="#">4</a>	<a href="#">CVE-2020-11415</a> <a href="#">CONFIRM</a>
teampass -- teampass	TeamPass 2.1.27.36 allows an unauthenticated attacker to retrieve files from the TeamPass web root. This may include backups or LDAP debug files.	2020-04-29	<a href="#">5</a>	<a href="#">CVE-2020-12478</a> <a href="#">MISC</a>
teampass -- teampass	TeamPass 2.1.27.36 allows any authenticated TeamPass user to trigger a PHP file include vulnerability via a crafted HTTP request with sources/users.queries.php newValue directory traversal.	2020-04-29	<a href="#">6.5</a>	<a href="#">CVE-2020-12479</a> <a href="#">MISC</a>
whoopsie_project -- whoopsie	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12135</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
windriver -- vxworks	The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference.	2020-04-27	<a href="#">5</a>	<a href="#">CVE-2020-10664</a> <a href="#">CONFIRM</a>
wordpress --	The Advanced Woo Search plugin version through 1.99 for Wordpress suffers from a sensitive information	2020-04-		<a href="#">CVE-2020-12070</a>

wordpress	disclosure vulnerability in every ajax search request via the sql field to includes/class-aws-search.php.	24	5	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
-----------	---	----	---	--

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bluezone_global -- bluezone	React Native Bluetooth Scan in Bluezone 1.0.0 uses six-character alphanumeric IDs, which might make it easier for remote attackers to interfere with COVID-19 contact tracing by using many IDs.	2020-04-27	<a href="#">3.3</a>	<a href="#">CVE-2020-12270</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
croogo -- croogo	Croogo before 3.0.7 allows XSS via the title to admin/menus/menus or admin/taxonomy/vocabularies.	2020-04-26	<a href="#">3.5</a>	<a href="#">CVE-2019-20789</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.188(C00E74R3P8) have an improper authorization vulnerability. The software does not properly restrict certain user's modification of certain configuration file, successful exploit could allow the attacker to bypass app lock after a series of operation in ADB mode.	2020-04-27	<a href="#">3.6</a>	<a href="#">CVE-2020-1807</a> <a href="#">CONFIRM</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly sensitive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160514.	2020-04-29	<a href="#">2.1</a>	<a href="#">CVE-2019-4286</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly sensitive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160631.	2020-04-29	<a href="#">2.1</a>	<a href="#">CVE-2019-4288</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
mozilla -- firefox	Initially, a user opens a Private Browsing Window and generates a password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new password - the generated passwords would have been identical, rather than	2020-04-24	<a href="#">1.9</a>	<a href="#">CVE-2020-6824</a> <a href="#">MISC</a> <a href="#">MISC</a>



	independent. This vulnerability affects Firefox < 75.			
netgear --multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R6900P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8500 before 1.0.2.106, R8300 before 1.0.2.106, and WNDR3400v3 before 1.0.1.16.	2020-04-24	3.3	<a href="#">CVE-2017-18704 CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	3.3	<a href="#">CVE-2017-18712 CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	3.3	<a href="#">CVE-2017-18713 CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R7500v2 before 1.0.3.20, R7800 before 1.0.2.38, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	3.3	<a href="#">CVE-2018-21229 CONFIRM</a>
netgear --r8300_and_r8500_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04-24	3.3	<a href="#">CVE-2017-18710 CONFIRM</a>
netgear --srr60_and_srs60_devices	Certain NETGEAR devices are affected by stored XSS. This affects SRR60 before 2.2.1.210 and SRS60 before 2.2.1.210.	2020-04-27	2.3	<a href="#">CVE-2018-21095 CONFIRM</a>
netgear --wndr4500_devices	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	2020-04-24	3.3	<a href="#">CVE-2017-18714 CONFIRM</a>

ni_consulting -- sales_force_assistant	Cross-site scripting vulnerability in Sales Force Assistant version 11.2.48 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-04-28	3.5	<a href="#">CVE-2020-5570</a> <a href="#">JVN</a> <a href="#">MISC</a> <a href="#">MISC</a>
---	---	------------	-----	--

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a-pdf_wav -- a-pdf_wav	A-PDF WAV to MP3 version 1.0.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5618</a> <a href="#">MISC</a>
aasync -- aasync	AASync.com AASync version 2.2.1.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5619</a> <a href="#">MISC</a>
abb -- microscada_pro_sys600	ABB MicroSCADA Pro SYS600 version 9.3 suffers from an instance of CWE-306: Missing Authentication for Critical Function.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5620</a> <a href="#">MISC</a>
abb -- multiple_products	Insufficient folder permissions used by system functions in ABB System 800xA products OPCServer for AC800M (versions 6.0 and earlier) and Control Builder M Professional, MMSServer for AC800M, Base Software for SoftControl (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploited the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8472</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2, Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS	2020-04-29	not yet calculated	<a href="#">CVE-2020-8476</a> <a href="#">CONFIRM</a>

	Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, a weakness in validation of input exists that allows an attacker to alter licenses assigned to the system nodes by sending specially crafted messages to the CLS web service.			<a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, weak file permissions allow an authenticated attacker to block the license handling, escalate his/her privileges and execute arbitrary code.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8471</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS	2020-04-29	not yet calculated	<a href="#">CVE-2020-8475</a> <a href="#">CONFIRM</a>

	Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, a weakness in validation of input exists that allows an attacker to block license handling by sending specially crafted messages to the CLS web service.			<a href="#">CONFIRM</a>
abb -- multiple_products	For ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, confidential data is written in an unprotected file. An attacker who successfully exploited this vulnerability could take full control of the computer.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8481</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and	2020-04-29	not yet calculated	<a href="#">CVE-2020-8479</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	6.1, Composer CTK 6.1 and 6.2, AdvBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, an XML External Entity Injection vulnerability exists that allows an attacker to read or call arbitrary files from the license server and/or from the network and also block the license handling.			
abb -- system_800xa_base	Insufficient protection of the inter-process communication functions in ABB System 800xA Base (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8487</a> <a href="#">CONFIRM</a>
abb -- system_800xa_base	Insufficient folder permissions used by system functions in ABB System 800xA Base (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploit the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8473</a> <a href="#">CONFIRM</a>
abb -- system_800xa_batch_management	Insufficient protection of the inter-process communication functions in ABB System 800xA Batch Management (all published versions) enables an attacker authenticated on the local system to inject data, affecting User Interface update during batch execution and/or compare/printing functionalities.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8488</a> <a href="#">CONFIRM</a>
abb -- system_800xa_for_dci	Insufficient protection of the inter-process communication functions in ABB System 800xA for DCI (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8484</a> <a href="#">CONFIRM</a>
abb -- system_800xa_for_mod_300	Insufficient protection of the inter-process communication functions in ABB System 800xA for MOD 300 (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8485</a> <a href="#">CONFIRM</a>
	Insufficient protection of the inter-process communication functions in ABB System 800xA Information Management (all			



abb -- system_800xa_information_management	published versions) enables an attacker authenticated on the local system to inject data, affecting the runtime values to be stored in the archive, or making Information Management history services unavailable.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8489</a> <a href="#">CONFIRM</a>
abb -- system_800xa_products	Insufficient protection of the inter-process communication functions in ABB System 800xA products OPC Server for AC 800M, MMS Server for AC 800M and Base Software for SoftControl (all published versions) enables an attacker authenticated on the local system to inject data, affecting the online view of runtime data shown in Control Builder.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8478</a> <a href="#">CONFIRM</a>
abb -- system_800xa_rnrp	Insufficient protection of the inter-process communication functions in ABB System 800xA RNRP (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8486</a> <a href="#">CONFIRM</a>
accellion -- file_transfer_appliance	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').	2020-04-29	not yet calculated	<a href="#">CVE-2019-5623</a> <a href="#">MISC</a>
accellion -- file_transfer_appliance	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-798: Use of Hard-coded Credentials.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5622</a> <a href="#">MISC</a>
amd -- ati_atilk64.sys	AMD ATI atilk64.sys 5.11.9.0 allows low-privileged users to interact directly with physical memory by calling one of several driver routines that map physical memory into the virtual address space of the calling process. This could enable low-privileged users to achieve NT AUTHORITY\SYSTEM privileges via a DeviceIoControl call associated with MmMapIoSpace, IoAllocateMdl, MmBuildMdlForNonPagedPool, or MmMapLockedPages.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12138</a> <a href="#">MISC</a> <a href="#">MISC</a>
apache -- iotdb	An issue was found in Apache IoTDB .9.0 to 0.9.1 and 0.8.0 to 0.8.2. When starting IoTDB, the JMX port 31999 is exposed with no certification. Then, clients could execute code remotely.	2020-04-27	not yet calculated	<a href="#">CVE-2020-1952</a> <a href="#">CONFIRM</a>
apache -- nifi_registry	If NiFi Registry 0.1.0 to 0.5.0 uses an authentication mechanism other than PKI, when the user clicks Log Out, NiFi Registry invalidates the authentication token on the client side but not on the	2020-04-	not yet	<a href="#">CVE-2020-9482</a>

	server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to NiFi Registry.	28	calculated	<a href="#">CONFIRM</a>
apache -- ofbiz	Apache OFBiz 17.12.01 is vulnerable to some CSRF attacks.	2020-04-30	not yet calculated	<a href="#">CVE-2019-0235</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
apache -- tika	A carefully crafted or corrupt file may trigger a System.exit in Tika's OneNote Parser. Crafted or corrupted files can also cause out of memory errors and/or infinite loops in Tika's ICNSParser, MP3Parser, MP4Parser, SAS7BDATParser, OneNoteParser and ImageParser. Apache Tika users should upgrade to 1.24.1 or later. The vulnerabilities in the MP4Parser were partially fixed by upgrading the com.googlecode:isoparser:1.1.22 dependency to org.tallison:isoparser:1.9.41.2. For unrelated security reasons, we upgraded org.apache.cxf to 3.3.6 as part of the 1.24.1 release.	2020-04-27	not yet calculated	<a href="#">CVE-2020-9489</a> <a href="#">MISC</a>
apport -- apport	Apport reads and writes information on a crashed process to /proc/pid with elevated privileges. Apport then determines which user the crashed process belongs to by reading /proc/pid through get_pid_info() in data/apport. An unprivileged user could exploit this to read information about a privileged running process by exploiting PID recycling. This information could then be used to obtain ASLR offsets for a process with an existing memory corruption vulnerability. The initial fix introduced regressions in the Python Apport library due to a missing argument in Report.add_proc_envirion in apport/report.py. It also caused an autopkgtest failure when reading /proc/pid and with Python 2 compatibility by reading /proc maps. The initial and subsequent regression fixes are in 2.20.11-0ubuntu16, 2.20.11-0ubuntu8.6, 2.20.9-0ubuntu7.12, 2.20.1-0ubuntu2.22 and 2.14.1-0ubuntu3.29+esm3.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15790</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
b&r_industrial_automation --	A directory traversal vulnerability in SharpZipLib used in the upgrade service in B&R Automation Studio versions 4.0.x,	2020-04-	not yet	<a href="#">CVE-2019-19102</a>

b&r_automation_studio	4.1.x and 4.2.x allow unauthenticated users to write to certain local directories. The vulnerability is also known as zip slip.	29	calculated	<a href="#">CONFIRM</a>
b&r_industrial_automation -- b&r_automation_studio	A privilege escalation vulnerability in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.4SP, < 4.6.3SP, < 4.7.2 and < 4.8.1 allow authenticated users to delete arbitrary files via an exposed interface.	2020-04-29	not yet calculated	<a href="#">CVE-2019-19100</a> <a href="#">CONFIRM</a>
b&r_industrial_automation -- b&r_automation_studio	A missing secure communication definition and an incomplete TLS validation in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.5SP, < 4.6.4 and < 4.7.2 enable unauthenticated users to perform MITM attacks via the B&R upgrade server.	2020-04-29	not yet calculated	<a href="#">CVE-2019-19101</a> <a href="#">CONFIRM</a>
beeline -- smart_box	Beeline Smart Box 2.0.38 routers allow "Advanced settings > Other > Diagnostics" OS command injection via the Ping ping_ipaddr parameter, the Nslookup nslookup_ipaddr parameter, or the Traceroute traceroute_ipaddr parameter.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12246</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.6 allows remote attackers to read arbitrary files because the presfilename (lowercase) value can be a .pdf filename while the presFilename (mixed case) value has a ../ sequence. This can be leveraged for privilege escalation via a directory traversal to bigbluebutton.properties. NOTE: this issue exists because of an ineffective mitigation to CVE-2020-12112 in which there was an attempted fix within an NGINX configuration file, without considering that the relevant part of NGINX is case-insensitive.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12443</a> <a href="#">MISC</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection (issue 2 of 2).	2020-04-30	not yet calculated	<a href="#">CVE-2019-19220</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19217</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 has Insecure Password Storage.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19218</a> <a href="#">MISC</a>
	A buffer overflow vulnerability in BMC Control-M/Agent 7.0.00.000 when the On-Do action destination is Mail and the			<a href="#">CVE-2019-</a>

bmc -- control-m/agent	Control-M/Agent is configured to send the email, allows remote attackers to have unspecified impact via vectors related to the configured IP address or SMTP server.	2020-04-30	not yet calculated	<a href="#">19215</a> <a href="#">MISC</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 has an Insecure File Copy.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19216</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows Arbitrary File Download.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19219</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 1 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11675</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 allows variable reuse, possibly causing data corruption.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11674</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 3 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11677</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 2 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11676</a> <a href="#">MISC</a>
cisco -- ios_xe_sd-wan_software	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16011</a> <a href="#">CISCO</a>
dom4j -- dom4j	dom4j before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.	2020-05-01	not yet calculated	<a href="#">CVE-2020-10683</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ebiz4u -- ebiz4u	AxECM.cab(ActiveX Control) in Inogard Ebiz4u contains a vulnerability that could allow remote files to be downloaded and executed by setting arguments to the activeX method. Download of Code Without Integrity Check vulnerability in ActiveX control of Inogard Co.,LTD Ebiz4u ActiveX of Inogard	2020-04-29	not yet calculated	<a href="#">CVE-2019-19165</a> <a href="#">CONFIRM</a>

	Co.,LTD(AxECM.cab) allows ATTACKER to cause a file download to Windows user's folder and execute. This issue affects: Inogard Co.,LTD Ebiz4u ActiveX of Inogard Co.,LTD(AxECM.cab) version 1.0.5.0 and later versions on windows 7/8/10.			<a href="#">CONFIRM</a>
eset -- antivirus_and_antispyware_module	ESET Antivirus and Antispyware Module module 1553 through 1560 allows a user with limited access rights to create hard links in some ESET directories and then force the product to write through these links into files that would normally not be write-able by the user, thus achieving privilege escalation.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11446</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, when a virtual server is configured with HTTP explicit proxy and has an attached HTTP_PROXY_REQUEST iRule, POST requests sent to the virtual server cause an xdata memory leak.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5883</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5, and 11.6.1-11.6.5.1, under certain conditions, the Intel QuickAssist Technology (QAT) cryptography driver may produce a Traffic Management Microkernel (TMM) core file.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5882</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.4, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the default deployment mode for BIG-IP high availability (HA) pair mirroring is insecure. This is a control plane issue that is exposed only on the network used for mirroring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5884</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, a race condition exists where mcpd and other processes may make unencrypted connection attempts to a new configuration sync peer. The race condition can occur when changing the ConfigSync IP address of a peer, adding a new peer, or when the Traffic Management Microkernel (TMM) first starts up.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5876</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.2.3, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.4.1, when processing TLS traffic with hardware cryptographic acceleration	2020-04-	not yet	<a href="#">CVE-2020-5872</a>



	enabled on platforms with Intel QAT hardware, the Traffic Management Microkernel (TMM) may stop responding and cause a failover event.	30	calculated	<a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3 and 14.1.0-14.1.2.3, the restjavad process may expose a way for attackers to upload arbitrary files on the BIG-IP system, bypassing the authorization system. Resulting error messages may also reveal internal paths of the server.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5880</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.2.3, undisclosed requests can lead to a denial of service (DoS) when sent to BIG-IP HTTP/2 virtual servers. The problem can occur when ciphers, which have been blacklisted by the HTTP/2 RFC, are used on backend servers. This is a data-plane issue. There is no control-plane exposure.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5871</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1 and BIG-IQ 5.2.0-7.1.0, when creating a QKView, credentials for binding to LDAP servers used for remote authentication of the BIG-IP administrative interface will not fully obfuscate if they contain whitespace.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5890</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1 and 14.1.0-14.1.2.3, under certain conditions, the Traffic Management Microkernel (TMM) may generate a core file and restart while processing SSL traffic with an HTTP/2 full proxy.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5875</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, undisclosed HTTP/2 requests can lead to a denial of service when sent to a virtual server configured with the Fallback Host setting and a server-side HTTP/2 profile.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5891</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems setup for connection mirroring in a High Availability (HA) pair transfers sensitive cryptographic objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5886</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems set up for connection mirroring in a high availability (HA) pair transfer sensitive cryptographic	2020-04-	not yet	<a href="#">CVE-2020-5885</a>

	objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	30	calculated	<a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, malformed input to the DATAGRAM::tcp iRules command within a FLOW_INIT event may lead to a denial of service.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5877</a> <a href="#">CONFIRM</a>
f5 -- big-ip_and_big-iq	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.1-11.6.5 and BIG-IQ 5.2.0-7.1.0, a user associated with the Resource Administrator role who has access to the secure copy (scp) utility but does not have access to Advanced Shell (bash) can execute arbitrary commands using a maliciously crafted scp request.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5873</a> <a href="#">MISC</a>
f5 -- big-ip_apm	On BIG-IP APM 15.0.0-15.0.1.2, 14.1.0-14.1.2.3, and 14.0.0-14.0.1, in certain circumstances, an attacker sending specifically crafted requests to a BIG-IP APM virtual server may cause a disruption of service provided by the Traffic Management Microkernel(TMM).	2020-04-30	not yet calculated	<a href="#">CVE-2020-5874</a> <a href="#">CONFIRM</a>
f5 -- big-ip_apm	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, in BIG-IP APM portal access, a specially crafted HTTP request can lead to reflected XSS after the BIG-IP APM system rewrites the HTTP response from the untrusted backend server and sends it to the client.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5889</a> <a href="#">CONFIRM</a>
f5 -- big-ip_apm_and_edge_gateway_and_firepass	In versions 7.1.5-7.1.8, the BIG-IP Edge Client components in BIG-IP APM, Edge Gateway, and FirePass legacy allow attackers to obtain the full session ID from process memory.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5892</a> <a href="#">CONFIRM</a>
f5 -- big-ip_asm	On BIG-IP ASM 11.6.1-11.6.5.1, under certain configurations, the BIG-IP system sends data plane traffic to back-end servers unencrypted, even when a Server SSL profile is applied.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5879</a> <a href="#">CONFIRM</a>
f5 -- big-ip_edge_client	In versions 7.1.5-7.1.8, when a user connects to a VPN using BIG-IP Edge Client over an unsecure network, BIG-IP Edge Client responds to authentication requests over HTTP while sending probes for captive portal detection.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5893</a> <a href="#">CONFIRM</a>
	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.3, Traffic			<a href="#">CVE-2020-</a>

f5 -- big-ip_virtual_edition	Management Microkernel (TMM) may restart on BIG-IP Virtual Edition (VE) while processing unusual IP traffic.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5878</a> <a href="#">MISC</a>
f5 -- big-ip_virtual_edition	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for remote attackers to access local daemons and bypass port lockdown settings.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5887</a> <a href="#">CONFIRM</a>
f5 -- big-ip_virtual_edition	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when the BIG-IP Virtual Edition (VE) is configured with VLAN groups and there are devices configured with OSPF connected to it, the Network Device Abstraction Layer (NDAL) Interfaces can lock up and in turn disrupting the communication between the mcpd and tmm processes.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5881</a> <a href="#">CONFIRM</a>
f5 -- big-ip_virtual_edition	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for adjacent network (layer 2) attackers to access local daemons and bypass port lockdown settings.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5888</a> <a href="#">CONFIRM</a>
faye_gem_for_ruby_on_rails -- faye_gem_for_ruby_on_rails	Faye (NPM, RubyGem) versions greater than 0.5.0 and before 1.0.4, 1.1.3 and 1.2.5, has the potential for authentication bypass in the extension system. The vulnerability allows any client to bypass checks put in place by server-side extensions, by appending extra segments to the message channel. It is patched in versions 1.0.4, 1.1.3 and 1.2.5.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11020</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ffmpeg -- ffmpeg	cbs_jpeg_split_fragment in libavcodec/cbs_jpeg.c in FFmpeg 4.2.2 has a heap-based buffer overflow during JPEG_MARKER_SOS handling because of a missing length check.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12284</a> <a href="#">MISC</a> <a href="#">MISC</a>
fonality -- trixbox_community_edition	An OS Command Injection vulnerability in the endpoint_devicemap.php component of Fonality Trixbox Community Edition allows an attacker to execute commands on the underlying operating system as the "asterisk" user. Note that Trixbox Community Edition has been unsupported by the vendor since 2012. This issue affects: Fonality Trixbox Community Edition, versions 1.2.0 through 2.8.0.4. Versions 1.0 and 1.1 are unaffected.	2020-05-01	not yet calculated	<a href="#">CVE-2020-7351</a> <a href="#">MISC</a>
	An improper authentication vulnerability in FortiMail 5.4.10, 6.0.7, 6.2.2 and earlier			

fortiguard -- fortimail_and_foritvoiceenterprise	and FortiVoiceEnterprise 6.0.0 and 6.0.1 enterprise allow a remote unauthenticated attacker to access the system as a legitimate user by requesting a password change via the user interface.	2020-04-27	not yet calculated	<a href="#">CVE-2020-9294</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in accessing out-of-bounds memory leading to a kernel panic or other unpredictable results.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5614</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r357490, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r357489, and 11.3-RELEASE before 11.3-RELEASE-p7, incorrect use of a user-controlled pointer in the epair virtual network module allowed vnet jailed privileged users to panic the host system and potentially execute arbitrary code in the kernel.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7452</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in memory access after it has been freed leading to a kernel panic or other unpredictable results.	2020-04-29	not yet calculated	<a href="#">CVE-2019-15874</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356089, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r356090, and 11.3-RELEASE before 11.3-RELEASE-p7, driver specific ioctl command handlers in the oce network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to send passthrough commands to the device firmware.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15876</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356606 and 12.1-RELEASE before 12.1-RELEASE-p3, driver specific ioctl command handlers in the ixl network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to trigger updates to the device's non-volatile memory.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15877</a> <a href="#">CONFIRM</a>
	In FreeBSD 12.1-STABLE before r359021, 12.1-RELEASE before 12.1-			

freebsd -- freebsd	RELEASE-p3, 11.3-STABLE before r359020, and 11.3-RELEASE before 11.3-RELEASE-p7, a missing null termination check in the jail_set configuration option "osrelease" may return more bytes with a subsequent jail_get system call allowing a malicious jail superuser with permission to create nested jails to read kernel memory.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7453</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r358739, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r358740, and 11.3-RELEASE before 11.3-RELEASE-p7, a TCP SYN-ACK or challenge TCP-ACK segment over IPv6 that is transmitted or retransmitted does not properly initialize the Traffic Class field disclosing one byte of kernel memory over the network.	2020-04-28	not yet calculated	<a href="#">CVE-2020-7451</a> <a href="#">CONFIRM</a>
freeipa -- freeipa	A flaw was found in all ipa versions 4.x.x through 4.8.0. When sending a very long password (>= 1,000,000 characters) to the server, the password hashing process could exhaust memory and CPU leading to a denial of service and the website becoming unresponsive. The highest threat from this vulnerability is to system availability.	2020-04-27	not yet calculated	<a href="#">CVE-2020-1722</a> <a href="#">CONFIRM</a>
fun-map -- fun-map	fun-map through 3.3.1 is vulnerable to Prototype Pollution. The function assocInM could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload.	2020-04-28	not yet calculated	<a href="#">CVE-2020-7644</a> <a href="#">MISC</a> <a href="#">MISC</a>
g.skill -- trident_z_lighting_control	The ene.sys driver in G.SKILL Trident Z Lighting Control through 1.00.08 exposes mapping and un-mapping of physical memory, reading and writing to Model Specific Register (MSR) registers, and input from and output to I/O ports to local non-privileged users. This leads to privilege escalation to NT AUTHORITY\SYSTEM.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12446</a> <a href="#">MISC</a>
generix -- upsadapter_cs141	UPS Adapter CS141 before 1.90 allows Directory Traversal. An attacker with Admin or Engineer login credentials could exploit the vulnerability by manipulating variables that reference files and by doing this achieve access to files and directories outside the web root folder. An attacker may access arbitrary files and directories stored in the file system, but integrity of the files are not jeopardized as	2020-04-27	not yet calculated	<a href="#">CVE-2020-11420</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>



	attacker have read access rights only.			
genius_bytes -- genius_server	An application plugin in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to gain admin privileges.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16653</a> <a href="#">MISC</a>
genius_bytes -- genius_server	The BPM component in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to execute arbitrary commands.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16652</a> <a href="#">MISC</a> <a href="#">MISC</a>
gigamon -- gigavue	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an arbitrary file upload for an authenticated user. If an executable file is uploaded into the www-root directory, then it could yield remote code execution via the filename parameter.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12252</a> <a href="#">MISC</a> <a href="#">MISC</a>
gigamon -- gigavue	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an authenticated user to change the filename value (in the POST method) from the original filename to achieve directory traversal via a ../ sequence and, for example, obtain a complete directory listing of the machine.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12251</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab 12.6 through 12.9 is vulnerable to a privilege escalation that allows an external user to create a personal snippet through the API.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12275</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab 9.5.9 through 12.9 is vulnerable to stored XSS in an admin notification feature.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12276</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab 10.8 through 12.9 has a vulnerability that allows someone to mirror a repository even if the feature is not activated.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12277</a> <a href="#">CONFIRM</a>
glibc -- glibc	A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.	2020-04-30	not yet calculated	<a href="#">CVE-2020-1752</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
google -- chrome-launcher	All versions of chrome-launcher allow execution of arbitrary commands, by controlling the \$HOME environment variable in Linux operating systems.	2020-05-02	not yet calculated	<a href="#">CVE-2020-7645</a> <a href="#">MISC</a>

grafana -- grafana	An information-disclosure flaw was found in Grafana through 6.7.3. The database directory /var/lib/grafana and database file /var/lib/grafana/grafana.db are world readable. This can result in exposure of sensitive information (e.g., cleartext or encrypted datasource passwords).	2020-04-29	not yet calculated	<a href="#">CVE-2020-12458</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	In certain Red Hat packages for Grafana 6.x through 6.3.6, the configuration files /etc/grafana/grafana.ini and /etc/grafana/ldap.toml (which contain a secret_key and a bind_password) are world readable.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12459</a> <a href="#">MISC</a> <a href="#">MISC</a>
handysoft -- handy_groupware	ActiveX Control(HShell.dll) in Handy Groupware 1.7.3.1 for Windows 7, 8, and 10 allows an attacker to execute arbitrary command via the ShellExec method.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7804</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.4 contained a cross-site scripting vulnerability such that files from a malicious workload could cause arbitrary JavaScript to execute in the web UI. Fixed in 0.10.5.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10944</a> <a href="#">CONFIRM</a>
hcl -- connections	HCL Connections v5.5, v6.0, and v6.5 contains an open redirect vulnerability which could be exploited by an attacker to conduct phishing attacks.	2020-05-01	not yet calculated	<a href="#">CVE-2019-4209</a> <a href="#">CONFIRM</a>
hp -- multiple_products	A potential security vulnerability has been identified in the disk drive firmware installers named Supplemental Update / Online ROM Flash Component on HPE servers running Linux. The vulnerable software is included in the HPE Service Pack for ProLiant (SPP) releases 2018.06.0, 2018.09.0, and 2018.11.0. The vulnerable software is the Supplemental Update / Online ROM Flash Component for Linux (x64) software. The installer in this software component could be locally exploited to execute arbitrary code. Drive Models can be found in the Vulnerability Resolution field of the security bulletin. The 2019_03 SPP and Supplemental update / Online ROM Flash Component for Linux (x64) after 2019.03.0 has fixed this issue.	2020-04-27	not yet calculated	<a href="#">CVE-2020-7135</a> <a href="#">CONFIRM</a>
hp --	A security vulnerability in HPE Smart Update Manager (SUM) prior to version 8.5.6 could allow remote unauthorized access. Hewlett Packard Enterprise has provided a software update to resolve this vulnerability in HPE Smart Update			<a href="#">CVE-2020-</a>

smart_update_manager	Manager (SUM) prior to 8.5.6. Please visit the HPE Support Center at <a href="https://support.hpe.com/hpesc/public/home">https://support.hpe.com/hpesc/public/home</a> to download the latest version of HPE Smart Update Manager (SUM). Download the latest version of HPE Smart Update Manager (SUM) or download the latest Service Pack For ProLiant (SPP).	2020-04-30	not yet calculated	<a href="#">7136</a> <a href="#">CONFIRM</a>
http-client -- http-client	Actions Http-Client (NPM @actions/http-client) before version 1.0.8 can disclose Authorization headers to incorrect domain in certain redirect scenarios. The conditions in which this happens are if consumers of the http-client: 1. make an http request with an authorization header 2. that request leads to a redirect (302) and 3. the redirect url redirects to another domain or hostname Then the authorization header will get passed to the other domain. The problem is fixed in version 1.0.8.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11021</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 2 out of 2 vulnerabilities. Different than CVE-2020-5302. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than 9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than 9.1.0.350(C10E3R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8), earlier than 9.1.0.350(C636E4R1P13T8) Charlotte-L09C: earlier than 9.1.0.311(C185E4R1P11T8), earlier than 9.1.0.345(C432E8R1P11T8) Charlotte-L29C: earlier than 9.1.0.325(C185E4R1P11T8), earlier than 9.1.0.335(C636E3R1P13T8), earlier than 9.1.0.345(C432E8R1P11T8), earlier than			

huawei -- multiple_smartphones	<p>9.1.0.336(C605E3R1P12T8) Columbia-AL10B: earlier than</p> <p>9.1.0.333(C00E333R1P1T8) Columbia-L29D: earlier than</p> <p>9.1.0.350(C461E3R1P11T8), earlier than</p> <p>9.1.0.350(C185E3R1P12T8), earlier than</p> <p>9.1.0.350(C10E5R1P14T8), earlier than</p> <p>9.1.0.351(C432E5R1P13T8) Cornell-AL00A: earlier than</p> <p>9.1.0.333(C00E333R1P1T8) Cornell-L29A: earlier than</p> <p>9.1.0.328(C185E1R1P9T8), earlier than</p> <p>9.1.0.328(C432E1R1P9T8), earlier than</p> <p>9.1.0.330(C461E1R1P9T8), earlier than</p> <p>9.1.0.328(C636E2R1P12T8) Emily-L09C: earlier than 9.1.0.336(C605E4R1P12T8), earlier than 9.1.0.311(C185E2R1P12T8), earlier than 9.1.0.345(C432E10R1P12T8) Emily-L29C: earlier than</p> <p>9.1.0.311(C605E2R1P12T8), earlier than</p> <p>9.1.0.311(C636E7R1P13T8), earlier than</p> <p>9.1.0.311(C432E7R1P11T8) Ever-L29B: earlier than 9.1.0.311(C185E3R3P1), earlier than 9.1.0.310(C636E3R2P1), earlier than 9.1.0.310(C432E3R1P12)</p> <p>HUAWEI Mate 20: earlier than</p> <p>9.1.0.131(C00E131R3P1) HUAWEI Mate 20 Pro: earlier than</p> <p>9.1.0.310(C185E10R2P1) HUAWEI Mate 20 RS: earlier than</p> <p>9.1.0.135(C786E133R3P1) HUAWEI Mate 20 X: earlier than</p> <p>9.1.0.135(C00E133R2P1) HUAWEI P20: earlier than 9.1.0.333(C00E333R1P1T8)</p> <p>HUAWEI P20 Pro: earlier than</p> <p>9.1.0.333(C00E333R1P1T8) HUAWEI P30: earlier than 9.1.0.193 HUAWEI P30 Pro: earlier than</p> <p>9.1.0.186(C00E180R2P1) HUAWEI Y9 2019: earlier than</p> <p>9.1.0.220(C605E3R1P1T8) HUAWEI nova lite 3: earlier than</p> <p>9.1.0.305(C635E8R2P2) Honor 10 Lite: earlier than 9.1.0.283(C605E8R2P2)</p> <p>Honor 8X: earlier than</p> <p>9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than 9.1.0.238(C432E1R3P1)</p> <p>Jackman-L22: earlier than</p> <p>9.1.0.247(C636E2R4P1T8) Paris-L21B: earlier than 9.1.0.331(C432E1R1P2T8)</p> <p>Paris-L21MEB: earlier than</p> <p>9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than 9.1.0.331(C636E1R1P3T8)</p> <p>Sydney-AL00: earlier than</p>	2020-04-27	not yet calculated	<a href="#">CVE-2019-5303</a> <a href="#">CONFIRM</a>
-----------------------------------	--	------------	--------------------	--

	<p>9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than 9.1.0.215(C432E1R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than 9.1.0.213(C185E1R1P2T8) Sydney-L22: earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than 9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)</p>			
	<p>There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 1 out of 2 vulnerabilities. Different than CVE-2020-5303. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than 9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than</p>			



huawei --  
multiple\_smartphones

9.1.0.350(C10E3R1P14T8), earlier than  
9.1.0.351(C432E5R1P13T8), earlier than  
9.1.0.350(C636E4R1P13T8) Charlotte-  
L09C: earlier than  
9.1.0.311(C185E4R1P11T8), earlier than  
9.1.0.345(C432E8R1P11T8) Charlotte-  
L29C: earlier than  
9.1.0.325(C185E4R1P11T8), earlier than  
9.1.0.335(C636E3R1P13T8), earlier than  
9.1.0.345(C432E8R1P11T8), earlier than  
9.1.0.336(C605E3R1P12T8) Columbia-  
AL10B: earlier than  
9.1.0.333(C00E333R1P1T8) Columbia-  
L29D: earlier than  
9.1.0.350(C461E3R1P11T8), earlier than  
9.1.0.350(C185E3R1P12T8), earlier than  
9.1.0.350(C10E5R1P14T8), earlier than  
9.1.0.351(C432E5R1P13T8) Cornell-  
AL00A: earlier than  
9.1.0.333(C00E333R1P1T8) Cornell-  
L29A: earlier than  
9.1.0.328(C185E1R1P9T8), earlier than  
9.1.0.328(C432E1R1P9T8), earlier than  
9.1.0.330(C461E1R1P9T8), earlier than  
9.1.0.328(C636E2R1P12T8) Emily-L09C:  
earlier than 9.1.0.336(C605E4R1P12T8),  
earlier than 9.1.0.311(C185E2R1P12T8),  
earlier than 9.1.0.345(C432E10R1P12T8)  
Emily-L29C: earlier than  
9.1.0.311(C605E2R1P12T8), earlier than  
9.1.0.311(C636E7R1P13T8), earlier than  
9.1.0.311(C432E7R1P11T8) Ever-L29B:  
earlier than 9.1.0.311(C185E3R3P1),  
earlier than 9.1.0.310(C636E3R2P1),  
earlier than 9.1.0.310(C432E3R1P12)  
HUAWEI Mate 20: earlier than  
9.1.0.131(C00E131R3P1) HUAWEI Mate  
20 Pro: earlier than  
9.1.0.310(C185E10R2P1) HUAWEI Mate  
20 RS: earlier than  
9.1.0.135(C786E133R3P1) HUAWEI  
Mate 20 X: earlier than  
9.1.0.135(C00E133R2P1) HUAWEI P20:  
earlier than 9.1.0.333(C00E333R1P1T8)  
HUAWEI P20 Pro: earlier than  
9.1.0.333(C00E333R1P1T8) HUAWEI  
P30: earlier than 9.1.0.193 HUAWEI P30  
Pro: earlier than  
9.1.0.186(C00E180R2P1) HUAWEI Y9  
2019: earlier than  
9.1.0.220(C605E3R1P1T8) HUAWEI  
nova lite 3: earlier than  
9.1.0.305(C635E8R2P2) Honor 10 Lite:  
earlier than 9.1.0.283(C605E8R2P2)

2020-04-  
27 not yet  
calculated

[CVE-2019-  
5302  
CONFIRM](#)

	<p>Honor 8X: earlier than 9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than 9.1.0.238(C432E1R3P1) Jackman-L22: earlier than 9.1.0.247(C636E2R4P1T8) Paris-L21B: earlier than 9.1.0.331(C432E1R1P2T8) Paris-L21MEB: earlier than 9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than 9.1.0.331(C636E1R1P3T8) Sydney-AL00: earlier than 9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than 9.1.0.215(C432E1R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than 9.1.0.213(C185E1R1P2T8) Sydney-L22: earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than 9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)</p>			
huawei -- oceanstor_5310	<p>Huawei OceanStor 5310 product with version of V500R007C60SPC100 has an invalid pointer access vulnerability. The software system access an invalid pointer when attacker malformed packet. Due to the insufficient validation of some parameter, successful exploit could cause device reboot.</p>	2020-04-30	not yet calculated	<a href="#">CVE-2020-9098</a> CONFIRM CONFIRM
	<p>Huawei OSD product with versions earlier than OSD_uwp_9.0.32.0 have a local privilege escalation vulnerability. An</p>			<a href="#">CVE-2020-</a>

huawei -- osd	authenticated, local attacker can constructs a specific file path to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	2020-04-27	not yet calculated	<a href="#">9072</a> <a href="#">CONFIRM</a>
huawei -- pcmanager	Huawei PCManager with versions earlier than 10.0.1.36 has a privilege escalation vulnerability. Due to improper permission management of specific files, local attackers with low permissions can inject commands to exploit this vulnerability. Successful exploit may cause privilege escalation.	2020-04-30	not yet calculated	<a href="#">CVE-2020-1817</a> <a href="#">CONFIRM</a>
inductive_automation - - ignition_8_gateway	An unprotected logging route may allow an attacker to write endless log statements into the database without space limits or authentication. This results in consuming the entire available hard-disk space on the Ignition 8 Gateway (versions prior to 8.0.10), causing a denial-of-service condition.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10641</a> <a href="#">MISC</a>
intelliants -- subrion_cms	admin/blocks.php in Subrion CMS through 4.2.1 allows PHP Object Injection (with resultant file deletion) via serialized data in the subpages value within a block to blocks/edit.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12469</a> <a href="#">MISC</a>
intelmq_manager -- intelmq_manager	IntelMQ Manager from version 1.1.0 and before version 2.1.1 has a vulnerability where the backend incorrectly handled messages given by user-input in the "send" functionality of the Inspect-tool of the Monitor component. An attacker with access to the IntelMQ Manager could possibly use this issue to execute arbitrary code with the privileges of the webserver. Version 2.1.1 fixes the vulnerability.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11016</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jquery -- jquery	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11023</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jquery -- jquery	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched	2020-04-29	not yet calculated	<a href="#">CVE-2020-11022</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	in jQuery 3.5.0.			
json_gem_for_ruby_on_rails -- json_gem_for_ruby_on_rails	<p>The JSON gem through 2.2.0 for Ruby, as used in Ruby 2.4 through 2.4.9, 2.5 through 2.5.7, and 2.6 through 2.6.5, has an Unsafe Object Creation Vulnerability. This is quite similar to CVE-2013-0269, but does not rely on poor garbage-collection behavior within Ruby. Specifically, use of JSON parsing methods can lead to creation of a malicious object within the interpreter, with adverse effects that are application-dependent.</p>	2020-04-28	not yet calculated	<a href="#">CVE-2020-10663</a> <a href="#">SUSE MLIST</a> <a href="#">FEDORA CONFIRM</a>
kiali -- kiali	<p>An insufficient JWT validation vulnerability was found in Kiali versions 0.4.0 to 1.15.0 and was fixed in Kiali version 1.15.1, wherein a remote attacker could abuse this flaw by stealing a valid JWT cookie and using that to spoof a user session, possibly gaining privileges to view and alter the Istio configuration.</p>	2020-04-27	not yet calculated	<a href="#">CVE-2020-1762</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
lexmark -- multiple_devices	<p>A cross-site scripting (XSS) vulnerability in Lexmark CS31x before LW74.VYL.P273; CS41x before LW74.VY2.P273; CS51x before LW74.VY4.P273; CX310 before LW74.GM2.P273; CX410 &amp; XC2130 before LW74.GM4.P273; CX510 &amp; XC2132 before LW74.GM7.P273; MS310, MS312, MS317 before LW74.PRL.P273; MS410, M1140 before LW74.PRL.P273; MS315, MS415, MS417 before LW74.TL2.P273; MS51x, MS610dn, MS617 before LW74.PR2.P273; M1145, M3150dn before LW74.PR2.P273; MS610de, M3150 before LW74.PR4.P273; MS71x, M5163dn before LW74.DN2.P273; MS810, MS811, MS812, MS817, MS818 before LW74.DN2.P273; MS810de, M5155, M5163 before LW74.DN4.P273; MS812de, M5170 before LW74.DN7.P273; MS91x before LW74.SA.P273; MX31x, XM1135 before LW74.SB2.P273; MX410, MX510 &amp; MX511 before LW74.SB4.P273; XM1140, XM1145 before LW74.SB4.P273; MX610 &amp; MX611 before LW74.SB7.P273; XM3150 before LW74.SB7.P273; MX71x, MX81x before LW74.TU.P273; XM51xx &amp; XM71xx before LW74.TU.P273; MX91x &amp; XM91x before LW74.MG.P273; MX6500e</p>	2020-04-28	not yet calculated	<a href="#">CVE-2020-10094</a> <a href="#">CONFIRM</a>

	before LW74.JD.P273; C746 before LHS60.CM2.P738; C748, CS748 before LHS60.CM4.P738; C792, CS796 before LHS60.HC.P738; C925 before LHS60.HV.P738; C950 before LHS60.TP.P738; X548 & XS548 before LHS60.VK.P738; X74x & XS748 before LHS60.NY.P738; X792 & XS79x before LHS60.MR.P738; X925 & XS925 before LHS60.HK.P738; X95x & XS95x before LHS60.TQ.P738; 6500e before LHS60.JR.P738; C734 LR.SK.P824 and earlier; C736 LR.SKE.P824 and earlier; E46x LR.LBH.P824 and earlier; T65x LR.JP.P824 and earlier; X46x LR.BS.P824 and earlier; X65x LR.MN.P824 and earlier; X73x LR.FL.P824 and earlier; W850 LP.JB.P823 and earlier; and X86x LP.SP.P823 and earlier.			
lexmark -- pro910_series_devices	A cross-site scripting (XSS) vulnerability in Lexmark Pro910 series inkjet and other discontinued products.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10093</a> <a href="#">CONFIRM</a>
lg -- bridge	An issue was discovered in LG Bridge before April 2019 on Windows. DLL Hijacking can occur.	2020-04-29	not yet calculated	<a href="#">CVE-2019-20781</a> <a href="#">CONFIRM</a>
libgit2 -- libgit2	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. path.c mishandles equivalent filenames that exist because of NTFS Alternate Data Streams. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1352.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12278</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgit2 -- libgit2	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. checkout.c mishandles equivalent filenames that exist because of NTFS short names. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1353.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12279</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libvirt -- libvirt	An issue was discovered in qemuDomainGetStatsIOThread in qemu/qemu_driver.c in libvirt 4.10.0 though 6.x before 6.1.0. A memory leak was found in the virDomainListGetStats libvirt API that is responsible for retrieving domain statistics when managing QEMU guests. This flaw allows unprivileged users with a read-only connection to cause a memory leak in the domstats command, resulting in a potential denial of service.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12430</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



linux -- linux_kernel	In the Linux kernel through 5.6.7 on the s390 platform, code execution may occur because of a race condition, as demonstrated by code in enable_sacf_uaccess in arch/s390/lib/uaccess.c that fails to protect against a concurrent page table upgrade, aka CID-3f777e19d171. A crash could also occur.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11884</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
linux -- linux_kernel	An array overflow was discovered in mt76_add_fragment in drivers/net/wireless/mediatek/mt76/dma.c in the Linux kernel before 5.5.10, aka CID-b102f0c522cf. An oversized packet with too many rx fragments can corrupt memory of adjacent pages.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	usb_sg_cancel in drivers/usb/core/message.c in the Linux kernel before 5.6.8 has a use-after-free because a transfer occurs without a reference, aka CID-056ad39ee925.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12464</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mahara -- mahara	In Mahara 19.04 before 19.04.5 and 19.10 before 19.10.3, account details are shared in the Elasticsearch results for accounts that are not accessible when the config setting 'Isolated institutions' is turned on.	2020-04-30	not yet calculated	<a href="#">CVE-2020-9387</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
monox -- monox	MonoX through 5.1.40.5152 allows remote code execution via HTML5Upload.ashx or Pages/SocialNetworking/Ing/en-US/PhotoGallery.aspx because of deserialization in ModuleGallery.HTML5Upload, ModuleGallery.SilverLightUploadModule, HTML5Upload, and SilverLightUploadHandler.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12471</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows stored XSS via User Status, Blog Comments, or Blog Description.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12472</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows admins to execute arbitrary programs by reconfiguring the Converter Executable setting from ffmpeg.exe to a different program.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12473</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows administrators to execute arbitrary code by modifying an ASPX template.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12470</a> <a href="#">MISC</a>
	In Moonlight iOS/tvOS before 4.0.1, the			<a href="#">CVE-2020-</a>

moonlight -- moonlight_ios/tvos	pairing process is vulnerable to a man-in-the-middle attack. The bug has been fixed in Moonlight v4.0.1 for iOS and tvOS.	2020-04-29	not yet calculated	<a href="#">11024</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
moxa -- nport_5150a	Moxa Service in Moxa NPort 5150A firmware version 1.5 and earlier allows attackers to obtain sensitive configuration values via a crafted packet to UDP port 4800. NOTE: Moxa Service is an unauthenticated service that runs upon a first-time installation but can be disabled without ill effect.	2020-05-01	not yet calculated	<a href="#">CVE-2020-12117</a> <a href="#">CONFIRM</a>
multiple_vendors -- multiple_products	The Apros Evolution, ConsciusMap, and Furukawa provisioning systems through 2.8.1 allow remote code execution because of javax.faces.ViewState Java deserialization.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12133</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- dgn2200_devices	NETGEAR DGN2200v4 devices before 2017-01-06 are affected by command execution and an FTP insecure root directory.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11054</a> <a href="#">CONFIRM</a>
netgear -- genie_applicaiton_for_android	The NETGEAR genie application before 2.4.34 for Android is affected by mishandling of hard-coded API keys and session IDs.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11058</a> <a href="#">CONFIRM</a>
netgear -- insight_application	The NETGEAR Insight application before 2.42 for Android and iOS is affected by password mismanagement.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18857</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21204</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.62, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R8900 before 1.0.3.10, R9000 before 1.0.3.10,	2020-04-27	not yet calculated	<a href="#">CVE-2018-21153</a> <a href="#">CONFIRM</a>

	WN2000RPTv3 before 1.0.1.26, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21188</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.10, R6220 before 1.1.0.60, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21209</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, and WNDR4300 before 1.0.2.98.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21199</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6100 before 1.0.0.57, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.78, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21167</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WAC120 before 2.1.7, WN604 before 3.3.10, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, and WND930 before 2.1.5.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21097</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21222</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by debugging command execution. This affects FS752TP 5.4.2.19 and earlier, GS108Tv2 5.4.2.29 and earlier, GS110TP 5.4.2.29 and earlier, GS418TPP 6.6.2.6 and earlier, GS510TLP 6.6.2.6 and earlier, GS510TP 5.04.2.27 and earlier, GS510TPP 6.6.2.6 and earlier, GS716Tv2 5.4.2.27 and earlier, GS716Tv3 6.3.1.16 and earlier, GS724Tv3 5.4.2.27 and earlier, GS724Tv4 6.3.1.16 and earlier, GS728TPSB 5.3.0.29 and earlier, GS728TSB 5.3.0.29 and earlier, GS728TXS 6.1.0.35 and earlier, GS748Tv4 5.4.2.27 and earlier, GS748Tv5 6.3.1.16 and earlier, GS752TPSB 5.3.0.29 and earlier, GS752TSB 5.3.0.29 and earlier, GS752TXS 6.1.0.35 and earlier, M4200 12.0.2.10 and earlier, M4300 12.0.2.10 and earlier, M5300 11.0.0.28 and earlier, M6100 11.0.0.28 and earlier, M7100 11.0.0.28 and earlier, S3300 6.6.1.4 and earlier, XS708T 6.6.0.11 and earlier, XS712T 6.1.0.34 and earlier, and XS716T 6.6.0.11 and earlier.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18860</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100			

netgear -- multiple_devices	before 1.0.0.57, R7800 before 1.2.0.44, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21198</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21220</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, EX2700 before 1.0.1.28, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21215</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21219</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21208</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.52, R6100			



netgear -- multiple_devices	before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.4.2, R9000 before 1.0.3.16, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21155</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.38, D6400 before 1.0.0.74, D7000v2 before 1.0.0.74, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.102, DGN2200Bv4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.20, R6300v2 before 1.0.4.22, R6400 before 1.0.1.32, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R6900P before 1.3.0.18, R7000 before 1.0.9.28, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900 before 1.0.2.10, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, R8300 before 1.0.2.116, R8500 before 1.0.2.116, WN2500RPv2 before 1.0.1.52, WNDR3400v3 before 1.0.1.18, and WNR3500Lv2 before 1.2.0.46.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21156</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.94.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21183</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98,	2020-04-28	not yet calculated	<a href="#">CVE-2018-21212</a> <a href="#">CONFIRM</a>

	WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21211</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects CM400 before 2017-01-11, CM600 before 2017-01-11, D1500 before 2017-01-11, D500 before 2017-01-11, DST6501 before 2017-01-11, JNR1010v1 before 2017-01-11, JWNR2000Tv3 before 2017-01-11, JWNR2010v3 before 2017-01-11, PLW1000 before 2017-01-11, PLW1010 before 2017-01-11, WNR500 before 2017-01-11, WNR612v3 before 2017-01-11, N450 before 2017-01-11, and CG3000Dv2 before 2017-01-11.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11055</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7000 before 2018-03-01, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 2018-03-01, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before	2020-04-27	not yet calculated	<a href="#">CVE-2018-21169</a> <a href="#">CONFIRM</a>

	1.1.0.46.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, and R7800 before 1.0.2.42.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21154</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, and R9000 before 1.0.3.6.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21184</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21224</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21175</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21174</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52,	2020-04-27	not yet calculated	<a href="#">CVE-2018-21176</a>

	WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7000 before 1.0.1.52, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21168</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21185</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R7000 before 1.0.9.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.38, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21157</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects			

netgear -- multiple_devices	D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21205</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21214</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21223</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21218</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before	2020-04-28	not yet calculated	<a href="#">CVE-2018-21195</a> <a href="#">CONFIRM</a>



	1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command execution. This affects M4200-10MG-POE+ 12.0.2.11 and earlier, M4300-28G 12.0.2.11 and earlier, M4300-52G 12.0.2.11 and earlier, M4300-28G-POE+ 12.0.2.11 and earlier, M4300-52G-POE+ 12.0.2.11 and earlier, M4300-8X8F 12.0.2.11 and earlier, M4300-12X12F 12.0.2.11 and earlier, M4300-24X24F 12.0.2.11 and earlier, M4300-24X 12.0.2.11 and earlier, and M4300-48X 12.0.2.11 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18858 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21096 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21196 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21197 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94,	2020-04-28	not yet calculated	<a href="#">CVE-2018-21201 CONFIRM</a>

	WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21202</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6100 before 1.0.1.20, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21203</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21206</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6700 before 1.0.1.30, R6700v2 before 1.2.0.16, R6800 before 1.2.0.16, R6900 before 1.0.1.30, R6900P before 1.2.0.22, R6900v2 before 1.2.0.16, R7000 before 1.0.9.12, R7000P before 1.2.0.22, R7500v2 before 1.0.3.20, R7800 before 1.0.2.44, R8300 before 1.0.2.106, R8500 before 1.0.2.106, and R9000 before 1.0.2.52.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21225</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an			

netgear -- multiple_devices	unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21207</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects JNR1010v2 before 1.1.0.48, JWNR2010v5 before 1.1.0.48, WNR1000v4 before 1.1.0.48, WNR2020 before 1.1.0.48, and WNR2050 before 1.1.0.48.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21226</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21210</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by slowdown/stoppage. This affects C6300 before 2017-05-30, CM400 before 2017-05-30, CM700 before 2017-05-30, and CMD31T before 2017-05-30.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18859</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21094</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected			

netgear -- multiple_devices	by mishandling of repeated URL calls. This affects JNR1010v2 before 2017-01-06, WNR614 before 2017-01-06, WNR618 before 2017-01-06, JWNR2000v5 before 2017-01-06, WNR2020 before 2017-01-06, JWNR2010v5 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2020v2 before 2017-01-06, R6220 before 2017-01-06, and WNDR3700v5 before 2017-01-06.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11057</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21186</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.0.54, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21149</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by password exposure. This affects AC1450 before 2017-01-06, C6300 before 2017-01-06, D500 before 2017-01-06, D1500 before 2017-01-06, D3600 before 2017-01-06, D6000 before 2017-01-06, D6100 before 2017-01-06, D6200 before 2017-01-06, D6200B before 2017-01-06, D6300B before 2017-01-06, D6300 before 2017-01-06, DGN1000v3 before 2017-01-06, DGN2200v1 before 2017-01-06, DGN2200v3 before 2017-01-06, DGN2200V4 before 2017-01-06, DGN2200Bv3 before 2017-01-06, DGN2200Bv4 before 2017-01-06, DGND3700v1 before 2017-01-06, DGND3700v2 before 2017-01-06, DGND3700Bv2 before 2017-01-06, JNR1010v1 before 2017-01-06,			

netgear -- multiple_devices	JNR1010v2 before 2017-01-06, JNR3300 before 2017-01-06, JR6100 before 2017-01-06, JR6150 before 2017-01-06, JWNR2000v5 before 2017-01-06, R2000 before 2017-01-06, R6050 before 2017-01-06, R6100 before 2017-01-06, R6200 before 2017-01-06, R6200v2 before 2017-01-06, R6220 before 2017-01-06, R6250 before 2017-01-06, R6300 before 2017-01-06, R6300v2 before 2017-01-06, R6700 before 2017-01-06, R7000 before 2017-01-06, R7900 before 2017-01-06, R7500 before 2017-01-06, R8000 before 2017-01-06, WGR614v10 before 2017-01-06, WNR1000v2 before 2017-01-06, WNR1000v3 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2000v3 before 2017-01-06, WNR2000v4 before 2017-01-06, WNR2000v5 before 2017-01-06, WNR2200 before 2017-01-06, WNR2500 before 2017-01-06, WNR3500Lv2 before 2017-01-06, WNDR3400v2 before 2017-01-06, WNDR3400v3 before 2017-01-06, WNDR3700v3 before 2017-01-06, WNDR3700v4 before 2017-01-06, WNDR3700v5 before 2017-01-06, WNDR4300 before 2017-01-06, WNDR4300v2 before 2017-01-06, WNDR4500v1 before 2017-01-06, WNDR4500v2 before 2017-01-06, and WNDR4500v3 before 2017-01-06.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11059</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21152</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D8500 before 1.0.3.42, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.26, R6300-2CXNAS before 1.0.3.60, R6300v2 before 1.0.4.28, R6400 before 1.0.1.36, R6400v2 before	2020-04-27	not yet calculated	<a href="#">CVE-2018-21093</a> <a href="#">CONFIRM</a>



	1.0.2.52, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R7100LG before 1.0.0.46, R7300 before 1.0.0.68, R7900 before 1.0.2.10, R8000 before 1.0.4.18, R8000P before 1.3.0.10, R7900P before 1.3.0.10, R8500 before 1.0.2.122, R8300 before 1.0.2.122, RBW30 before 2.1.2.6, WN2500RPv2 before 1.0.0.54, and WNR3500Lv2 before 1.2.0.56.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command execution via a PHP form. This affects WN604 3.3.3 and earlier, WNAP210v2 3.5.20.0 and earlier, WNAP320 3.5.20.0 and earlier, WNDAP350 3.5.20.0 and earlier, WNDAP360 3.5.20.0 and earlier, WNDAP620 2.0.11 and earlier, WNDAP660 3.5.20.0 and earlier, WND930 2.0.11 and earlier, and WAC120 2.0.7 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18863</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects JGS516PE before 2017-05-11, JGS524Ev2 before 2017-05-11, JGS524PE before 2017-05-11, GS105Ev2 before 2017-05-11, GS105PE before 2017-05-11, GS108Ev3 before 2017-05-11, GS108PEv3 before 2017-05-11, GS116Ev2 before 2017-05-11, GSS108E before 2017-05-11, GSS116E before 2017-05-11, XS708Ev2 before 2017-05-11, and XS716E before 2017-05-11.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18862</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by insecure renegotiation. This affects SRX5308 before 2017-02-10, FVS336Gv3 before 2017-02-10, FVS318N before 2017-02-10, and FVS318Gv2 before 2017-02-10.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11060</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by password recovery and file access. This affects D8500 1.0.3.27 and earlier, DGN2200v4 1.0.0.82 and earlier, R6300v2 1.0.4.06 and earlier, R6400 1.0.1.20 and earlier, R6400v2 1.0.2.18 and earlier, R6700 1.0.1.22 and earlier, R6900 1.0.1.20 and earlier, R7000 1.0.7.10 and earlier, R7000P 1.0.0.58 and earlier, R7100LG 1.0.0.28 and earlier, R7300DST 1.0.0.52 and earlier, R7900 1.0.1.12 and earlier, R8000 1.0.3.46 and	2020-04-29	not yet calculated	<a href="#">CVE-2017-18853</a> <a href="#">CONFIRM</a>

	earlier, R8300 1.0.2.86 and earlier, R8500 1.0.2.86 and earlier, WNDR3400v3 1.0.1.8 and earlier, and WNDR4500v2 1.0.0.62 and earlier.			
netgear -- readynas_devices	NETGEAR ReadyNAS 6.6.1 and earlier is affected by command injection.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18854</a> <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.6.1 are affected by command injection.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18856</a> <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by incorrect configuration of security settings.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21159</a> <a href="#">CONFIRM</a>
netgear -- readynas_surveillance_devices	Certain NETGEAR devices are affected by anonymous root access. This affects ReadyNAS Surveillance 1.1.1-3-armel and earlier and ReadyNAS Surveillance 1.4.1-3-amd64 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11056</a> <a href="#">CONFIRM</a>
netgear -- readynas_surveillance_services	Certain NETGEAR devices are affected by CSRF. This affects ReadyNAS Surveillance 1.4.3-15-x86 and earlier and ReadyNAS Surveillance 1.1.4-5-ARM and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18861</a> <a href="#">CONFIRM</a>
node.js -- node.js	The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.	2020-04-26	not yet calculated	<a href="#">CVE-2020-12265</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
octopus -- deploy	In Octopus Deploy before 2019.12.9 and 2020 before 2020.1.12, the TaskView permission is not scoped to any dimension. For example, a scoped user who is scoped to only one tenant can view server tasks scoped to any other tenant.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12286</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
onkyo -- tx-nr585_devices	A Local File Inclusion (LFI) issue on Onkyo TX-NR585 1000-0000-000-0008-0000 devices allows remote unauthenticated users on the network to read sensitive files via %2e%2e%2f directory traversal, as demonstrated by reading /etc/shadow.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12447</a> <a href="#">MISC</a>
opendmarc -- opendmarc	OpenDMARC through 1.3.2 and 1.4.x, when used with pypolicyd-spf 2.0.2, allows attacks that bypass SPF and DMARC authentication in situations where the HELO field is inconsistent with the MAIL FROM field.	2020-04-27	not yet calculated	<a href="#">CVE-2019-20790</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	OpenDMARC through 1.3.2 and 1.4.x allows attacks that inject authentication results to provide false information about			

opendmarc -- opendmarc	the domain that originated an e-mail message. This is caused by incorrect parsing and interpretation of SPF/DKIM authentication results, as demonstrated by the example.net(.example.com substring.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12272</a> <a href="#">MISC</a> <a href="#">MISC</a>
openldap -- openldap	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).	2020-04-28	not yet calculated	<a href="#">CVE-2020-12243</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a>
opensc -- opensc	OpenSC before 0.20.0 has a double free in coolkey_free_private_data because coolkey_add_object in libopensc/card-coolkey.c lacks a uniqueness check.	2020-04-29	not yet calculated	<a href="#">CVE-2019-20792</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openvpn -- openvpn	An issue was discovered in OpenVPN 2.4.x before 2.4.9. An attacker can inject a data channel v2 (P_DATA_V2) packet using a victim's peer-id. Normally such packets are dropped, but if this packet arrives before the data channel crypto parameters have been initialized, the victim's connection will be dropped. This requires careful timing due to the small time window (usually within a few seconds) between the victim client connection starting and the server PUSH_REPLY response back to the client. This attack will only work if Negotiable Cipher Parameters (NCP) is in use.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11810</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
opmantek -- open-audit	Open-Audit 3.3.0 allows an XSS attack after login.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12261</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There is Arbitrary file upload.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11943</a> <a href="#">MISC</a> <a href="#">MISC</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.3.1. There is shell metacharacter injection via attributes to an open-audit/configuration/ URI. An attacker can exploit this by adding an excluded IP address to the global discovery settings (internally called exclude_ip). This exclude_ip value is passed to the exec function in the discoveries_helper.php file (inside the all_ip_list function) without	2020-04-28	not yet calculated	<a href="#">CVE-2020-12078</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	being filtered, which means that the attacker can provide a payload instead of a valid IP address.			
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There are Multiple SQL Injections.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11942</a> <a href="#">MISC</a> <a href="#">MISC</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There is OS Command injection in Discovery.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11941</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2020-04-29	not yet calculated	<a href="#">CVE-2020-2575</a> <a href="#">MISC</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system	When user downloads PGP or S/MIME keys/certificates, exported file has same name for private and public keys. Therefore it's possible to mix them and to send private key to the third-party instead of public key. This issue affects ((OTRS)) Community Edition: 5.0.42 and prior versions, 6.0.27 and prior versions. OTRS: 7.0.16 and prior versions.	2020-04-28	not yet calculated	<a href="#">CVE-2020-1774</a> <a href="#">LIST</a> <a href="#">CONFIRM</a>
percona -- xtrabackup	Percona XtraBackup before 2.4.20 unintentionally writes the command line to any resulting backup file output. This may include sensitive arguments passed at run time. In addition, when --history is passed at run time, this command line is also written to the PERCONA_SCHEMA.xtrabackup_history table.	2020-04-27	not yet calculated	<a href="#">CVE-2020-10997</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
percona -- xtradb_cluster	An issue was discovered in Percona XtraDB Cluster before 5.7.28-31.42. A bundled script inadvertently sets a static transition_key for SST processes in place	2020-04-27	not yet calculated	<a href="#">CVE-2020-10996</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	of the random key expected.			<a href="#">CONFIRM</a>
php -- php	In PHP versions 7.2.x below 7.2.30, 7.3.x below 7.3.17 and 7.4.x below 7.4.5, if PHP is compiled with EBCDIC support (uncommon), urldecode() function can be made to access locations past the allocated memory, due to erroneously using signed numbers as array indexes.	2020-04-27	not yet calculated	<a href="#">CVE-2020-7067</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
php-fusion -- php-fusion	An XSS vulnerability exists in the banners.php page of PHP-Fusion 9.03.50. This can be exploited because the only security measure used against XSS is the stripping of SCRIPT tags. A malicious actor can use HTML event handlers to run JavaScript instead of using SCRIPT tags.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12438</a> <a href="#">MISC</a> <a href="#">MISC</a>
php-fusion -- php-fusion	PHP-Fusion 9.03.50 allows SQL Injection because maincore.php has an insufficient protection mechanism. An attacker can develop a crafted payload that can be inserted into the sort_order GET parameter on the members.php members search page. This parameter allows for control over anything after the ORDER BY clause in the SQL query.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12461</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phpgurukul -- online_course_registration	Online Course Registration 2.0 has multiple SQL injections that would can lead to a complete database compromise and authentication bypass in the login pages: admin/change-password.php, admin/check_availability.php, admin/index.php, change-password.php, check_availability.php, includes/header.php, index.php, and pincode-verification.php.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12429</a> <a href="#">MISC</a>
prestashop -- prestashop	The Correos Express addon for PrestaShop 1.6 through 1.7 allows remote attackers to obtain sensitive information, such as a service's owner password that can be used to modify orders via SOAP. Attackers can also retrieve information about orders or buyers.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12120</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	An integer overflow was found in QEMU 4.0.1 through 4.2.0 in the way it implemented ATI VGA emulation. This flaw occurs in the ati_2d_blt() routine in hw/display/ati-2d.c while handling MMIO write operations through the ati_mm_write() callback. A malicious guest could abuse this flaw to crash the QEMU process, resulting in a denial of	2020-04-27	not yet calculated	<a href="#">CVE-2020-11869</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



	service.			
re2c -- re2c	re2c before 2.0 has uncontrolled recursion that causes stack consumption in find_fixed_tags.	2020-04-29	not yet calculated	<a href="#">CVE-2018-21232</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible	An archive traversal flaw was found in all ansible-engine versions 2.9.x prior to 2.9.7, when running ansible-galaxy collection install. When extracting a collection .tar.gz file, the directory is created without sanitizing the filename. An attacker could take advantage to overwrite any file within the system.	2020-04-30	not yet calculated	<a href="#">CVE-2020-10691</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
red_hat -- undertow	A file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in Undertow version 2.0.29.Final and before and was fixed in 2.0.30.Final. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution.	2020-04-28	not yet calculated	<a href="#">CVE-2020-1745</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel V2.5.2, attackers can upload an arbitrary file to the server just changing the the content-type value. As a result of that, an attacker can execute a command on the server. This specific attack only occurs with the Maintenance Mode setting.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11817</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel 2.5.2, users' passwords and usernames are stored in a cookie with URL encoding, base64 encoding, and hashing. Thus, an attacker can easily apply brute force on them.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11821</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel 2.5.2, there is a stored XSS vulnerability on the application structure --> user access groups page. Thus, an attacker can inject malicious script to steal all users' valuable data.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11822</a> <a href="#">MISC</a>
	In Rundeck before version 3.2.6, authenticated users can craft a request that reveals Execution data and logs and Job details that they are not authorized to see. Depending on the configuration and the way that Rundeck is used, this could result in anything between a high severity risk, or a very low risk. If access is tightly			

rundeck -- rundeck	restricted and all users on the system have access to all projects, this is not really much of an issue. If access is wider and allows login for users that do not have access to any projects, or project access is restricted, there is a larger issue. If access is meant to be restricted and secrets, sensitive data, or intellectual property are exposed in Rundeck execution output and job data, the risk becomes much higher. This vulnerability is patched in version 3.2.6	2020-04-29	not yet calculated	<a href="#">CVE-2020-11009</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
saltstack -- salt	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class allows access to some methods that improperly sanitize paths. These methods allow arbitrary directory access to authenticated users.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11652</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
saltstack -- salt	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11651</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- erp	Egypt localized withholding tax reports Clearing of Liabilities and Remittance Statement and Summary in SAP ERP (versions 618, 730, EAPPLGLO 607) and S/4 HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user, allowing reading or modification of some tax reports, due to Missing Authorization Check.	2020-04-24	not yet calculated	<a href="#">CVE-2020-6212</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver_as_abap_business_server_pages_test_application	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_PHTMLB, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754 is vulnerable to reflected application Scripting (XSS) via different URL parameters as it does not sufficiently encode user controlled inputs.	2020-04-24	not yet calculated	<a href="#">CVE-2020-6213</a> <a href="#">MISC</a> <a href="#">MISC</a>
simple_ledger -- electron-cash-slp	Electron-Cash-SLP before version 3.6.2 has a vulnerability. All token creators that use the "Mint Tool" feature of the Electron Cash SLP Edition are at risk of sending the minting authority baton to the wrong SLP address. Sending the mint baton to	2020-04-28	not yet calculated	<a href="#">CVE-2020-11014</a> <a href="#">MISC</a> <a href="#">MISC</a>

	the wrong address will give another party the ability to issue new tokens or permanently destroy future minting capability. This is fixed version 3.6.2.			<a href="#">MISC CONFIRM</a>
simplisafe -- ss3_devices	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to pair a rogue keypad to an armed system.	2020-05-02	not yet calculated	<a href="#">CVE-2020-5727 CONFIRM</a>
solarwinds -- webhelpdesk	Formula Injection exists in the export feature in SolarWinds WebHelpDesk 12.7.1 via a value (provided by a low-privileged user in the Subject field of a help request form) that is mishandled in a TicketActions/view?tab=group TSV export by an admin user.	2020-04-27	not yet calculated	<a href="#">CVE-2019-20002 MISC</a>
sourcegraph -- sourcegraph	Sourcegraph before 3.15.1 has a vulnerable authentication workflow because of improper validation in the SafeRedirectURL method in cmd/frontend/auth/redirect.go, such as for the //foo//example.com substring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12283 CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
suap -- suap	SUAP V2 allows XSS during the update of user information.	2020-04-29	not yet calculated	<a href="#">CVE-2019-7634 MISC</a>
suculent -- think-device-api	A vulnerability has been disclosed in thinx-device-api IoT Device Management Server before version 2.5.0. Device MAC address can be spoofed. This means initial registration requests without UDID and spoofed MAC address may pass to create new UDID with same MAC address. Full impact needs to be reviewed further. Applies to all (mostly ESP8266/ESP32) users. This has been fixed in firmware version 2.5.0.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11015 CONFIRM</a>
teampass -- teampass	The REST API functions in TeamPass 2.1.27.36 allow any user with a valid API token to bypass IP address whitelist restrictions via an X-Forwarded-For client HTTP header to the getIp function.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12477 MISC</a>
telegram -- telegram_desktop_and_telegram_group_and_chat_and_bot	Telegram Desktop through 2.0.1, Telegram through 6.0.1 for Android, and Telegram through 6.0.1 for iOS allow an attacker to perform a Denial of Service attack via a public URL or a group chat invitation URL.	2020-05-01	not yet calculated	<a href="#">CVE-2020-12474 MISC</a>
testlink -- testlink	In TestLink 1.9.20, the lib/cfields/cfieldsExport.php goback_url parameter causes a security risk because it depends on client input and is not	2020-04-27	not yet calculated	<a href="#">CVE-2020-12274 MISC</a>

	constrained to lib/cfields/cfieldsView.php at the web site associated with the session.			<a href="#">MISC</a>
testlink -- testlink	In TestLink 1.9.20, a crafted login.php viewer parameter exposes cleartext credentials.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12273</a> <a href="#">MISC</a> <a href="#">MISC</a>
tiny_file_manager -- tiny_file_manager	In Tiny File Manager 2.4.1, there is a Path Traversal vulnerability in the ajax recursive directory listing functionality. This allows authenticated users to enumerate directories and files on the filesystem (outside of the application scope).	2020-04-28	not yet calculated	<a href="#">CVE-2020-12102</a> <a href="#">MISC</a> <a href="#">MISC</a>
tiny_file_manager -- tiny_file_manager	In Tiny File Manager 2.4.1 there is a vulnerability in the ajax file backup copy functionality which allows authenticated users to create backup copies of files (with .bak extension) outside the scope in the same directory in which they are stored.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12103</a> <a href="#">MISC</a> <a href="#">MISC</a>
torchbox -- wagtail	In Wagtail before versions 2.7.2 and 2.8.2, a potential timing attack exists on pages or documents that have been protected with a shared password through Wagtail's "Privacy" controls. This password check is performed through a character-by-character string comparison, and so an attacker who is able to measure the time taken by this check to a high degree of accuracy could potentially use timing differences to gain knowledge of the password. This is understood to be feasible on a local network, but not on the public internet. Privacy settings that restrict access to pages/documents on a per-user or per-group basis (as opposed to a shared password) are unaffected by this vulnerability. This has been patched in 2.7.3, 2.8.2, 2.9.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11037</a> <a href="#">CONFIRM</a>
ubiquiti -- unifi_cloud_key_devices	UniFi Cloud Key firmware <= v1.1.10 for Cloud Key gen2 and Cloud Key gen2 Plus contains a vulnerability that allows unrestricted root access through the serial interface (UART).	2020-05-02	not yet calculated	<a href="#">CVE-2020-8157</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
university_of_wisconsin -- htcondor	HTCondor up to and including stable series 8.8.6 and development series 8.9.4 has Incorrect Access Control. It is possible to use a different authentication method to submit a job than the administrator has specified. If the administrator has configured the READ or	2020-04-27	not yet calculated	<a href="#">CVE-2019-18823</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	WRITE methods to include CLAIMTOBE, then it is possible to impersonate another user to the condor_schedd. (For example to submit or remove jobs)			<a href="#">CONFIRM</a> <a href="#">MISC</a>
valve -- source	Valve Source allows local users to gain privileges by writing to the /tmp/hl2_relaunch file, which is later executed in the context of a different user account.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12242</a> <a href="#">MISC</a>
wavlink -- multiple_devices	An issue was discovered on WAVLINK WL-WN579G3 M79X3.V5030.180719, WL-WN575A3 RPT75A3.V4300.180801, and WL-WN530HG4 M30HG4.V5030.191116 devices. There are multiple externally accessible pages that do not require any sort of authentication, and store system information for internal usage. The devices automatically query these pages to update dashboards and other statistics, but the pages can be accessed externally without any authentication. All the pages follow the naming convention live_(string).shtml. Among the information disclosed is: interface status logs, IP address of the device, MAC address of the device, model and current firmware version, location, all running processes, all interfaces and their statuses, all current DHCP leases and the associated hostnames, all other wireless networks in range of the router, memory statistics, and components of the configuration of the device such as enabled features.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12266</a> <a href="#">MISC</a> <a href="#">MISC</a>
werner -- sqliteodbc	SQLiteODBC 0.9996, as packaged for certain Linux distributions as 0.9996-4, has a race condition leading to root privilege escalation because any user can replace a /tmp/sqliteodbc\$\$ file with new contents that cause loading of an arbitrary library.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12050</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">MISC</a>
wind_river -- vxworks	Wind River VxWorks tftp client library, as distributed in VxWorks 6.9 through 7 SR0630, has a double free	2020-04-27	not yet calculated	<a href="#">CVE-2020-10647</a> <a href="#">CONFIRM</a>
vmware -- esxi	ESXi 6.5 without patch ESXi650-201912104-SG and ESXi 6.7 without patch ESXi670-202004103-SG do not properly neutralize script-related HTML when viewing virtual machines attributes. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of	2020-04-29	not yet calculated	<a href="#">CVE-2020-3955</a> <a href="#">CONFIRM</a>



	8.3.			
wordpress -- wordpress	In affected versions of WordPress, a special payload can be crafted that can lead to scripts getting executed within the search block of the block editor. This requires an authenticated user with the ability to add content. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11030</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11028</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a vulnerability in the stats() method of class-wp-object-cache.php can be exploited to execute cross-site scripting (XSS) attacks. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11029</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	LearnPress Wordpress plugin version prior and including 3.2.6.7 is vulnerable to SQL Injection	2020-04-30	not yet calculated	<a href="#">CVE-2020-6010</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a cross-site scripting (XSS) vulnerability in the navigation section of Customizer allows JavaScript code to be executed. Exploitation requires an authenticated user. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11025</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

wordpress -- wordpress	The ninja-forms plugin before 3.4.24.2 for WordPress allows CSRF with resultant XSS.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12462</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, files with a specially crafted name when uploaded to the Media section can lead to script execution upon accessing the file. This requires an authenticated user with privileges to upload files. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11026</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11027</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
xerox -- multiple_workcentre_devices	Xerox WorkCentre 3655, 3655i, 58XX, 58XXi, 59XX, 59XXi, 6655, 6655i, 72XX, 72XXi, 78XX, 78XXi, 7970, and 7970i devices before 073.xxx.086.15410 do not properly escape parameters in the support/remoteUI/configui.php script, which can allow an unauthenticated attacker to execute OS commands on the device.	2020-04-29	not yet calculated	<a href="#">CVE-2016-11061</a> <a href="#">MISC</a>
xt:commerce -- xt:commerce	The address-management feature in xt:Commerce 5.1 to 6.2.2 allows remote authenticated users to zero out other user's stored addresses by manipulating an id field in the POST request for altering an address.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12101</a> <a href="#">FULLDISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zoom -- international_call_recording	ZOOM International Call Recording 6.3.1 suffers from multiple authenticated stored XSS vulnerabilities via the phoneNumber field in the (1) User Edit or (2) User Add form, (3) name field in the Role Add form, (4) name or number field in the Edit Group form, (5) tagKey or tagValue field in the Recording Rules Configuration, or (6) txt_69735:/VemailAddress/value or txt_75767:/VemailFrom/value field in	2020-04-27	not yet calculated	<a href="#">CVE-2019-18223</a> <a href="#">MISC</a>

	callrec/config.			
zte -- oscp	ZTE SDN controller platform is impacted by an information leakage vulnerability. Due to the program's failure to optimize the response of failure to the request, the caller can directly view the internal error code location of the component. Attackers could exploit this vulnerability to obtain sensitive information. This affects: OSCP versions V16.19.10 and V16.19.20.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6865</a> <a href="#">CONFIRM</a>
zte -- zenic_one_r22b_devices	ZTE's SDON controller is impacted by the resource management error vulnerability. When RPC is frequently called by other applications in the case of mass traffic data in the system, it will result in no response for a long time and memory overflow risk. This affects: ZENIC ONE R22b versions V16.19.10P02SP002 and V16.19.10P02SP005.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6867</a> <a href="#">CONFIRM</a>
zte -- zxctn_6500_devices	A ZTE product is impacted by a resource management error vulnerability. An attacker could exploit this vulnerability to cause a denial of service by issuing a specific command. This affects: ZXCTN 6500 version V2.10.00R3B87.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6866</a> <a href="#">CONFIRM</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [edigiovanna@sunnyvale.ca.gov](mailto:edigiovanna@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of April 27, 2020  
**Date:** Monday, May 04, 2020 10:19:55 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of April 27, 2020](#)

05/04/2020 06:45 AM EDT

Original release date: May 4, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atrifex -- jbig2dec	jbig2_image_compose in jbig2_image.c in Artifex jbig2dec before 0.18 has a heap-based buffer overflow.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12268</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Overlayfs in the Linux kernel and shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points. On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patches change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount	2020-04-24	<a href="#">7.2</a>	<a href="#">CVE-2019-15794</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	underflow.			
f5 -- big-iq	In BIG-IQ 6.0.0-7.0.0, a remote access vulnerability has been discovered that may allow a remote user to execute shell commands on affected systems using HTTP requests to the BIG-IQ user interface.	2020-04-24	10	<a href="#">CVE-2020-5868</a> <a href="#">MISC</a>
google -- openthread	OpenThread before 2019-12-13 has a stack-based buffer overflow in MeshCoP::Commissioner::GeneratePskc.	2020-04-28	7.5	<a href="#">CVE-2019-20791</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- ar3200_products	Huawei AR3200 products with versions of V200R007C00SPC900, V200R007C00SPCa00, V200R007C00SPCb00, V200R007C00SPCc00, V200R009C00SPC500 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device.	2020-04-27	7.5	<a href="#">CVE-2020-9068</a> <a href="#">CONFIRM</a>
ivanti -- avalanche	Ivanti Avalanche 6.3 allows a SQL injection that is vaguely associated with the Apache HTTP Server, aka Bug 683250.	2020-04-28	7.5	<a href="#">CVE-2020-12442</a> <a href="#">MISC</a>
mozilla -- firefox	A malicious extension could have called <code>browser.identity.launchWebAuthFlow</code> , controlling the <code>redirect_uri</code> , and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. This vulnerability affects Firefox < 75.	2020-04-24	7.5	<a href="#">CVE-2020-6823</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 75.	2020-04-24	7.5	<a href="#">CVE-2020-6826</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects	2020-04-24	7.5	<a href="#">CVE-2020-6825</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.			
netgear -- wnr854t_devices	NETGEAR WNR854T devices before 1.5.2 are affected by command execution.	2020-04-29	<a href="#">8.3</a>	<a href="#">CVE-2017-18855</a> <a href="#">CONFIRM</a>
node-rules -- node-rules	node-rules including 3.0.0 and prior to 5.0.0 allows injection of arbitrary commands. The argument rules of function "fromJSON()" can be controlled by users without any sanitization.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-7609</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
pixlcore -- pixl-class	pixl-class prior to 1.0.3 allows execution of arbitrary commands. The members argument of the create function can be controlled by users without any sanitization.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-7640</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qt -- qt	setMarkdown in Qt before 5.14.2 has a use-after-free related to QTextMarkdownImporter::insertBlock.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12267</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
shareit -- shareit	SHAREit through 4.0.6.177 does not check the body length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation.	2020-04-27	<a href="#">7.8</a>	<a href="#">CVE-2019-14941</a> <a href="#">MISC</a> <a href="#">MISC</a>
shareit -- shareit	SHAREit through 4.0.6.177 does not check the full message length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation. This is different from CVE-2019-14941.	2020-04-27	<a href="#">7.8</a>	<a href="#">CVE-2019-15234</a> <a href="#">MISC</a> <a href="#">MISC</a>
sophos -- xg_firewall_devices	A SQL injection issue was found in SFOS 17.0, 17.1, 17.5, and 18.0 before 2020-04-25 on Sophos XG Firewall devices, as exploited in the wild in April 2020. This affected devices configured with either the administration (HTTPS) service or the User Portal exposed on the WAN zone. A successful attack may have caused remote code execution that exfiltrated usernames and hashed passwords for the local device admin(s), portal admins, and user accounts used for remote access (but not external Active Directory or LDAP passwords)	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12271</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abbs -- software_audio_media_player	ABBS Software Audio Media Player version 3.1 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	<a href="#">6.8</a>	<a href="#">CVE-2019-5621</a> <a href="#">MISC</a>
admidio -- admidio	SQL Injection was discovered in Admidio before version 3.3.13. The main cookie parameter is concatenated into a SQL query without any input validation/sanitization, thus an attacker without logging in, can send a GET request with arbitrary SQL queries appended to the cookie parameter and execute SQL queries. The vulnerability impacts the confidentiality of the system. This has been patched in version 3.3.13.	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2020-11004</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
apache -- ats	Apache ATS 6.0.0 to 6.2.3, 7.0.0 to 7.1.9, and 8.0.0 to 8.0.6 is vulnerable to a HTTP/2 slow read attack.	2020-04-27	<a href="#">5</a>	<a href="#">CVE-2020-9481</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
apache -- log4j	Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-9488</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
apache -- ofbiz	Apache OFBiz 17.12.01 is vulnerable to Host header injection by accepting arbitrary host	2020-04-30	<a href="#">5</a>	<a href="#">CVE-2019-12425</a> <a href="#">CONFIRM</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12130</a> <a href="#">MISC</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12129</a> <a href="#">MISC</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12131</a> <a href="#">MISC</a>
avira -- antivirus	Avira Antivirus before 5.0.2003.1821 on Windows allows privilege escalation or a denial of service via abuse of a symlink.	2020-04-26	<a href="#">4.6</a>	<a href="#">CVE-2020-12254</a> <a href="#">MISC</a>
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shiftfs_btrfs_ioctl_fd_replace() installs an fd referencing a file from the lower filesystem without taking an additional	2020-04-24	<a href="#">4.6</a>	<a href="#">CVE-2019-15791</a> <a href="#">MISC</a> <a href="#">MISC</a>

	reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a refcount underflow.			<a href="#">MISC</a>
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shiftfs_btrfs_ioctl_fd_replace() calls fdget(oldfd), then without further checks passes the resulting file* into shiftfs_real_fdget(), which casts file->private_data, a void* that points to a filesystem-dependent type, to a "struct shiftfs_file_info *". As the private_data is not required to be a pointer, an attacker can use this to cause a denial of service or possibly execute arbitrary code.	2020-04-24	<a href="#">4.6</a>	<a href="#">CVE-2019-15792</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into init_user_ns, whereas they should have been translated into the s_user_ns for the lower filesystem. This resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts s_user_ns. A local attacker could use this to possibly bypass discretionary access control permissions.	2020-04-24	<a href="#">4.6</a>	<a href="#">CVE-2019-15793</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Improper authorization vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote authenticated attackers to alter the application's data via the applications 'E-mail' and 'Messages'.	2020-04-28	<a href="#">4</a>	<a href="#">CVE-2020-5566</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Improper input validation vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows a remote authenticated attacker to alter the application's data via the applications 'Workflow' and 'MultiReport'.	2020-04-28	<a href="#">4</a>	<a href="#">CVE-2020-5565</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Server-side request forgery (SSRF) vulnerability in Cybozu Garoon 4.6.0 to 4.6.3 allows a remote attacker with an administrative privilege to issue arbitrary HTTP requests to other web servers via V-CUBE Meeting function.	2020-04-28	<a href="#">4</a>	<a href="#">CVE-2020-5562</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Improper authentication vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in Application Menu.	2020-04-28	<a href="#">5</a>	<a href="#">CVE-2020-5567</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Improper authentication vulnerability in			<a href="#">CVE-2020-</a>

cybozu -- garoon	Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in the affected product via the API.	2020-04-28	<a href="#">5</a>	<a href="#">5563</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to inject arbitrary web script or HTML via the application 'E-mail'.	2020-04-28	<a href="#">4.3</a>	<a href="#">CVE-2020-5564</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.6.0 to 5.0.0 allows remote attackers to inject arbitrary web script or HTML via the applications 'Messages' and 'Bulletin Board'.	2020-04-28	<a href="#">4.3</a>	<a href="#">CVE-2020-5568</a> <a href="#">MISC</a> <a href="#">MISC</a>
dong_joo_cho -- file_transfer_ifamily	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the ./etc/ path.	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2020-12128</a> <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer.	2020-04-24	<a href="#">4.8</a>	<a href="#">CVE-2020-5870</a> <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit.	2020-04-24	<a href="#">6.4</a>	<a href="#">CVE-2020-5869</a> <a href="#">MISC</a>
gnu -- mailman	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12137</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12245</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	Grafana version < 6.7.3 is vulnerable for annotation popup XSS.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-12052</a> <a href="#">CONFIRM</a>
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 2	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1805</a> <a href="#">CONFIRM</a>

	out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1806.			
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 1 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1805 and CVE-2020-1806.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1804</a> <a href="#">CONFIRM</a>
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 3 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1805.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1806</a> <a href="#">CONFIRM</a>
huawei -- lion- al00c_devices	Huawei smartphone Lion-AL00C with versions earlier than 10.0.0.205(C00E202R7P2) have a denial of service vulnerability. An attacker crafted specially file to the affected device. Due to insufficient input validation of the value when executing the file, successful exploit may cause device abnormal.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-1880</a> <a href="#">CONFIRM</a>
huawei -- pcmanager	Huawei PCManager product with versions earlier than 10.0.5.53 have a local privilege escalation vulnerability. An authenticated, local attacker can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	2020-04-27	<a href="#">4.6</a>	<a href="#">CVE-2020-1845</a> <a href="#">CONFIRM</a>
ibm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 173310.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2019-4750</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
	IBM Cloud App Management 2019.3.0			



ibm -- cloud_app_management	and 2019.4.0 reveals a stack trace on certain API requests which can allow an attacker further information about the implementation of the offering. IBM X-Force ID: 173311.	2020-04-24	5	<a href="#">CVE-2019-4751</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 172519.	2020-04-27	4	<a href="#">CVE-2019-4729</a> <a href="#">XE</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- mq_appliance	IBM MQ and MQ Appliance 8.0, 9.1 LTS, and 9.1 CD could allow an authenticated user cause a denial of service due to a memory leak. IBM X-Force ID: 175840.	2020-04-24	4	<a href="#">CVE-2020-4267</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server_and_liberty	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 20.0.0.4 could allow a remote, authenticated attacker to obtain sensitive information, caused by improper parameter checking. This could be exploited to conduct spoofing attacks. IBM X-Force ID: 177841.	2020-04-28	4	<a href="#">CVE-2020-4329</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows session fixation via an alphanumeric value in a session cookie.	2020-04-29	6.4	<a href="#">CVE-2020-12467</a> <a href="#">MISC</a>
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows CSV injection via a phrase value within a language. This is related to phrases/add/ and languages/download/.	2020-04-29	6.8	<a href="#">CVE-2020-12468</a> <a href="#">MISC</a>
mailbeez -- mailbeez	Cross-site scripting (XSS) vulnerability in mailhive/cloudbeez/cloudloader.php and mailhive/cloudbeez/cloudloader_core.php in the MailBeez plugin for ZenCart before 3.9.22 allows remote attackers to inject arbitrary web script or HTML via the cloudloader_mode parameter.	2020-04-30	4.3	<a href="#">CVE-2020-6579</a> <a href="#">MISC</a>
mozilla -- firefox_esr	When following a link that opened an intent://-schemed URL, causing a custom tab to be opened, Firefox for Android could be tricked into displaying the incorrect URI.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	2020-04-24	4.3	<a href="#">CVE-2020-6827</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A malicious Android application could craft an Intent that would have been processed by Firefox for Android and potentially result in a file overwrite in the user's profile directory. One exploitation			

mozilla -- firefox_esr	vector for this would be to supply a user.js file providing arbitrary malicious preference values. Control of arbitrary preferences can lead to sufficient compromise such that it is generally equivalent to arbitrary code execution.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	2020-04-24	6.4	<a href="#">CVE-2020-6828</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	When reading from areas partially or fully outside the source resource with WebGL's <code>copyTexSubImage</code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	5	<a href="#">CVE-2020-6821</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	6.8	<a href="#">CVE-2020-6820</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	6.8	<a href="#">CVE-2020-6819</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code>GMPDecodeData</code> . It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	6.8	<a href="#">CVE-2020-6822</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgate -- pfsense	An XSS vulnerability resides in the hostname field of the diag_ping.php page in pfsense before 2.4.5 version. After passing inputs to the command and executing this command, the \$result variable is not sanitized before it is printed.	2020-04-29	4.3	<a href="#">CVE-2020-10797</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear --	Certain NETGEAR devices are affected by a stack-based buffer overflow by an	2020-04-		<a href="#">CVE-2017-</a>

multiple_devices	authenticated user. This affects R6100 before 1.0.1.20, R7800 before 1.0.2.40, and R9000 before 1.0.2.52.	24	<a href="#">5.2</a>	<a href="#">18698 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21213 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21194 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21193 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects EX3700 before 1.0.0.66, EX3800 before 1.0.0.66, EX6100 before 1.0.2.20, EX6120 before 1.0.0.34, EX6150 before 1.0.0.36, EX6200 before 1.0.3.84, and EX7000 before 1.0.0.60.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2017-18715 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, EX6100v2 before 1.0.1.50, EX6150v2 before 1.0.1.50, EX6200v2 before 1.0.1.44, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60,	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2018-21228 CONFIRM</a>

	R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.2.30, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18723</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1., JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98,	2020-04-24	<a href="#">4.8</a>	<a href="#">CVE-2018-21230</a> <a href="#">CONFIRM</a>

	WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.			
netgear -- multiple_devices	<p>Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1.78, JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.</p>	2020-04-24	<a href="#">4.8</a>	<a href="#">CVE-2018-21231</a> <a href="#">CONFIRM</a>



netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6400 before 1.0.0.60, D7000 before 1.0.1.50, D8500 before 1.0.3.29, EX6200 before 1.0.3.84, EX7000 before 1.0.0.60, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R9000 before 1.0.2.52, WNDR3400v3 before 1.0.1.16, WNR3500Lv2 before 1.2.0.46, and WNDR3700v5 before 1.1.0.48.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2017-18700</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D1500 before 1.0.0.25, D500 before 1.0.0.25, D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, EX6100v2 before 1.0.1.60, EX6150v2 before 1.0.1.60, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.16, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.18, R6020 before 1.0.0.26, R6050 before 1.0.1.16, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6220 before 1.1.0.60, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3700v5 before 1.1.0.48, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.46, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2017-18703</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18727</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92,	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21189</a>

	WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21191</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18722</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21187</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18729</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18728</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18726</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18725</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18724</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21192</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R6400v2 before 1.0.2.34, R6700 before 1.0.1.30, R6900 before 1.0.1.30, R6900P before 1.0.0.62, R7000 before 1.0.9.12, R7000P before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2018-21227</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21173</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18721</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21216</a> <a href="#">CONFIRM</a>

	1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.			
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18718</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18717</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18716</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18730</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18705</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.28, EX2700 before 1.0.1.32, EX6200v2 before 1.0.1.56, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.52, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and	2020-04-28	<a href="#">6.5</a>	<a href="#">CVE-2018-21181</a> <a href="#">CONFIRM</a>

	WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">6.5</a>	<a href="#">CVE-2018-21177</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, and WNR2000v5 before 1.0.0.58.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18731</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX2700 before 1.0.1.28, R7800 before 1.0.2.40, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2018-21170</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21190</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.98.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21171</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21180</a> <a href="#">CONFIRM</a>



netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21179</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21178</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21172</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.94.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21182</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, and R9000 before 1.0.2.52.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21221</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21217</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18720</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected			

netgear -- multiple_devices	by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.1.00.26, R6080 before 1.1.00.26; R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	<a href="#">CVE-2017-18719</a> <a href="#">CONFIRM</a>
netgear -- r6220_devices	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	2020-04-24	4.8	<a href="#">CVE-2017-18702</a> <a href="#">CONFIRM</a>
netgear -- r6700_and_r6900_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	2020-04-24	4.3	<a href="#">CVE-2017-18701</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04-24	5.2	<a href="#">CVE-2017-18699</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.3.6.	2020-04-28	5.2	<a href="#">CVE-2018-21200</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04-24	5.2	<a href="#">CVE-2017-18697</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	5.2	<a href="#">CVE-2018-21099</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	5.2	<a href="#">CVE-2018-21098</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.46 are affected by incorrect configuration of security settings.	2020-04-27	5.8	<a href="#">CVE-2018-21158</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-27	5.2	<a href="#">CVE-2018-21100</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020-04-24	4.6	<a href="#">CVE-2017-18709</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04-24	5.2	<a href="#">CVE-2017-18707</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by CSRF. This affects R8300 before	2020-04-24	6.8	<a href="#">CVE-2017-18708</a>

	1.0.2.94 and R8500 before 1.0.2.94.			<a href="#">CONFIRM</a>
pegasystems -- pega_platform	Pega Platform before version 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability in the comment tags.	2020-04-29	<a href="#">6</a>	<a href="#">CVE-2020-8775</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
pegasystems -- pega_platform	The Richtext Editor in Pega Platform before 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability.	2020-04-29	<a href="#">6</a>	<a href="#">CVE-2020-8773</a> <a href="#">CONFIRM</a>
pegasystems -- pega_platform	Pega Platform before version 8.2.6 is affected by a Reflected Cross-Site Scripting vulnerability in the "ActionStringID" function.	2020-04-29	<a href="#">6.8</a>	<a href="#">CVE-2020-8774</a> <a href="#">CONFIRM</a>
red_hat -- openshift_container_platform	A flaw was found in openshift-ansible. OpenShift Container Platform (OCP) 3.11 is too permissive in the way it specified CORS allowed origins during installation. An attacker, able to man-in-the-middle the connection between the user's browser and the openshift console, could use this flaw to perform a phishing attack. The main threat from this vulnerability is data confidentiality.	2020-04-24	<a href="#">4</a>	<a href="#">CVE-2020-1741</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	An issue was discovered in Sonatype Nexus Repository Manager 2.x before 2.14.17 and 3.x before 3.22.1. Admin users can retrieve the LDAP server system username/password (as configured in nxrm) in cleartext.	2020-04-27	<a href="#">4</a>	<a href="#">CVE-2020-11415</a> <a href="#">CONFIRM</a>
teampass -- teampass	TeamPass 2.1.27.36 allows an unauthenticated attacker to retrieve files from the TeamPass web root. This may include backups or LDAP debug files.	2020-04-29	<a href="#">5</a>	<a href="#">CVE-2020-12478</a> <a href="#">MISC</a>
teampass -- teampass	TeamPass 2.1.27.36 allows any authenticated TeamPass user to trigger a PHP file include vulnerability via a crafted HTTP request with sources/users.queries.php newValue directory traversal.	2020-04-29	<a href="#">6.5</a>	<a href="#">CVE-2020-12479</a> <a href="#">MISC</a>
whoopsie_project -- whoopsie	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12135</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
windriver -- vxworks	The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference.	2020-04-27	<a href="#">5</a>	<a href="#">CVE-2020-10664</a> <a href="#">CONFIRM</a>
wordpress --	The Advanced Woo Search plugin version through 1.99 for Wordpress suffers from a sensitive information	2020-04-		<a href="#">CVE-2020-12070</a>

wordpress	disclosure vulnerability in every ajax search request via the sql field to includes/class-aws-search.php.	24	5	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
-----------	---	----	---	--

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bluezone_global -- bluezone	React Native Bluetooth Scan in Bluezone 1.0.0 uses six-character alphanumeric IDs, which might make it easier for remote attackers to interfere with COVID-19 contact tracing by using many IDs.	2020-04-27	<a href="#">3.3</a>	<a href="#">CVE-2020-12270</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
croogo -- croogo	Croogo before 3.0.7 allows XSS via the title to admin/menus/menus or admin/taxonomy/vocabularies.	2020-04-26	<a href="#">3.5</a>	<a href="#">CVE-2019-20789</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.188(C00E74R3P8) have an improper authorization vulnerability. The software does not properly restrict certain user's modification of certain configuration file, successful exploit could allow the attacker to bypass app lock after a series of operation in ADB mode.	2020-04-27	<a href="#">3.6</a>	<a href="#">CVE-2020-1807</a> <a href="#">CONFIRM</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly sensitive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160514.	2020-04-29	<a href="#">2.1</a>	<a href="#">CVE-2019-4286</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly sensitive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160631.	2020-04-29	<a href="#">2.1</a>	<a href="#">CVE-2019-4288</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
mozilla -- firefox	Initially, a user opens a Private Browsing Window and generates a password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new password - the generated passwords would have been identical, rather than	2020-04-24	<a href="#">1.9</a>	<a href="#">CVE-2020-6824</a> <a href="#">MISC</a> <a href="#">MISC</a>

	independent. This vulnerability affects Firefox < 75.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R6900P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8500 before 1.0.2.106, R8300 before 1.0.2.106, and WNDR3400v3 before 1.0.1.16.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18704 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18712 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18713 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R7500v2 before 1.0.3.20, R7800 before 1.0.2.38, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2018-21229 CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18710 CONFIRM</a>
netgear -- srr60_and_srs60_devices	Certain NETGEAR devices are affected by stored XSS. This affects SRR60 before 2.2.1.210 and SRS60 before 2.2.1.210.	2020-04-27	<a href="#">2.3</a>	<a href="#">CVE-2018-21095 CONFIRM</a>
netgear -- wndr4500_devices	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18714 CONFIRM</a>



ni_consulting -- sales_force_assistant	Cross-site scripting vulnerability in Sales Force Assistant version 11.2.48 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-04-28	3.5	<a href="#">CVE-2020-5570</a> <a href="#">JVN</a> <a href="#">MISC</a> <a href="#">MISC</a>
---	---	------------	-----	--

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a-pdf_wav -- a-pdf_wav	A-PDF WAV to MP3 version 1.0.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5618</a> <a href="#">MISC</a>
aasync -- aasync	AASync.com AASync version 2.2.1.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5619</a> <a href="#">MISC</a>
abb -- microscada_pro_sys600	ABB MicroSCADA Pro SYS600 version 9.3 suffers from an instance of CWE-306: Missing Authentication for Critical Function.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5620</a> <a href="#">MISC</a>
abb -- multiple_products	Insufficient folder permissions used by system functions in ABB System 800xA products OPCServer for AC800M (versions 6.0 and earlier) and Control Builder M Professional, MMSServer for AC800M, Base Software for SoftControl (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploited the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8472</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2, Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS	2020-04-29	not yet calculated	<a href="#">CVE-2020-8476</a> <a href="#">CONFIRM</a>

	Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, a weakness in validation of input exists that allows an attacker to alter licenses assigned to the system nodes by sending specially crafted messages to the CLS web service.			<a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, weak file permissions allow an authenticated attacker to block the license handling, escalate his/her privileges and execute arbitrary code.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8471</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS	2020-04-29	not yet calculated	<a href="#">CVE-2020-8475</a> <a href="#">CONFIRM</a>

	Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, a weakness in validation of input exists that allows an attacker to block license handling by sending specially crafted messages to the CLS web service.			<a href="#">CONFIRM</a>
abb -- multiple_products	For ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, confidential data is written in an unprotected file. An attacker who successfully exploited this vulnerability could take full control of the computer.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8481</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and	2020-04-29	not yet calculated	<a href="#">CVE-2020-8479</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	6.1, Composer CTK 6.1 and 6.2, AdvBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, an XML External Entity Injection vulnerability exists that allows an attacker to read or call arbitrary files from the license server and/or from the network and also block the license handling.			
abb -- system_800xa_base	Insufficient protection of the inter-process communication functions in ABB System 800xA Base (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8487</a> <a href="#">CONFIRM</a>
abb -- system_800xa_base	Insufficient folder permissions used by system functions in ABB System 800xA Base (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploit the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8473</a> <a href="#">CONFIRM</a>
abb -- system_800xa_batch_management	Insufficient protection of the inter-process communication functions in ABB System 800xA Batch Management (all published versions) enables an attacker authenticated on the local system to inject data, affecting User Interface update during batch execution and/or compare/printing functionalities.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8488</a> <a href="#">CONFIRM</a>
abb -- system_800xa_for_dci	Insufficient protection of the inter-process communication functions in ABB System 800xA for DCI (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8484</a> <a href="#">CONFIRM</a>
abb -- system_800xa_for_mod_300	Insufficient protection of the inter-process communication functions in ABB System 800xA for MOD 300 (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8485</a> <a href="#">CONFIRM</a>
	Insufficient protection of the inter-process communication functions in ABB System 800xA Information Management (all			

abb -- system_800xa_information_management	published versions) enables an attacker authenticated on the local system to inject data, affecting the runtime values to be stored in the archive, or making Information Management history services unavailable.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8489</a> <a href="#">CONFIRM</a>
abb -- system_800xa_products	Insufficient protection of the inter-process communication functions in ABB System 800xA products OPC Server for AC 800M, MMS Server for AC 800M and Base Software for SoftControl (all published versions) enables an attacker authenticated on the local system to inject data, affecting the online view of runtime data shown in Control Builder.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8478</a> <a href="#">CONFIRM</a>
abb -- system_800xa_rnrp	Insufficient protection of the inter-process communication functions in ABB System 800xA RNRP (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8486</a> <a href="#">CONFIRM</a>
accellion -- file_transfer_appliance	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').	2020-04-29	not yet calculated	<a href="#">CVE-2019-5623</a> <a href="#">MISC</a>
accellion -- file_transfer_appliance	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-798: Use of Hard-coded Credentials.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5622</a> <a href="#">MISC</a>
amd -- ati_atilk64.sys	AMD ATI atilk64.sys 5.11.9.0 allows low-privileged users to interact directly with physical memory by calling one of several driver routines that map physical memory into the virtual address space of the calling process. This could enable low-privileged users to achieve NT AUTHORITY\SYSTEM privileges via a DeviceIoControl call associated with MmMapIoSpace, IoAllocateMdl, MmBuildMdlForNonPagedPool, or MmMapLockedPages.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12138</a> <a href="#">MISC</a> <a href="#">MISC</a>
apache -- iotdb	An issue was found in Apache IoTDB .9.0 to 0.9.1 and 0.8.0 to 0.8.2. When starting IoTDB, the JMX port 31999 is exposed with no certification. Then, clients could execute code remotely.	2020-04-27	not yet calculated	<a href="#">CVE-2020-1952</a> <a href="#">CONFIRM</a>
apache -- nifi_registry	If NiFi Registry 0.1.0 to 0.5.0 uses an authentication mechanism other than PKI, when the user clicks Log Out, NiFi Registry invalidates the authentication token on the client side but not on the	2020-04-	not yet	<a href="#">CVE-2020-9482</a>



	server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to NiFi Registry.	28	calculated	<a href="#">CONFIRM</a>
apache -- ofbiz	Apache OFBiz 17.12.01 is vulnerable to some CSRF attacks.	2020-04-30	not yet calculated	<a href="#">CVE-2019-0235</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
apache -- tika	A carefully crafted or corrupt file may trigger a System.exit in Tika's OneNote Parser. Crafted or corrupted files can also cause out of memory errors and/or infinite loops in Tika's ICNSParser, MP3Parser, MP4Parser, SAS7BDATParser, OneNoteParser and ImageParser. Apache Tika users should upgrade to 1.24.1 or later. The vulnerabilities in the MP4Parser were partially fixed by upgrading the com.googlecode.isoparser:1.1.22 dependency to org.tallison:isoparser:1.9.41.2. For unrelated security reasons, we upgraded org.apache.cxf to 3.3.6 as part of the 1.24.1 release.	2020-04-27	not yet calculated	<a href="#">CVE-2020-9489</a> <a href="#">MISC</a>
apport -- apport	Apport reads and writes information on a crashed process to /proc/pid with elevated privileges. Apport then determines which user the crashed process belongs to by reading /proc/pid through get_pid_info() in data/apport. An unprivileged user could exploit this to read information about a privileged running process by exploiting PID recycling. This information could then be used to obtain ASLR offsets for a process with an existing memory corruption vulnerability. The initial fix introduced regressions in the Python Apport library due to a missing argument in Report.add_proc_envIRON in apport/report.py. It also caused an autopkgtest failure when reading /proc/pid and with Python 2 compatibility by reading /proc maps. The initial and subsequent regression fixes are in 2.20.11-0ubuntu16, 2.20.11-0ubuntu8.6, 2.20.9-0ubuntu7.12, 2.20.1-0ubuntu2.22 and 2.14.1-0ubuntu3.29+esm3.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15790</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
b&r_industrial_automation --	A directory traversal vulnerability in SharpZipLib used in the upgrade service in B&R Automation Studio versions 4.0.x,	2020-04-	not yet	<a href="#">CVE-2019-19102</a>

b&r_automation_studio	4.1.x and 4.2.x allow unauthenticated users to write to certain local directories. The vulnerability is also known as zip slip.	29	calculated	<a href="#">CONFIRM</a>
b&r_industrial_automation -- b&r_automation_studio	A privilege escalation vulnerability in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.4SP, < 4.6.3SP, < 4.7.2 and < 4.8.1 allow authenticated users to delete arbitrary files via an exposed interface.	2020-04-29	not yet calculated	<a href="#">CVE-2019-19100</a> <a href="#">CONFIRM</a>
b&r_industrial_automation -- b&r_automation_studio	A missing secure communication definition and an incomplete TLS validation in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.5SP, < 4.6.4 and < 4.7.2 enable unauthenticated users to perform MITM attacks via the B&R upgrade server.	2020-04-29	not yet calculated	<a href="#">CVE-2019-19101</a> <a href="#">CONFIRM</a>
beeline -- smart_box	Beeline Smart Box 2.0.38 routers allow "Advanced settings > Other > Diagnostics" OS command injection via the Ping ping_ipaddr parameter, the Nslookup nslookup_ipaddr parameter, or the Traceroute traceroute_ipaddr parameter.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12246</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.6 allows remote attackers to read arbitrary files because the presfilename (lowercase) value can be a .pdf filename while the presFilename (mixed case) value has a ../ sequence. This can be leveraged for privilege escalation via a directory traversal to bigbluebutton.properties. NOTE: this issue exists because of an ineffective mitigation to CVE-2020-12112 in which there was an attempted fix within an NGINX configuration file, without considering that the relevant part of NGINX is case-insensitive.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12443</a> <a href="#">MISC</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection (issue 2 of 2).	2020-04-30	not yet calculated	<a href="#">CVE-2019-19220</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19217</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 has Insecure Password Storage.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19218</a> <a href="#">MISC</a>
	A buffer overflow vulnerability in BMC Control-M/Agent 7.0.00.000 when the On-Do action destination is Mail and the			<a href="#">CVE-2019-</a>

bmc -- control-m/agent	Control-M/Agent is configured to send the email, allows remote attackers to have unspecified impact via vectors related to the configured IP address or SMTP server.	2020-04-30	not yet calculated	<a href="#">19215</a> <a href="#">MISC</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 has an Insecure File Copy.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19216</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows Arbitrary File Download.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19219</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 1 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11675</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 allows variable reuse, possibly causing data corruption.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11674</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 3 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11677</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 2 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11676</a> <a href="#">MISC</a>
cisco -- ios_xe_sd-wan_software	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16011</a> <a href="#">CISCO</a>
dom4j -- dom4j	dom4j before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.	2020-05-01	not yet calculated	<a href="#">CVE-2020-10683</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ebiz4u -- ebiz4u	AxECM.cab(ActiveX Control) in Inogard Ebiz4u contains a vulnerability that could allow remote files to be downloaded and executed by setting arguments to the activeX method. Download of Code Without Integrity Check vulnerability in ActiveX control of Inogard Co.,LTD Ebiz4u ActiveX of Inogard	2020-04-29	not yet calculated	<a href="#">CVE-2019-19165</a> <a href="#">CONFIRM</a>

	Co.,LTD(AxECM.cab) allows ATTACKER to cause a file download to Windows user's folder and execute. This issue affects: Inogard Co.,LTD Ebiz4u ActiveX of Inogard Co.,LTD(AxECM.cab) version 1.0.5.0 and later versions on windows 7/8/10.			<a href="#">CONFIRM</a>
eset -- antivirus_and_antispyware_module	ESET Antivirus and Antispyware Module module 1553 through 1560 allows a user with limited access rights to create hard links in some ESET directories and then force the product to write through these links into files that would normally not be write-able by the user, thus achieving privilege escalation.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11446</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, when a virtual server is configured with HTTP explicit proxy and has an attached HTTP_PROXY_REQUEST iRule, POST requests sent to the virtual server cause an xdata memory leak.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5883</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5, and 11.6.1-11.6.5.1, under certain conditions, the Intel QuickAssist Technology (QAT) cryptography driver may produce a Traffic Management Microkernel (TMM) core file.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5882</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.4, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the default deployment mode for BIG-IP high availability (HA) pair mirroring is insecure. This is a control plane issue that is exposed only on the network used for mirroring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5884</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, a race condition exists where mcpd and other processes may make unencrypted connection attempts to a new configuration sync peer. The race condition can occur when changing the ConfigSync IP address of a peer, adding a new peer, or when the Traffic Management Microkernel (TMM) first starts up.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5876</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.2.3, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.4.1, when processing TLS traffic with hardware cryptographic acceleration	2020-04-	not yet	<a href="#">CVE-2020-5872</a>

	enabled on platforms with Intel QAT hardware, the Traffic Management Microkernel (TMM) may stop responding and cause a failover event.	30	calculated	<a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3 and 14.1.0-14.1.2.3, the restjavad process may expose a way for attackers to upload arbitrary files on the BIG-IP system, bypassing the authorization system. Resulting error messages may also reveal internal paths of the server.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5880</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.2.3, undisclosed requests can lead to a denial of service (DoS) when sent to BIG-IP HTTP/2 virtual servers. The problem can occur when ciphers, which have been blacklisted by the HTTP/2 RFC, are used on backend servers. This is a data-plane issue. There is no control-plane exposure.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5871</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1 and BIG-IQ 5.2.0-7.1.0, when creating a QKView, credentials for binding to LDAP servers used for remote authentication of the BIG-IP administrative interface will not fully obfuscate if they contain whitespace.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5890</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1 and 14.1.0-14.1.2.3, under certain conditions, the Traffic Management Microkernel (TMM) may generate a core file and restart while processing SSL traffic with an HTTP/2 full proxy.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5875</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, undisclosed HTTP/2 requests can lead to a denial of service when sent to a virtual server configured with the Fallback Host setting and a server-side HTTP/2 profile.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5891</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems setup for connection mirroring in a High Availability (HA) pair transfers sensitive cryptographic objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5886</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems set up for connection mirroring in a high availability (HA) pair transfer sensitive cryptographic	2020-04-	not yet	<a href="#">CVE-2020-5885</a>



	objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	30	calculated	<a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, malformed input to the DATAGRAM::tcp iRules command within a FLOW_INIT event may lead to a denial of service.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5877</a> <a href="#">CONFIRM</a>
f5 -- big-ip_and_big-iq	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.1-11.6.5 and BIG-IQ 5.2.0-7.1.0, a user associated with the Resource Administrator role who has access to the secure copy (scp) utility but does not have access to Advanced Shell (bash) can execute arbitrary commands using a maliciously crafted scp request.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5873</a> <a href="#">MISC</a>
f5 -- big-ip_apm	On BIG-IP APM 15.0.0-15.0.1.2, 14.1.0-14.1.2.3, and 14.0.0-14.0.1, in certain circumstances, an attacker sending specifically crafted requests to a BIG-IP APM virtual server may cause a disruption of service provided by the Traffic Management Microkernel(TMM).	2020-04-30	not yet calculated	<a href="#">CVE-2020-5874</a> <a href="#">CONFIRM</a>
f5 -- big-ip_apm	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, in BIG-IP APM portal access, a specially crafted HTTP request can lead to reflected XSS after the BIG-IP APM system rewrites the HTTP response from the untrusted backend server and sends it to the client.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5889</a> <a href="#">CONFIRM</a>
f5 -- big-ip_apm_and_edge_gateway_and_firepass	In versions 7.1.5-7.1.8, the BIG-IP Edge Client components in BIG-IP APM, Edge Gateway, and FirePass legacy allow attackers to obtain the full session ID from process memory.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5892</a> <a href="#">CONFIRM</a>
f5 -- big-ip_asm	On BIG-IP ASM 11.6.1-11.6.5.1, under certain configurations, the BIG-IP system sends data plane traffic to back-end servers unencrypted, even when a Server SSL profile is applied.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5879</a> <a href="#">CONFIRM</a>
f5 -- big-ip_edge_client	In versions 7.1.5-7.1.8, when a user connects to a VPN using BIG-IP Edge Client over an unsecure network, BIG-IP Edge Client responds to authentication requests over HTTP while sending probes for captive portal detection.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5893</a> <a href="#">CONFIRM</a>
	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.3, Traffic			<a href="#">CVE-2020-</a>

f5 -- big-ip_virtual_edition	Management Microkernel (TMM) may restart on BIG-IP Virtual Edition (VE) while processing unusual IP traffic.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5878</a> <a href="#">MISC</a>
f5 -- big-ip_virtual_edition	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for remote attackers to access local daemons and bypass port lockdown settings.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5887</a> <a href="#">CONFIRM</a>
f5 -- big-ip_virtual_edition	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when the BIG-IP Virtual Edition (VE) is configured with VLAN groups and there are devices configured with OSPF connected to it, the Network Device Abstraction Layer (NDAL) Interfaces can lock up and in turn disrupting the communication between the mcpd and tmm processes.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5881</a> <a href="#">CONFIRM</a>
f5 -- big-ip_virtual_edition	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for adjacent network (layer 2) attackers to access local daemons and bypass port lockdown settings.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5888</a> <a href="#">CONFIRM</a>
faye_gem_for_ruby_on_rails -- faye_gem_for_ruby_on_rails	Faye (NPM, RubyGem) versions greater than 0.5.0 and before 1.0.4, 1.1.3 and 1.2.5, has the potential for authentication bypass in the extension system. The vulnerability allows any client to bypass checks put in place by server-side extensions, by appending extra segments to the message channel. It is patched in versions 1.0.4, 1.1.3 and 1.2.5.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11020</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ffmpeg -- ffmpeg	cbs_jpeg_split_fragment in libavcodec/cbs_jpeg.c in FFmpeg 4.2.2 has a heap-based buffer overflow during JPEG_MARKER_SOS handling because of a missing length check.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12284</a> <a href="#">MISC</a> <a href="#">MISC</a>
fonality -- trixbox_community_edition	An OS Command Injection vulnerability in the endpoint_devicemap.php component of Fonality Trixbox Community Edition allows an attacker to execute commands on the underlying operating system as the "asterisk" user. Note that Trixbox Community Edition has been unsupported by the vendor since 2012. This issue affects: Fonality Trixbox Community Edition, versions 1.2.0 through 2.8.0.4. Versions 1.0 and 1.1 are unaffected.	2020-05-01	not yet calculated	<a href="#">CVE-2020-7351</a> <a href="#">MISC</a>
	An improper authentication vulnerability in FortiMail 5.4.10, 6.0.7, 6.2.2 and earlier			

fortiguard -- fortimail_and_foritvoiceenterprise	and FortiVoiceEnterprise 6.0.0 and 6.0.1 enterprise allow a remote unauthenticated attacker to access the system as a legitimate user by requesting a password change via the user interface.	2020-04-27	not yet calculated	<a href="#">CVE-2020-9294</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in accessing out-of-bounds memory leading to a kernel panic or other unpredictable results.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5614</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r357490, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r357489, and 11.3-RELEASE before 11.3-RELEASE-p7, incorrect use of a user-controlled pointer in the epair virtual network module allowed vnet jailed privileged users to panic the host system and potentially execute arbitrary code in the kernel.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7452</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in memory access after it has been freed leading to a kernel panic or other unpredictable results.	2020-04-29	not yet calculated	<a href="#">CVE-2019-15874</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356089, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r356090, and 11.3-RELEASE before 11.3-RELEASE-p7, driver specific ioctl command handlers in the oce network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to send passthrough commands to the device firmware.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15876</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356606 and 12.1-RELEASE before 12.1-RELEASE-p3, driver specific ioctl command handlers in the ixl network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to trigger updates to the device's non-volatile memory.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15877</a> <a href="#">CONFIRM</a>
	In FreeBSD 12.1-STABLE before r359021, 12.1-RELEASE before 12.1-			

freebsd -- freebsd	RELEASE-p3, 11.3-STABLE before r359020, and 11.3-RELEASE before 11.3-RELEASE-p7, a missing null termination check in the jail_set configuration option "osrelease" may return more bytes with a subsequent jail_get system call allowing a malicious jail superuser with permission to create nested jails to read kernel memory.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7453</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r358739, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r358740, and 11.3-RELEASE before 11.3-RELEASE-p7, a TCP SYN-ACK or challenge TCP-ACK segment over IPv6 that is transmitted or retransmitted does not properly initialize the Traffic Class field disclosing one byte of kernel memory over the network.	2020-04-28	not yet calculated	<a href="#">CVE-2020-7451</a> <a href="#">CONFIRM</a>
freeipa -- freeipa	A flaw was found in all ipa versions 4.x.x through 4.8.0. When sending a very long password (>= 1,000,000 characters) to the server, the password hashing process could exhaust memory and CPU leading to a denial of service and the website becoming unresponsive. The highest threat from this vulnerability is to system availability.	2020-04-27	not yet calculated	<a href="#">CVE-2020-1722</a> <a href="#">CONFIRM</a>
fun-map -- fun-map	fun-map through 3.3.1 is vulnerable to Prototype Pollution. The function assocInM could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload.	2020-04-28	not yet calculated	<a href="#">CVE-2020-7644</a> <a href="#">MISC</a> <a href="#">MISC</a>
g.skill -- trident_z_lighting_control	The ene.sys driver in G.SKILL Trident Z Lighting Control through 1.00.08 exposes mapping and un-mapping of physical memory, reading and writing to Model Specific Register (MSR) registers, and input from and output to I/O ports to local non-privileged users. This leads to privilege escalation to NT AUTHORITY\SYSTEM.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12446</a> <a href="#">MISC</a>
generix -- upsadapter_cs141	UPS Adapter CS141 before 1.90 allows Directory Traversal. An attacker with Admin or Engineer login credentials could exploit the vulnerability by manipulating variables that reference files and by doing this achieve access to files and directories outside the web root folder. An attacker may access arbitrary files and directories stored in the file system, but integrity of the files are not jeopardized as	2020-04-27	not yet calculated	<a href="#">CVE-2020-11420</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	attacker have read access rights only.			
genius_bytes -- genius_server	An application plugin in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to gain admin privileges.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16653</a> <a href="#">MISC</a>
genius_bytes -- genius_server	The BPM component in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to execute arbitrary commands.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16652</a> <a href="#">MISC</a> <a href="#">MISC</a>
gigamon -- gigavue	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an arbitrary file upload for an authenticated user. If an executable file is uploaded into the www-root directory, then it could yield remote code execution via the filename parameter.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12252</a> <a href="#">MISC</a> <a href="#">MISC</a>
gigamon -- gigavue	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an authenticated user to change the filename value (in the POST method) from the original filename to achieve directory traversal via a ../ sequence and, for example, obtain a complete directory listing of the machine.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12251</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab 12.6 through 12.9 is vulnerable to a privilege escalation that allows an external user to create a personal snippet through the API.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12275</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab 9.5.9 through 12.9 is vulnerable to stored XSS in an admin notification feature.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12276</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab 10.8 through 12.9 has a vulnerability that allows someone to mirror a repository even if the feature is not activated.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12277</a> <a href="#">CONFIRM</a>
glibc -- glibc	A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.	2020-04-30	not yet calculated	<a href="#">CVE-2020-1752</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
google -- chrome-launcher	All versions of chrome-launcher allow execution of arbitrary commands, by controlling the \$HOME environment variable in Linux operating systems.	2020-05-02	not yet calculated	<a href="#">CVE-2020-7645</a> <a href="#">MISC</a>



grafana -- grafana	An information-disclosure flaw was found in Grafana through 6.7.3. The database directory /var/lib/grafana and database file /var/lib/grafana/grafana.db are world readable. This can result in exposure of sensitive information (e.g., cleartext or encrypted datasource passwords).	2020-04-29	not yet calculated	<a href="#">CVE-2020-12458</a> MISC MISC
grafana -- grafana	In certain Red Hat packages for Grafana 6.x through 6.3.6, the configuration files /etc/grafana/grafana.ini and /etc/grafana/ldap.toml (which contain a secret_key and a bind_password) are world readable.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12459</a> MISC MISC
handysoft -- handy_groupware	ActiveX Control(HShell.dll) in Handy Groupware 1.7.3.1 for Windows 7, 8, and 10 allows an attacker to execute arbitrary command via the ShellExec method.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7804</a> CONFIRM CONFIRM
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.4 contained a cross-site scripting vulnerability such that files from a malicious workload could cause arbitrary JavaScript to execute in the web UI. Fixed in 0.10.5.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10944</a> CONFIRM
hcl -- connections	HCL Connections v5.5, v6.0, and v6.5 contains an open redirect vulnerability which could be exploited by an attacker to conduct phishing attacks.	2020-05-01	not yet calculated	<a href="#">CVE-2019-4209</a> CONFIRM
hp -- multiple_products	A potential security vulnerability has been identified in the disk drive firmware installers named Supplemental Update / Online ROM Flash Component on HPE servers running Linux. The vulnerable software is included in the HPE Service Pack for ProLiant (SPP) releases 2018.06.0, 2018.09.0, and 2018.11.0. The vulnerable software is the Supplemental Update / Online ROM Flash Component for Linux (x64) software. The installer in this software component could be locally exploited to execute arbitrary code. Drive Models can be found in the Vulnerability Resolution field of the security bulletin. The 2019_03 SPP and Supplemental update / Online ROM Flash Component for Linux (x64) after 2019.03.0 has fixed this issue.	2020-04-27	not yet calculated	<a href="#">CVE-2020-7135</a> CONFIRM
hp --	A security vulnerability in HPE Smart Update Manager (SUM) prior to version 8.5.6 could allow remote unauthorized access. Hewlett Packard Enterprise has provided a software update to resolve this vulnerability in HPE Smart Update			<a href="#">CVE-2020-</a>

smart_update_manager	Manager (SUM) prior to 8.5.6. Please visit the HPE Support Center at <a href="https://support.hpe.com/hpesc/public/home">https://support.hpe.com/hpesc/public/home</a> to download the latest version of HPE Smart Update Manager (SUM). Download the latest version of HPE Smart Update Manager (SUM) or download the latest Service Pack For ProLiant (SPP).	2020-04-30	not yet calculated	<a href="#">7136</a> <a href="#">CONFIRM</a>
http-client -- http-client	Actions Http-Client (NPM @actions/http-client) before version 1.0.8 can disclose Authorization headers to incorrect domain in certain redirect scenarios. The conditions in which this happens are if consumers of the http-client: 1. make an http request with an authorization header 2. that request leads to a redirect (302) and 3. the redirect url redirects to another domain or hostname Then the authorization header will get passed to the other domain. The problem is fixed in version 1.0.8.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11021</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 2 out of 2 vulnerabilities. Different than CVE-2020-5302. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than 9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than 9.1.0.350(C10E3R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8), earlier than 9.1.0.350(C636E4R1P13T8) Charlotte-L09C: earlier than 9.1.0.311(C185E4R1P11T8), earlier than 9.1.0.345(C432E8R1P11T8) Charlotte-L29C: earlier than 9.1.0.325(C185E4R1P11T8), earlier than 9.1.0.335(C636E3R1P13T8), earlier than 9.1.0.345(C432E8R1P11T8), earlier than			

<p>huawei -- multiple_smartphones</p>	<p>9.1.0.336(C605E3R1P12T8) Columbia-AL10B: earlier than  9.1.0.333(C00E333R1P1T8) Columbia-L29D: earlier than  9.1.0.350(C461E3R1P11T8), earlier than  9.1.0.350(C185E3R1P12T8), earlier than  9.1.0.350(C10E5R1P14T8), earlier than  9.1.0.351(C432E5R1P13T8) Cornell-AL00A: earlier than  9.1.0.333(C00E333R1P1T8) Cornell-L29A: earlier than  9.1.0.328(C185E1R1P9T8), earlier than  9.1.0.328(C432E1R1P9T8), earlier than  9.1.0.330(C461E1R1P9T8), earlier than  9.1.0.328(C636E2R1P12T8) Emily-L09C: earlier than 9.1.0.336(C605E4R1P12T8), earlier than 9.1.0.311(C185E2R1P12T8), earlier than 9.1.0.345(C432E10R1P12T8) Emily-L29C: earlier than  9.1.0.311(C605E2R1P12T8), earlier than  9.1.0.311(C636E7R1P13T8), earlier than  9.1.0.311(C432E7R1P11T8) Ever-L29B: earlier than 9.1.0.311(C185E3R3P1), earlier than 9.1.0.310(C636E3R2P1), earlier than 9.1.0.310(C432E3R1P12) HUAWEI Mate 20: earlier than  9.1.0.131(C00E131R3P1) HUAWEI Mate 20 Pro: earlier than  9.1.0.310(C185E10R2P1) HUAWEI Mate 20 RS: earlier than  9.1.0.135(C786E133R3P1) HUAWEI Mate 20 X: earlier than  9.1.0.135(C00E133R2P1) HUAWEI P20: earlier than 9.1.0.333(C00E333R1P1T8) HUAWEI P20 Pro: earlier than  9.1.0.333(C00E333R1P1T8) HUAWEI P30: earlier than 9.1.0.193 HUAWEI P30 Pro: earlier than  9.1.0.186(C00E180R2P1) HUAWEI Y9 2019: earlier than  9.1.0.220(C605E3R1P1T8) HUAWEI nova lite 3: earlier than  9.1.0.305(C635E8R2P2) Honor 10 Lite: earlier than 9.1.0.283(C605E8R2P2) Honor 8X: earlier than  9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than 9.1.0.238(C432E1R3P1) Jackman-L22: earlier than  9.1.0.247(C636E2R4P1T8) Paris-L21B: earlier than 9.1.0.331(C432E1R1P2T8) Paris-L21MEB: earlier than  9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than 9.1.0.331(C636E1R1P3T8) Sydney-AL00: earlier than</p>	<p>2020-04-27</p>	<p>not yet calculated</p>
---	--	-------------------	---------------------------

[CVE-2019-5303](#)  
[CONFIRM](#)

	<p>9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than 9.1.0.215(C432E1R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than 9.1.0.213(C185E1R1P2T8) Sydney-L22: earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than 9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)</p>			
	<p>There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 1 out of 2 vulnerabilities. Different than CVE-2020-5303. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than 9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than</p>			

huawei --  
multiple\_smartphones

9.1.0.350(C10E3R1P14T8), earlier than  
9.1.0.351(C432E5R1P13T8), earlier than  
9.1.0.350(C636E4R1P13T8) Charlotte-  
L09C: earlier than  
9.1.0.311(C185E4R1P11T8), earlier than  
9.1.0.345(C432E8R1P11T8) Charlotte-  
L29C: earlier than  
9.1.0.325(C185E4R1P11T8), earlier than  
9.1.0.335(C636E3R1P13T8), earlier than  
9.1.0.345(C432E8R1P11T8), earlier than  
9.1.0.336(C605E3R1P12T8) Columbia-  
AL10B: earlier than  
9.1.0.333(C00E333R1P1T8) Columbia-  
L29D: earlier than  
9.1.0.350(C461E3R1P11T8), earlier than  
9.1.0.350(C185E3R1P12T8), earlier than  
9.1.0.350(C10E5R1P14T8), earlier than  
9.1.0.351(C432E5R1P13T8) Cornell-  
AL00A: earlier than  
9.1.0.333(C00E333R1P1T8) Cornell-  
L29A: earlier than  
9.1.0.328(C185E1R1P9T8), earlier than  
9.1.0.328(C432E1R1P9T8), earlier than  
9.1.0.330(C461E1R1P9T8), earlier than  
9.1.0.328(C636E2R1P12T8) Emily-L09C:  
earlier than 9.1.0.336(C605E4R1P12T8),  
earlier than 9.1.0.311(C185E2R1P12T8),  
earlier than 9.1.0.345(C432E10R1P12T8)  
Emily-L29C: earlier than  
9.1.0.311(C605E2R1P12T8), earlier than  
9.1.0.311(C636E7R1P13T8), earlier than  
9.1.0.311(C432E7R1P11T8) Ever-L29B:  
earlier than 9.1.0.311(C185E3R3P1),  
earlier than 9.1.0.310(C636E3R2P1),  
earlier than 9.1.0.310(C432E3R1P12)  
HUAWEI Mate 20: earlier than  
9.1.0.131(C00E131R3P1) HUAWEI Mate  
20 Pro: earlier than  
9.1.0.310(C185E10R2P1) HUAWEI Mate  
20 RS: earlier than  
9.1.0.135(C786E133R3P1) HUAWEI  
Mate 20 X: earlier than  
9.1.0.135(C00E133R2P1) HUAWEI P20:  
earlier than 9.1.0.333(C00E333R1P1T8)  
HUAWEI P20 Pro: earlier than  
9.1.0.333(C00E333R1P1T8) HUAWEI  
P30: earlier than 9.1.0.193 HUAWEI P30  
Pro: earlier than  
9.1.0.186(C00E180R2P1) HUAWEI Y9  
2019: earlier than  
9.1.0.220(C605E3R1P1T8) HUAWEI  
nova lite 3: earlier than  
9.1.0.305(C635E8R2P2) Honor 10 Lite:  
earlier than 9.1.0.283(C605E8R2P2)

2020-04-  
27 not yet  
calculated

[CVE-2019-  
5302  
CONFIRM](#)



	<p>Honor 8X: earlier than 9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than 9.1.0.238(C432E1R3P1) Jackman-L22: earlier than 9.1.0.247(C636E2R4P1T8) Paris-L21B: earlier than 9.1.0.331(C432E1R1P2T8) Paris-L21MEB: earlier than 9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than 9.1.0.331(C636E1R1P3T8) Sydney-AL00: earlier than 9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than 9.1.0.215(C432E1R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than 9.1.0.213(C185E1R1P2T8) Sydney-L22: earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than 9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)</p>			
huawei -- oceanstor_5310	<p>Huawei OceanStor 5310 product with version of V500R007C60SPC100 has an invalid pointer access vulnerability. The software system access an invalid pointer when attacker malformed packet. Due to the insufficient validation of some parameter, successful exploit could cause device reboot.</p>	2020-04-30	not yet calculated	<a href="#">CVE-2020-9098</a> CONFIRM CONFIRM
	<p>Huawei OSD product with versions earlier than OSD_uwp_9.0.32.0 have a local privilege escalation vulnerability. An</p>			<a href="#">CVE-2020-</a>

huawei -- osd	authenticated, local attacker can constructs a specific file path to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	2020-04-27	not yet calculated	<a href="#">9072</a> <a href="#">CONFIRM</a>
huawei -- pcmanager	Huawei PCManager with versions earlier than 10.0.1.36 has a privilege escalation vulnerability. Due to improper permission management of specific files, local attackers with low permissions can inject commands to exploit this vulnerability. Successful exploit may cause privilege escalation.	2020-04-30	not yet calculated	<a href="#">CVE-2020-1817</a> <a href="#">CONFIRM</a>
inductive_automation - - ignition_8_gateway	An unprotected logging route may allow an attacker to write endless log statements into the database without space limits or authentication. This results in consuming the entire available hard-disk space on the Ignition 8 Gateway (versions prior to 8.0.10), causing a denial-of-service condition.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10641</a> <a href="#">MISC</a>
intelliants -- subrion_cms	admin/blocks.php in Subrion CMS through 4.2.1 allows PHP Object Injection (with resultant file deletion) via serialized data in the subpages value within a block to blocks/edit.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12469</a> <a href="#">MISC</a>
intelmq_manager -- intelmq_manager	IntelMQ Manager from version 1.1.0 and before version 2.1.1 has a vulnerability where the backend incorrectly handled messages given by user-input in the "send" functionality of the Inspect-tool of the Monitor component. An attacker with access to the IntelMQ Manager could possibly use this issue to execute arbitrary code with the privileges of the webserver. Version 2.1.1 fixes the vulnerability.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11016</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jquery -- jquery	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11023</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jquery -- jquery	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched	2020-04-29	not yet calculated	<a href="#">CVE-2020-11022</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	in jQuery 3.5.0.			
json_gem_for_ruby_on_rails -- json_gem_for_ruby_on_rails	<p>The JSON gem through 2.2.0 for Ruby, as used in Ruby 2.4 through 2.4.9, 2.5 through 2.5.7, and 2.6 through 2.6.5, has an Unsafe Object Creation Vulnerability. This is quite similar to CVE-2013-0269, but does not rely on poor garbage-collection behavior within Ruby. Specifically, use of JSON parsing methods can lead to creation of a malicious object within the interpreter, with adverse effects that are application-dependent.</p>	2020-04-28	not yet calculated	<a href="#">CVE-2020-10663</a> <a href="#">SUSE MLIST</a> <a href="#">FEDORA CONFIRM</a>
kiali -- kiali	<p>An insufficient JWT validation vulnerability was found in Kiali versions 0.4.0 to 1.15.0 and was fixed in Kiali version 1.15.1, wherein a remote attacker could abuse this flaw by stealing a valid JWT cookie and using that to spoof a user session, possibly gaining privileges to view and alter the Istio configuration.</p>	2020-04-27	not yet calculated	<a href="#">CVE-2020-1762</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
lexmark -- multiple_devices	<p>A cross-site scripting (XSS) vulnerability in Lexmark CS31x before LW74.VYL.P273; CS41x before LW74.VY2.P273; CS51x before LW74.VY4.P273; CX310 before LW74.GM2.P273; CX410 &amp; XC2130 before LW74.GM4.P273; CX510 &amp; XC2132 before LW74.GM7.P273; MS310, MS312, MS317 before LW74.PRL.P273; MS410, M1140 before LW74.PRL.P273; MS315, MS415, MS417 before LW74.TL2.P273; MS51x, MS610dn, MS617 before LW74.PR2.P273; M1145, M3150dn before LW74.PR2.P273; MS610de, M3150 before LW74.PR4.P273; MS71x, M5163dn before LW74.DN2.P273; MS810, MS811, MS812, MS817, MS818 before LW74.DN2.P273; MS810de, M5155, M5163 before LW74.DN4.P273; MS812de, M5170 before LW74.DN7.P273; MS91x before LW74.SA.P273; MX31x, XM1135 before LW74.SB2.P273; MX410, MX510 &amp; MX511 before LW74.SB4.P273; XM1140, XM1145 before LW74.SB4.P273; MX610 &amp; MX611 before LW74.SB7.P273; XM3150 before LW74.SB7.P273; MX71x, MX81x before LW74.TU.P273; XM51xx &amp; XM71xx before LW74.TU.P273; MX91x &amp; XM91x before LW74.MG.P273; MX6500e</p>	2020-04-28	not yet calculated	<a href="#">CVE-2020-10094</a> <a href="#">CONFIRM</a>

	before LW74.JD.P273; C746 before LHS60.CM2.P738; C748, CS748 before LHS60.CM4.P738; C792, CS796 before LHS60.HC.P738; C925 before LHS60.HV.P738; C950 before LHS60.TP.P738; X548 & XS548 before LHS60.VK.P738; X74x & XS748 before LHS60.NY.P738; X792 & XS79x before LHS60.MR.P738; X925 & XS925 before LHS60.HK.P738; X95x & XS95x before LHS60.TQ.P738; 6500e before LHS60.JR.P738; C734 LR.SK.P824 and earlier; C736 LR.SKE.P824 and earlier; E46x LR.LBH.P824 and earlier; T65x LR.JP.P824 and earlier; X46x LR.BS.P824 and earlier; X65x LR.MN.P824 and earlier; X73x LR.FL.P824 and earlier; W850 LP.JB.P823 and earlier; and X86x LP.SP.P823 and earlier.			
lexmark -- pro910_series_devices	A cross-site scripting (XSS) vulnerability in Lexmark Pro910 series inkjet and other discontinued products.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10093</a> <a href="#">CONFIRM</a>
lg -- bridge	An issue was discovered in LG Bridge before April 2019 on Windows. DLL Hijacking can occur.	2020-04-29	not yet calculated	<a href="#">CVE-2019-20781</a> <a href="#">CONFIRM</a>
libgit2 -- libgit2	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. path.c mishandles equivalent filenames that exist because of NTFS Alternate Data Streams. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1352.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12278</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgit2 -- libgit2	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. checkout.c mishandles equivalent filenames that exist because of NTFS short names. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1353.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12279</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libvirt -- libvirt	An issue was discovered in qemuDomainGetStatsIOThread in qemu/qemu_driver.c in libvirt 4.10.0 though 6.x before 6.1.0. A memory leak was found in the virDomainListGetStats libvirt API that is responsible for retrieving domain statistics when managing QEMU guests. This flaw allows unprivileged users with a read-only connection to cause a memory leak in the domstats command, resulting in a potential denial of service.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12430</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

linux -- linux_kernel	In the Linux kernel through 5.6.7 on the s390 platform, code execution may occur because of a race condition, as demonstrated by code in enable_sacf_uaccess in arch/s390/lib/uaccess.c that fails to protect against a concurrent page table upgrade, aka CID-3f777e19d171. A crash could also occur.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11884</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
linux -- linux_kernel	An array overflow was discovered in mt76_add_fragment in drivers/net/wireless/mediatek/mt76/dma.c in the Linux kernel before 5.5.10, aka CID-b102f0c522cf. An oversized packet with too many rx fragments can corrupt memory of adjacent pages.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	usb_sg_cancel in drivers/usb/core/message.c in the Linux kernel before 5.6.8 has a use-after-free because a transfer occurs without a reference, aka CID-056ad39ee925.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12464</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mahara -- mahara	In Mahara 19.04 before 19.04.5 and 19.10 before 19.10.3, account details are shared in the Elasticsearch results for accounts that are not accessible when the config setting 'Isolated institutions' is turned on.	2020-04-30	not yet calculated	<a href="#">CVE-2020-9387</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
monox -- monox	MonoX through 5.1.40.5152 allows remote code execution via HTML5Upload.ashx or Pages/SocialNetworking/Ing/en-US/PhotoGallery.aspx because of deserialization in ModuleGallery.HTML5Upload, ModuleGallery.SilverLightUploadModule, HTML5Upload, and SilverLightUploadHandler.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12471</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows stored XSS via User Status, Blog Comments, or Blog Description.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12472</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows admins to execute arbitrary programs by reconfiguring the Converter Executable setting from ffmpeg.exe to a different program.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12473</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows administrators to execute arbitrary code by modifying an ASPX template.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12470</a> <a href="#">MISC</a>
	In Moonlight iOS/tvOS before 4.0.1, the			<a href="#">CVE-2020-</a>



moonlight -- moonlight_ios/tvos	pairing process is vulnerable to a man-in-the-middle attack. The bug has been fixed in Moonlight v4.0.1 for iOS and tvOS.	2020-04-29	not yet calculated	<a href="#">11024</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
moxa -- nport_5150a	Moxa Service in Moxa NPort 5150A firmware version 1.5 and earlier allows attackers to obtain sensitive configuration values via a crafted packet to UDP port 4800. NOTE: Moxa Service is an unauthenticated service that runs upon a first-time installation but can be disabled without ill effect.	2020-05-01	not yet calculated	<a href="#">CVE-2020-12117</a> <a href="#">CONFIRM</a>
multiple_vendors -- multiple_products	The Apros Evolution, ConsciusMap, and Furukawa provisioning systems through 2.8.1 allow remote code execution because of javax.faces.ViewState Java deserialization.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12133</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- dgn2200_devices	NETGEAR DGN2200v4 devices before 2017-01-06 are affected by command execution and an FTP insecure root directory.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11054</a> <a href="#">CONFIRM</a>
netgear -- genie_applicaiton_for_android	The NETGEAR genie application before 2.4.34 for Android is affected by mishandling of hard-coded API keys and session IDs.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11058</a> <a href="#">CONFIRM</a>
netgear -- insight_application	The NETGEAR Insight application before 2.42 for Android and iOS is affected by password mismanagement.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18857</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21204</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.62, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R8900 before 1.0.3.10, R9000 before 1.0.3.10,	2020-04-27	not yet calculated	<a href="#">CVE-2018-21153</a> <a href="#">CONFIRM</a>

	WN2000RPTv3 before 1.0.1.26, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21188</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.10, R6220 before 1.1.0.60, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21209</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, and WNDR4300 before 1.0.2.98.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21199</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6100 before 1.0.0.57, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.78, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21167</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WAC120 before 2.1.7, WN604 before 3.3.10, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, and WND930 before 2.1.5.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21097</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21222</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by debugging command execution. This affects FS752TP 5.4.2.19 and earlier, GS108Tv2 5.4.2.29 and earlier, GS110TP 5.4.2.29 and earlier, GS418TPP 6.6.2.6 and earlier, GS510TLP 6.6.2.6 and earlier, GS510TP 5.04.2.27 and earlier, GS510TPP 6.6.2.6 and earlier, GS716Tv2 5.4.2.27 and earlier, GS716Tv3 6.3.1.16 and earlier, GS724Tv3 5.4.2.27 and earlier, GS724Tv4 6.3.1.16 and earlier, GS728TPSB 5.3.0.29 and earlier, GS728TSB 5.3.0.29 and earlier, GS728TXS 6.1.0.35 and earlier, GS748Tv4 5.4.2.27 and earlier, GS748Tv5 6.3.1.16 and earlier, GS752TPSB 5.3.0.29 and earlier, GS752TSB 5.3.0.29 and earlier, GS752TXS 6.1.0.35 and earlier, M4200 12.0.2.10 and earlier, M4300 12.0.2.10 and earlier, M5300 11.0.0.28 and earlier, M6100 11.0.0.28 and earlier, M7100 11.0.0.28 and earlier, S3300 6.6.1.4 and earlier, XS708T 6.6.0.11 and earlier, XS712T 6.1.0.34 and earlier, and XS716T 6.6.0.11 and earlier.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18860</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100			

netgear -- multiple_devices	before 1.0.0.57, R7800 before 1.2.0.44, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21198</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21220</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, EX2700 before 1.0.1.28, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21215</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21219</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21208</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.52, R6100			

netgear -- multiple_devices	before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.4.2, R9000 before 1.0.3.16, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21155</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.38, D6400 before 1.0.0.74, D7000v2 before 1.0.0.74, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.102, DGN2200Bv4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.20, R6300v2 before 1.0.4.22, R6400 before 1.0.1.32, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R6900P before 1.3.0.18, R7000 before 1.0.9.28, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900 before 1.0.2.10, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, R8300 before 1.0.2.116, R8500 before 1.0.2.116, WN2500RPv2 before 1.0.1.52, WNDR3400v3 before 1.0.1.18, and WNR3500Lv2 before 1.2.0.46.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21156</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.94.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21183</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98,	2020-04-28	not yet calculated	<a href="#">CVE-2018-21212</a> <a href="#">CONFIRM</a>



	WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21211</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects CM400 before 2017-01-11, CM600 before 2017-01-11, D1500 before 2017-01-11, D500 before 2017-01-11, DST6501 before 2017-01-11, JNR1010v1 before 2017-01-11, JWNR2000Tv3 before 2017-01-11, JWNR2010v3 before 2017-01-11, PLW1000 before 2017-01-11, PLW1010 before 2017-01-11, WNR500 before 2017-01-11, WNR612v3 before 2017-01-11, N450 before 2017-01-11, and CG3000Dv2 before 2017-01-11.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11055</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7000 before 2018-03-01, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 2018-03-01, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before	2020-04-27	not yet calculated	<a href="#">CVE-2018-21169</a> <a href="#">CONFIRM</a>

	1.1.0.46.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, and R7800 before 1.0.2.42.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21154</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, and R9000 before 1.0.3.6.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21184</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21224</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21175</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21174</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52,	2020-04-27	not yet calculated	<a href="#">CVE-2018-21176</a>

	WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7000 before 1.0.1.52, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21168</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21185</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R7000 before 1.0.9.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.38, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21157</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects			

netgear -- multiple_devices	D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21205</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21214</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21223</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21218</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before	2020-04-28	not yet calculated	<a href="#">CVE-2018-21195</a> <a href="#">CONFIRM</a>

	1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command execution. This affects M4200-10MG-POE+ 12.0.2.11 and earlier, M4300-28G 12.0.2.11 and earlier, M4300-52G 12.0.2.11 and earlier, M4300-28G-POE+ 12.0.2.11 and earlier, M4300-52G-POE+ 12.0.2.11 and earlier, M4300-8X8F 12.0.2.11 and earlier, M4300-12X12F 12.0.2.11 and earlier, M4300-24X24F 12.0.2.11 and earlier, M4300-24X 12.0.2.11 and earlier, and M4300-48X 12.0.2.11 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18858 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21096 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21196 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21197 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94,	2020-04-28	not yet calculated	<a href="#">CVE-2018-21201 CONFIRM</a>



	WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21202</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6100 before 1.0.1.20, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21203</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21206</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6700 before 1.0.1.30, R6700v2 before 1.2.0.16, R6800 before 1.2.0.16, R6900 before 1.0.1.30, R6900P before 1.2.0.22, R6900v2 before 1.2.0.16, R7000 before 1.0.9.12, R7000P before 1.2.0.22, R7500v2 before 1.0.3.20, R7800 before 1.0.2.44, R8300 before 1.0.2.106, R8500 before 1.0.2.106, and R9000 before 1.0.2.52.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21225</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an			

netgear -- multiple_devices	unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21207</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects JNR1010v2 before 1.1.0.48, JWNR2010v5 before 1.1.0.48, WNR1000v4 before 1.1.0.48, WNR2020 before 1.1.0.48, and WNR2050 before 1.1.0.48.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21226</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21210</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by slowdown/stoppage. This affects C6300 before 2017-05-30, CM400 before 2017-05-30, CM700 before 2017-05-30, and CMD31T before 2017-05-30.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18859</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21094</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected			

netgear -- multiple_devices	by mishandling of repeated URL calls. This affects JNR1010v2 before 2017-01-06, WNR614 before 2017-01-06, WNR618 before 2017-01-06, JWNR2000v5 before 2017-01-06, WNR2020 before 2017-01-06, JWNR2010v5 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2020v2 before 2017-01-06, R6220 before 2017-01-06, and WNDR3700v5 before 2017-01-06.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11057</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21186</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.0.54, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21149</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by password exposure. This affects AC1450 before 2017-01-06, C6300 before 2017-01-06, D500 before 2017-01-06, D1500 before 2017-01-06, D3600 before 2017-01-06, D6000 before 2017-01-06, D6100 before 2017-01-06, D6200 before 2017-01-06, D6200B before 2017-01-06, D6300B before 2017-01-06, D6300 before 2017-01-06, DGN1000v3 before 2017-01-06, DGN2200v1 before 2017-01-06, DGN2200v3 before 2017-01-06, DGN2200V4 before 2017-01-06, DGN2200Bv3 before 2017-01-06, DGN2200Bv4 before 2017-01-06, DGND3700v1 before 2017-01-06, DGND3700v2 before 2017-01-06, DGND3700Bv2 before 2017-01-06, JNR1010v1 before 2017-01-06,			

netgear -- multiple_devices	JNR1010v2 before 2017-01-06, JNR3300 before 2017-01-06, JR6100 before 2017-01-06, JR6150 before 2017-01-06, JWNR2000v5 before 2017-01-06, R2000 before 2017-01-06, R6050 before 2017-01-06, R6100 before 2017-01-06, R6200 before 2017-01-06, R6200v2 before 2017-01-06, R6220 before 2017-01-06, R6250 before 2017-01-06, R6300 before 2017-01-06, R6300v2 before 2017-01-06, R6700 before 2017-01-06, R7000 before 2017-01-06, R7900 before 2017-01-06, R7500 before 2017-01-06, R8000 before 2017-01-06, WGR614v10 before 2017-01-06, WNR1000v2 before 2017-01-06, WNR1000v3 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2000v3 before 2017-01-06, WNR2000v4 before 2017-01-06, WNR2000v5 before 2017-01-06, WNR2200 before 2017-01-06, WNR2500 before 2017-01-06, WNR3500Lv2 before 2017-01-06, WNDR3400v2 before 2017-01-06, WNDR3400v3 before 2017-01-06, WNDR3700v3 before 2017-01-06, WNDR3700v4 before 2017-01-06, WNDR3700v5 before 2017-01-06, WNDR4300 before 2017-01-06, WNDR4300v2 before 2017-01-06, WNDR4500v1 before 2017-01-06, WNDR4500v2 before 2017-01-06, and WNDR4500v3 before 2017-01-06.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11059</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21152</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D8500 before 1.0.3.42, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.26, R6300-2CXNAS before 1.0.3.60, R6300v2 before 1.0.4.28, R6400 before 1.0.1.36, R6400v2 before	2020-04-27	not yet calculated	<a href="#">CVE-2018-21093</a> <a href="#">CONFIRM</a>

	1.0.2.52, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R7100LG before 1.0.0.46, R7300 before 1.0.0.68, R7900 before 1.0.2.10, R8000 before 1.0.4.18, R8000P before 1.3.0.10, R7900P before 1.3.0.10, R8500 before 1.0.2.122, R8300 before 1.0.2.122, RBW30 before 2.1.2.6, WN2500RPv2 before 1.0.0.54, and WNR3500Lv2 before 1.2.0.56.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command execution via a PHP form. This affects WN604 3.3.3 and earlier, WNAP210v2 3.5.20.0 and earlier, WNAP320 3.5.20.0 and earlier, WNDAP350 3.5.20.0 and earlier, WNDAP360 3.5.20.0 and earlier, WNDAP620 2.0.11 and earlier, WNDAP660 3.5.20.0 and earlier, WND930 2.0.11 and earlier, and WAC120 2.0.7 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18863</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects JGS516PE before 2017-05-11, JGS524Ev2 before 2017-05-11, JGS524PE before 2017-05-11, GS105Ev2 before 2017-05-11, GS105PE before 2017-05-11, GS108Ev3 before 2017-05-11, GS108PEv3 before 2017-05-11, GS116Ev2 before 2017-05-11, GSS108E before 2017-05-11, GSS116E before 2017-05-11, XS708Ev2 before 2017-05-11, and XS716E before 2017-05-11.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18862</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by insecure renegotiation. This affects SRX5308 before 2017-02-10, FVS336Gv3 before 2017-02-10, FVS318N before 2017-02-10, and FVS318Gv2 before 2017-02-10.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11060</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by password recovery and file access. This affects D8500 1.0.3.27 and earlier, DGN2200v4 1.0.0.82 and earlier, R6300v2 1.0.4.06 and earlier, R6400 1.0.1.20 and earlier, R6400v2 1.0.2.18 and earlier, R6700 1.0.1.22 and earlier, R6900 1.0.1.20 and earlier, R7000 1.0.7.10 and earlier, R7000P 1.0.0.58 and earlier, R7100LG 1.0.0.28 and earlier, R7300DST 1.0.0.52 and earlier, R7900 1.0.1.12 and earlier, R8000 1.0.3.46 and	2020-04-29	not yet calculated	<a href="#">CVE-2017-18853</a> <a href="#">CONFIRM</a>



	earlier, R8300 1.0.2.86 and earlier, R8500 1.0.2.86 and earlier, WNDR3400v3 1.0.1.8 and earlier, and WNDR4500v2 1.0.0.62 and earlier.			
netgear -- readynas_devices	NETGEAR ReadyNAS 6.6.1 and earlier is affected by command injection.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18854</a> <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.6.1 are affected by command injection.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18856</a> <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by incorrect configuration of security settings.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21159</a> <a href="#">CONFIRM</a>
netgear -- readynas_surveillance_devices	Certain NETGEAR devices are affected by anonymous root access. This affects ReadyNAS Surveillance 1.1.1-3-armel and earlier and ReadyNAS Surveillance 1.4.1-3-amd64 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11056</a> <a href="#">CONFIRM</a>
netgear -- readynas_surveillance_services	Certain NETGEAR devices are affected by CSRF. This affects ReadyNAS Surveillance 1.4.3-15-x86 and earlier and ReadyNAS Surveillance 1.1.4-5-ARM and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18861</a> <a href="#">CONFIRM</a>
node.js -- node.js	The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.	2020-04-26	not yet calculated	<a href="#">CVE-2020-12265</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
octopus -- deploy	In Octopus Deploy before 2019.12.9 and 2020 before 2020.1.12, the TaskView permission is not scoped to any dimension. For example, a scoped user who is scoped to only one tenant can view server tasks scoped to any other tenant.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12286</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
onkyo -- tx-nr585_devices	A Local File Inclusion (LFI) issue on Onkyo TX-NR585 1000-0000-000-0008-0000 devices allows remote unauthenticated users on the network to read sensitive files via %2e%2e%2f directory traversal, as demonstrated by reading /etc/shadow.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12447</a> <a href="#">MISC</a>
opendmarc -- opendmarc	OpenDMARC through 1.3.2 and 1.4.x, when used with pypolicyd-spf 2.0.2, allows attacks that bypass SPF and DMARC authentication in situations where the HELO field is inconsistent with the MAIL FROM field.	2020-04-27	not yet calculated	<a href="#">CVE-2019-20790</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	OpenDMARC through 1.3.2 and 1.4.x allows attacks that inject authentication results to provide false information about			

opendmarc -- opendmarc	the domain that originated an e-mail message. This is caused by incorrect parsing and interpretation of SPF/DKIM authentication results, as demonstrated by the example.net(.example.com substring).	2020-04-27	not yet calculated	<a href="#">CVE-2020-12272</a> <a href="#">MISC</a> <a href="#">MISC</a>
openldap -- openldap	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).	2020-04-28	not yet calculated	<a href="#">CVE-2020-12243</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a>
opensc -- opensc	OpenSC before 0.20.0 has a double free in coolkey_free_private_data because coolkey_add_object in libopensc/card-coolkey.c lacks a uniqueness check.	2020-04-29	not yet calculated	<a href="#">CVE-2019-20792</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openvpn -- openvpn	An issue was discovered in OpenVPN 2.4.x before 2.4.9. An attacker can inject a data channel v2 (P_DATA_V2) packet using a victim's peer-id. Normally such packets are dropped, but if this packet arrives before the data channel crypto parameters have been initialized, the victim's connection will be dropped. This requires careful timing due to the small time window (usually within a few seconds) between the victim client connection starting and the server PUSH_REPLY response back to the client. This attack will only work if Negotiable Cipher Parameters (NCP) is in use.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11810</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
opmantek -- open-audit	Open-Audit 3.3.0 allows an XSS attack after login.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12261</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There is Arbitrary file upload.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11943</a> <a href="#">MISC</a> <a href="#">MISC</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.3.1. There is shell metacharacter injection via attributes to an open-audit/configuration/ URI. An attacker can exploit this by adding an excluded IP address to the global discovery settings (internally called exclude_ip). This exclude_ip value is passed to the exec function in the discoveries_helper.php file (inside the all_ip_list function) without	2020-04-28	not yet calculated	<a href="#">CVE-2020-12078</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	being filtered, which means that the attacker can provide a payload instead of a valid IP address.			
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There are Multiple SQL Injections.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11942</a> <a href="#">MISC</a> <a href="#">MISC</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There is OS Command injection in Discovery.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11941</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2020-04-29	not yet calculated	<a href="#">CVE-2020-2575</a> <a href="#">MISC</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system	When user downloads PGP or S/MIME keys/certificates, exported file has same name for private and public keys. Therefore it's possible to mix them and to send private key to the third-party instead of public key. This issue affects ((OTRS)) Community Edition: 5.0.42 and prior versions, 6.0.27 and prior versions. OTRS: 7.0.16 and prior versions.	2020-04-28	not yet calculated	<a href="#">CVE-2020-1774</a> <a href="#">LIST</a> <a href="#">CONFIRM</a>
percona -- xtrabackup	Percona XtraBackup before 2.4.20 unintentionally writes the command line to any resulting backup file output. This may include sensitive arguments passed at run time. In addition, when --history is passed at run time, this command line is also written to the PERCONA_SCHEMA.xtrabackup_history table.	2020-04-27	not yet calculated	<a href="#">CVE-2020-10997</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
percona -- xtradb_cluster	An issue was discovered in Percona XtraDB Cluster before 5.7.28-31.42. A bundled script inadvertently sets a static transition_key for SST processes in place	2020-04-27	not yet calculated	<a href="#">CVE-2020-10996</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	of the random key expected.			<a href="#">CONFIRM</a>
php -- php	In PHP versions 7.2.x below 7.2.30, 7.3.x below 7.3.17 and 7.4.x below 7.4.5, if PHP is compiled with EBCDIC support (uncommon), urldecode() function can be made to access locations past the allocated memory, due to erroneously using signed numbers as array indexes.	2020-04-27	not yet calculated	<a href="#">CVE-2020-7067</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
php-fusion -- php-fusion	An XSS vulnerability exists in the banners.php page of PHP-Fusion 9.03.50. This can be exploited because the only security measure used against XSS is the stripping of SCRIPT tags. A malicious actor can use HTML event handlers to run JavaScript instead of using SCRIPT tags.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12438</a> <a href="#">MISC</a> <a href="#">MISC</a>
php-fusion -- php-fusion	PHP-Fusion 9.03.50 allows SQL Injection because maincore.php has an insufficient protection mechanism. An attacker can develop a crafted payload that can be inserted into the sort_order GET parameter on the members.php members search page. This parameter allows for control over anything after the ORDER BY clause in the SQL query.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12461</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phpgurukul -- online_course_registration	Online Course Registration 2.0 has multiple SQL injections that would can lead to a complete database compromise and authentication bypass in the login pages: admin/change-password.php, admin/check_availability.php, admin/index.php, change-password.php, check_availability.php, includes/header.php, index.php, and pincode-verification.php.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12429</a> <a href="#">MISC</a>
prestashop -- prestashop	The Correos Express addon for PrestaShop 1.6 through 1.7 allows remote attackers to obtain sensitive information, such as a service's owner password that can be used to modify orders via SOAP. Attackers can also retrieve information about orders or buyers.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12120</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	An integer overflow was found in QEMU 4.0.1 through 4.2.0 in the way it implemented ATI VGA emulation. This flaw occurs in the ati_2d_blit() routine in hw/display/ati-2d.c while handling MMIO write operations through the ati_mm_write() callback. A malicious guest could abuse this flaw to crash the QEMU process, resulting in a denial of	2020-04-27	not yet calculated	<a href="#">CVE-2020-11869</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	service.			
re2c -- re2c	re2c before 2.0 has uncontrolled recursion that causes stack consumption in find_fixed_tags.	2020-04-29	not yet calculated	<a href="#">CVE-2018-21232</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible	An archive traversal flaw was found in all ansible-engine versions 2.9.x prior to 2.9.7, when running ansible-galaxy collection install. When extracting a collection .tar.gz file, the directory is created without sanitizing the filename. An attacker could take advantage to overwrite any file within the system.	2020-04-30	not yet calculated	<a href="#">CVE-2020-10691</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
red_hat -- undertow	A file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in Undertow version 2.0.29.Final and before and was fixed in 2.0.30.Final. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution.	2020-04-28	not yet calculated	<a href="#">CVE-2020-1745</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel V2.5.2, attackers can upload an arbitrary file to the server just changing the the content-type value. As a result of that, an attacker can execute a command on the server. This specific attack only occurs with the Maintenance Mode setting.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11817</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel 2.5.2, users' passwords and usernames are stored in a cookie with URL encoding, base64 encoding, and hashing. Thus, an attacker can easily apply brute force on them.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11821</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel 2.5.2, there is a stored XSS vulnerability on the application structure --> user access groups page. Thus, an attacker can inject malicious script to steal all users' valuable data.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11822</a> <a href="#">MISC</a>
	In Rundeck before version 3.2.6, authenticated users can craft a request that reveals Execution data and logs and Job details that they are not authorized to see. Depending on the configuration and the way that Rundeck is used, this could result in anything between a high severity risk, or a very low risk. If access is tightly			



rundeck -- rundeck	restricted and all users on the system have access to all projects, this is not really much of an issue. If access is wider and allows login for users that do not have access to any projects, or project access is restricted, there is a larger issue. If access is meant to be restricted and secrets, sensitive data, or intellectual property are exposed in Rundeck execution output and job data, the risk becomes much higher. This vulnerability is patched in version 3.2.6	2020-04-29	not yet calculated	<a href="#">CVE-2020-11009</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
saltstack -- salt	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class allows access to some methods that improperly sanitize paths. These methods allow arbitrary directory access to authenticated users.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11652</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
saltstack -- salt	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11651</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- erp	Egypt localized withholding tax reports Clearing of Liabilities and Remittance Statement and Summary in SAP ERP (versions 618, 730, EAPPLGLO 607) and S/4 HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user, allowing reading or modification of some tax reports, due to Missing Authorization Check.	2020-04-24	not yet calculated	<a href="#">CVE-2020-6212</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver_as_abap_business_server_pages_test_application	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_PHTMLB, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754 is vulnerable to reflected application Scripting (XSS) via different URL parameters as it does not sufficiently encode user controlled inputs.	2020-04-24	not yet calculated	<a href="#">CVE-2020-6213</a> <a href="#">MISC</a> <a href="#">MISC</a>
simple_ledger -- electron-cash-slp	Electron-Cash-SLP before version 3.6.2 has a vulnerability. All token creators that use the "Mint Tool" feature of the Electron Cash SLP Edition are at risk of sending the minting authority baton to the wrong SLP address. Sending the mint baton to	2020-04-28	not yet calculated	<a href="#">CVE-2020-11014</a> <a href="#">MISC</a> <a href="#">MISC</a>

	the wrong address will give another party the ability to issue new tokens or permanently destroy future minting capability. This is fixed version 3.6.2.			<a href="#">MISC CONFIRM</a>
simplisafe -- ss3_devices	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to pair a rogue keypad to an armed system.	2020-05-02	not yet calculated	<a href="#">CVE-2020-5727 CONFIRM</a>
solarwinds -- webhelpdesk	Formula Injection exists in the export feature in SolarWinds WebHelpDesk 12.7.1 via a value (provided by a low-privileged user in the Subject field of a help request form) that is mishandled in a TicketActions/view?tab=group TSV export by an admin user.	2020-04-27	not yet calculated	<a href="#">CVE-2019-20002 MISC</a>
sourcegraph -- sourcegraph	Sourcegraph before 3.15.1 has a vulnerable authentication workflow because of improper validation in the SafeRedirectURL method in cmd/frontend/auth/redirect.go, such as for the //foo//example.com substring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12283 CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
suap -- suap	SUAP V2 allows XSS during the update of user information.	2020-04-29	not yet calculated	<a href="#">CVE-2019-7634 MISC</a>
suculent -- think-device-api	A vulnerability has been disclosed in thinx-device-api IoT Device Management Server before version 2.5.0. Device MAC address can be spoofed. This means initial registration requests without UDID and spoofed MAC address may pass to create new UDID with same MAC address. Full impact needs to be reviewed further. Applies to all (mostly ESP8266/ESP32) users. This has been fixed in firmware version 2.5.0.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11015 CONFIRM</a>
teampass -- teampass	The REST API functions in TeamPass 2.1.27.36 allow any user with a valid API token to bypass IP address whitelist restrictions via an X-Forwarded-For client HTTP header to the getIp function.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12477 MISC</a>
telegram -- telegram_desktop_and_telegram_group_and_chat_and_bot	Telegram Desktop through 2.0.1, Telegram through 6.0.1 for Android, and Telegram through 6.0.1 for iOS allow an attacker to perform a Denial of Service (DoS) attack via a public URL or a group chat invitation URL.	2020-05-01	not yet calculated	<a href="#">CVE-2020-12474 MISC</a>
testlink -- testlink	In TestLink 1.9.20, the lib/cfields/cfieldsExport.php goback_url parameter causes a security risk because it depends on client input and is not	2020-04-27	not yet calculated	<a href="#">CVE-2020-12274 MISC</a>

	constrained to lib/cfields/cfieldsView.php at the web site associated with the session.			<a href="#">MISC</a>
testlink -- testlink	In TestLink 1.9.20, a crafted login.php viewer parameter exposes cleartext credentials.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12273</a> <a href="#">MISC</a> <a href="#">MISC</a>
tiny_file_manager -- tiny_file_manager	In Tiny File Manager 2.4.1, there is a Path Traversal vulnerability in the ajax recursive directory listing functionality. This allows authenticated users to enumerate directories and files on the filesystem (outside of the application scope).	2020-04-28	not yet calculated	<a href="#">CVE-2020-12102</a> <a href="#">MISC</a> <a href="#">MISC</a>
tiny_file_manager -- tiny_file_manager	In Tiny File Manager 2.4.1 there is a vulnerability in the ajax file backup copy functionality which allows authenticated users to create backup copies of files (with .bak extension) outside the scope in the same directory in which they are stored.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12103</a> <a href="#">MISC</a> <a href="#">MISC</a>
torchbox -- wagtail	In Wagtail before versions 2.7.2 and 2.8.2, a potential timing attack exists on pages or documents that have been protected with a shared password through Wagtail's "Privacy" controls. This password check is performed through a character-by-character string comparison, and so an attacker who is able to measure the time taken by this check to a high degree of accuracy could potentially use timing differences to gain knowledge of the password. This is understood to be feasible on a local network, but not on the public internet. Privacy settings that restrict access to pages/documents on a per-user or per-group basis (as opposed to a shared password) are unaffected by this vulnerability. This has been patched in 2.7.3, 2.8.2, 2.9.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11037</a> <a href="#">CONFIRM</a>
ubiquiti -- unifi_cloud_key_devices	UniFi Cloud Key firmware <= v1.1.10 for Cloud Key gen2 and Cloud Key gen2 Plus contains a vulnerability that allows unrestricted root access through the serial interface (UART).	2020-05-02	not yet calculated	<a href="#">CVE-2020-8157</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
university_of_wisconsin -- htcondor	HTCondor up to and including stable series 8.8.6 and development series 8.9.4 has Incorrect Access Control. It is possible to use a different authentication method to submit a job than the administrator has specified. If the administrator has configured the READ or	2020-04-27	not yet calculated	<a href="#">CVE-2019-18823</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	WRITE methods to include CLAIMTOBE, then it is possible to impersonate another user to the condor_schedd. (For example to submit or remove jobs)			<a href="#">CONFIRM</a> <a href="#">MISC</a>
valve -- source	Valve Source allows local users to gain privileges by writing to the /tmp/hl2_relaunch file, which is later executed in the context of a different user account.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12242</a> <a href="#">MISC</a>
wavlink -- multiple_devices	An issue was discovered on WAVLINK WL-WN579G3 M79X3.V5030.180719, WL-WN575A3 RPT75A3.V4300.180801, and WL-WN530HG4 M30HG4.V5030.191116 devices. There are multiple externally accessible pages that do not require any sort of authentication, and store system information for internal usage. The devices automatically query these pages to update dashboards and other statistics, but the pages can be accessed externally without any authentication. All the pages follow the naming convention live_(string).shtml. Among the information disclosed is: interface status logs, IP address of the device, MAC address of the device, model and current firmware version, location, all running processes, all interfaces and their statuses, all current DHCP leases and the associated hostnames, all other wireless networks in range of the router, memory statistics, and components of the configuration of the device such as enabled features.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12266</a> <a href="#">MISC</a> <a href="#">MISC</a>
werner -- sqliteodbc	SQLiteODBC 0.9996, as packaged for certain Linux distributions as 0.9996-4, has a race condition leading to root privilege escalation because any user can replace a /tmp/sqliteodbc\$\$ file with new contents that cause loading of an arbitrary library.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12050</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">MISC</a>
wind_river -- vxworks	Wind River VxWorks tftp client library, as distributed in VxWorks 6.9 through 7 SR0630, has a double free	2020-04-27	not yet calculated	<a href="#">CVE-2020-10647</a> <a href="#">CONFIRM</a>
vmware -- esxi	ESXi 6.5 without patch ESXi650-201912104-SG and ESXi 6.7 without patch ESXi670-202004103-SG do not properly neutralize script-related HTML when viewing virtual machines attributes. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of	2020-04-29	not yet calculated	<a href="#">CVE-2020-3955</a> <a href="#">CONFIRM</a>

	8.3.			
wordpress -- wordpress	In affected versions of WordPress, a special payload can be crafted that can lead to scripts getting executed within the search block of the block editor. This requires an authenticated user with the ability to add content. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11030</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11028</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a vulnerability in the stats() method of class-wp-object-cache.php can be exploited to execute cross-site scripting (XSS) attacks. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11029</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	LearnPress Wordpress plugin version prior and including 3.2.6.7 is vulnerable to SQL Injection	2020-04-30	not yet calculated	<a href="#">CVE-2020-6010</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a cross-site scripting (XSS) vulnerability in the navigation section of Customizer allows JavaScript code to be executed. Exploitation requires an authenticated user. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11025</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>



wordpress -- wordpress	The ninja-forms plugin before 3.4.24.2 for WordPress allows CSRF with resultant XSS.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12462</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, files with a specially crafted name when uploaded to the Media section can lead to script execution upon accessing the file. This requires an authenticated user with privileges to upload files. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11026</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11027</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
xerox -- multiple_workcentre_devices	Xerox WorkCentre 3655, 3655i, 58XX, 58XXi, 59XX, 59XXi, 6655, 6655i, 72XX, 72XXi, 78XX, 78XXi, 7970, and 7970i devices before 073.xxx.086.15410 do not properly escape parameters in the support/remoteUI/configui.php script, which can allow an unauthenticated attacker to execute OS commands on the device.	2020-04-29	not yet calculated	<a href="#">CVE-2016-11061</a> <a href="#">MISC</a>
xt:commerce -- xt:commerce	The address-management feature in xt:Commerce 5.1 to 6.2.2 allows remote authenticated users to zero out other user's stored addresses by manipulating an id field in the POST request for altering an address.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12101</a> <a href="#">FULLDISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zoom -- international_call_recording	ZOOM International Call Recording 6.3.1 suffers from multiple authenticated stored XSS vulnerabilities via the phoneNumber field in the (1) User Edit or (2) User Add form, (3) name field in the Role Add form, (4) name or number field in the Edit Group form, (5) tagKey or tagValue field in the Recording Rules Configuration, or (6) txt_69735:/VemailAddress/value or txt_75767:/VemailFrom/value field in	2020-04-27	not yet calculated	<a href="#">CVE-2019-18223</a> <a href="#">MISC</a>

	callrec/config.			
zte -- oscp	ZTE SDN controller platform is impacted by an information leakage vulnerability. Due to the program's failure to optimize the response of failure to the request, the caller can directly view the internal error code location of the component. Attackers could exploit this vulnerability to obtain sensitive information. This affects: OSCP versions V16.19.10 and V16.19.20.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6865</a> <a href="#">CONFIRM</a>
zte -- zenic_one_r22b_devices	ZTE's SDON controller is impacted by the resource management error vulnerability. When RPC is frequently called by other applications in the case of mass traffic data in the system, it will result in no response for a long time and memory overflow risk. This affects: ZENIC ONE R22b versions V16.19.10P02SP002 and V16.19.10P02SP005.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6867</a> <a href="#">CONFIRM</a>
zte -- zxctn_6500_devices	A ZTE product is impacted by a resource management error vulnerability. An attacker could exploit this vulnerability to cause a denial of service by issuing a specific command. This affects: ZXCTN 6500 version V2.10.00R3B87.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6866</a> <a href="#">CONFIRM</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of April 27, 2020  
**Date:** Monday, May 04, 2020 10:14:53 AM



National Cyber Awareness System:

## [Vulnerability Summary for the Week of April 27, 2020](#)

05/04/2020 06:45 AM EDT

Original release date: May 4, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atrifex -- jbig2dec	jbig2_image_compose in jbig2_image.c in Artifex jbig2dec before 0.18 has a heap-based buffer overflow.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12268</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Overlayfs in the Linux kernel and shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points. On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patches change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount underflow.	2020-04-24	<a href="#">7.2</a>	<a href="#">CVE-2019-15794</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In BIG-IQ 6.0.0-7.0.0, a remote access vulnerability has been discovered that			<a href="#">CVE-2020-</a>

f5 -- big-iq	may allow a remote user to execute shell commands on affected systems using HTTP requests to the BIG-IQ user interface.	2020-04-24	<a href="#">10</a>	<a href="#">5868</a> <a href="#">MISC</a>
google -- openthread	OpenThread before 2019-12-13 has a stack-based buffer overflow in MeshCoP::Commissioner::GeneratePskc.	2020-04-28	<a href="#">7.5</a>	<a href="#">CVE-2019-20791</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- ar3200_products	Huawei AR3200 products with versions of V200R007C00SPC900, V200R007C00SPCa00, V200R007C00SPCb00, V200R007C00SPCc00, V200R009C00SPC500 have an improper authentication vulnerability. Attackers need to perform some operations to exploit the vulnerability. Successful exploit may obtain certain permissions on the device.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-9068</a> <a href="#">CONFIRM</a>
ivanti -- avalanche	Ivanti Avalanche 6.3 allows a SQL injection that is vaguely associated with the Apache HTTP Server, aka Bug 683250.	2020-04-28	<a href="#">7.5</a>	<a href="#">CVE-2020-12442</a> <a href="#">MISC</a>
mozilla -- firefox	A malicious extension could have called <code>browser.identity.launchWebAuthFlow</code> , controlling the <code>redirect_uri</code> , and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. This vulnerability affects Firefox < 75.	2020-04-24	<a href="#">7.5</a>	<a href="#">CVE-2020-6823</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 75.	2020-04-24	<a href="#">7.5</a>	<a href="#">CVE-2020-6826</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	<a href="#">7.5</a>	<a href="#">CVE-2020-6825</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear --				<a href="#">CVE-2017-</a>

wnr854t_devices	NETGEAR WNR854T devices before 1.5.2 are affected by command execution.	2020-04-29	<a href="#">8.3</a>	<a href="#">18855</a> <a href="#">CONFIRM</a>
node-rules -- node-rules	node-rules including 3.0.0 and prior to 5.0.0 allows injection of arbitrary commands. The argument rules of function "fromJson()" can be controlled by users without any sanitization.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-7609</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
pixlcore -- pixl-class	pixl-class prior to 1.0.3 allows execution of arbitrary commands. The members argument of the create function can be controlled by users without any sanitization.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-7640</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qt -- qt	setMarkdown in Qt before 5.14.2 has a use-after-free related to QTextMarkdownImporter::insertBlock.	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12267</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
shareit -- shareit	SHAREit through 4.0.6.177 does not check the body length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation.	2020-04-27	<a href="#">7.8</a>	<a href="#">CVE-2019-14941</a> <a href="#">MISC</a> <a href="#">MISC</a>
shareit -- shareit	SHAREit through 4.0.6.177 does not check the full message length from the received packet header (which is used to allocate memory for the next set of data). This could lead to a system denial of service due to uncontrolled memory allocation. This is different from CVE-2019-14941.	2020-04-27	<a href="#">7.8</a>	<a href="#">CVE-2019-15234</a> <a href="#">MISC</a> <a href="#">MISC</a>
sophos -- xg_firewall_devices	A SQL injection issue was found in SFOS 17.0, 17.1, 17.5, and 18.0 before 2020-04-25 on Sophos XG Firewall devices, as exploited in the wild in April 2020. This affected devices configured with either the administration (HTTPS) service or the User Portal exposed on the WAN zone. A successful attack may have caused remote code execution that exfiltrated usernames and hashed passwords for the local device admin(s), portal admins, and user accounts used for remote access (but not external Active Directory or LDAP passwords)	2020-04-27	<a href="#">7.5</a>	<a href="#">CVE-2020-12271</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary			CVSS	Source &
---------	--	--	------	----------



Vendor -- Product	Description	Published	Score	Patch Info
abbs -- software_audio_media_player	ABBS Software Audio Media Player version 3.1 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	<a href="#">6.8</a>	<a href="#">CVE-2019-5621</a> <a href="#">MISC</a>
admidio -- admidio	SQL Injection was discovered in Admidio before version 3.3.13. The main cookie parameter is concatenated into a SQL query without any input validation/sanitization, thus an attacker without logging in, can send a GET request with arbitrary SQL queries appended to the cookie parameter and execute SQL queries. The vulnerability impacts the confidentiality of the system. This has been patched in version 3.3.13.	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2020-11004</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
apache -- ats	Apache ATS 6.0.0 to 6.2.3, 7.0.0 to 7.1.9, and 8.0.0 to 8.0.6 is vulnerable to a HTTP/2 slow read attack.	2020-04-27	<a href="#">5</a>	<a href="#">CVE-2020-9481</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
apache -- log4j	Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-9488</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
apache -- ofbiz	Apache OFBiz 17.12.01 is vulnerable to Host header injection by accepting arbitrary host	2020-04-30	<a href="#">5</a>	<a href="#">CVE-2019-12425</a> <a href="#">CONFIRM</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12130</a> <a href="#">MISC</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12129</a> <a href="#">MISC</a>
app2pro -- airdisk_pro	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12131</a> <a href="#">MISC</a>
avira -- antivirus	Avira Antivirus before 5.0.2003.1821 on Windows allows privilege escalation or a denial of service via abuse of a symlink.	2020-04-26	<a href="#">4.6</a>	<a href="#">CVE-2020-12254</a> <a href="#">MISC</a>
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shifts_btrfs_ioctl_fd_replace() installs an fd referencing a file from the lower filesystem without taking an additional reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a	2020-04-24	<a href="#">4.6</a>	<a href="#">CVE-2019-15791</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	refcount underflow.			
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shiftfs_btrfs_ioctl_fd_replace() calls fdget(oldfd), then without further checks passes the resulting file* into shiftfs_real_fdget(), which casts file->private_data, a void* that points to a filesystem-dependent type, to a "struct shiftfs_file_info *". As the private_data is not required to be a pointer, an attacker can use this to cause a denial of service or possibly execute arbitrary code.	2020-04-24	4.6	<a href="#">CVE-2019-15792</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	In shiftfs, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into init_user_ns, whereas they should have been translated into the s_user_ns for the lower filesystem. This resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts s_user_ns. A local attacker could use this to possibly bypass discretionary access control permissions.	2020-04-24	4.6	<a href="#">CVE-2019-15793</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Improper authorization vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote authenticated attackers to alter the application's data via the applications 'E-mail' and 'Messages'.	2020-04-28	4	<a href="#">CVE-2020-5566</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Improper input validation vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows a remote authenticated attacker to alter the application's data via the applications 'Workflow' and 'MultiReport'.	2020-04-28	4	<a href="#">CVE-2020-5565</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozo -- garoon	Server-side request forgery (SSRF) vulnerability in Cybozu Garoon 4.6.0 to 4.6.3 allows a remote attacker with an administrative privilege to issue arbitrary HTTP requests to other web servers via V-CUBE Meeting function.	2020-04-28	4	<a href="#">CVE-2020-5562</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Improper authentication vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in Application Menu.	2020-04-28	5	<a href="#">CVE-2020-5567</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Improper authentication vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to obtain data in the affected product via the API.	2020-04-28	5	<a href="#">CVE-2020-5563</a> <a href="#">MISC</a> <a href="#">MISC</a>

cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.0.0 to 4.10.3 allows remote attackers to inject arbitrary web script or HTML via the application 'E-mail'.	2020-04-28	<a href="#">4.3</a>	<a href="#">CVE-2020-5564</a> <a href="#">MISC</a> <a href="#">MISC</a>
cybozu -- garoon	Cross-site scripting vulnerability in Cybozu Garoon 4.6.0 to 5.0.0 allows remote attackers to inject arbitrary web script or HTML via the applications 'Messages' and 'Bulletin Board'.	2020-04-28	<a href="#">4.3</a>	<a href="#">CVE-2020-5568</a> <a href="#">MISC</a> <a href="#">MISC</a>
dong_joo_cho -- file_transfer_ifamily	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the .etc/ path.	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2020-12128</a> <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer.	2020-04-24	<a href="#">4.8</a>	<a href="#">CVE-2020-5870</a> <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit.	2020-04-24	<a href="#">6.4</a>	<a href="#">CVE-2020-5869</a> <a href="#">MISC</a>
gnu -- mailman	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12137</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12245</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	Grafana version < 6.7.3 is vulnerable for annotation popup XSS.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-12052</a> <a href="#">CONFIRM</a>
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 2 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1806.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1805</a> <a href="#">CONFIRM</a>

huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 1 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1805 and CVE-2020-1806.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1804</a> <a href="#">CONFIRM</a>
huawei -- honor_v10_smartphones	Huawei Honor V10 smartphones with versions earlier than 10.0.0.156(C00E156R2P4) has three out of bounds vulnerabilities. Certain driver program does not sufficiently validate certain parameters received, that would lead to several bytes out of bound read. Successful exploit may cause information disclosure or service abnormal. This is 3 out of 3 out of bounds vulnerabilities found. Different than CVE-2020-1804 and CVE-2020-1805.	2020-04-27	<a href="#">5.8</a>	<a href="#">CVE-2020-1806</a> <a href="#">CONFIRM</a>
huawei -- lion- al00c_devices	Huawei smartphone Lion-AL00C with versions earlier than 10.0.0.205(C00E202R7P2) have a denial of service vulnerability. An attacker crafted specially file to the affected device. Due to insufficient input validation of the value when executing the file, successful exploit may cause device abnormal.	2020-04-27	<a href="#">4.3</a>	<a href="#">CVE-2020-1880</a> <a href="#">CONFIRM</a>
huawei -- pcmanager	Huawei PCManager product with versions earlier than 10.0.5.53 have a local privilege escalation vulnerability. An authenticated, local attacker can perform specific operation to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.	2020-04-27	<a href="#">4.6</a>	<a href="#">CVE-2020-1845</a> <a href="#">CONFIRM</a>
ibm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 173310.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2019-4750</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 reveals a stack trace on certain API requests which can allow an attacker further information about the	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2019-4751</a> <a href="#">XE</a>

	implementation of the offering. IBM X-Force ID: 173311.			<a href="#">CONFIRM</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 172519.	2020-04-27	<a href="#">4</a>	<a href="#">CVE-2019-4729</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- mq_appliance	IBM MQ and MQ Appliance 8.0, 9.1 LTS, and 9.1 CD could allow an authenticated user cause a denial of service due to a memory leak. IBM X-Force ID: 175840.	2020-04-24	<a href="#">4</a>	<a href="#">CVE-2020-4267</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server_and_liberty	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 20.0.0.4 could allow a remote, authenticated attacker to obtain sensitive information, caused by improper parameter checking. This could be exploited to conduct spoofing attacks. IBM X-Force ID: 177841.	2020-04-28	<a href="#">4</a>	<a href="#">CVE-2020-4329</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows session fixation via an alphanumeric value in a session cookie.	2020-04-29	<a href="#">6.4</a>	<a href="#">CVE-2020-12467</a> <a href="#">MISC</a>
intelliants -- subrion_cms	Subrion CMS 4.2.1 allows CSV injection via a phrase value within a language. This is related to phrases/add/ and languages/download/.	2020-04-29	<a href="#">6.8</a>	<a href="#">CVE-2020-12468</a> <a href="#">MISC</a>
mailbeez -- mailbeez	Cross-site scripting (XSS) vulnerability in mailhive/cloudbeez/cloudloader.php and mailhive/cloudbeez/cloudloader_core.php in the MailBeez plugin for ZenCart before 3.9.22 allows remote attackers to inject arbitrary web script or HTML via the cloudloader_mode parameter.	2020-04-30	<a href="#">4.3</a>	<a href="#">CVE-2020-6579</a> <a href="#">MISC</a>
mozilla -- firefox_esr	When following a link that opened an intent://-schemed URL, causing a custom tab to be opened, Firefox for Android could be tricked into displaying the incorrect URI.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-6827</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox_esr	A malicious Android application could craft an Intent that would have been processed by Firefox for Android and potentially result in a file overwrite in the user's profile directory. One exploitation vector for this would be to supply a user.js file providing arbitrary malicious preference values. Control of arbitrary	2020-04-24	<a href="#">6.4</a>	<a href="#">CVE-2020-6828</a> <a href="#">MISC</a>



	preferences can lead to sufficient compromise such that it is generally equivalent to arbitrary code execution.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.			<a href="#">MISC</a>
mozilla -- multiple_products	When reading from areas partially or fully outside the source resource with WebGL's <code>copyTexSubImage</code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2020-6821</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2020-6820</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2020-6819</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- multiple_products	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code>GMPDecodeData</code>. It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2020-6822</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgate -- pfsense	An XSS vulnerability resides in the hostname field of the diag_ping.php page in pfsense before 2.4.5 version. After passing inputs to the command and executing this command, the \$result variable is not sanitized before it is printed.	2020-04-29	<a href="#">4.3</a>	<a href="#">CVE-2020-10797</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6100 before 1.0.1.20, R7800 before 1.0.2.40, and R9000 before 1.0.2.52.	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2017-18698</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21213</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21194</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21193</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects EX3700 before 1.0.0.66, EX3800 before 1.0.0.66, EX6100 before 1.0.2.20, EX6120 before 1.0.0.34, EX6150 before 1.0.0.36, EX6200 before 1.0.3.84, and EX7000 before 1.0.0.60.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2017-18715</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, EX6100v2 before 1.0.1.50, EX6150v2 before 1.0.1.50, EX6200v2 before 1.0.1.44, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.2.30, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50,	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2018-21228</a> <a href="#">CONFIRM</a>

	and WNDR4500v3 before 1.0.0.50.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	5.8	<a href="#">CVE-2017-18723</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1., JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020	2020-04-24	4.8	<a href="#">CVE-2018-21230</a> <a href="#">CONFIRM</a>

	before 1.1.0.42, and WNR2050 before 1.1.0.42.			
netgear -- multiple_devices	<p>Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1.78, JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.</p>	2020-04-24	4.8	<a href="#">CVE-2018-21231 CONFIRM</a>
	Certain NETGEAR devices are affected by stored XSS. This affects D6400 before 1.0.0.60, D7000 before 1.0.1.50, D8500			

netgear -- multiple_devices	before 1.0.3.29, EX6200 before 1.0.3.84, EX7000 before 1.0.0.60, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R9000 before 1.0.2.52, WNDR3400v3 before 1.0.1.16, WNR3500Lv2 before 1.2.0.46, and WNDR3700v5 before 1.1.0.48.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2017-18700</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D1500 before 1.0.0.25, D500 before 1.0.0.25, D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, EX6100v2 before 1.0.1.60, EX6150v2 before 1.0.1.60, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.16, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.18, R6020 before 1.0.0.26, R6050 before 1.0.1.16, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6220 before 1.1.0.60, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3700v5 before 1.1.0.48, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.46, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-24	<a href="#">6.8</a>	<a href="#">CVE-2017-18703</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18727</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21189</a> <a href="#">CONFIRM</a>



	WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21191</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18722</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21187</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18729</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18728</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18726</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24. R6700v2 before	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18725</a>

	1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.			<a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18724</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21192</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R6400v2 before 1.0.2.34, R6700 before 1.0.1.30, R6900 before 1.0.1.30, R6900P before 1.0.0.62, R7000 before 1.0.9.12, R7000P before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	<a href="#">5.2</a>	<a href="#">CVE-2018-21227</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21173</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18721</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21216</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected			

netgear --multiple_devices	by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18718</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18717</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18716</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18730</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18705</a> <a href="#">CONFIRM</a>
netgear --multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.28, EX2700 before 1.0.1.32, EX6200v2 before 1.0.1.56, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.52, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	<a href="#">6.5</a>	<a href="#">CVE-2018-21181</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an			

netgear -- multiple_devices	authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	6.5	<a href="#">CVE-2018-21177</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, and WNR2000v5 before 1.0.0.58.	2020-04-24	5.8	<a href="#">CVE-2017-18731</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX2700 before 1.0.1.28, R7800 before 1.0.2.40, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-27	5.8	<a href="#">CVE-2018-21170</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	5.2	<a href="#">CVE-2018-21190</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.98.	2020-04-27	5.2	<a href="#">CVE-2018-21171</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	5.2	<a href="#">CVE-2018-21180</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100			

netgear -- multiple_devices	before 1.0.0.57, D7800 before 1.0.1.30, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21179</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21178</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	<a href="#">5.2</a>	<a href="#">CVE-2018-21172</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.94.	2020-04-28	<a href="#">5.2</a>	<a href="#">CVE-2018-21182</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, and R9000 before 1.0.2.52.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21221</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, and R6100 before 1.0.1.20.	2020-04-28	<a href="#">5.8</a>	<a href="#">CVE-2018-21217</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-24	<a href="#">5.8</a>	<a href="#">CVE-2017-18720</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before	2020-04-	<a href="#">5.8</a>	<a href="#">CVE-2017-18719</a>



	1.1.00.26, R6080 before 1.1.00.26; R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	24		<a href="#">CONFIRM</a>
netgear -- r6220_devices	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	2020-04- 24	<a href="#">4.8</a>	<a href="#">CVE-2017- 18702 CONFIRM</a>
netgear -- r6700_and_r6900_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	2020-04- 24	<a href="#">4.3</a>	<a href="#">CVE-2017- 18701 CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04- 24	<a href="#">5.2</a>	<a href="#">CVE-2017- 18699 CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.3.6.	2020-04- 28	<a href="#">5.2</a>	<a href="#">CVE-2018- 21200 CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020-04- 24	<a href="#">5.2</a>	<a href="#">CVE-2017- 18697 CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04- 27	<a href="#">5.2</a>	<a href="#">CVE-2018- 21099 CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04- 27	<a href="#">5.2</a>	<a href="#">CVE-2018- 21098 CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.46 are affected by incorrect configuration of security settings.	2020-04- 27	<a href="#">5.8</a>	<a href="#">CVE-2018- 21158 CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04- 27	<a href="#">5.2</a>	<a href="#">CVE-2018- 21100 CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020-04- 24	<a href="#">4.6</a>	<a href="#">CVE-2017- 18709 CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04- 24	<a href="#">5.2</a>	<a href="#">CVE-2017- 18707 CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by CSRF. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020-04- 24	<a href="#">6.8</a>	<a href="#">CVE-2017- 18708 CONFIRM</a>
	Pega Platform before version 8.2.6 is			<a href="#">CVE-2020-</a>

pegasystems -- pega_platform	affected by a Stored Cross-Site Scripting (XSS) vulnerability in the comment tags.	2020-04-29	<a href="#">6</a>	<a href="#">8775</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
pegasystems -- pega_platform	The Richtext Editor in Pega Platform before 8.2.6 is affected by a Stored Cross-Site Scripting (XSS) vulnerability.	2020-04-29	<a href="#">6</a>	<a href="#">CVE-2020-8773</a> <a href="#">CONFIRM</a>
pegasystems -- pega_platform	Pega Platform before version 8.2.6 is affected by a Reflected Cross-Site Scripting vulnerability in the "ActionStringID" function.	2020-04-29	<a href="#">6.8</a>	<a href="#">CVE-2020-8774</a> <a href="#">CONFIRM</a>
red_hat -- openshift_container_platform	A flaw was found in openshift-ansible. OpenShift Container Platform (OCP) 3.11 is too permissive in the way it specified CORS allowed origins during installation. An attacker, able to man-in-the-middle the connection between the user's browser and the openshift console, could use this flaw to perform a phishing attack. The main threat from this vulnerability is data confidentiality.	2020-04-24	<a href="#">4</a>	<a href="#">CVE-2020-1741</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	An issue was discovered in Sonatype Nexus Repository Manager 2.x before 2.14.17 and 3.x before 3.22.1. Admin users can retrieve the LDAP server system username/password (as configured in nxrm) in cleartext.	2020-04-27	<a href="#">4</a>	<a href="#">CVE-2020-11415</a> <a href="#">CONFIRM</a>
teampass -- teampass	TeamPass 2.1.27.36 allows an unauthenticated attacker to retrieve files from the TeamPass web root. This may include backups or LDAP debug files.	2020-04-29	<a href="#">5</a>	<a href="#">CVE-2020-12478</a> <a href="#">MISC</a>
teampass -- teampass	TeamPass 2.1.27.36 allows any authenticated TeamPass user to trigger a PHP file include vulnerability via a crafted HTTP request with sources/users.queries.php newValue directory traversal.	2020-04-29	<a href="#">6.5</a>	<a href="#">CVE-2020-12479</a> <a href="#">MISC</a>
whoopsie_project -- whoopsie	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.	2020-04-24	<a href="#">4.3</a>	<a href="#">CVE-2020-12135</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
windriver -- vxworks	The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference.	2020-04-27	<a href="#">5</a>	<a href="#">CVE-2020-10664</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The Advanced Woo Search plugin version through 1.99 for Wordpress suffers from a sensitive information disclosure vulnerability in every ajax search request via the sql field to	2020-04-24	<a href="#">5</a>	<a href="#">CVE-2020-12070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	includes/class-aws-search.php.			
--	--------------------------------	--	--	--

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bluezone_global -- bluezone	React Native Bluetooth Scan in Bluezone 1.0.0 uses six-character alphanumeric IDs, which might make it easier for remote attackers to interfere with COVID-19 contact tracing by using many IDs.	2020-04-27	<a href="#">3.3</a>	<a href="#">CVE-2020-12270</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
croogo -- croogo	Croogo before 3.0.7 allows XSS via the title to admin/menus/menus or admin/taxonomy/vocabularies.	2020-04-26	<a href="#">3.5</a>	<a href="#">CVE-2019-20789</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- mate_20_smartphones	HUAWEI Mate 20 smartphones with versions earlier than 10.0.0.188(C00E74R3P8) have an improper authorization vulnerability. The software does not properly restrict certain user's modification of certain configuration file, successful exploit could allow the attacker to bypass app lock after a series of operation in ADB mode.	2020-04-27	<a href="#">3.6</a>	<a href="#">CVE-2020-1807</a> <a href="#">CONFIRM</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly sensitive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160514.	2020-04-29	<a href="#">2.1</a>	<a href="#">CVE-2019-4286</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.2.0, 7.6.2.1, 7.6.3.0, and 7.6.3.1 could disclose highly sensitive user information to an authenticated user with physical access to the device. IBM X-Force ID: 160631.	2020-04-29	<a href="#">2.1</a>	<a href="#">CVE-2019-4288</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
mozilla -- firefox	Initially, a user opens a Private Browsing Window and generates a password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new password - the generated passwords would have been identical, rather than independent. This vulnerability affects Firefox < 75.	2020-04-24	<a href="#">1.9</a>	<a href="#">CVE-2020-6824</a> <a href="#">MISC</a> <a href="#">MISC</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R6900P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8500 before 1.0.2.106, R8300 before 1.0.2.106, and WNDR3400v3 before 1.0.1.16.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18704</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18712</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18713</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R7500v2 before 1.0.3.20, R7800 before 1.0.2.38, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2018-21229</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18710</a> <a href="#">CONFIRM</a>
netgear -- srr60_and_srs60_devices	Certain NETGEAR devices are affected by stored XSS. This affects SRR60 before 2.2.1.210 and SRS60 before 2.2.1.210.	2020-04-27	<a href="#">2.3</a>	<a href="#">CVE-2018-21095</a> <a href="#">CONFIRM</a>
netgear -- wndr4500_devices	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	2020-04-24	<a href="#">3.3</a>	<a href="#">CVE-2017-18714</a> <a href="#">CONFIRM</a>
ni_consulting -- sales_force_assistant	Cross-site scripting vulnerability in Sales Force Assistant version 11.2.48 and earlier allows remote authenticated	2020-04-	<a href="#">3.5</a>	<a href="#">CVE-2020-5570</a> <a href="#">JVN</a>

	attackers to inject arbitrary web script or HTML via unspecified vectors.	28		<a href="#">MISC</a> <a href="#">MISC</a>
--	---	----	--	--

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a-pdf_wav -- a-pdf_wav	A-PDF WAV to MP3 version 1.0.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5618</a> <a href="#">MISC</a>
aasync -- aasync	AASync.com AASync version 2.2.1.0 suffers from an instance of CWE-121: Stack-based Buffer Overflow.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5619</a> <a href="#">MISC</a>
abb -- microscada_pro_sys600	ABB MicroSCADA Pro SYS600 version 9.3 suffers from an instance of CWE-306: Missing Authentication for Critical Function.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5620</a> <a href="#">MISC</a>
abb -- multiple_products	Insufficient folder permissions used by system functions in ABB System 800xA products OPCServer for AC800M (versions 6.0 and earlier) and Control Builder M Professional, MMSServer for AC800M, Base Software for SoftControl (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploited the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8472</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2,	2020-04-29	not yet calculated	<a href="#">CVE-2020-8476</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>



	AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, a weakness in validation of input exists that allows an attacker to alter licenses assigned to the system nodes by sending specially crafted messages to the CLS web service.			
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, weak file permissions allow an authenticated attacker to block the license handling, escalate his/her privileges and execute arbitrary code.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8471</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2,	2020-04-29	not yet calculated	<a href="#">CVE-2020-8475</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, a weakness in validation of input exists that allows an attacker to block license handling by sending specially crafted messages to the CLS web service.			
abb -- multiple_products	For ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, confidential data is written in an unprotected file. An attacker who successfully exploited this vulnerability could take full control of the computer.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8481</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
abb -- multiple_products	For the Central Licensing Server component used in ABB products ABB Ability™ System 800xA and related system extensions versions 5.1, 6.0 and 6.1, Compact HMI versions 5.1 and 6.0, Control Builder Safe 1.0, 1.1 and 2.0, Symphony Plus -S+ Operations 3.0 to 3.2 Symphony Plus -S+ Engineering 1.1 to 2.2, Composer Harmony 5.1, 6.0 and 6.1, Melody Composer 5.3, 6.1/6.2 and SPE for Melody 1.0SPx (Composer 6.3), Harmony OPC Server (HAOPC) Standalone 6.0, 6.1 and 7.0, ABB Ability™ System 800xA/ Advant® OCS Control Builder A 1.3 and 1.4, Advant® OCS AC100 OPC Server 5.1, 6.0 and 6.1, Composer CTK 6.1 and 6.2, AdvaBuild 3.7 SP1 and SP2, OPCServer for MOD 300 (non-800xA) 1.4, OPC Data	2020-04-29	not yet calculated	<a href="#">CVE-2020-8479</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	Link 2.1 and 2.2, Knowledge Manager 8.0, 9.0 and 9.1, Manufacturing Operations Management 1812 and 1909, an XML External Entity Injection vulnerability exists that allows an attacker to read or call arbitrary files from the license server and/or from the network and also block the license handling.			
abb -- system_800xa_base	Insufficient protection of the inter-process communication functions in ABB System 800xA Base (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8487</a> <a href="#">CONFIRM</a>
abb -- system_800xa_base	Insufficient folder permissions used by system functions in ABB System 800xA Base (version 6.1 and earlier) allow low privileged users to read, modify, add and delete system and application files. An authenticated attacker who successfully exploit the vulnerabilities could escalate his/her privileges, cause system functions to stop and to corrupt user applications.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8473</a> <a href="#">CONFIRM</a>
abb -- system_800xa_batch_management	Insufficient protection of the inter-process communication functions in ABB System 800xA Batch Management (all published versions) enables an attacker authenticated on the local system to inject data, affecting User Interface update during batch execution and/or compare/printing functionalities.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8488</a> <a href="#">CONFIRM</a>
abb -- system_800xa_for_dci	Insufficient protection of the inter-process communication functions in ABB System 800xA for DCI (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8484</a> <a href="#">CONFIRM</a>
abb -- system_800xa_for_mod_300	Insufficient protection of the inter-process communication functions in ABB System 800xA for MOD 300 (all published versions) enables an attacker authenticated on the local system to inject data, allowing reads and writes to the controllers or cause windows processes to crash.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8485</a> <a href="#">CONFIRM</a>
abb -- system_800xa_information_management	Insufficient protection of the inter-process communication functions in ABB System 800xA Information Management (all published versions) enables an attacker authenticated on the local system to inject data, affecting the runtime values to be	2020-04-29	not yet calculated	<a href="#">CVE-2020-8489</a> <a href="#">CONFIRM</a>

	stored in the archive, or making Information Management history services unavailable.			
abb -- system_800xa_products	Insufficient protection of the inter-process communication functions in ABB System 800xA products OPC Server for AC 800M, MMS Server for AC 800M and Base Software for SoftControl (all published versions) enables an attacker authenticated on the local system to inject data, affecting the online view of runtime data shown in Control Builder.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8478</a> <a href="#">CONFIRM</a>
abb -- system_800xa_rnrp	Insufficient protection of the inter-process communication functions in ABB System 800xA RNRP (all published versions) enables an attacker authenticated on the local system to inject data, affect node redundancy handling.	2020-04-29	not yet calculated	<a href="#">CVE-2020-8486</a> <a href="#">CONFIRM</a>
accellion -- file_transfer_appliance	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection').	2020-04-29	not yet calculated	<a href="#">CVE-2019-5623</a> <a href="#">MISC</a>
accellion -- file_transfer_appliance	Accellion File Transfer Appliance version FTA_8_0_540 suffers from an instance of CWE-798: Use of Hard-coded Credentials.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5622</a> <a href="#">MISC</a>
amd -- ati_atilk64.sys	AMD ATI atilk64.sys 5.11.9.0 allows low-privileged users to interact directly with physical memory by calling one of several driver routines that map physical memory into the virtual address space of the calling process. This could enable low-privileged users to achieve NT AUTHORITY\SYSTEM privileges via a DeviceIoControl call associated with MmMapIoSpace, IoAllocateMdl, MmBuildMdlForNonPagedPool, or MmMapLockedPages.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12138</a> <a href="#">MISC</a> <a href="#">MISC</a>
apache -- iotdb	An issue was found in Apache IoTDB .9.0 to 0.9.1 and 0.8.0 to 0.8.2. When starting IoTDB, the JMX port 31999 is exposed with no certification. Then, clients could execute code remotely.	2020-04-27	not yet calculated	<a href="#">CVE-2020-1952</a> <a href="#">CONFIRM</a>
apache -- nifi_registry	If NiFi Registry 0.1.0 to 0.5.0 uses an authentication mechanism other than PKI, when the user clicks Log Out, NiFi Registry invalidates the authentication token on the client side but not on the server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to	2020-04-28	not yet calculated	<a href="#">CVE-2020-9482</a> <a href="#">CONFIRM</a>

	NiFi Registry.			
apache -- ofbiz	Apache OFBiz 17.12.01 is vulnerable to some CSRF attacks.	2020-04-30	not yet calculated	<a href="#">CVE-2019-0235</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
apache -- tika	A carefully crafted or corrupt file may trigger a System.exit in Tika's OneNote Parser. Crafted or corrupted files can also cause out of memory errors and/or infinite loops in Tika's ICNSParser, MP3Parser, MP4Parser, SAS7BDATParser, OneNoteParser and ImageParser. Apache Tika users should upgrade to 1.24.1 or later. The vulnerabilities in the MP4Parser were partially fixed by upgrading the com.googlecode.isoparser:1.1.22 dependency to org.tallison:isoparser:1.9.41.2. For unrelated security reasons, we upgraded org.apache.cxf to 3.3.6 as part of the 1.24.1 release.	2020-04-27	not yet calculated	<a href="#">CVE-2020-9489</a> <a href="#">MISC</a>
apport -- apport	Apport reads and writes information on a crashed process to /proc/pid with elevated privileges. Apport then determines which user the crashed process belongs to by reading /proc/pid through get_pid_info() in data/apport. An unprivileged user could exploit this to read information about a privileged running process by exploiting PID recycling. This information could then be used to obtain ASLR offsets for a process with an existing memory corruption vulnerability. The initial fix introduced regressions in the Python Apport library due to a missing argument in Report.add_proc_environ in apport/report.py. It also caused an autopkgtest failure when reading /proc/pid and with Python 2 compatibility by reading /proc/maps. The initial and subsequent regression fixes are in 2.20.11-0ubuntu16, 2.20.11-0ubuntu8.6, 2.20.9-0ubuntu7.12, 2.20.1-0ubuntu2.22 and 2.14.1-0ubuntu3.29+esm3.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15790</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
b&r_industrial_automation -- b&r_automation_studio	A directory traversal vulnerability in SharpZipLib used in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x and 4.2.x allow unauthenticated users to write to certain local directories. The vulnerability is also known as zip slip.	2020-04-29	not yet calculated	<a href="#">CVE-2019-19102</a> <a href="#">CONFIRM</a>



b&r_industrial_automation -- b&r_automation_studio	A privilege escalation vulnerability in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.4SP, < 4.6.3SP, < 4.7.2 and < 4.8.1 allow authenticated users to delete arbitrary files via an exposed interface.	2020-04-29	not yet calculated	<a href="#">CVE-2019-19100</a> <a href="#">CONFIRM</a>
b&r_industrial_automation -- b&r_automation_studio	A missing secure communication definition and an incomplete TLS validation in the upgrade service in B&R Automation Studio versions 4.0.x, 4.1.x, 4.2.x, < 4.3.11SP, < 4.4.9SP, < 4.5.5SP, < 4.6.4 and < 4.7.2 enable unauthenticated users to perform MITM attacks via the B&R upgrade server.	2020-04-29	not yet calculated	<a href="#">CVE-2019-19101</a> <a href="#">CONFIRM</a>
beeline -- smart_box	Beeline Smart Box 2.0.38 routers allow "Advanced settings > Other > Diagnostics" OS command injection via the Ping ping_ipaddr parameter, the Nslookup nslookup_ipaddr parameter, or the Traceroute traceroute_ipaddr parameter.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12246</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.6 allows remote attackers to read arbitrary files because the presfilename (lowercase) value can be a .pdf filename while the presFilename (mixed case) value has a ../ sequence. This can be leveraged for privilege escalation via a directory traversal to bigbluebutton.properties. NOTE: this issue exists because of an ineffective mitigation to CVE-2020-12112 in which there was an attempted fix within an NGINX configuration file, without considering that the relevant part of NGINX is case-insensitive.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12443</a> <a href="#">MISC</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection (issue 2 of 2).	2020-04-30	not yet calculated	<a href="#">CVE-2019-19220</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows OS Command Injection.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19217</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 has Insecure Password Storage.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19218</a> <a href="#">MISC</a>
bmc -- control-m/agent	A buffer overflow vulnerability in BMC Control-M/Agent 7.0.00.000 when the On-Do action destination is Mail and the Control-M/Agent is configured to send the email, allows remote attackers to have unspecified impact via vectors related to the configured IP address or SMTP	2020-04-30	not yet calculated	<a href="#">CVE-2019-19215</a> <a href="#">MISC</a> <a href="#">MISC</a>

	server.			
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 has an Insecure File Copy.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19216</a> <a href="#">MISC</a>
bmc -- control-m/agent	BMC Control-M/Agent 7.0.00.000 allows Arbitrary File Download.	2020-04-30	not yet calculated	<a href="#">CVE-2019-19219</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 1 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11675</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 allows variable reuse, possibly causing data corruption.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11674</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 3 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11677</a> <a href="#">MISC</a>
cerner -- medico	Cerner medico 26.00 has a Local Buffer Overflow (issue 2 of 3).	2020-04-29	not yet calculated	<a href="#">CVE-2020-11676</a> <a href="#">MISC</a>
cisco -- ios_xe_sd-wan_software	A vulnerability in the CLI of Cisco IOS XE SD-WAN Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI utility. The attacker must be authenticated to access the CLI utility. A successful exploit could allow the attacker to execute commands with root privileges.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16011</a> <a href="#">CISCO</a>
dom4j -- dom4j	dom4j before 2.1.3 allows external DTDs and External Entities by default, which might enable XXE attacks. However, there is popular external documentation from OWASP showing how to enable the safe, non-default behavior in any application that uses dom4j.	2020-05-01	not yet calculated	<a href="#">CVE-2020-10683</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ebiz4u -- ebiz4u	AxEcm.cab(ActiveX Control) in Inogard Ebiz4u contains a vulnerability that could allow remote files to be downloaded and executed by setting arguments to the activeX method. Download of Code Without Integrity Check vulnerability in ActiveX control of Inogard Co.,LTD Ebiz4u ActiveX of Inogard Co.,LTD(AxEcm.cab) allows ATTACKER to cause a file download to Windows user's folder and execute. This issue affects: Inogard Co.,LTD Ebiz4u ActiveX	2020-04-29	not yet calculated	<a href="#">CVE-2019-19165</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	of Inogard Co.,LTD(AxECM.cab) version 1.0.5.0 and later versions on windows 7/8/10.			
eset -- antivirus_and_antispyware_module	ESET Antivirus and Antispyware Module module 1553 through 1560 allows a user with limited access rights to create hard links in some ESET directories and then force the product to write through these links into files that would normally not be write-able by the user, thus achieving privilege escalation.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11446</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 14.0.0-14.0.1, and 13.1.0-13.1.3.1, when a virtual server is configured with HTTP explicit proxy and has an attached HTTP_PROXY_REQUEST iRule, POST requests sent to the virtual server cause an xdata memory leak.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5883</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5, and 11.6.1-11.6.5.1, under certain conditions, the Intel QuickAssist Technology (QAT) cryptography driver may produce a Traffic Management Microkernel (TMM) core file.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5882</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.4, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the default deployment mode for BIG-IP high availability (HA) pair mirroring is insecure. This is a control plane issue that is exposed only on the network used for mirroring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5884</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, a race condition exists where mcpd and other processes may make unencrypted connection attempts to a new configuration sync peer. The race condition can occur when changing the ConfigSync IP address of a peer, adding a new peer, or when the Traffic Management Microkernel (TMM) first starts up.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5876</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.2.3, 14.0.0-14.0.1, 13.1.0-13.1.3.1, and 12.1.0-12.1.4.1, when processing TLS traffic with hardware cryptographic acceleration enabled on platforms with Intel QAT hardware, the Traffic Management Microkernel (TMM) may stop responding and cause a failover event.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5872</a> <a href="#">CONFIRM</a>

f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.3 and 14.1.0-14.1.2.3, the restjavad process may expose a way for attackers to upload arbitrary files on the BIG-IP system, bypassing the authorization system. Resulting error messages may also reveal internal paths of the server.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5880</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.2.3, undisclosed requests can lead to a denial of service (DoS) when sent to BIG-IP HTTP/2 virtual servers. The problem can occur when ciphers, which have been blacklisted by the HTTP/2 RFC, are used on backend servers. This is a data-plane issue. There is no control-plane exposure.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5871</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1 and BIG-IQ 5.2.0-7.1.0, when creating a QKView, credentials for binding to LDAP servers used for remote authentication of the BIG-IP administrative interface will not fully obfuscate if they contain whitespace.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5890</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1 and 14.1.0-14.1.2.3, under certain conditions, the Traffic Management Microkernel (TMM) may generate a core file and restart while processing SSL traffic with an HTTP/2 full proxy.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5875</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, undisclosed HTTP/2 requests can lead to a denial of service when sent to a virtual server configured with the Fallback Host setting and a server-side HTTP/2 profile.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5891</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems setup for connection mirroring in a High Availability (HA) pair transfers sensitive cryptographic objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5886</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, and 12.1.0-12.1.5.1, BIG-IP systems set up for connection mirroring in a high availability (HA) pair transfer sensitive cryptographic objects over an insecure communications channel. This is a control plane issue which is exposed only on the network used for connection mirroring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5885</a> <a href="#">CONFIRM</a>

f5 -- big-ip	On BIG-IP 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, malformed input to the DATAGRAM::tcp iRules command within a FLOW_INIT event may lead to a denial of service.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5877</a> <a href="#">CONFIRM</a>
f5 -- big-ip_and_big-iq	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.3, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.1-11.6.5 and BIG-IQ 5.2.0-7.1.0, a user associated with the Resource Administrator role who has access to the secure copy (scp) utility but does not have access to Advanced Shell (bash) can execute arbitrary commands using a maliciously crafted scp request.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5873</a> <a href="#">MISC</a>
f5 -- big-ip_apm	On BIG-IP APM 15.0.0-15.0.1.2, 14.1.0-14.1.2.3, and 14.0.0-14.0.1, in certain circumstances, an attacker sending specifically crafted requests to a BIG-IP APM virtual server may cause a disruption of service provided by the Traffic Management Microkernel(TMM).	2020-04-30	not yet calculated	<a href="#">CVE-2020-5874</a> <a href="#">CONFIRM</a>
f5 -- big-ip_apm	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, in BIG-IP APM portal access, a specially crafted HTTP request can lead to reflected XSS after the BIG-IP APM system rewrites the HTTP response from the untrusted backend server and sends it to the client.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5889</a> <a href="#">CONFIRM</a>
f5 -- big-ip_apm_and_edge_gateway_and_firepass	In versions 7.1.5-7.1.8, the BIG-IP Edge Client components in BIG-IP APM, Edge Gateway, and FirePass legacy allow attackers to obtain the full session ID from process memory.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5892</a> <a href="#">CONFIRM</a>
f5 -- big-ip_asm	On BIG-IP ASM 11.6.1-11.6.5.1, under certain configurations, the BIG-IP system sends data plane traffic to back-end servers unencrypted, even when a Server SSL profile is applied.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5879</a> <a href="#">CONFIRM</a>
f5 -- big-ip_edge_client	In versions 7.1.5-7.1.8, when a user connects to a VPN using BIG-IP Edge Client over an unsecure network, BIG-IP Edge Client responds to authentication requests over HTTP while sending probes for captive portal detection.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5893</a> <a href="#">CONFIRM</a>
f5 -- big-ip_virtual_edition	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.3, Traffic Management Microkernel (TMM) may restart on BIG-IP Virtual Edition (VE) while processing unusual IP traffic.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5878</a> <a href="#">MISC</a>
	On versions 15.1.0-15.1.0.1, 15.0.0-			



f5 -- big-ip_virtual_edition	15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for remote attackers to access local daemons and bypass port lockdown settings.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5887</a> <a href="#">CONFIRM</a>
f5 -- big-ip_virtual_edition	On versions 15.0.0-15.1.0.1, 14.1.0-14.1.2.3, and 13.1.0-13.1.3.3, when the BIG-IP Virtual Edition (VE) is configured with VLAN groups and there are devices configured with OSPF connected to it, the Network Device Abstraction Layer (NDAL) Interfaces can lock up and in turn disrupting the communication between the mcpd and tmm processes.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5881</a> <a href="#">CONFIRM</a>
f5 -- big-ip_virtual_edition	On versions 15.1.0-15.1.0.1, 15.0.0-15.0.1.2, and 14.1.0-14.1.2.3, BIG-IP Virtual Edition (VE) may expose a mechanism for adjacent network (layer 2) attackers to access local daemons and bypass port lockdown settings.	2020-04-30	not yet calculated	<a href="#">CVE-2020-5888</a> <a href="#">CONFIRM</a>
faye_gem_for_ruby_on_rails -- faye_gem_for_ruby_on_rails	Faye (NPM, RubyGem) versions greater than 0.5.0 and before 1.0.4, 1.1.3 and 1.2.5, has the potential for authentication bypass in the extension system. The vulnerability allows any client to bypass checks put in place by server-side extensions, by appending extra segments to the message channel. It is patched in versions 1.0.4, 1.1.3 and 1.2.5.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11020</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ffmpeg -- ffmpeg	cbs_jpeg_split_fragment in libavcodec/cbs_jpeg.c in FFmpeg 4.2.2 has a heap-based buffer overflow during JPEG_MARKER_SOS handling because of a missing length check.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12284</a> <a href="#">MISC</a> <a href="#">MISC</a>
fonality -- trixbox_community_edition	An OS Command Injection vulnerability in the endpoint_devicemap.php component of Fonality Trixbox Community Edition allows an attacker to execute commands on the underlying operating system as the "asterisk" user. Note that Trixbox Community Edition has been unsupported by the vendor since 2012. This issue affects: Fonality Trixbox Community Edition, versions 1.2.0 through 2.8.0.4. Versions 1.0 and 1.1 are unaffected.	2020-05-01	not yet calculated	<a href="#">CVE-2020-7351</a> <a href="#">MISC</a>
fortiguard -- fortimail_and_foritvoiceenterprise	An improper authentication vulnerability in FortiMail 5.4.10, 6.0.7, 6.2.2 and earlier and FortiVoiceEnterprise 6.0.0 and 6.0.1 may allow a remote unauthenticated attacker to access the system as a legitimate user by requesting a password change via the user interface.	2020-04-27	not yet calculated	<a href="#">CVE-2020-9294</a> <a href="#">CONFIRM</a>

freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in accessing out-of-bounds memory leading to a kernel panic or other unpredictable results.	2020-04-29	not yet calculated	<a href="#">CVE-2019-5614</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r357490, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r357489, and 11.3-RELEASE before 11.3-RELEASE-p7, incorrect use of a user-controlled pointer in the epair virtual network module allowed vnet jailed privileged users to panic the host system and potentially execute arbitrary code in the kernel.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7452</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356035, 12.1-RELEASE before 12.1-RELEASE-p4, 11.3-STABLE before r356036, and 11.3-RELEASE before 11.3-RELEASE-p8, incomplete packet data validation may result in memory access after it has been freed leading to a kernel panic or other unpredictable results.	2020-04-29	not yet calculated	<a href="#">CVE-2019-15874</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356089, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r356090, and 11.3-RELEASE before 11.3-RELEASE-p7, driver specific ioctl command handlers in the oce network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to send passthrough commands to the device firmware.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15876</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r356606 and 12.1-RELEASE before 12.1-RELEASE-p3, driver specific ioctl command handlers in the ixl network driver failed to check whether the caller has sufficient privileges allowing unprivileged users to trigger updates to the device's non-volatile memory.	2020-04-28	not yet calculated	<a href="#">CVE-2019-15877</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r359021, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r359020, and 11.3-RELEASE before 11.3-RELEASE-p7, a missing null termination check in the jail_set configuration option "osrelease" may	2020-04-29	not yet calculated	<a href="#">CVE-2020-7453</a> <a href="#">CONFIRM</a>

	return more bytes with a subsequent jail_get system call allowing a malicious jail superuser with permission to create nested jails to read kernel memory.			
freebsd -- freebsd	In FreeBSD 12.1-STABLE before r358739, 12.1-RELEASE before 12.1-RELEASE-p3, 11.3-STABLE before r358740, and 11.3-RELEASE before 11.3-RELEASE-p7, a TCP SYN-ACK or challenge TCP-ACK segment over IPv6 that is transmitted or retransmitted does not properly initialize the Traffic Class field disclosing one byte of kernel memory over the network.	2020-04-28	not yet calculated	<a href="#">CVE-2020-7451</a> <a href="#">CONFIRM</a>
freeipa -- freeipa	A flaw was found in all ipa versions 4.x.x through 4.8.0. When sending a very long password (>= 1,000,000 characters) to the server, the password hashing process could exhaust memory and CPU leading to a denial of service and the website becoming unresponsive. The highest threat from this vulnerability is to system availability.	2020-04-27	not yet calculated	<a href="#">CVE-2020-1722</a> <a href="#">CONFIRM</a>
fun-map -- fun-map	fun-map through 3.3.1 is vulnerable to Prototype Pollution. The function assocInM could be tricked into adding or modifying properties of 'Object.prototype' using a '__proto__' payload.	2020-04-28	not yet calculated	<a href="#">CVE-2020-7644</a> <a href="#">MISC</a> <a href="#">MISC</a>
g.skill -- trident_z_lighting_control	The ene.sys driver in G.SKILL Trident Z Lighting Control through 1.00.08 exposes mapping and un-mapping of physical memory, reading and writing to Model Specific Register (MSR) registers, and input from and output to I/O ports to local non-privileged users. This leads to privilege escalation to NT AUTHORITY\SYSTEM.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12446</a> <a href="#">MISC</a>
generix -- upsadapter_cs141	UPS Adapter CS141 before 1.90 allows Directory Traversal. An attacker with Admin or Engineer login credentials could exploit the vulnerability by manipulating variables that reference files and by doing this achieve access to files and directories outside the web root folder. An attacker may access arbitrary files and directories stored in the file system, but integrity of the files are not jeopardized as attacker have read access rights only.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11420</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
genius_bytes -- genius_server	An application plugin in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to gain admin privileges.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16653</a> <a href="#">MISC</a>

genius_bytes -- genius_server	The BPM component in Genius Bytes Genius Server (Genius CDDS) 3.2.2 allows remote authenticated users to execute arbitrary commands.	2020-04-29	not yet calculated	<a href="#">CVE-2019-16652</a> <a href="#">MISC</a> <a href="#">MISC</a>
gigamon -- gigavue	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an arbitrary file upload for an authenticated user. If an executable file is uploaded into the www-root directory, then it could yield remote code execution via the filename parameter.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12252</a> <a href="#">MISC</a> <a href="#">MISC</a>
gigamon -- gigavue	An issue was discovered in Gigamon GigaVUE 5.5.01.11. The upload functionality allows an authenticated user to change the filename value (in the POST method) from the original filename to achieve directory traversal via a ../ sequence and, for example, obtain a complete directory listing of the machine.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12251</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab 12.6 through 12.9 is vulnerable to a privilege escalation that allows an external user to create a personal snippet through the API.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12275</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab 9.5.9 through 12.9 is vulnerable to stored XSS in an admin notification feature.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12276</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab 10.8 through 12.9 has a vulnerability that allows someone to mirror a repository even if the feature is not activated.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12277</a> <a href="#">CONFIRM</a>
glibc -- glibc	A use-after-free vulnerability introduced in glibc upstream version 2.14 was found in the way the tilde expansion was carried out. Directory paths containing an initial tilde followed by a valid username were affected by this issue. A local attacker could exploit this flaw by creating a specially crafted path that, when processed by the glob function, would potentially lead to arbitrary code execution. This was fixed in version 2.32.	2020-04-30	not yet calculated	<a href="#">CVE-2020-1752</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
google -- chrome-launcher	All versions of chrome-launcher allow execution of arbitrary commands, by controlling the \$HOME environment variable in Linux operating systems.	2020-05-02	not yet calculated	<a href="#">CVE-2020-7645</a> <a href="#">MISC</a>
grafana -- grafana	An information-disclosure flaw was found in Grafana through 6.7.3. The database directory /var/lib/grafana and database file /var/lib/grafana/grafana.db are world readable. This can result in exposure of	2020-04-29	not yet calculated	<a href="#">CVE-2020-12458</a> <a href="#">MISC</a> <a href="#">MISC</a>

	sensitive information (e.g., cleartext or encrypted datasource passwords).			
grafana -- grafana	In certain Red Hat packages for Grafana 6.x through 6.3.6, the configuration files /etc/grafana/grafana.ini and /etc/grafana/ldap.toml (which contain a secret_key and a bind_password) are world readable.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12459</a> <a href="#">MISC</a> <a href="#">MISC</a>
handysoft -- handy_groupware	ActiveX Control(HShell.dll) in Handy Groupware 1.7.3.1 for Windows 7, 8, and 10 allows an attacker to execute arbitrary command via the ShellExec method.	2020-04-29	not yet calculated	<a href="#">CVE-2020-7804</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.4 contained a cross-site scripting vulnerability such that files from a malicious workload could cause arbitrary JavaScript to execute in the web UI. Fixed in 0.10.5.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10944</a> <a href="#">CONFIRM</a>
hcl -- connections	HCL Connections v5.5, v6.0, and v6.5 contains an open redirect vulnerability which could be exploited by an attacker to conduct phishing attacks.	2020-05-01	not yet calculated	<a href="#">CVE-2019-4209</a> <a href="#">CONFIRM</a>
hp -- multiple_products	A potential security vulnerability has been identified in the disk drive firmware installers named Supplemental Update / Online ROM Flash Component on HPE servers running Linux. The vulnerable software is included in the HPE Service Pack for ProLiant (SPP) releases 2018.06.0, 2018.09.0, and 2018.11.0. The vulnerable software is the Supplemental Update / Online ROM Flash Component for Linux (x64) software. The installer in this software component could be locally exploited to execute arbitrary code. Drive Models can be found in the Vulnerability Resolution field of the security bulletin. The 2019_03 SPP and Supplemental update / Online ROM Flash Component for Linux (x64) after 2019.03.0 has fixed this issue.	2020-04-27	not yet calculated	<a href="#">CVE-2020-7135</a> <a href="#">CONFIRM</a>
hp -- smart_update_manager	A security vulnerability in HPE Smart Update Manager (SUM) prior to version 8.5.6 could allow remote unauthorized access. Hewlett Packard Enterprise has provided a software update to resolve this vulnerability in HPE Smart Update Manager (SUM) prior to 8.5.6. Please visit the HPE Support Center at <a href="https://support.hpe.com/hpesc/public/home">https://support.hpe.com/hpesc/public/home</a> to download the latest version of HPE Smart Update Manager (SUM). Download	2020-04-30	not yet calculated	<a href="#">CVE-2020-7136</a> <a href="#">CONFIRM</a>



	the latest version of HPE Smart Update Manager (SUM) or download the latest Service Pack For ProLiant (SPP).			
http-client -- http-client	<p>Actions Http-Client (NPM @actions/http-client) before version 1.0.8 can disclose Authorization headers to incorrect domain in certain redirect scenarios. The conditions in which this happens are if consumers of the http-client: 1. make an http request with an authorization header 2. that request leads to a redirect (302) and 3. the redirect url redirects to another domain or hostname Then the authorization header will get passed to the other domain. The problem is fixed in version 1.0.8.</p>	2020-04-29	not yet calculated	<a href="#">CVE-2020-11021</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	<p>There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 2 out of 2 vulnerabilities. Different than CVE-2020-5302. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than 9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than 9.1.0.350(C10E3R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8), earlier than 9.1.0.350(C636E4R1P13T8) Charlotte-L09C: earlier than 9.1.0.311(C185E4R1P11T8), earlier than 9.1.0.345(C432E8R1P11T8) Charlotte-L29C: earlier than 9.1.0.325(C185E4R1P11T8), earlier than 9.1.0.335(C636E3R1P13T8), earlier than 9.1.0.345(C432E8R1P11T8), earlier than 9.1.0.336(C605E3R1P12T8) Columbia-AL10B: earlier than 9.1.0.333(C00E333R1P1T8) Columbia-L29D: earlier than 9.1.0.350(C461E3R1P11T8), earlier than</p>			

huawei -- multiple_smartphones	<p>9.1.0.350(C185E3R1P12T8), earlier than  9.1.0.350(C10E5R1P14T8), earlier than  9.1.0.351(C432E5R1P13T8) Cornell-AL00A: earlier than  9.1.0.333(C00E333R1P1T8) Cornell-L29A: earlier than  9.1.0.328(C185E1R1P9T8), earlier than  9.1.0.328(C432E1R1P9T8), earlier than  9.1.0.330(C461E1R1P9T8), earlier than  9.1.0.328(C636E2R1P12T8) Emily-L09C: earlier than  9.1.0.336(C605E4R1P12T8), earlier than  9.1.0.311(C185E2R1P12T8), earlier than  9.1.0.345(C432E10R1P12T8) Emily-L29C: earlier than  9.1.0.311(C605E2R1P12T8), earlier than  9.1.0.311(C636E7R1P13T8), earlier than  9.1.0.311(C432E7R1P11T8) Ever-L29B: earlier than  9.1.0.311(C185E3R3P1), earlier than  9.1.0.310(C636E3R2P1), earlier than  9.1.0.310(C432E3R1P12) HUAWEI Mate 20: earlier than  9.1.0.131(C00E131R3P1) HUAWEI Mate 20 Pro: earlier than  9.1.0.310(C185E10R2P1) HUAWEI Mate 20 RS: earlier than  9.1.0.135(C786E133R3P1) HUAWEI Mate 20 X: earlier than  9.1.0.135(C00E133R2P1) HUAWEI P20: earlier than  9.1.0.333(C00E333R1P1T8) HUAWEI P20 Pro: earlier than  9.1.0.333(C00E333R1P1T8) HUAWEI P30: earlier than  9.1.0.193 HUAWEI P30 Pro: earlier than  9.1.0.186(C00E180R2P1) HUAWEI Y9 2019: earlier than  9.1.0.220(C605E3R1P1T8) HUAWEI nova lite 3: earlier than  9.1.0.305(C635E8R2P2) Honor 10 Lite: earlier than  9.1.0.283(C605E8R2P2) Honor 8X: earlier than  9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than  9.1.0.238(C432E1R3P1) Jackman-L22: earlier than  9.1.0.247(C636E2R4P1T8) Paris-L21B: earlier than  9.1.0.331(C432E1R1P2T8) Paris-L21MEB: earlier than  9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than  9.1.0.331(C636E1R1P3T8) Sydney-AL00: earlier than  9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than  9.1.0.215(C432E1R1P1T8), earlier than  9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than  9.1.0.213(C185E1R1P2T8) Sydney-L22:</p>	2020-04-27	not yet calculated	<a href="#">CVE-2019-5303</a> <a href="#">CONFIRM</a>
-----------------------------------	---	------------	--------------------	--

	<p>earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than 9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)</p>			
	<p>There are two denial of service vulnerabilities on some Huawei smartphones. An attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices. Due to insufficient input validation of two values when parsing the messages, successful exploit may cause device abnormal. This is 1 out of 2 vulnerabilities. Different than CVE-2020-5303. Affected products are: ALP-AL00B: earlier than 9.1.0.333(C00E333R2P1T8) ALP-L09: earlier than 9.1.0.300(C432E4R1P9T8) ALP-L29: earlier than 9.1.0.315(C636E5R1P13T8) BLA-L29C: earlier than 9.1.0.321(C636E4R1P14T8), earlier than 9.1.0.330(C432E6R1P12T8), earlier than 9.1.0.302(C635E4R1P13T8) Berkeley-AL20: earlier than 9.1.0.333(C00E333R2P1T8) Berkeley-L09: earlier than 9.1.0.350(C10E3R1P14T8), earlier than 9.1.0.351(C432E5R1P13T8), earlier than 9.1.0.350(C636E4R1P13T8) Charlotte-L09C: earlier than 9.1.0.311(C185E4R1P11T8), earlier than</p>			

huawei -- multiple_smartphones	<p>9.1.0.345(C432E8R1P11T8) Charlotte-L29C: earlier than</p> <p>9.1.0.325(C185E4R1P11T8), earlier than</p> <p>9.1.0.335(C636E3R1P13T8), earlier than</p> <p>9.1.0.345(C432E8R1P11T8), earlier than</p> <p>9.1.0.336(C605E3R1P12T8) Columbia-AL10B: earlier than</p> <p>9.1.0.333(C00E333R1P1T8) Columbia-L29D: earlier than</p> <p>9.1.0.350(C461E3R1P11T8), earlier than</p> <p>9.1.0.350(C185E3R1P12T8), earlier than</p> <p>9.1.0.350(C10E5R1P14T8), earlier than</p> <p>9.1.0.351(C432E5R1P13T8) Cornell-AL00A: earlier than</p> <p>9.1.0.333(C00E333R1P1T8) Cornell-L29A: earlier than</p> <p>9.1.0.328(C185E1R1P9T8), earlier than</p> <p>9.1.0.328(C432E1R1P9T8), earlier than</p> <p>9.1.0.330(C461E1R1P9T8), earlier than</p> <p>9.1.0.328(C636E2R1P12T8) Emily-L09C: earlier than</p> <p>9.1.0.336(C605E4R1P12T8), earlier than</p> <p>9.1.0.311(C185E2R1P12T8), earlier than</p> <p>9.1.0.345(C432E10R1P12T8) Emily-L29C: earlier than</p> <p>9.1.0.311(C605E2R1P12T8), earlier than</p> <p>9.1.0.311(C636E7R1P13T8), earlier than</p> <p>9.1.0.311(C432E7R1P11T8) Ever-L29B: earlier than</p> <p>9.1.0.311(C185E3R3P1), earlier than</p> <p>9.1.0.310(C636E3R2P1), earlier than</p> <p>9.1.0.310(C432E3R1P12) HUAWEI Mate 20: earlier than</p> <p>9.1.0.131(C00E131R3P1) HUAWEI Mate 20 Pro: earlier than</p> <p>9.1.0.310(C185E10R2P1) HUAWEI Mate 20 RS: earlier than</p> <p>9.1.0.135(C786E133R3P1) HUAWEI Mate 20 X: earlier than</p> <p>9.1.0.135(C00E133R2P1) HUAWEI P20: earlier than</p> <p>9.1.0.333(C00E333R1P1T8) HUAWEI P20 Pro: earlier than</p> <p>9.1.0.333(C00E333R1P1T8) HUAWEI P30: earlier than</p> <p>9.1.0.193 HUAWEI P30 Pro: earlier than</p> <p>9.1.0.186(C00E180R2P1) HUAWEI Y9 2019: earlier than</p> <p>9.1.0.220(C605E3R1P1T8) HUAWEI nova lite 3: earlier than</p> <p>9.1.0.305(C635E8R2P2) Honor 10 Lite: earlier than</p> <p>9.1.0.283(C605E8R2P2) Honor 8X: earlier than</p> <p>9.1.0.221(C461E2R1P1T8) Honor View 20: earlier than</p> <p>9.1.0.238(C432E1R3P1) Jackman-L22: earlier than</p> <p>9.1.0.247(C636E2R4P1T8) Paris-L21B:</p>	2020-04-27	not yet calculated	<a href="#">CVE-2019-5302</a> <a href="#">CONFIRM</a>
-----------------------------------	---	------------	--------------------	--

	<p>earlier than 9.1.0.331(C432E1R1P2T8) Paris-L21MEB: earlier than 9.1.0.331(C185E4R1P3T8) Paris-L29B: earlier than 9.1.0.331(C636E1R1P3T8) Sydney-AL00: earlier than 9.1.0.212(C00E62R1P7T8) Sydney-L21: earlier than 9.1.0.215(C432E1R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8) Sydney-L21BR: earlier than 9.1.0.213(C185E1R1P2T8) Sydney-L22: earlier than 9.1.0.258(C636E1R1P1T8) Sydney-L22BR: earlier than 9.1.0.258(C636E1R1P1T8) SydneyM-AL00: earlier than 9.1.0.228(C00E78R1P7T8) SydneyM-L01: earlier than 9.1.0.215(C782E2R1P1T8), earlier than 9.1.0.213(C185E1R1P1T8), earlier than 9.1.0.270(C432E3R1P1T8) SydneyM-L03: earlier than 9.1.0.217(C605E1R1P1T8) SydneyM-L21: earlier than 9.1.0.221(C461E1R1P1T8), earlier than 9.1.0.215(C432E4R1P1T8) SydneyM-L22: earlier than 9.1.0.259(C185E1R1P2T8), earlier than 9.1.0.220(C635E1R1P2T8), earlier than 9.1.0.216(C569E1R1P1T8) SydneyM-L23: earlier than 9.1.0.226(C605E2R1P1T8) Yale-L21A: earlier than 9.1.0.154(C432E2R3P2), earlier than 9.1.0.154(C461E2R2P1), earlier than 9.1.0.154(C636E2R2P1) Honor 20: earlier than 9.1.0.152(C00E150R5P1) Honor Magic2: earlier than 10.0.0.187 Honor V20: earlier than 9.1.0.234(C00E234R4P3)</p>			
huawei -- oceanstor_5310	<p>Huawei OceanStor 5310 product with version of V500R007C60SPC100 has an invalid pointer access vulnerability. The software system access an invalid pointer when attacker malformed packet. Due to the insufficient validation of some parameter, successful exploit could cause device reboot.</p>	2020-04-30	not yet calculated	<a href="#">CVE-2020-9098</a> CONFIRM CONFIRM
huawei -- osd	<p>Huawei OSD product with versions earlier than OSD_uwp_9.0.32.0 have a local privilege escalation vulnerability. An authenticated, local attacker can constructs a specific file path to exploit this vulnerability. Successful exploitation may cause the attacker to obtain a higher privilege.</p>	2020-04-27	not yet calculated	<a href="#">CVE-2020-9072</a> CONFIRM CONFIRM



huawei -- pcmanager	Huawei PCManager with versions earlier than 10.0.1.36 has a privilege escalation vulnerability. Due to improper permission management of specific files, local attackers with low permissions can inject commands to exploit this vulnerability. Successful exploit may cause privilege escalation.	2020-04-30	not yet calculated	<a href="#">CVE-2020-1817</a> <a href="#">CONFIRM</a>
inductive_automation - - ignition_8_gateway	An unprotected logging route may allow an attacker to write endless log statements into the database without space limits or authentication. This results in consuming the entire available hard-disk space on the Ignition 8 Gateway (versions prior to 8.0.10), causing a denial-of-service condition.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10641</a> <a href="#">MISC</a>
intelliants -- subrion_cms	admin/blocks.php in Subrion CMS through 4.2.1 allows PHP Object Injection (with resultant file deletion) via serialized data in the subpages value within a block to blocks/edit.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12469</a> <a href="#">MISC</a>
intelmq_manager -- intelmq_manager	IntelMQ Manager from version 1.1.0 and before version 2.1.1 has a vulnerability where the backend incorrectly handled messages given by user-input in the "send" functionality of the Inspect-tool of the Monitor component. An attacker with access to the IntelMQ Manager could possibly use this issue to execute arbitrary code with the privileges of the webserver. Version 2.1.1 fixes the vulnerability.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11016</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jquery -- jquery	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11023</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jquery -- jquery	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11022</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
	The JSON gem through 2.2.0 for Ruby, as used in Ruby 2.4 through 2.4.9, 2.5 through 2.5.7, and 2.6 through 2.6.5, has an Unsafe Object Creation Vulnerability.			<a href="#">CVE-2020-10663</a>

json_gem_for_ruby_on_rails -- json_gem_for_ruby_on_rails	This is quite similar to CVE-2013-0269, but does not rely on poor garbage-collection behavior within Ruby. Specifically, use of JSON parsing methods can lead to creation of a malicious object within the interpreter, with adverse effects that are application-dependent.	2020-04-28	not yet calculated	<a href="#">SUSE MLIST</a> <a href="#">FEDORA CONFIRM</a>
kiali -- kiali	An insufficient JWT validation vulnerability was found in Kiali versions 0.4.0 to 1.15.0 and was fixed in Kiali version 1.15.1, wherein a remote attacker could abuse this flaw by stealing a valid JWT cookie and using that to spoof a user session, possibly gaining privileges to view and alter the Istio configuration.	2020-04-27	not yet calculated	<a href="#">CVE-2020-1762</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
lexmark -- multiple_devices	A cross-site scripting (XSS) vulnerability in Lexmark CS31x before LW74.VYL.P273; CS41x before LW74.VY2.P273; CS51x before LW74.VY4.P273; CX310 before LW74.GM2.P273; CX410 & XC2130 before LW74.GM4.P273; CX510 & XC2132 before LW74.GM7.P273; MS310, MS312, MS317 before LW74.PRL.P273; MS410, M1140 before LW74.PRL.P273; MS315, MS415, MS417 before LW74.TL2.P273; MS51x, MS610dn, MS617 before LW74.PR2.P273; M1145, M3150dn before LW74.PR2.P273; MS610de, M3150 before LW74.PR4.P273; MS71x, M5163dn before LW74.DN2.P273; MS810, MS811, MS812, MS817, MS818 before LW74.DN2.P273; MS810de, M5155, M5163 before LW74.DN4.P273; MS812de, M5170 before LW74.DN7.P273; MS91x before LW74.SA.P273; MX31x, XM1135 before LW74.SB2.P273; MX410, MX510 & MX511 before LW74.SB4.P273; XM1140, XM1145 before LW74.SB4.P273; MX610 & MX611 before LW74.SB7.P273; XM3150 before LW74.SB7.P273; MX71x, MX81x before LW74.TU.P273; XM51xx & XM71xx before LW74.TU.P273; MX91x & XM91x before LW74.MG.P273; MX6500e before LW74.JD.P273; C746 before LHS60.CM2.P738; C748, CS748 before LHS60.CM4.P738; C792, CS796 before LHS60.HC.P738; C925 before LHS60.HV.P738; C950 before	2020-04-28	not yet calculated	<a href="#">CVE-2020-10094</a> <a href="#">CONFIRM</a>

	LHS60.TP.P738; X548 & XS548 before LHS60.VK.P738; X74x & XS748 before LHS60.NY.P738; X792 & XS79x before LHS60.MR.P738; X925 & XS925 before LHS60.HK.P738; X95x & XS95x before LHS60.TQ.P738; 6500e before LHS60.JR.P738; C734 LR.SK.P824 and earlier; C736 LR.SKE.P824 and earlier; E46x LR.LBH.P824 and earlier; T65x LR.JP.P824 and earlier; X46x LR.BS.P824 and earlier; X65x LR.MN.P824 and earlier; X73x LR.FL.P824 and earlier; W850 LP.JB.P823 and earlier; and X86x LP.SP.P823 and earlier.			
lexmark -- pro910_series_devices	A cross-site scripting (XSS) vulnerability in Lexmark Pro910 series inkjet and other discontinued products.	2020-04-28	not yet calculated	<a href="#">CVE-2020-10093</a> <a href="#">CONFIRM</a>
lg -- bridge	An issue was discovered in LG Bridge before April 2019 on Windows. DLL Hijacking can occur.	2020-04-29	not yet calculated	<a href="#">CVE-2019-20781</a> <a href="#">CONFIRM</a>
libgit2 -- libgit2	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. path.c mishandles equivalent filenames that exist because of NTFS Alternate Data Streams. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1352.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12278</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgit2 -- libgit2	An issue was discovered in libgit2 before 0.28.4 and 0.9x before 0.99.0. checkout.c mishandles equivalent filenames that exist because of NTFS short names. This may allow remote code execution when cloning a repository. This issue is similar to CVE-2019-1353.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12279</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libvirt -- libvirt	An issue was discovered in qemuDomainGetStatsIOThread in qemu/qemu_driver.c in libvirt 4.10.0 though 6.x before 6.1.0. A memory leak was found in the virDomainListGetStats libvirt API that is responsible for retrieving domain statistics when managing QEMU guests. This flaw allows unprivileged users with a read-only connection to cause a memory leak in the domstats command, resulting in a potential denial of service.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12430</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel through 5.6.7 on the s390 platform, code execution may occur because of a race condition, as demonstrated by code in enable_sacf_uaccess in	2020-04-29	not yet calculated	<a href="#">CVE-2020-11884</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a>

	arch/s390/lib/uaccess.c that fails to protect against a concurrent page table upgrade, aka CID-3f777e19d171. A crash could also occur.			<a href="#">FEDORA</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
linux -- linux_kernel	An array overflow was discovered in mt76_add_fragment in drivers/net/wireless/mediatek/mt76/dma.c in the Linux kernel before 5.5.10, aka CID-b102f0c522cf. An oversized packet with too many rx fragments can corrupt memory of adjacent pages.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	usb_sg_cancel in drivers/usb/core/message.c in the Linux kernel before 5.6.8 has a use-after-free because a transfer occurs without a reference, aka CID-056ad39ee925.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12464</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mahara -- mahara	In Mahara 19.04 before 19.04.5 and 19.10 before 19.10.3, account details are shared in the Elasticsearch results for accounts that are not accessible when the config setting 'Isolated institutions' is turned on.	2020-04-30	not yet calculated	<a href="#">CVE-2020-9387</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
monox -- monox	MonoX through 5.1.40.5152 allows remote code execution via HTML5Upload.ashx or Pages/SocialNetworking/Ing/en-US/PhotoGallery.aspx because of deserialization in ModuleGallery.HTML5Upload, ModuleGallery.SilverLightUploadModule, HTML5Upload, and SilverLightUploadHandler.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12471</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows stored XSS via User Status, Blog Comments, or Blog Description.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12472</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows admins to execute arbitrary programs by reconfiguring the Converter Executable setting from ffmpeg.exe to a different program.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12473</a> <a href="#">MISC</a>
monox -- monox	MonoX through 5.1.40.5152 allows administrators to execute arbitrary code by modifying an ASPX template.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12470</a> <a href="#">MISC</a>
moonlight -- moonlight_ios/tvos	In Moonlight iOS/tvOS before 4.0.1, the pairing process is vulnerable to a man-in-the-middle attack. The bug has been fixed in Moonlight v4.0.1 for iOS and tvOS.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11024</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Moxa Service in Moxa NPort 5150A			

moxa -- nport_5150a	firmware version 1.5 and earlier allows attackers to obtain sensitive configuration values via a crafted packet to UDP port 4800. NOTE: Moxa Service is an unauthenticated service that runs upon a first-time installation but can be disabled without ill effect.	2020-05-01	not yet calculated	<a href="#">CVE-2020-12117</a> <a href="#">CONFIRM</a>
multiple_vendors -- multiple_products	The Apros Evolution, ConsciusMap, and Furukawa provisioning systems through 2.8.1 allow remote code execution because of javax.faces.ViewState Java deserialization.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12133</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- dgn2200_devices	NETGEAR DGN2200v4 devices before 2017-01-06 are affected by command execution and an FTP insecure root directory.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11054</a> <a href="#">CONFIRM</a>
netgear -- genie_applicaition_for_android	The NETGEAR genie application before 2.4.34 for Android is affected by mishandling of hard-coded API keys and session IDs.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11058</a> <a href="#">CONFIRM</a>
netgear -- insight_application	The NETGEAR Insight application before 2.42 for Android and iOS is affected by password mismanagement.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18857</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21204</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.62, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR4300 before 1.0.2.98,	2020-04-27	not yet calculated	<a href="#">CVE-2018-21153</a> <a href="#">CONFIRM</a>



	WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21188</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.10, R6220 before 1.1.0.60, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21209</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, and WNDR4300 before 1.0.2.98.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21199</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6100 before 1.0.0.57, DM200 before 1.0.0.50, EX2700 before 1.0.1.32, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.70, EX6200v2 before 1.0.1.62, EX6400 before 1.0.1.78, EX7300 before 1.0.1.78, EX8000 before 1.0.0.114, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.42, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21167</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.5.4, WAC510 before			

netgear -- multiple_devices	5.0.5.4, WAC120 before 2.1.7, WN604 before 3.3.10, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, and WND930 before 2.1.5.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21097</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21222</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by debugging command execution. This affects FS752TP 5.4.2.19 and earlier, GS108Tv2 5.4.2.29 and earlier, GS110TP 5.4.2.29 and earlier, GS418TPP 6.6.2.6 and earlier, GS510TLP 6.6.2.6 and earlier, GS510TP 5.04.2.27 and earlier, GS510TPP 6.6.2.6 and earlier, GS716Tv2 5.4.2.27 and earlier, GS716Tv3 6.3.1.16 and earlier, GS724Tv3 5.4.2.27 and earlier, GS724Tv4 6.3.1.16 and earlier, GS728TPSB 5.3.0.29 and earlier, GS728TSB 5.3.0.29 and earlier, GS728TXS 6.1.0.35 and earlier, GS748Tv4 5.4.2.27 and earlier, GS748Tv5 6.3.1.16 and earlier, GS752TPSB 5.3.0.29 and earlier, GS752TSB 5.3.0.29 and earlier, GS752TXS 6.1.0.35 and earlier, M4200 12.0.2.10 and earlier, M4300 12.0.2.10 and earlier, M5300 11.0.0.28 and earlier, M6100 11.0.0.28 and earlier, M7100 11.0.0.28 and earlier, S3300 6.6.1.4 and earlier, XS708T 6.6.0.11 and earlier, XS712T 6.1.0.34 and earlier, and XS716T 6.6.0.11 and earlier.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18860</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7800 before 1.2.0.44, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.54,	2020-04-28	not yet calculated	<a href="#">CVE-2018-21198</a> <a href="#">CONFIRM</a>

	WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21220</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, EX2700 before 1.0.1.28, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21215</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21219</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21208</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.52, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.4.2, R9000 before 1.0.3.16, WNDR4300 before	2020-04-27	not yet calculated	<a href="#">CVE-2018-21155</a> <a href="#">CONFIRM</a>

	1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D6220 before 1.0.0.38, D6400 before 1.0.0.74, D7000v2 before 1.0.0.74, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.102, DGN2200Bv4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.20, R6300v2 before 1.0.4.22, R6400 before 1.0.1.32, R6400v2 before 1.0.2.52, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R6900P before 1.3.0.18, R7000 before 1.0.9.28, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900 before 1.0.2.10, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, R8300 before 1.0.2.116, R8500 before 1.0.2.116, WN2500RPv2 before 1.0.1.52, WNDR3400v3 before 1.0.1.18, and WNR3500Lv2 before 1.2.0.46.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21156</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, and WNDR4300 before 1.0.2.94.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21183</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21212</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a buffer overflow by an			

netgear -- multiple_devices	unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21211</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects CM400 before 2017-01-11, CM600 before 2017-01-11, D1500 before 2017-01-11, D500 before 2017-01-11, DST6501 before 2017-01-11, JNR1010v1 before 2017-01-11, JWNR2000Tv3 before 2017-01-11, JWNR2010v3 before 2017-01-11, PLW1000 before 2017-01-11, PLW1010 before 2017-01-11, WNR500 before 2017-01-11, WNR612v3 before 2017-01-11, N450 before 2017-01-11, and CG3000Dv2 before 2017-01-11.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11055</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7000 before 2018-03-01, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 2018-03-01, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21169</a> <a href="#">CONFIRM</a>
netgear --	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800	2020-04-	not yet	<a href="#">CVE-2018-</a>



multiple_devices	before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, and R7800 before 1.0.2.42.	27	calculated	<a href="#">21154 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, and R9000 before 1.0.3.6.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21184 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21224 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21175 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21174 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7500 before 1.0.0.122, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21176 CONFIRM</a>

	WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D7000 before 1.0.1.52, D7800 before 1.0.1.31, D8500 before 1.0.3.36, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.46, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21168 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R7500 before 1.0.0.122, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21185 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.44, R6900 before 1.0.1.44, R7000 before 1.0.9.28, R7500v2 before 1.0.3.24, R7800 before 1.0.2.38, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21157 CONFIRM</a>
netgear --	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000	2020-04-	not yet	<a href="#">CVE-2018-</a>

multiple_devices	before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	28	calculated	<a href="#">21205 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, and WN3100RPv2 before 1.0.0.56.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21214 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21223 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21218 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, D7800 before 1.0.1.34, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.3.6, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and	2020-04-28	not yet calculated	<a href="#">CVE-2018-21195 CONFIRM</a>

	WNR2000v5 before 1.0.0.62.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command execution. This affects M4200-10MG-POE+ 12.0.2.11 and earlier, M4300-28G 12.0.2.11 and earlier, M4300-52G 12.0.2.11 and earlier, M4300-28G-POE+ 12.0.2.11 and earlier, M4300-52G-POE+ 12.0.2.11 and earlier, M4300-8X8F 12.0.2.11 and earlier, M4300-12X12F 12.0.2.11 and earlier, M4300-24X24F 12.0.2.11 and earlier, M4300-24X 12.0.2.11 and earlier, and M4300-48X 12.0.2.11 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18858</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21096</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21196</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21197</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D6100 before 1.0.0.57, R6100 before 1.0.1.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21201</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21202</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6100 before 1.0.1.20, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21203</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21206</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6700 before 1.0.1.30, R6700v2 before 1.2.0.16, R6800 before 1.2.0.16, R6900 before 1.0.1.30, R6900P before 1.2.0.22, R6900v2 before 1.2.0.16, R7000 before 1.0.9.12, R7000P before 1.2.0.22, R7500v2 before 1.0.3.20, R7800 before 1.0.2.44, R8300 before 1.0.2.106, R8500 before 1.0.2.106, and R9000 before 1.0.2.52.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21225</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20,			



netgear -- multiple_devices	R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21207</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects JNR1010v2 before 1.1.0.48, JWNR2010v5 before 1.1.0.48, WNR1000v4 before 1.1.0.48, WNR2020 before 1.1.0.48, and WNR2050 before 1.1.0.48.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21226</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D7800 before 1.0.1.30, EX2700 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.20, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.56, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21210</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by slowdown/stoppage. This affects C6300 before 2017-05-30, CM400 before 2017-05-30, CM700 before 2017-05-30, and CMD31T before 2017-05-30.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18859</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21094</a> <a href="#">CONFIRM</a>
netgear --	Certain NETGEAR devices are affected by mishandling of repeated URL calls. This affects JNR1010v2 before 2017-01-06, WNR614 before 2017-01-06, WNR618 before 2017-01-06,			<a href="#">CVE-2016-</a>

multiple_devices	JWNR2000v5 before 2017-01-06, WNR2020 before 2017-01-06, JWNR2010v5 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2020v2 before 2017-01-06, R6220 before 2017-01-06, and WNDR3700v5 before 2017-01-06.	2020-04-28	not yet calculated	<a href="#">11057 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.20, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.92, WNDR4300 before 1.0.2.94, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, and WNR2000v5 before 1.0.0.62.	2020-04-28	not yet calculated	<a href="#">CVE-2018-21186 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.0.54, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21149 CONFIRM</a>
	Certain NETGEAR devices are affected by password exposure. This affects AC1450 before 2017-01-06, C6300 before 2017-01-06, D500 before 2017-01-06, D1500 before 2017-01-06, D3600 before 2017-01-06, D6000 before 2017-01-06, D6100 before 2017-01-06, D6200 before 2017-01-06, D6200B before 2017-01-06, D6300B before 2017-01-06, D6300 before 2017-01-06, DGN1000v3 before 2017-01-06, DGN2200v1 before 2017-01-06, DGN2200v3 before 2017-01-06, DGN2200V4 before 2017-01-06, DGN2200Bv3 before 2017-01-06, DGN2200Bv4 before 2017-01-06, DGND3700v1 before 2017-01-06, DGND3700v2 before 2017-01-06, DGND3700Bv2 before 2017-01-06, JNR1010v1 before 2017-01-06, JNR1010v2 before 2017-01-06, JNR3300 before 2017-01-06, JR6100 before 2017-01-06, JR6150 before 2017-01-06, JWNR2000v5 before 2017-01-06, R2000			

netgear -- multiple_devices	before 2017-01-06, R6050 before 2017-01-06, R6100 before 2017-01-06, R6200 before 2017-01-06, R6200v2 before 2017-01-06, R6220 before 2017-01-06, R6250 before 2017-01-06, R6300 before 2017-01-06, R6300v2 before 2017-01-06, R6700 before 2017-01-06, R7000 before 2017-01-06, R7900 before 2017-01-06, R7500 before 2017-01-06, R8000 before 2017-01-06, WGR614v10 before 2017-01-06, WNR1000v2 before 2017-01-06, WNR1000v3 before 2017-01-06, WNR1000v4 before 2017-01-06, WNR2000v3 before 2017-01-06, WNR2000v4 before 2017-01-06, WNR2000v5 before 2017-01-06, WNR2200 before 2017-01-06, WNR2500 before 2017-01-06, WNR3500Lv2 before 2017-01-06, WNDR3400v2 before 2017-01-06, WNDR3400v3 before 2017-01-06, WNDR3700v3 before 2017-01-06, WNDR3700v4 before 2017-01-06, WNDR3700v5 before 2017-01-06, WNDR4300 before 2017-01-06, WNDR4300v2 before 2017-01-06, WNDR4500v1 before 2017-01-06, WNDR4500v2 before 2017-01-06, and WNDR4500v3 before 2017-01-06.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11059</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21152</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D8500 before 1.0.3.42, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.24, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, R6250 before 1.0.4.26, R6300-2CXNAS before 1.0.3.60, R6300v2 before 1.0.4.28, R6400 before 1.0.1.36, R6400v2 before 1.0.2.52, R6700 before 1.0.1.46, R6900 before 1.0.1.46, R7000 before 1.0.9.28, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R7100LG before 1.0.0.46,	2020-04-27	not yet calculated	<a href="#">CVE-2018-21093</a> <a href="#">CONFIRM</a>

	R7300 before 1.0.0.68, R7900 before 1.0.2.10, R8000 before 1.0.4.18, R8000P before 1.3.0.10, R7900P before 1.3.0.10, R8500 before 1.0.2.122, R8300 before 1.0.2.122, RBW30 before 2.1.2.6, WN2500Rv2 before 1.0.0.54, and WNR3500Lv2 before 1.2.0.56.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command execution via a PHP form. This affects WN604 3.3.3 and earlier, WNP210v2 3.5.20.0 and earlier, WNP320 3.5.20.0 and earlier, WNDAP350 3.5.20.0 and earlier, WNDAP360 3.5.20.0 and earlier, WNDAP620 2.0.11 and earlier, WNDAP660 3.5.20.0 and earlier, WND930 2.0.11 and earlier, and WAC120 2.0.7 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18863</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects JGS516PE before 2017-05-11, JGS524Ev2 before 2017-05-11, JGS524PE before 2017-05-11, GS105Ev2 before 2017-05-11, GS105PE before 2017-05-11, GS108Ev3 before 2017-05-11, GS108PEv3 before 2017-05-11, GS116Ev2 before 2017-05-11, GSS108E before 2017-05-11, GSS116E before 2017-05-11, XS708Ev2 before 2017-05-11, and XS716E before 2017-05-11.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18862</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by insecure renegotiation. This affects SRX5308 before 2017-02-10, FVS336Gv3 before 2017-02-10, FVS318N before 2017-02-10, and FVS318Gv2 before 2017-02-10.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11060</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by password recovery and file access. This affects D8500 1.0.3.27 and earlier, DGN2200v4 1.0.0.82 and earlier, R6300v2 1.0.4.06 and earlier, R6400 1.0.1.20 and earlier, R6400v2 1.0.2.18 and earlier, R6700 1.0.1.22 and earlier, R6900 1.0.1.20 and earlier, R7000 1.0.7.10 and earlier, R7000P 1.0.0.58 and earlier, R7100LG 1.0.0.28 and earlier, R7300DST 1.0.0.52 and earlier, R7900 1.0.1.12 and earlier, R8000 1.0.3.46 and earlier, R8300 1.0.2.86 and earlier, R8500 1.0.2.86 and earlier, WNDR3400v3 1.0.1.8 and earlier, and WNDR4500v2 1.0.0.62 and earlier.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18853</a> <a href="#">CONFIRM</a>

netgear -- readynas_devices	NETGEAR ReadyNAS 6.6.1 and earlier is affected by command injection.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18854</a> <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.6.1 are affected by command injection.	2020-04-29	not yet calculated	<a href="#">CVE-2017-18856</a> <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by incorrect configuration of security settings.	2020-04-27	not yet calculated	<a href="#">CVE-2018-21159</a> <a href="#">CONFIRM</a>
netgear -- readynas_surveillance_devices	Certain NETGEAR devices are affected by anonymous root access. This affects ReadyNAS Surveillance 1.1.1-3-armel and earlier and ReadyNAS Surveillance 1.4.1-3-amd64 and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2016-11056</a> <a href="#">CONFIRM</a>
netgear -- readynas_surveillance_servers	Certain NETGEAR devices are affected by CSRF. This affects ReadyNAS Surveillance 1.4.3-15-x86 and earlier and ReadyNAS Surveillance 1.1.4-5-ARM and earlier.	2020-04-28	not yet calculated	<a href="#">CVE-2017-18861</a> <a href="#">CONFIRM</a>
node.js -- node.js	The decompress package before 4.2.1 for Node.js is vulnerable to Arbitrary File Write via ../ in an archive member, when a symlink is used, because of Directory Traversal.	2020-04-26	not yet calculated	<a href="#">CVE-2020-12265</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
octopus -- deploy	In Octopus Deploy before 2019.12.9 and 2020 before 2020.1.12, the TaskView permission is not scoped to any dimension. For example, a scoped user who is scoped to only one tenant can view server tasks scoped to any other tenant.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12286</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
onkyo -- tx-nr585_devices	A Local File Inclusion (LFI) issue on Onkyo TX-NR585 1000-0000-000-0008-0000 devices allows remote unauthenticated users on the network to read sensitive files via %2e%2e%2f directory traversal, as demonstrated by reading /etc/shadow.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12447</a> <a href="#">MISC</a>
opendmarc -- opendmarc	OpenDMARC through 1.3.2 and 1.4.x, when used with pypolicyd-spf 2.0.2, allows attacks that bypass SPF and DMARC authentication in situations where the HELO field is inconsistent with the MAIL FROM field.	2020-04-27	not yet calculated	<a href="#">CVE-2019-20790</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opendmarc -- opendmarc	OpenDMARC through 1.3.2 and 1.4.x allows attacks that inject authentication results to provide false information about the domain that originated an e-mail message. This is caused by incorrect parsing and interpretation of SPF/DKIM authentication results, as demonstrated	2020-04-27	not yet calculated	<a href="#">CVE-2020-12272</a> <a href="#">MISC</a> <a href="#">MISC</a>



	by the example.net(.example.com substring.			
openldap -- openldap	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).	2020-04-28	not yet calculated	<a href="#">CVE-2020-12243</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a>
opensc -- opensc	OpenSC before 0.20.0 has a double free in coolkey_free_private_data because coolkey_add_object in libopensc/card-coolkey.c lacks a uniqueness check.	2020-04-29	not yet calculated	<a href="#">CVE-2019-20792</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openvpn -- openvpn	An issue was discovered in OpenVPN 2.4.x before 2.4.9. An attacker can inject a data channel v2 (P_DATA_V2) packet using a victim's peer-id. Normally such packets are dropped, but if this packet arrives before the data channel crypto parameters have been initialized, the victim's connection will be dropped. This requires careful timing due to the small time window (usually within a few seconds) between the victim client connection starting and the server PUSH_REPLY response back to the client. This attack will only work if Negotiable Cipher Parameters (NCP) is in use.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11810</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
opmantek -- open-audit	Open-Audit 3.3.0 allows an XSS attack after login.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12261</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There is Arbitrary file upload.	2020-04-29	not yet calculated	<a href="#">CVE-2020-11943</a> <a href="#">MISC</a> <a href="#">MISC</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.3.1. There is shell metacharacter injection via attributes to an open-audit/configuration/ URI. An attacker can exploit this by adding an excluded IP address to the global discovery settings (internally called exclude_ip). This exclude_ip value is passed to the exec function in the discoveries_helper.php file (inside the all_ip_list function) without being filtered, which means that the attacker can provide a payload instead of a valid IP address.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12078</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There are Multiple SQL Injections.	2020-04-29	not yet calculated	<a href="#">11942</a> <a href="#">MISC</a> <a href="#">MISC</a>
opmantek -- open-audit	An issue was discovered in Open-Audit 3.2.2. There is OS Command injection in Discovery.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11941</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 5.2.40, prior to 6.0.20 and prior to 6.1.6. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	2020-04-29	not yet calculated	<a href="#">CVE-2020-2575</a> <a href="#">MISC</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system	When user downloads PGP or S/MIME keys/certificates, exported file has same name for private and public keys. Therefore it's possible to mix them and to send private key to the third-party instead of public key. This issue affects ((OTRS)) Community Edition: 5.0.42 and prior versions, 6.0.27 and prior versions. OTRS: 7.0.16 and prior versions.	2020-04-28	not yet calculated	<a href="#">CVE-2020-1774</a> <a href="#">LIST</a> <a href="#">CONFIRM</a>
percona -- xtrabackup	Percona XtraBackup before 2.4.20 unintentionally writes the command line to any resulting backup file output. This may include sensitive arguments passed at run time. In addition, when --history is passed at run time, this command line is also written to the PERCONA_SCHEMA.xtrabackup_history table.	2020-04-27	not yet calculated	<a href="#">CVE-2020-10997</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
percona -- xtradb_cluster	An issue was discovered in Percona XtraDB Cluster before 5.7.28-31.42. A bundled script inadvertently sets a static transition_key for SST processes in place of the random key expected.	2020-04-27	not yet calculated	<a href="#">CVE-2020-10996</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
	In PHP versions 7.2.x below 7.2.30, 7.3.x below 7.3.17 and 7.4.x below 7.4.5, if PHP is compiled with EBCDIC support			<a href="#">CVE-2020-</a>

php -- php	(uncommon), urldecode() function can be made to access locations past the allocated memory, due to erroneously using signed numbers as array indexes.	2020-04-27	not yet calculated	<a href="#">7067</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
php-fusion -- php-fusion	An XSS vulnerability exists in the banners.php page of PHP-Fusion 9.03.50. This can be exploited because the only security measure used against XSS is the stripping of SCRIPT tags. A malicious actor can use HTML event handlers to run JavaScript instead of using SCRIPT tags.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12438</a> <a href="#">MISC</a> <a href="#">MISC</a>
php-fusion -- php-fusion	PHP-Fusion 9.03.50 allows SQL Injection because maincore.php has an insufficient protection mechanism. An attacker can develop a crafted payload that can be inserted into the sort_order GET parameter on the members.php members search page. This parameter allows for control over anything after the ORDER BY clause in the SQL query.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12461</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phpgurukul -- online_course_registration	Online Course Registration 2.0 has multiple SQL injections that would can lead to a complete database compromise and authentication bypass in the login pages: admin/change-password.php, admin/check_availability.php, admin/index.php, change-password.php, check_availability.php, includes/header.php, index.php, and pincode-verification.php.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12429</a> <a href="#">MISC</a>
prestashop -- prestashop	The Correos Express addon for PrestaShop 1.6 through 1.7 allows remote attackers to obtain sensitive information, such as a service's owner password that can be used to modify orders via SOAP. Attackers can also retrieve information about orders or buyers.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12120</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	An integer overflow was found in QEMU 4.0.1 through 4.2.0 in the way it implemented ATI VGA emulation. This flaw occurs in the ati_2d_blt() routine in hw/display/ati-2d.c while handling MMIO write operations through the ati_mm_write() callback. A malicious guest could abuse this flaw to crash the QEMU process, resulting in a denial of service.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11869</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
re2c -- re2c	re2c before 2.0 has uncontrolled recursion that causes stack consumption	2020-04-29	not yet calculated	<a href="#">CVE-2018-21232</a> <a href="#">MISC</a>

	in find_fixed_tags.			<a href="#">MISC</a>
red_hat -- ansible	An archive traversal flaw was found in all ansible-engine versions 2.9.x prior to 2.9.7, when running ansible-galaxy collection install. When extracting a collection .tar.gz file, the directory is created without sanitizing the filename. An attacker could take advantage to overwrite any file within the system.	2020-04-30	not yet calculated	<a href="#">CVE-2020-10691</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
red_hat -- undertow	A file inclusion vulnerability was found in the AJP connector enabled with a default AJP configuration port of 8009 in Undertow version 2.0.29.Final and before and was fixed in 2.0.30.Final. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and trigger this vulnerability to gain remote code execution.	2020-04-28	not yet calculated	<a href="#">CVE-2020-1745</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel V2.5.2, attackers can upload an arbitrary file to the server just changing the the content-type value. As a result of that, an attacker can execute a command on the server. This specific attack only occurs with the Maintenance Mode setting.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11817</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel 2.5.2, users' passwords and usernames are stored in a cookie with URL encoding, base64 encoding, and hashing. Thus, an attacker can easily apply brute force on them.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11821</a> <a href="#">MISC</a>
rukovoditel -- rukovoditel	In Rukovoditel 2.5.2, there is a stored XSS vulnerability on the application structure --> user access groups page. Thus, an attacker can inject malicious script to steal all users' valuable data.	2020-04-27	not yet calculated	<a href="#">CVE-2020-11822</a> <a href="#">MISC</a>
rundeck -- rundeck	In Rundeck before version 3.2.6, authenticated users can craft a request that reveals Execution data and logs and Job details that they are not authorized to see. Depending on the configuration and the way that Rundeck is used, this could result in anything between a high severity risk, or a very low risk. If access is tightly restricted and all users on the system have access to all projects, this is not really much of an issue. If access is wider and allows login for users that do not	2020-04-29	not yet calculated	<a href="#">CVE-2020-11009</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	have access to any projects, or project access is restricted, there is a larger issue. If access is meant to be restricted and secrets, sensitive data, or intellectual property are exposed in Rundeck execution output and job data, the risk becomes much higher. This vulnerability is patched in version 3.2.6			
saltstack -- salt	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class allows access to some methods that improperly sanitize paths. These methods allow arbitrary directory access to authenticated users.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11652</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
saltstack -- salt	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11651</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- erp	Egypt localized withholding tax reports Clearing of Liabilities and Remittance Statement and Summary in SAP ERP (versions 618, 730, EAPPLGLO 607) and S/4 HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user, allowing reading or modification of some tax reports, due to Missing Authorization Check.	2020-04-24	not yet calculated	<a href="#">CVE-2020-6212</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver_as_abap_business_server_pages_test_application	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_PHTMLB, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754 is vulnerable to reflected cross-site Scripting (XSS) via different URL parameters as it does not sufficiently encode user controlled inputs.	2020-04-24	not yet calculated	<a href="#">CVE-2020-6213</a> <a href="#">MISC</a> <a href="#">MISC</a>
simple_ledger -- electron-cash-slp	Electron-Cash-SLP before version 3.6.2 has a vulnerability. All token creators that use the "Mint Tool" feature of the Electron Cash SLP Edition are at risk of sending the minting authority baton to the wrong SLP address. Sending the mint baton to the wrong address will give another party the ability to issue new tokens or permanently destroy future minting capability. This is fixed version 3.6.2.	2020-04-28	not yet calculated	<a href="#">CVE-2020-11014</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



simplisafe -- ss3_devices	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to pair a rogue keypad to an armed system.	2020-05-02	not yet calculated	<a href="#">CVE-2020-5727</a> <a href="#">CONFIRM</a>
solarwinds -- webhelpdesk	Formula Injection exists in the export feature in SolarWinds WebHelpDesk 12.7.1 via a value (provided by a low-privileged user in the Subject field of a help request form) that is mishandled in a TicketActions/view?tab=group TSV export by an admin user.	2020-04-27	not yet calculated	<a href="#">CVE-2019-20002</a> <a href="#">MISC</a>
sourcegraph -- sourcegraph	Sourcegraph before 3.15.1 has a vulnerable authentication workflow because of improper validation in the SafeRedirectURL method in cmd/frontend/auth/redirect.go, such as for the //foo//example.com substring.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12283</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
suap -- suap	SUAP V2 allows XSS during the update of user information.	2020-04-29	not yet calculated	<a href="#">CVE-2019-7634</a> <a href="#">MISC</a>
suculent -- think-device-api	A vulnerability has been disclosed in thinx-device-api IoT Device Management Server before version 2.5.0. Device MAC address can be spoofed. This means initial registration requests without UDID and spoofed MAC address may pass to create new UDID with same MAC address. Full impact needs to be reviewed further. Applies to all (mostly ESP8266/ESP32) users. This has been fixed in firmware version 2.5.0.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11015</a> <a href="#">CONFIRM</a>
teampass -- teampass	The REST API functions in TeamPass 2.1.27.36 allow any user with a valid API token to bypass IP address whitelist restrictions via an X-Forwarded-For client HTTP header to the getIp function.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12477</a> <a href="#">MISC</a>
telegram -- telegram_desktop_and_telegram_group_and_private_chat	Telegram Desktop through 2.0.1, Telegram through 6.0.1 for Android, and Telegram through 6.0.1 for iOS allow an attacker to inject arbitrary JavaScript code in a public URL or a group chat invitation URL.	2020-05-01	not yet calculated	<a href="#">CVE-2020-12474</a> <a href="#">MISC</a>
testlink -- testlink	In TestLink 1.9.20, the lib/cfields/cfieldsExport.php goback_url parameter causes a security risk because it depends on client input and is not constrained to lib/cfields/cfieldsView.php at the web site associated with the session.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12274</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In TestLink 1.9.20, a crafted login.php			<a href="#">CVE-2020-</a>

testlink -- testlink	viewer parameter exposes cleartext credentials.	2020-04-27	not yet calculated	<a href="#">12273</a> <a href="#">MISC</a> <a href="#">MISC</a>
tiny_file_manager -- tiny_file_manager	In Tiny File Manager 2.4.1, there is a Path Traversal vulnerability in the ajax recursive directory listing functionality. This allows authenticated users to enumerate directories and files on the filesystem (outside of the application scope).	2020-04-28	not yet calculated	<a href="#">CVE-2020-12102</a> <a href="#">MISC</a> <a href="#">MISC</a>
tiny_file_manager -- tiny_file_manager	In Tiny File Manager 2.4.1 there is a vulnerability in the ajax file backup copy functionality which allows authenticated users to create backup copies of files (with .bak extension) outside the scope in the same directory in which they are stored.	2020-04-28	not yet calculated	<a href="#">CVE-2020-12103</a> <a href="#">MISC</a> <a href="#">MISC</a>
torchbox -- wagtail	In Wagtail before versions 2.7.2 and 2.8.2, a potential timing attack exists on pages or documents that have been protected with a shared password through Wagtail's "Privacy" controls. This password check is performed through a character-by-character string comparison, and so an attacker who is able to measure the time taken by this check to a high degree of accuracy could potentially use timing differences to gain knowledge of the password. This is understood to be feasible on a local network, but not on the public internet. Privacy settings that restrict access to pages/documents on a per-user or per-group basis (as opposed to a shared password) are unaffected by this vulnerability. This has been patched in 2.7.3, 2.8.2, 2.9.	2020-04-30	not yet calculated	<a href="#">CVE-2020-11037</a> <a href="#">CONFIRM</a>
ubiquiti -- unifi_cloud_key_devices	UniFi Cloud Key firmware <= v1.1.10 for Cloud Key gen2 and Cloud Key gen2 Plus contains a vulnerability that allows unrestricted root access through the serial interface (UART).	2020-05-02	not yet calculated	<a href="#">CVE-2020-8157</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
university_of_wisconsin -- htcondor	HTCondor up to and including stable series 8.8.6 and development series 8.9.4 has Incorrect Access Control. It is possible to use a different authentication method to submit a job than the administrator has specified. If the administrator has configured the READ or WRITE methods to include CLAIMTOBE, then it is possible to impersonate another user to the condor_schedd. (For example to submit or remove jobs)	2020-04-27	not yet calculated	<a href="#">CVE-2019-18823</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

valve -- source	Valve Source allows local users to gain privileges by writing to the /tmp/hl2_relaunch file, which is later executed in the context of a different user account.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12242</a> <a href="#">MISC</a>
wavlink -- multiple_devices	An issue was discovered on WAVLINK WL-WN579G3 M79X3.V5030.180719, WL-WN575A3 RPT75A3.V4300.180801, and WL-WN530HG4 M30HG4.V5030.191116 devices. There are multiple externally accessible pages that do not require any sort of authentication, and store system information for internal usage. The devices automatically query these pages to update dashboards and other statistics, but the pages can be accessed externally without any authentication. All the pages follow the naming convention live_(string).shtml. Among the information disclosed is: interface status logs, IP address of the device, MAC address of the device, model and current firmware version, location, all running processes, all interfaces and their statuses, all current DHCP leases and the associated hostnames, all other wireless networks in range of the router, memory statistics, and components of the configuration of the device such as enabled features.	2020-04-27	not yet calculated	<a href="#">CVE-2020-12266</a> <a href="#">MISC</a> <a href="#">MISC</a>
werner -- sqliteodbc	SQLiteODBC 0.9996, as packaged for certain Linux distributions as 0.9996-4, has a race condition leading to root privilege escalation because any user can replace a /tmp/sqliteodbc\$\$ file with new contents that cause loading of an arbitrary library.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12050</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">MISC</a>
wind_river -- vxworks	Wind River VxWorks tftp client library, as distributed in VxWorks 6.9 through 7 SR0630, has a double free	2020-04-27	not yet calculated	<a href="#">CVE-2020-10647</a> <a href="#">CONFIRM</a>
vmware -- esxi	ESXi 6.5 without patch ESXi650-201912104-SG and ESXi 6.7 without patch ESXi670-202004103-SG do not properly neutralize script-related HTML when viewing virtual machines attributes. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.3.	2020-04-29	not yet calculated	<a href="#">CVE-2020-3955</a> <a href="#">CONFIRM</a>
	In affected versions of WordPress, a special payload can be crafted that can lead to scripts getting executed within the			

wordpress -- wordpress	search block of the block editor. This requires an authenticated user with the ability to add content. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11030</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, some private posts, which were previously public, can result in unauthenticated disclosure under a specific set of conditions. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11028</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a vulnerability in the stats() method of class-wp-object-cache.php can be exploited to execute cross-site scripting (XSS) attacks. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11029</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	LearnPress Wordpress plugin version prior and including 3.2.6.7 is vulnerable to SQL Injection	2020-04-30	not yet calculated	<a href="#">CVE-2020-6010</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a cross-site scripting (XSS) vulnerability in the navigation section of Customizer allows JavaScript code to be executed. Exploitation requires an authenticated user. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11025</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	The ninja-forms plugin before 3.4.24.2 for WordPress allows CSRF with resultant XSS.	2020-04-29	not yet calculated	<a href="#">CVE-2020-12462</a> <a href="#">MISC</a>
	In affected versions of WordPress, files			

wordpress -- wordpress	with a specially crafted name when uploaded to the Media section can lead to script execution upon accessing the file. This requires an authenticated user with privileges to upload files. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11026</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).	2020-04-30	not yet calculated	<a href="#">CVE-2020-11027</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
xerox -- multiple_workcentre_devices	Xerox WorkCentre 3655, 3655i, 58XX, 58XXi, 59XX, 59XXi, 6655, 6655i, 72XX, 72XXi, 78XX, 78XXi, 7970, and 7970i devices before 073.xxx.086.15410 do not properly escape parameters in the support/remoteUI/configui.php script, which can allow an unauthenticated attacker to execute OS commands on the device.	2020-04-29	not yet calculated	<a href="#">CVE-2016-11061</a> <a href="#">MISC</a>
xt:commerce -- xt:commerce	The address-management feature in xt:Commerce 5.1 to 6.2.2 allows remote authenticated users to zero out other user's stored addresses by manipulating an id field in the POST request for altering an address.	2020-04-30	not yet calculated	<a href="#">CVE-2020-12101</a> <a href="#">FULLDISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zoom -- international_call_recording	ZOOM International Call Recording 6.3.1 suffers from multiple authenticated stored XSS vulnerabilities via the phoneNumber field in the (1) User Edit or (2) User Add form, (3) name field in the Role Add form, (4) name or number field in the Edit Group form, (5) tagKey or tagValue field in the Recording Rules Configuration, or (6) txt_69735:/VemailAddress/value or txt_75767:/VemailFrom/value field in callrec/config.	2020-04-27	not yet calculated	<a href="#">CVE-2019-18223</a> <a href="#">MISC</a>
	ZTE SDN controller platform is impacted by an information leakage vulnerability. Due to the program's failure to optimize			



zte -- oscp	the response of failure to the request, the caller can directly view the internal error code location of the component. Attackers could exploit this vulnerability to obtain sensitive information. This affects: OSCP versions V16.19.10 and V16.19.20.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6865</a> <a href="#">CONFIRM</a>
zte -- zenic_one_r22b_devices	ZTE's SDON controller is impacted by the resource management error vulnerability. When RPC is frequently called by other applications in the case of mass traffic data in the system, it will result in no response for a long time and memory overflow risk. This affects: ZENIC ONE R22b versions V16.19.10P02SP002 and V16.19.10P02SP005.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6867</a> <a href="#">CONFIRM</a>
zte -- zxctn_6500_devices	A ZTE product is impacted by a resource management error vulnerability. An attacker could exploit this vulnerability to cause a denial of service by issuing a specific command. This affects: ZXCTN 6500 version V2.10.00R3B87.	2020-04-30	not yet calculated	<a href="#">CVE-2020-6866</a> <a href="#">CONFIRM</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [CLA Public Section](#)  
**To:** [Melissa Tronquet](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, May 01, 2020 3:02:03 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive](#) (972,542 articles)



[North America](#) | [Global](#)

**USA**

[North America](#)

[Employee Benefits & Pensions](#)



### **IRS Extends Filing Deadlines for Employee Benefit Plans**

**Faegre Drinker Biddle & Reath LLP**

In response to the COVID-19 pandemic, the IRS has issued Notice 2020-23, which automatically extends the deadlines for certain filing obligations...

### **Ninth Circuit Reverses Denial of Longshore Act Benefits to California Widows**

[California](#)

**Goldberg Segalla LLP**

Two widows of California shipyard workers, whose husbands were allegedly exposed to asbestos and died as a result, sought compensation under the...

### **Tax-Qualified Deferred Compensation Plan Sponsors: Considerations for Administration During the COVID-19 Pandemic**

**McCarter & English LLP**

This Alert discusses certain considerations for tax-qualified retirement plan (in particular, 401(k) and 403(b) Plan) sponsors and fiduciaries in...

### **ERISA Settlements - The Non-Monetary Concessions Continue to Mount**

**Thompson Hine LLP**

In a prior post, we commented on the growing trend of fiduciaries making non-monetary concessions to settle ERISA fee litigation cases. We observed...

---

### **Cutting Costs in a COVID-19 World - Reducing or Suspending Company Contributions to a 401(k) or 403(b) Plan**

#### **Faegre Drinker Biddle & Reath LLP**

In response to the current economic crisis caused by COVID-19, many companies are considering cost-savings measures to improve their companies'...

---

### **IRS Releases FAQs on Federal Tax Consequences of Payroll Support for Air Carriers and Contractors under CARES Act**

#### **Covington & Burling LLP**

The Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") authorizes the Treasury Department to provide payments to passenger air carriers...

---

### **Why an ESOP? Advantages to Employer of Deductible Cash Dividends to ESOP Participants**

#### **Hall Benefits Law**

An Employee Stock Ownership Program or ESOP is a way for owners to share the wealth and success of a company with employees. It is often used for...

---

### **Relief . . . Just a Little Bit - IRS Notice 2020-23: Limited Extensions of Form 5500**

#### **Holland & Hart LLP**

In the midst of everything going on, we wanted to point out a few "under the radar" implications of IRS Notice 2020-23. The Notice, issued on April...

---

### **Webinar Recording: WARN, Furloughs, and RIFs: Obligations and Best Practices when considering COVID-19 Workforce Reductions**

[Video](#)

#### **Seyfarth Shaw LLP**

Is this the time to hold tightly to your current workforce or let some of them go? This remains the No. 1 question on nearly every US employer's mind...

---

### **IRS and PBGC Issue Relief Extending Certain Employee Benefit Plan Deadlines Due to COVID-19 Pandemic**

#### **McCarter & English LLP**

On April 9, 2020, the IRS released Notice 2020-23, which postpones (automatically, without the need for the taxpayer to file for an extension) numer...

---

### **Employee Retirement Plans: Cost-Saving Measures and Increasing Employee Monetary Access During COVID-19**

#### **Akerman LLP**

With today's uncertainties, employers are addressing their own short term cash needs as well as their employees'/former employees' ability to support...

---

### **COVID-19 and Retirement Plan Partial Terminations**

#### **Greenberg Traurig LLP**

Among the longer-term considerations for employer layoff and furlough decisions is the impact on a single employer pension, profit sharing, or 401(k)...

---

### **State and Local Tax Responses to COVID-19: Nexus and Apportionment Relief for Employers With Telecommuting Employees [Updated April 22, 2020]**

**Baker McKenzie**

Many employees continue to telecommute due to the COVID-19 outbreak. As discussed in our previous blog post on state tax nexus and apportionment...

---

### **Tri-Agency FAQs Clarify Group Health Plan Obligations under FFCRA and CARES Act**

**McDermott Will & Emery**

Earlier this month, the Departments of Labor (DOL), Health and Human Services (HHS) and the Treasury jointly issued an FAQ (found here, as updated...

---

### **Defined Benefit Plan Annual Funding Notices Have Not Been Delayed**

**Haynes and Boone LLP**

Although the CARES Act permitted the DOL to delay the deadline for distributing defined benefit plan Annual Funding Notices ("AFNs"), the DOL has not...

---

### **United States: Important Implications Coronavirus Aid, Relief, and Economic Security Act in US**

**Baker McKenzie**

Coronavirus-Related Distributions. The Act would allow participants in eligible retirement plans to take distributions in 2020 of up to USD 100,000...

---

### **Retirement Plan Participant QRDOs**

**Hall Benefits Law**

Benefits attorneys like to focus on businesses and benefit plan structures for employees. However, there is an overlap between benefits law, family...

---

### **Considerations for Angel and VC Funded Startups and Emerging Growth Companies Considering a Loan under the Paycheck Protection Program**

**Procopio Cory Hargreaves & Savitch LLP**

What are the eligibility criteria most likely to be of concern to emerging growth companies funded by angel or institutional investors considering...

---

### **San Francisco Unveils Plan To Allow Employees to Use Employer Healthcare Funds For Food, Rent, And Utilities During The COVID-19 Pandemic**

**Fisher Phillips**

Mayor Breed just announced a plan to allow employees in San Francisco to now use funds their employers have contributed in compliance with San...

---

### **IRS Repurposes Military and Disaster Relief For COVID-19 Deadline Extensions**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 9, 2020, the IRS issued Notice 2020-23, extending federal tax filing deadlines and payment obligations to July 15, 2020...



---

## **Illinois Withdraws Emergency COVID-19 Workers' Compensation Rule** Illinois

### **Duane Morris LLP**

The Illinois Workers' Compensation Commission has withdrawn its April 16, 2020, emergency rule that would have established that all first responders...

---

## **Client Alert: National Emergency Enables Tax-Free Employee Relief Fund**

### **Bowditch & Dewey LLP**

Once the President declared the COVID-19 pandemic a national emergency on March 13, 2020, in addition to opening access to billions of federal dollars...

---

## **Cafeteria Plan Considerations During a Pandemic**

### **Foster Swift Collins & Smith PC**

Many employers sponsor a Code Section 125 cafeteria plan that allows eligible employees to pay for certain health and welfare benefits on a pretax...

---

## **US DOL Provides More Guidance On Pandemic Unemployment Assistance: Restrictions on Eligibility, Summer Break Limitations, Gig Worker Benefits, and More (US)**

### **Squire Patton Boggs**

As most everyone now knows, among other things, the massive \$2 trillion-plus CARES Act created multiple federal unemployment compensation programs...

---

## **IRS FAQs on Retention Credit Highlight Aggregation Concerns and Narrow Potential Eligibility**

### **Covington & Burling LLP**

Late Wednesday, the IRS released extensive new guidance in the form of Frequently Asked Questions ("FAQs") on the IRS website addressing various...

---

## **The CARES Act Impact: Retirement Plans**

### **Hall Render Killian Heath & Lyman PC**

This is the first in a series of articles covering the employee benefits provisions of the Coronavirus Aid, Relief, and Economic Security Act ("CARES...

---

## **ERISA Claims for Cross-Marketing Participant Data Hit a Snag**

### **Thompson Hine LLP**

The Seventh Circuit has issued its decision in the much-anticipated case of *Divane v. Northwestern*. The district court below had refused to allow...

---

## **Benefits Briefs in the Time of COVID-19, Part 2: Temporary Expansion of Educational Assistance Programs to Cover Employees' Student Loan Debt**

### **Dickinson Wright**

The CARES Act gives employers a way to pay employees' student loan debt on a pre-tax basis during a portion of 2020 through an educational assistance...

---

## **California Provides COVID-19 Paid Sick Leave for Food Sector Workers (US)**

California



### **Squire Patton Boggs**

In a move that mirrors the efforts of several local California communities to fill gaps not otherwise addressed by the federal Families First...

---

### **IRS Released New FAQs on Employee Retention Credit**

#### **Covington & Burling LLP**

On April 29, 2020, the IRS released new FAQs providing significant guidance on the employee retention credit. We are still analyzing the guidance...

---

### **Wisconsin Employers Making the Best of the Worst: Implementing a Work-Share Program**

Wisconsin

#### **Littler Mendelson PC**

The unprecedented economic conditions brought about by the COVID-19 pandemic have forced many Wisconsin employers to implement layoffs, partial...

---

### **Rolling Over Required Minimum Distributions Already Taken in 2020**

#### **Holland & Knight LLP**

To prevent individuals from being forced to liquidate assets in their retirement accounts at greatly reduced values to fund a Required Minimum...

---

### **I Think a Change, a Change Would Do You Good . . . Modifying Deferred Compensation Plan Contributions and Elections During the Pandemic**

#### **Holland & Hart LLP**

In response to the unprecedented worldwide COVID-19 pandemic, businesses are turning to cash flow issues resulting from the abrupt economic downturn...

---

### **The CARES Act Contains Changes to Retirement Plan Withdrawal Rules - What Are They? [Part I]**

#### **Hall Benefits Law**

Over the past few weeks, the 2019 Novel Coronavirus (or "Coronavirus") has hit businesses (and employees) financially across the U.S. in an...

---

### **SECURE Act Impacts Decision to Name Trust as Beneficiary of Retirement Plan**

#### **Lewis Rice LLC**

Signed into law on December 20, 2019, and effective for those individuals who die after December 31, 2019, the SECURE Act made a number of changes...

---

## **Employment & Labor**



### **UPDATED: Emergency legislation and measures around the world (COVID-19)**

#### **Lexology PRO**

A list of key recent emergency legislation and measures implemented by nations across the world in response to COVID-19.

---

### **Open for business: how 'essential' businesses can keep their workplace healthy and safe**

#### **McDermott Will & Emery**

Most states have issued some form of 'shelter in place' or 'stay at home' order to flatten the curve of COVID-19. As a result, many business...

---

### **IRS Concludes No Statute of Limitations Shields Employers from ACA Liability - Impacts on Family Businesses**

#### **Davis Wright Tremaine LLP**

On February 21, 2020, the Internal Revenue Service (IRS) released a memo to address whether the Employer Shared Responsibility Payment (ESRP) imposed...

---

### **Federal Stimulus Package Makes Loans Available to Tribal Business Concerns to Help Keep People Employed**

#### **Quarles & Brady LLP**

Tribal enterprises owned in whole or in part by Federally recognized Indian tribes may be eligible to receive some relief in the form of low-interest...

---

### **California Requires COVID-19 Supplemental Paid Sick Leave for Food Sector Workers**

California

#### **Barnes & Thornburg LLP**

California's Gov. Gavin Newsom has issued Executive Order N-51-20, which requires hiring entities to provide up to 80 hours of supplemental paid sick...

---

### **Developments in workplace discrimination guidance in the wake of covid-19**

New

Jersey

#### **Shearman & Sterling LLP**

Many employers have been forced to consider employee layoffs, furloughs or salary reductions as a way to manage some of the financial hardship...

---

### **U.S. COVID-19: New CDC Guidance Allows Potentially-Exposed "Critical Infrastructure Workers" to Remain at Work - with Precautions**

#### **Bryan Cave Leighton Paisner LLP**

The Centers for Disease Control and Prevention ("CDC") recently issued guidance applicable to "critical infrastructure workers," and safety...

---

### **New York City Commission on Human Rights Forms COVID-19 Response Team**

New York

#### **Littler Mendelson PC**

On April 19, 2020, the New York City Commission on Human Rights (the "Commission") announced that it has formed a COVID-19 response team to handle...

---

### **Updated EEOC COVID-19 Guidance: The Commission Adds New Q&A To Help Employers Understand Their EEO Obligations In These Trying Times**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The EEOC recently released updated guidance for employers trying to navigate the federal anti-discrimination laws in the COVID-19...

---



## **The CARES Act: What Midsize Business Owners and Not-For-Profit Organizations Need To Know**

### **Cahill Gordon & Reindel LLP**

On March 27, 2020, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act (H.R. 748) (the "CARES Act"). The CARES Act...

---

## **COVID-19-Inspired Changes to New Jersey Family Leave Act**

New Jersey

### **Davis Wright Tremaine LLP**

On Tuesday, April 14, 2020, New Jersey Governor Phil Murphy signed S2374 into law, extending New Jersey's Family Leave Act to provide job-protected...

---

## **Expect More Employment Discrimination Claims Under New Virginia Values Act**

Virginia

### **Quarles & Brady LLP**

On April 11, 2020, Virginia Governor Ralph Northam signed into law the Virginia Values Act. This law likely will fundamentally change how...

---

## **CARES Act Offers Assistance to Help Federal Contractors Who Offer Employees Paid Leave**

### **Hunton Andrews Kurth LLP**

CARES Act Offers Assistance to Help Federal Contractors Who Offer Employees Paid Leave The COVID-19 pandemic is a crisis of both public health and...

---

## **SBA Releases Additional Interim Final Rule Implementing the Paycheck Protection Program; Announces Lapse in PPP and EIDL Appropriations**

### **Kramer Levin Naftalis & Frankel LLP**

On April 14, the Small Business Administration (SBA) issued an interim final rule, effective immediately, regarding the implementation of the Paycheck...

---

## **Pennsylvania Orders Additional Worker Safety Measures to Combat COVID-19**

Pennsylvania

### **Seyfarth Shaw LLP**

Secretary of the Department of Health Dr. Rachel Levine signed an order on April 15, 2020, later approved by Governor Wolf, that significantly...

---

## **Small Business Coverage Under the Paid Leave Provisions of the FFRCA**

### **Holland & Hart LLP**

As covered elsewhere in this site, under the FFRCA, all private employers that employ fewer than 500 employees must comply with the emergency paid...

---

## **Key Takeaways for Employers from DOJ/FTC on Antitrust Enforcement Amid COVID-19 Pandemic**

### **Bass, Berry & Sims PLC**

On April 13, the Antitrust Division of the Department of Justice (DOJ) and the Bureau of Competition of the Federal Trade Commission (FTC)...

---

## **An Updated Practical Guide for Small Businesses to Obtain a Paycheck**

## **Protection Loan Under CARES Act**

### **Manatt Phelps & Phillips LLP**

On April 2, 2020 and April 4, 2020, the Small Business Administration (SBA) issued unusual interim final rules (the Rules) providing further detail...

---

## **Virginia adopts a wave of new employment laws. Part 1 - Expansive discrimination and retaliation protections**

Virginia

### **Reed Smith LLP**

In the midst of the COVID-19 pandemic that is dominating the news, Virginia Governor Ralph Northam signed into law a slew of bills passed by the...

---

## **Major Tax Changes in the CARES Act**

### **Roberts & Holland LLP**

The COVID-19 pandemic has disrupted economic life throughout the United States (as it has all over the globe), and Federal, state, and local...

---

## **DC expands COVID-19 related leave requirements**

Washington

### **Hogan Lovells**

The Mayor of the District of Columbia recently signed two emergency laws that expand obligations of employers to provide leave to employees for...

---

## **Employment Question of the Day: April 22, 2020 - Part 2**

### **Fredrikson & Byron PA**

Many states have greatly expanded the availability of unemployment compensation benefits to furloughed employees as a result of the economic downturn...

---

## **CARES Act Programs Available to Small Businesses**

### **Kilpatrick Townsend & Stockton LLP**

The CARES Act provides several programs to assist small businesses impacted by the COVID-19 pandemic, including favorable loan terms, significant...

---

## **Pennsylvania Governor Announces Three-Phase System for Reopening the Commonwealth**

Pennsylvania

### **Duane Morris LLP**

Governor Wolf stated he plans to begin easing some restrictions on May 8 in certain areas of Pennsylvania that have had a minimal COVID-19 impact...

---

## **A Reminder to Cover Up: When Face Mask Use May Be Required in the Workplace (US)**

### **Squire Patton Boggs**

As employers begin to plan for reopening their businesses after government-imposed shutdown orders, or plan for the return of more workers to their...

---

## **Should Employers Require Employees to Wear Facemasks?**

### **Morrison & Foerster LLP**

As employers begin considering return to work strategies, many are wondering



whether they should permit or require individuals to wear facemasks at...

---

### **Work-from-Home Fails**

#### **Ford & Harrison LLP**

The COVID-19 situation has left us all scrambling to maintain our professional lives as much as possible. We're coming up with alternate work...

---

### **The Next Normal: A Littler Insight on Returning to Work - Safety and Health**

#### **Littler Mendelson PC**

Over a roughly two-month period, COVID-19 has completely upended work as we know it. Businesses across the globe have struggled to function with...

---

### **Summary of CARES Act and FFCRA Tax Credit and Payroll Tax Relief**

#### **Troutman Sanders LLP**

The payroll and tax credit programs under the Coronavirus Aid, Relief and Economic Security (CARES) Act and the Families First Coronavirus Response...

---

### **Virginia Increases its Minimum Wage to \$12.00 per Hour by 2023**

Virginia

#### **Littler Mendelson PC**

On April 22, 2020, during a special legislative session, the Virginia General Assembly voted to approve Governor Ralph Northam's proposed amendment...

---

### **Trade Secret Litigation: Activity on the Rise**

#### **Seyfarth Shaw LLP**

As a special feature of our blog—guest postings by experts, clients, and other professionals—please enjoy this blog entry from Neil Eisgruber...

---

### **NEWARK POLICE ISSUE SUMMONSES TO MANUFACTURERS FOR VIOLATING GOVERNOR MURPHY'S EXECUTIVE ORDERS 104, 107, AND 108**

New Jersey

#### **Porzio Bromberg & Newman PC**

On behalf of manufacturing and logistic companies, Alan Zakin, representing NJMEP, contacted the Attorney General and Governor's office. They were...

---

### **Coronavirus (COVID-19) | Summary of Key International Tax Measures**

#### **Hogan Lovells**

This Hogan Lovells Global Tax Practice guide gives You a summary of key measures to date for MNEs In China, France, Germany, Italy, Luxembourg, Mexico...

---

### **COVID-19 Update: CISA Updates Critical Infrastructure Workers Guidance to Provide Additional Recommendations for Government and Businesses and Clarify Scope of Food and Agriculture Sector**

#### **Hogan Lovells**

The Department of Homeland Security's (DHS's) Cybersecurity & Infrastructure Security Agency (CISA) revised its interim guidance identifying critical...

---

### **Employment Question of the Day: April 20, 2020**



### **Fredrikson & Byron PA**

My company was either ineligible for, or did not receive, a loan under the Small Business Administration's Paycheck Protection Program (PPP). Is...

---

### **Defendant Seeks Rehearing En Banc On Seventh Circuit's Decision Rejecting Bristol-Myers Squibb In Rule 23 Class Actions**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The battle continues over the applicability of the U.S. Supreme Court's decision in Bristol-Myers Squibb v. Superior Court, 137 S...

---

### **COVID-19: Walking the Line Between Worker Safety and Privacy** Audio

#### **Sidley Austin LLP**

The COVID-19 pandemic poses unprecedented challenges for employers. Businesses must walk the line between keeping workers safe and respecting their...

---

### **New York Employers Must Prepare To Provide Sick Leave Benefits in Accordance With New Statewide Sick Leave Law** New York

#### **Kramer Levin Naftalis & Frankel LLP**

As part of its approval of the state budget, New York State recently enacted a paid sick leave law that will apply to all private employers in New...

---

### **Lessons Learned From Walmart: Best Practices For Employers Regarding COVID-19 Preparation and Communication**

#### **Porzio Bromberg & Newman PC**

The first COVID-19-related wrongful death lawsuit against an employer has been filed, specifically in Illinois state court, against Walmart[1]. The...

---

### **Unemployment Assistance and the CARES Act: Minimizing Liability for Withdrawing Job Offers**

#### **Ogletree Deakins**

Employers across the country are making difficult decisions due to the COVID-19 crisis. The economic downturn has affected current employees in a...

---

### **DOJ and FTC Issue Joint Statement Regarding COVID-19 and Antitrust Violations**

#### **Sheppard Mullin Richter & Hampton LLP**

The Department of Justice ("DOJ") and the Federal Trade Commission ("FTC") recently issued a joint statement (the "COVID-19 Statement") regarding...

---

### **All Non-Essential Employees Across New York State Required to Stay Home** New York

#### **Davis Wright Tremaine LLP**

At a press conference on March 20, 2020, New York Governor Andrew Cuomo announced what is effectively a state-wide shutdown, requiring 100 percent of...

---

### **Coronavirus (COVID-19) Update: States & Municipalities**

#### **Squire Patton Boggs**

State and municipal governments and other public entities are struggling to navigate unprecedented uncertainty and mounting financial demands. An...

---

### **COVID-19: Planning Ahead at a (Social) Distance—Considerations for Emerging Companies**

**Wilmer Cutler Pickering Hale and Dorr LLP**

COVID-19 continues to spread at an alarming rate, causing rippling effects throughout our daily lives and profoundly impacting our health, wellness...

---

### **OSHA Issues COVID-19 Guidance for the Construction Workforce**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: The Occupational Safety and Health Administration (OSHA) has issued an alert listing safety tips (Guidance) employers can follow...

---

### **Employment issues to consider as businesses get ready to re-open after covid-19**

**Thompson Hine LLP**

After weeks (if not months) of state "stay-at-home" and "shelter-in-place" orders, social distancing mandates and telework, there may be light at the...

---

### **The Ties That Bind: NLRB Division Of Advice Rebukes Union Limitations On Employees' Right to Resign Membership**

**Fisher Phillips**

A recently released Advice Memorandum from the National Labor Relations Board's Division of Advice found unlawful a union's attempt to restrict...

---

### **Minnesota Update: The Latest COVID-19 Developments Impacting Minnesota Employers**

Minnesota

**Littler Mendelson PC**

Note: Because the COVID-19 situation is dynamic, including with new governmental measures each day, employers should consult with counsel for the...

---

### **Bankruptcy is Not a "Get Out of Jail Free" Card: Enforcing Trade Secret Rights and Restrictive Covenants Against Financially Troubled Wrongdoers**

**Seyfarth Shaw LLP**

We have previously written about the effects of COVID-19 on the way we currently work, as well as how businesses need to adapt to protect their trade...

---

### **Proposed NYC Essential Workers Bill of Rights Provides Just Cause Termination and Premium Pay for Essential Workers, Sick Leave for Independent Contractors**

New York

**Littler Mendelson PC**

On April 22, 2020, the New York City Council introduced a series of bills in response to the COVID-19 crisis that is ravaging the city. In addition...

---

### **San Franciscans Ordered to Wear Face Masks - Who Pays For Them While At**



## **Work?**

### **Fisher Phillips**

San Francisco has ordered individuals to wear face coverings when they are shopping, taking transit, getting healthcare, or working in a job that...

---

### **San Francisco, San Jose Mandate New COVID-19 Paid Sick Leave Benefits**

#### **McGuireWoods LLP**

As previously reported, in response to the Families First Coronavirus Response Act (FFCRA), California's governor and a growing number of California...

---

### **Tribal Businesses Eligible for Loans / Tax Credits Under the CARES Act**

#### **Quarles & Brady LLP**

The Coronavirus Aid, Relief and Economic Security Act (CARES Act) establishes many significant loan programs and tax benefits to help tribal-owned...

---

### **Los Angeles Implements Multiple Employment-Related Measures Responding to COVID-19 Crisis (US)**

#### **Squire Patton Boggs**

Ordinances and Executive Orders require paid sick leave, provide additional protections for grocery, drug store, and food delivery employees, and...

---

### **South Carolina Unemployment Notice Requirements Updated**

[South Carolina](#)

#### **Jackson Lewis PC**

South Carolina's Department of Employment and Workforce (DEW) issued a notice effective April 16, 2020, requiring all employers to provide employees...

---

### **Employer Fears of Messing Up During COVID-19 Pandemic**

#### **Bradley Arant Boult Cummings LLP**

Even in pandemic-free times, the world of labor laws and employment regulations is at best confusing to an employer, and at worst...

---

### **NOL Changes and Opportunities in the CARES Act and Revenue Procedure 2020-24**

#### **Pepper Hamilton LLP**

In order to get cash into the hands of taxpayers during the international pandemic caused by COVID-19, Congress enacted the Coronavirus Aid, Relief...

---

### **Mask Up! New York "Essential" Businesses and Nonprofit Organizations Must Provide Face Masks to Public-Facing Employees**

[New York](#)

#### **Perlman & Perlman LLP**

All New York "essential" businesses, including nonprofit organizations, must provide face coverings to their employees when in direct contact with...

---

### **Connecticut Extends Time to Comply with Mandatory Sexual Harassment Prevention Training**

[Connecticut](#)

#### **Jackson Lewis PC**

Recognizing employers have challenges in ensuring employees complete

Connecticut's new mandatory sexual harassment training requirements during the...

---

#### **Updated "Stay-at-Home" Order: Executive Order 2020-59**

##### **Foster Swift Collins & Smith PC**

As expected, Governor Whitmer's newest order, Executive Order 2020-59 ("EO 2020-59"), extends Michigan's "stay-at-home" order until May 15, 2020. EO...

---

#### **Attendance Bonuses During COVID-19 Rebuilding Can Lead To Unintended Legal Consequences**

##### **Fisher Phillips**

As the nation's political leaders discuss the easing of the various shelter-in-place orders in an effort to re-start the economy, businesses have...

---

#### **GAO Set To Launch Flurry of COVID-19 Related Audits**

##### **Covington & Burling LLP**

The Government Accountability Office ("GAO"), often referred to as Congress' watchdog, is ramping up its oversight activities in preparation for an...

---

#### **Buchalter Client Alert COVID-19: Takeaways from the DOL's Latest FFCRA FAQs**

##### **Buchalter**

Earlier this week, the US Department of Labor (DOL) added to their long list of Frequently Asked Questions (FAQs) to the Families First Coronavirus...

---

#### **West Virginia Supreme Court Upholds Right-to-Work Law**

West Virginia

##### **Dinsmore & Shohl LLP**

The Supreme Court of Appeals of West Virginia upheld the constitutionality of the Workplace Freedom Act in a 5-0 decision, with one justice...

---

#### **AG Sues China over COVID-19 | Layoffs in AG's Office | FTC Settles with Rent-to-Own Payment Plan Co**

##### **Cozen O'Connor**

Cozen O'Connor Member and former Virginia AG Jerry Kilgore participated in the opening panel for the Attorney General Allianc...

---

#### **2020 is hereby incorporated by reference—Maximizing deal value through thoughtful disclosure**

##### **Eversheds Sutherland (US) LLP**

When the last of the cool spring days are behind us, stay-at-home orders are lifted, and M&A activity begins to resume in earnest, the high of the...

---

#### **Facing Your Face Mask Duties - A List of Statewide Orders, as of April 22, 2020**

##### **Littler Mendelson PC**

Governors and public health officials across the country have implemented stringent measures to help contain the spread of COVID-19, such as stay at...

---

#### **Texas Begins Reopening Businesses; Employers May Be Required To Provide**



## Face Coverings Texas

### Fisher Phillips

Texas Governor Greg Abbott issued a series of Executive Orders on April 17 aimed at beginning the process of reopening the State's businesses. In...

---

### Smile when you say that!

#### Constangy Brooks Smith & Prophete LLP

Online snark can be an unfair labor practice. If you're going to joke on Twitter about what you'll do to employees if they unionize, be sure to add...

---

### 5 Steps To Reopen Your Workplace, According To CDC's Latest Guidance

#### Fisher Phillips

The Centers for Disease Controls and Prevention (CDC) just released guidance to assist employers in making decisions regarding reopening during the...

---

### Texas employers who do not participate in workers' compensation face heightened workplace liability risks as employees return from COVID-19 quarantine Texas

#### Reed Smith LLP

Texas employers who have opted out of workers' compensation coverage may face significantly increased workplace risks in the weeks and months ahead...

---

### Webinar Recording: Coronavirus & Remote Work Force: Best Practices for Protecting Trade Secrets and Intellectual Capital Video

#### Seyfarth Shaw LLP

Enacting a remote work policy or expanding an existing policy to include remote work at all levels within an organization can have consequences for...

---

### This Won't Hurt a Bit: Employee Temperature and Health Screenings - A List of Statewide Orders, as of April 23, 2020

#### Little Mendelson PC

Governors and public health officials across the country have implemented stringent measures to help contain the spread of COVID-19, such as stay at...

---

### Fluctuating Workweek + Incentive Pay = No Problem—DOL Sends Final Rule to White House

#### Seyfarth Shaw LLP

Seyfarth Synopsis: The U.S. Department of Labor's Wage & Hour Division has entered the final phase of issuing a new rule concerning the fluctuating...

---

### Department of Labor Provides Further Guidance Regarding Unemployment Under the CARES Act

#### Ice Miller LLP

The U.S. Department of Labor ("DOL") provided additional guidance related to the massive expansion to unemployment benefits under the Coronavirus Aid...

---

### Employment Law Update: A Guide for Employers and Parents Regarding School



## **and Childcare Center Closures**

### **Greenbaum, Rowe, Smith & Davis LLP**

New Jersey Governor Phil Murphy recently announced that New Jersey primary and secondary schools (kindergarten through 12th grade) will be closed...

---

## **California grants additional paid sick leave rights to food sector workers**

California

### **Hogan Lovells**

California food sector workers now have the right to additional paid sick leave, even if they work for large employers exempted from the federal...

---

## **The Anticipated Rise in At-Home Work Injury Claims During the Coronavirus Pandemic**

Mississippi

Texas

### **Foster Swift Collins & Smith PC**

We remain in the midst of a worldwide pandemic. The federal government and all 50 states have declared states of emergency. In an effort to mitigate...

---

## **COVID-19 and Cross-Border Furloughs and RIFs**

### **Vinson & Elkins LLP**

During the last month, we have been talking a lot about the legal challenges involved in laying off or furloughing workers in the United States. How...

---

## **Employment Law Update: EEOC Issues New Guidance on Accommodation Requests; Expands “Undue Hardship” Definition; Provides Guidance for Employers on Employees Returning to Work**

### **Greenbaum, Rowe, Smith & Davis LLP**

On April 17, 2020, the U.S. Equal Employment Opportunity Commission (EEOC) issued updated guidance for employers navigating the complex issues...

---

## **COVID-19 Emergency Local Paid Sick Leave Chart (California)**

California

### **Davis Wright Tremaine LLP**

This summary is for general information only. It is not a full analysis of the matters presented and should not be relied on as legal advice. In...

---

## **Law on COVID19 in Poland - Handbook**

### **Baker McKenzie**

Among other things, new set of regulations contains solutions regarding the remote operation of companies. There are, however, no changes in the...

---

## **Prior Ruling on What Constitutes a Litigation “Emergency” May Not Be a Unicorn After All**

### **Seyfarth Shaw LLP**

As we previously reported, as a result of the COVID-19 crisis, courts across the country are adjourning most appearances, including trials, and...

---

## **New York Issues Guidance On Face Masks For Essential Business Employees**

New York

### **Fisher Phillips**

Governor Cuomo recently issued an Executive Order directing essential businesses to provide face coverings to their employees when in direct contact...

---

### **New York Challenges U.S. Department of Labor's Final Rule on FFCRA** New York

#### **Ogletree Deakins**

On April 14, 2020, the State of New York filed a lawsuit against the U.S. Department of Labor (DOL) seeking declaratory and injunctive relief in the...

---

### **Protecting Trade Secrets During the Pandemic**

#### **Paul Hastings LLP**

As more employees are furloughed and laid-off during the COVID-19 pandemic, now is the ideal time to update your trade secret protection program...

---

### **Facemasks Are the Rule in the Connecticut Workplace** Connecticut

#### **Ogletree Deakins**

On April 17, 2020, Governor Ned Lamont issued Executive Order 7BB requiring state residents "who [are] unable to or [do] not maintain a safe social...

---

### **COVID-19: Clarification measures to the JobKeeper Rules announced**

#### **MinterEllison**

On 24 April 2020 Treasury announced a number of measures which will be enacted to clarify the operation of the JobKeeper rules. We discuss these...

---

### **New Paid Supplemental Sick Leave for California Food Sector Employers**

California

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 16, 2020, California Governor Gavin Newsom issued Executive Order N-51-20, requiring employers of Food Sector Workers to...

---

### **Virginia Continues Sweeping Employment Reforms** Virginia

#### **McGuireWoods LLP**

Although Virginia's recent amendments to its Human Rights Act have garnered the most media attention, Gov. Ralph Northam has also signed or proposed...

---

### **Force Majeure in the Age of COVID-19: A Force to be Reckoned With** New Jersey

#### **Greenbaum, Rowe, Smith & Davis LLP**

As the COVID-19 pandemic continues to wreak havoc on our social, legal, financial, real estate, and healthcare systems, the widespread disruptions...

---

### **COVID-19 Compliance Conversations (VIDEO)** Video

#### **Bass, Berry & Sims PLC**

In this Episode, Lindsey Fetzer and John Kelly provide a brief overview of compliance considerations related to conducting internal investigations...

---

### **Minnesota Legislative Update: COVID-19 Testing Agreement Initiated** Minnesota



## **Faegre Drinker Biddle & Reath LLP**

Governor Walz announced an agreement with the University of Minnesota and the Mayo Clinic to expand the State's ability to test for COVID-19. The...

---

## **[FCRA] No Solace for the Solis's: Empty FCRA Allegation Ends in Dismissal** **Squire Patton Boggs**

In a consumer loan agreement that went south, Citibank wins dismissal of Fair Credit Reporting Act ("FCRA") allegations levied by pro se Plaintiffs...

---

## **EEOC Provides Updated Guidance on COVID-19 Testing**

### **Ogletree Deakins**

Employers continuing to operate as essential businesses under the various state closure orders, or that are now beginning to plan to reopen or return...

---

## **COVID-19 in California: Bay Area Counties Join Others in Mandating Face Coverings**

California

### **Morgan Lewis**

Several counties and cities in California are requiring individuals to wear cloth face coverings, including those working in or visiting...

---

## **States expand workers' compensation law for "front-line" workers in response to COVID-19**

### **Hogan Lovells**

Employers should be aware of recent changes in state workers' compensation laws which expand protections for "front-line" workers in response to the...

---

## **A Leadership Invitation on Inclusion & Belonging During the COVID-19 Pandemic** **Seyfarth Shaw LLP**

For weeks, leaders in our profession have been living, breathing, and reacting to COVID-19. Thank you for your continued leadership as things change...

---

## **OSHA Issues Temporary Guidance on Using Enforcement Discretion During the Coronavirus Pandemic**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The Occupational Safety and Health Administration (OSHA) has issued Interim Guidance to advise compliance safety and health...

---

## **COVID-19: Employers Have Options to Provide Relief to Employees and Their Communities**

### **Wilmer Cutler Pickering Hale and Dorr LLP**

As the COVID-19 pandemic spreads, the economy has struggled significantly under its new burdens. The impact both domestically and globally has been...

---

## **Employment and compensation**

### **Baker McKenzie**

Yes. Pursuant to the National Health emergency declared on March 12, 2020, employees have to notify employers if they have COVID- 19 symptoms...

---

## **DOT and FMCSA Guidance for Managing Disruptions to Regulated Drug and Alcohol Testing Due to COVID-19**

**Ansa Assuncao LLP**

On March 23, the Department of Transportation (“DOT”) issued guidance for conducting DOT-required drug and alcohol testing in safety-sensitive...

---

## **Minnesota Executive Order: Some Business May Reopen with ‘Non-Critical Exempt’ Workers**

Minnesota

**Jackson Lewis PC**

Minnesota State Governor Tim Walz has issued Emergency Executive Order 20-40, Allowing Workers in Certain Non-Critical Sectors to Return to Safe...

---

## **NLRB Affirms that Employers May Prohibit Employees from Discussing Ongoing Investigations**

**Vorys Sater Seymour and Pease LLP**

Hard to believe these days, but non-Covid-19-related developments do still pop up from time-to-time. Last week, the NLRB gave us one on an issue the...

---

## **What Colorado Employers Need To Know About New Face Covering Requirement**

Colorado

**Fisher Phillips**

Colorado Governor Jared Polis just issued a new Executive Order: “Ordering Workers in Critical Businesses and Critical Government Functions to Wear...

---

## **Michigan’s Newest Stay-At-Home Order: Amendments Employers Need to Know**

Michigan

**Miller Canfield PLC**

On April 24, 2020, Michigan Governor Gretchen Whitmer signed Executive Order 2020-59 (the “Order”). The Order rescinds Executive Order 2020-42 and...

---

## **Don’t Forget the Basics When Reopening Your Retail Business: A 5-Point Plan**

**Fisher Phillips**

The COVID-19 coronavirus pandemic that closed hundreds of thousands of business around the country is unprecedented. Fortunately, many retailers were...

---

## **OSHA Issues COVID-19 Guidance for Package Delivery Employers**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: OSHA has issued a COVID-19 guidance for package delivery employers. OSHA offers recommendations to help reduce employees’ risk of...

---

## **In the Trenches: Operating During the Crisis: Main Street Lending Program Webinar**

Video

**Nelson Mullins Riley & Scarborough LLP**

Nelson Mullins attorneys held a discussion on Tuesday, April 21 at 11 a.m. On all aspects of the new Main Street Lending Program — a \$600 billion...



---

## **Conducting Trade Secret and Restrictive Covenant Investigations Remotely** **Seyfarth Shaw LLP**

One of the first things a company should do when it suspects that its trade secrets have been compromised or that an employee has violated...

---

## **New Permitting Requirements Proposed for Construction Projects in the City of Boston** Massachusetts

### **Seyfarth Shaw LLP**

The City of Boston has proposed new safety protocols for construction work deemed essential during the ongoing health emergency caused by the...

---

## **What comes next: Reopening the workplace after COVID-19**

### **Reed Smith LLP**

In light of the COVID-19 pandemic, many U.S. businesses remain shuttered or operating at reduced levels. While the ultimate decision to allow...

---

## **COVID-19: New York State Governor Andrew Cuomo Press Conference Weekly Highlights** New York

### **Manatt Phelps & Phillips LLP**

Governor Andrew Cuomo provides daily press briefings on the status of New York State's COVID-19 response and expected executive actions. The Manatt...

---

## **Strategies For Developing A Return To Work Action Plan**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: While most of the country is subject to shutdown orders, federal and local leaders are contemplating when and how to bring people...

---

## **Non-Compete Agreements and Restrictive Covenants During COVID-19**

### **Crowell & Moring LLP**

Are non-competes still enforceable in middle of the unprecedented economic disruption caused by COVID-19? Many employers have reacted to the business...

---

## **The Roots Of The CROWN Act: What Employers Need To Know About Hairstyle Discrimination Laws**

### **Fisher Phillips**

Curly, straight, natural, relaxed, braids, dreads, Afro, or weave. Hair in the workplace is a controversial issue that has been flooding the media in...

---

## **Los Angeles Mayor Expands Social Distancing Protocols** California

### **Barnes & Thornburg LLP**

Los Angeles businesses must adhere to an emergency order issued by Mayor Eric Garcetti regarding providing face coverings. Effective April 16, Mayor...

---

## **Avoiding Employee Complaints and OSHA Inspections When Reopening the Workplace**



### **McGuireWoods LLP**

Since the COVID-19 crisis began, employees have submitted unsafe workplace complaints to the U.S. Occupational Safety and Health Administration...

---

### **Pennsylvania Supreme Court Narrows Independent Contractor Test Under State's Unemployment Law**

Pennsylvania

#### **Littler Mendelson PC**

On April 22, 2020, the Pennsylvania Supreme Court issued a decision affecting the classification of independent contractors for purposes of the state...

---

### **Alabama Implements New Strategies as UI Claims Overwhelm Current Structure**

Alabama

#### **Ogletree Deakins**

On April 21, 2020, Alabama Governor Kay Ivey held a press conference that addressed business concerns surrounding the COVID-19 pandemic and included...

---

### **Assessing the Pros and Cons of Class Action Waivers in Employment Arbitration Agreements**

#### **Davis Wright Tremaine LLP**

Last year, the U.S. Supreme Court held in *Epic Systems v. Lewis* that class action waivers in arbitration agreements between employers and employees...

---

### **Guidance for Employers Returning to Work; COVID Infections as Worker's Compensation Injuries, and More**

#### **Clingen Callow & McLean LLC**

Many of our clients are operating in a limited fashion pursuant to one of the many exemptions set forth in Governor Pritzker's stay at home order...

---

### **New COVID-19 Stimulus Measure Provides More Aid for Small Businesses, Health Care Providers, and Testing**

#### **Epstein Becker Green**

On the heels of its passage by the U.S. Senate two days earlier, the Paycheck Protection Program and Health Care Enhancement Act (the "Act") was...

---

### **Michigan: Gradual Reopening of Businesses**

Michigan

#### **Jackson Lewis PC**

To gradually reopen businesses in the state while continuing to slow the spread of COVID-19 in Michigan, Governor Gretchen Whitmer's Executive Order...

---

### **Return to Work Post-Coronavirus Checklist**

#### **Cozen O'Connor**

Monitor federal, state, and local closure orders, re-opening guidelines, industry practices, and geographic considerations...

---

### **Contractors Performing COVID-19 Relief Work Should Start Preparing for Whistleblower Complaints Now**

### **Venable LLP**

Congress has responded to the recent COVID-19 pandemic with relief spending at historic levels, including federal funds that are enabling agencies to...

---

### **COVID-19: Daily Report for Life Sciences and Health Care Companies (10 - 17 April 2020)**

#### **Hogan Lovells**

The Daily Report is a compilation of COVID-19 (coronavirus) news briefs from around the world to help life sciences and health care companies stay...

---

### **The Government's Friendly Reminder for Employers in Times of Crisis: No COVID-19 Exception to Antitrust Law Exists**

#### **Baker & Hostetler LLP**

The pandemic has resulted in worker layoffs, furloughs, and terminations erasing nearly overnight the nation's record low unemployment and ballooning...

---

### **What Does Governor Hogan's Roadmap to Recovery Mean for Maryland Employers?**

[Maryland](#)

#### **Shawe Rosenthal LLP**

On April 24, 2020, Governor Hogan issued "Maryland Strong: Roadmap to Recovery," his plan for reopening the state as the COVID-19 pandemic crisis...

---

### **Kentucky Launches 'Healthy at Work' Plan for Reopening Economy Safely**

[Kentucky](#)

#### **Jackson Lewis PC**

Kentucky Governor Andy Beshear is urging a gradual, phased re-opening of the economy — not just on a statewide basis, but on an individual business...

---

### **Employers: Are You Following Michigan's New Mandatory Employee Safety Requirements?**

[Michigan](#)

#### **Dickinson Wright**

Coronavirus continues to impose hardships on lives around the globe. Employers of American workers have to adjust to constantly-evolving laws and...

---

### **Now More Than Ever, California Employers Need To Stay Abreast Of Working Time and Control Issues**

[California](#)

#### **Fisher Phillips**

The California appellate courts, and the California Supreme Court, continue to weigh in on significant and compelling wage and hour issues that...

---

### **ERISA Rules Every ESOP Fiduciary Needs to Know to Avoid Breach Claims**

#### **Hall Benefits Law**

Employee Stock Ownership Plan (ESOP) fiduciaries are governed by ERISA rules just as administrators of other qualified retirement and benefit plans...

---

### **A Checklist for Loan Forgiveness Under the Payroll Protection Program**

#### **Bowditch & Dewey LLP**



With some necessary preparedness and a bit of luck, some U.S. small businesses were able to obtain some financial relief last week thanks to SBA loans...

---

### **President Trump Announces Suspension of Immigration Due to COVID-19, Details Not Yet Available**

#### **Greenberg Traurig LLP**

Late on April 20, President Trump tweeted his intention to issue an Executive Order (EO) that "temporarily" suspends immigration into the United...

---

### **COVID-19: PA Construction Guidance - May 1, 2020 Return to Work**

#### **Duane Morris LLP**

As the construction industry prepares to resume work, the Wolf Administration today issued guidance for all construction businesses and employees to...

---

### **Executive Order Provides California Food Sector Workers With COVID-19 Supplemental Paid Sick Leave**

#### **Davis Wright Tremaine LLP**

On April 16, 2020, California Governor Newsom signed Executive Order N-51-20, requiring qualifying "hiring entities" to provide two weeks of...

---

### **Potential Pitfalls of Temperature Screenings** California

#### **Cozen O'Connor**

A few short weeks ago, employer-mandated temperature checks would have been considered an overbroad medical exam under the Americans with...

---

### **COVID-19 Washington Update: April 24, 2020**

#### **Kelley Drye & Warren LLP**

Today's federal government actions in response to COVID-19, includes enactment of the Paycheck Protection Program and Health Care Enhancement Act...

---

### **EEOC Issues Technical Assistance on COVID-19 Workplace Issues**

#### **Davis Wright Tremaine LLP**

The Equal Employment Opportunity Commission (EEOC) has issued updated technical assistance to help employers address a number of workplace issues...

---

### **Delaware Employers Must Supply Face Coverings, Hand Sanitizer** Delaware

#### **Fox Rothschild LLP**

Businesses and individuals in Delaware are required to take additional protective measures in workplaces and public settings under Gov. John Carney's...

---

### **Pennsylvania Set to Reopen Construction Sites on May 1, with New COVID-19 Measures** Pennsylvania

#### **Greenberg Traurig LLP**

Pennsylvania construction sites are allowed to return-to-work as of May 1, pursuant to a new order issued April 24, 2020, by Gov. Tom Wolf. Pursuant...

---

## **Virginia Employers Get Ready: New Laws Dramatically Expand Employee Protections and Employer Liability in the Commonwealth**

Virginia

### **Proskauer Rose LLP**

In the wake of Virginia voting in Democratic majorities in both houses of the state legislature last year, the Virginia legislature has passed, and...

---

## **EEOC states that employers may administer COVID-19 tests before permitting employees to enter the workplace**

### **Hogan Lovells**

In an important development for critical workforces that continue to operate, as well as businesses planning to reopen, the Equal Employment...

---

## **Paid sick leave and handwashing for the food sector: new Californian rules**

California

### **Ius Laboris**

California Governor Gavin Newsom has issued an Executive Order requiring employers in the food sector to provide their employees with paid sick leave...

---

## **May an Employer Require Its Employees to Use a Contact Tracing App?**

### **Jenner & Block LLP**

Businesses around the United States are beginning to reopen and more and more will reopen in the coming months. There is, however, no vaccine for the...

---

## **COVID-19 Likely Responsible for Hike in OSHA "Fatality/Catastrophe" Investigations at Healthcare Facilities**

### **Ogletree Deakins**

Compared to the first three weeks of April in 2019, April 1, 2020, through April 21, 2020, had a 720 percent increase in healthcare facility...

---

## **The Families First Coronavirus Response Act**

### **Morgan, Brown & Joy LLP**

On March 18, 2020, the United States Senate approved, and President Trump signed into law, a revised version of a novel coronavirus relief measure, H...

---

## **Employment Question of the Day: April 22, 2020 - Part 1**

### **Fredrikson & Byron PA**

Some employers may be ready to recall employees furloughed during the prior four to five weeks. The COVID-19 pandemic is not over, but maybe funds...

---

## **Re-Opening for Business: Is Your Workplace Ready?**

### **Akerman LLP**

Employers face a myriad of issues in thinking through whether and how to re-open for business after mandatory closures, or how to thoughtfully phase...

---

## **The Reopening Playbook: What US Employers Should Be Thinking About Right Now**



### **Baker McKenzie**

With signs that the virus is peaking in the US, and with some state Shelter-in-Place Orders scheduled to be lifted in the coming weeks, employers are...

---

### **What You Need To Know About Kentucky OSHA's Proposed Injury and Illness Reporting Rule Change**

Kentucky

#### **Fisher Phillips**

The Kentucky Labor Cabinet's Department of Workplace Standards released its proposed amendments to its injury and illness recordkeeping and reporting...

---

### **Is the Future U.S. Workplace a Work Share Program?**

#### **Littler Mendelson PC**

In response to COVID-19 and the current economic downturn, employers across the country have experienced a dramatic decline in business and a lack of...

---

### **COVID-19: Re-Opening Issues Checklist**

#### **Kilpatrick Townsend & Stockton LLP**

The fluidity of the COVID-19 situation will require businesses to consider a myriad of issues as they navigate the decision as to whether, when, and...

---

### **Updated EEOC Guidance Allows Employee COVID-19 Testing**

#### **Barnes & Thornburg LLP**

How far is too far? That is a question most employers are struggling with as they work to maintain workplaces free from COVID-19 and ensure the...

---

### **Business lookouts during covid-19 (part 1)**

#### **ProLegal Law Chambers**

Businesses are experiencing unprecedented challenges and market disruption due to Covid-19 pandemic and consequential economic meltdown seems...

---

### **Los Angeles COVID-19 Guidance: Week in Review (April 27, 2020)**

#### **Manatt Phelps & Phillips LLP**

On April 22, 2020, the City Council passed Right of Recall and Worker Retention ordinances. The Mayor has indicated that he supports both and will...

---

### **CFAA Battle Heading to the Supreme Court**

#### **Seyfarth Shaw LLP**

While it can be hard to remember in a world dominated by COVID-19 headlines, the wheels of justice have not stopped turning at the Supreme Court—even...

---

### **Counting to 500 Under the PPP**

#### **Lane Powell PC**

The SBA has again updated their PPP loan FAQs to add FAQ 36. This FAQ, issued Sunday, April 26, provides guidance on how to count employees to...

---

### **Gardeners, Golfers, and Boaters Rejoice! Michigan Extends "Stay Home, Stay Safe" Order but Provides for the Reopening of Certain Businesses and**



## **Recreational Activities** Michigan

### **Littler Mendelson PC**

On April 24, 2020, Michigan Governor Whitmer issued an Executive Order extending her April 3, 2020 Stay Home, Stay Safe Order through May 15, 2020...

---

## **More Paid Sick Leave in Massachusetts? Bill Would Add Up to 80 Hours of Emergency Leave** Massachusetts

### **Fisher Phillips**

The Massachusetts legislature is considering expanding the State's generous paid sick leave statute to add up to 80 hours of emergency paid sick...

---

## **Washington State Reopens Some Construction, with Restrictions** Washington

### **Cozen O'Connor**

On April 24, 2020, Washington Governor, Jay Inslee, signed an addendum to Proclamation 20-25 that allows a limited restart to construction projects...

---

## **The Duty to Bargain During the COVID-19 Pandemic**

### **Morgan, Brown & Joy LLP**

In response to the COVID-19 pandemic and its severe nationwide impact to the economy, employers have had to make many difficult and time-sensitive...

---

## **Massachusetts Department of Unemployment Assistance Announces Implementation of CARES Act and Pandemic Unemployment Assistance**

Massachusetts

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: With the advent of the CARES Act, the Commonwealth of Massachusetts has taken steps to implement Pandemic Unemployment Assistance...

---

## **The Next Normal: A Littler Insight on Returning to Work - Some Lessons from Asia**

### **Littler Mendelson PC**

The COVID-19 pandemic has had an unprecedented impact on individuals and businesses across the globe. Governments closed their Borders, issued health...

---

## **COVID-19 weekly round-up (20-26 April 2020)**

### **Lexology PRO**

With new economic data heralding a potential global recession of a kind not seen since the 1930s and possible falls in gross domestic product of...

---

## **Protecting Trade Secrets Without Breaking the Bank (Or Even Negatively Affecting Profits)**

### **Seyfarth Shaw LLP**

As a result of the COVID-19 crisis, and the effective shut down of most of the US economy over the past several weeks (and for the foreseeable...

---

## **Antitrust Enforcers on Alert for Anticompetitive Conduct Targeting Health Care**

## **and Frontline Workers**

### **Morrison & Foerster LLP**

As much of the U.S. battles COVID-19 by self-quarantining, others fight on the front lines by providing healthcare services, maintaining supply...

---

## **COVID-19: U.S. Employer Checklist: Re-opening Strategies and Return to Work Policies After COVID-19 Outbreak**

### **K&L Gates**

The following PDF document is a list of suggested practices for businesses to consider during the reopening process. For additional industry-specific...

---

## **EEOC Releases Guidance on ADA Issues and COVID-19 for Employers**

### **McBrayer McGinnis Leslie & Kirkland PLLC**

On April 17, 2020, the EEOC published updated guidance for employers on how to comply with ADA and other antidiscrimination laws and regulations in...

---

## **Virginia adopts a wave of new employment laws. Part 2 - Worker classification and clampdown on restrictive covenants**

Virginia

### **Reed Smith LLP**

As we previously reported on April 23, 2020, in the midst of the COVID-19 pandemic that is dominating the news, Virginia Governor Ralph Northam...

---

## **San Jose + San Francisco Enact Temporary Emergency Paid Sick Leave Requirements for Employers Not Covered by FFCRA**

### **Cooley LLP**

As mentioned in previous Cooley alerts, the federal Families First Coronavirus Response Act (FFCRA) requires private employers with fewer than 500...

---

## **Best Practices for Commercial Property Owners/ Operators: Phase One of Reopening the Economy**

### **Wilson Elser**

The Federal Coronavirus Task Force issued a three-stage plan last week to reopen the economy, where authorities in each state - not the federal...

---

## **NYC Council Proposes Bills Providing Just Cause Discharge Requirements and Premium Pay for Essential Businesses and Expanding Paid Sick Time**

New York

### **Davis Wright Tremaine LLP**

On April 22, 2020, the New York City Council referred three bills to committee: two of which would greatly affect the employment practices of...

---

## **Reopening Amid COVID-19: Understanding Employees' Protest Rights**

### **Fox Rothschild LLP**

With some state and local shutdown orders imposed on nonessential businesses in response to the COVID-19 pandemic set to expire, many employers are...

---

## **Returning to Work in Arizona: What Employers Need to Do to Prepare**

Arizona

### **Ogletree Deakins**



On March 30, 2020, Arizona Governor Doug Ducey issued the "Stay Home, Stay Healthy, Stay Connected" order. The order, which went into effect on March...

---

**U.S. Department of Labor Issues Families First Coronavirus Response Act Notice**  
**Morgan, Brown & Joy LLP**

As set forth in our prior alert, and the text of the new Families First Coronavirus Response Act ("FFCRA"), on March 25, 2020, the United States...

---

**Seyfarth Policy Matters Newsletter - April 23, 2020**

New York

**Seyfarth Shaw LLP**

Congress Replenishes Paycheck Protection Program (PPP) Through its Phase Four Coronavirus Relief Package. On Tuesday, via unanimous consent, the...

---

**Furloughs as a Response to Coronavirus**

**Morgan, Brown & Joy LLP**

As employers face seemingly endless employment-related decisions as a result of the novel coronavirus (COVID-19) pandemic, many have asked about...

---

**Strong Whistleblower Protections Are Vital During Covid-19**

**Katz Marshall & Banks LLP**

During the coronavirus pandemic, we are now more than ever relying on our governments and health-care providers to take unprecedented action to save...

---

**U.S. Department of Labor Issues Regulations on the Families First Coronavirus Response Act**

**Morgan, Brown & Joy LLP**

Over the past few weeks, MBJ has published several client alerts relative to COVID-19 and the Families First Coronavirus Response Act ("FFCRA") which...

---

**Current State of Loan Forgiveness Under the Paycheck Protection Program**

**Lowenstein Sandler LLP**

Now that many clients have received (or are about to receive) the proceeds of Paycheck Protection Program (PPP) loans, we have been fielding many...

---

**Coronavirus Continues to Spread: What Employers Should Do**

**Morgan, Brown & Joy LLP**

On February 13, 2020 we published a Client Alert entitled "Coronavirus: Employer Considerations" that can be found here. We are continuing to monitor...

---

**FERC Reaffirms Obligations Requiring Public Utilities to Address Excess and Deficient Income Taxes Resulting from Tax Act Changes**

**Troutman Sanders LLP**

On April 16, 2020, FERC addressed the American Public Power Association ("APPA") and Exelon Corporation and its public utility subsidiaries...

---

**Coronavirus Aid, Relief, and Economic Security Act (CARES Act)**

**Morgan, Brown & Joy LLP**

On March 27, 2020, the U.S. House of Representatives approved and President Trump signed into law the Coronavirus Aid, Relief, and Economic Security...

---

### **San Francisco Grocery, Drug, And Restaurant Employees - And On-Demand Delivery Contractors - Receive New COVID-19 Protections**

**Fisher Phillips**

The San Francisco Board of Supervisors just passed the Grocery Store, Drug Store, Restaurant, and On-Demand Delivery Services Employee Protections...

---

### **California Cities Require Employers to Provide COVID-19 Sick Leave** California

**Pepper Hamilton LLP**

Client Alert Three California cities — Los Angeles, San Francisco and San Jose — have recently enacted paid sick leave laws in response to the...

---

### **Out of Sight is Not Out of Mind - Monitoring Workers Working From Home**

**Jackson Lewis PC**

Just over a month ago, we provided a high-level checklist to help organizations think about critical issues as employees begin working from home to...

---

### **Today in Washington - April 27, 2020: COVID-19 Updates** Washington

**Hall Render Killian Heath & Lyman PC**

Today, the Health Resources and Services Administration ("HRSA") launched a new COVID-19 Uninsured Program Portal so health care providers who have...

---

### **It Is A Global Pandemic, But Is It An FLSA Emergency?** California

**Seyfarth Shaw LLP**

Employees under heightened demands to care for their health and families are using time off and sick leave in record numbers. This has left many...

---

### **Illinois to extend stay-at-home order, require face masks May 1** Illinois

**Reed Smith LLP**

On April 23, 2020, Illinois Governor J.B. Pritzker announced he will be extending the state stay-at-home order through May 31, 2020. While the new...

---

### **COVID-19 Update: FDA Issues Guidance for Food and Agriculture Sector Businesses on the Use of Masks and What to Do if a Worker is Exposed to or Tests Positive for COVID-19**

**Hogan Lovells**

This post summarizes two recent documents the U.S. Food and Drug Administration (FDA) issued for the Food and Agriculture Sector in response to the...

---

### **Ninth Circuit Holds Employers May Provide a Standalone Background Check Disclosure Concurrently With Other Documents**

**Littler Mendelson PC**

On April 24, 2020, the Ninth Circuit held that the Fair Credit Reporting Act (FCRA) permits an employer to provide job applicants with a background...



---

## **Employment Question of the Day: April 23, 2020**

### **Fredrikson & Byron PA**

Under Internal Revenue Code (IRC) Section 139, employers may provide non-taxable financial assistance to their employees impacted by a qualified...

---

## **Opening the Doors: Return-to-Workplace Considerations During COVID-19, Part Three: General Workplace Safety Precautions**

### **Covington & Burling LLP**

Whether a company is an essential business or is expecting to reopen its doors in the coming weeks, a number of challenges must be addressed in order...

---

## **A Contractor's Guide for Maintaining OSHA Compliance in the Wake of COVID-19**

### **Gordon Rees Scully Mansukhani**

The U.S. Occupational Safety and Health Administration ("OSHA") requires construction employers to provide a safe workplace for employees...

---

## **The Next Normal: A Littler Insight on Returning to Work - Privacy and Data Security Implications of Employee Screening**

### **Littler Mendelson PC**

By April 30, 2020, the stay-at-home orders imposed in at least 15 U.S. states will have expired. Although the governors of some of these states are...

---

## **COVID-19 Update: Practical Considerations for Employers as They Prepare for a Return to the Workplace**

### **Paul Weiss**

As state and local governments modify stay-at-home directives and non-essential worker restrictions over the coming weeks, employers must consider...

---

## **COVID-19 RIF Checklist: Key Issues to Consider in Reductions in Force**

### **Holland & Knight LLP**

The COVID-19 crisis has demonstrated that even historically successful organizations may be forced to reduce employee headcount to maintain...

---

## **Human Rights Agencies Issue Discrimination / Harassment Guidance Amidst COVID-19 Concerns**

New York

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The U.S. Equal Employment Opportunity Commission ("EEOC"), the New York State Division of Human Rights (the "Division") and the...

---

## **Georgia Employers Receive Guidance On Governor's Back-To-Business Order**

Georgia

### **Fisher Phillips**

As expected, Governor Brian Kemp issued a detailed Executive Order to begin to re-open businesses throughout the state in the hopes that the worst of...

---

## **A Busy Month for the Paycheck Protection Program**



### **Jenner & Block LLP**

Earlier this month, the Small Business Administration (SBA) launched the Paycheck Protection Program (PPP), Congress's headline-making small business...

---

### **Virginia Minimum Wage Increase Will Take Effect on May 1, 2021** Virginia

#### **Jackson Lewis PC**

Virginia's legislation raising the hourly minimum wage has cleared its final hurdle and is set to take effect on May 1, 2021. As originally passed by...

---

### **Recent Wrongful Death Lawsuit Reveals Liability Theories for COVID-19 Exposure**

#### **Ansa Assuncao LLP**

A wrongful death lawsuit recently filed by the estate of a Walmart Inc. employee in Illinois provides a glimpse of emerging liability theories for...

---

### **Ohio Workers' Compensation System Approves \$1.6B Distribution for State Fund Employers (US)** Ohio

#### **Squire Patton Boggs**

By the end of the April, many Ohio employers with state funded workers' compensation coverage will receive a dividend from the Ohio Bureau of Workers'...

---

米国政府の支援による給与保護プログラム（PPP）の増額資金に基づくローン申込みに  
おける注意点－日系企業にありがちなミスを回避するには

#### **Masuda Funai Eifert & Mitchell Ltd**

米国政府は 給与保護プログラム(Paycheck Protection Program)（ PPP ）によ  
り提供されるローンを通じて さらに米国の中小企業を支援するために追加資  
金を投じると発表しました 中小...

---

### **COVID-19 Furloughs and Layoffs: Are you triggering pension fund withdrawal liability?**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In these uncertain economic times, temporary furloughs and longer-term layoffs have become the norm. One concern expressed by...

---

### **Considerations for Returning Employees to Work During COVID-19** Audio

#### **Ogletree Deakins**

As state and local governments begin to lift restrictions related to the COVID-19 pandemic, employers are preparing for the various permutations of...

---

### **EEOC Says Employers Can Administer COVID-19 Tests Before Employees Can Come to Work**

#### **Little Mendelson PC**

In guidance issued on April 23, 2020, the Equal Employment Opportunity Commission (EEOC) stated that employers may choose to administer COVID-19...

---

## **COVID-19 Update: CDC and OSHA Release Interim Guidance for Meat and Poultry Processing Workers and Employers**

**Hogan Lovells**

The Centers for Disease Control and Prevention (CDC) and Occupational Safety and Health Administration (OSHA) have issued Interim Guidance on COVID-19...

---

## **Covid-19 pandemic pushes the boundaries of employment law as U.S. sports come to a halt**

**Linklaters LLP**

The National Basketball Association (NBA) is credited with triggering the suspension of professional and collegiate sports across the United States...

---

## **New CDC Guidance for COVID-19 Exposed Employees of Essential Businesses**

**DLA Piper**

With expanded testing available, employers are increasingly faced with employees who may have been exposed to COVID-19, but want to continue working...

---

## **Los Angeles City Council Moves Forward With Right of Recall and Worker Retention Ordinances**

**Davis Wright Tremaine LLP**

On April 22, 2020, the Los Angeles City Council amended and moved forward with two controversial draft ordinances aimed at regulating the order of...

---

## **Georgia Pushes Forward: Latest Order Offers Detailed Reopening Steps and A Preview for Other States**

Georgia

**Littler Mendelson PC**

On April 23, 2020, Governor Brian Kemp signed an Executive Order (Order) relaxing the statewide Shelter in Place Order issued on April 2, 2020, and...

---

## **North Carolina Announces Three-Phase Plan to Reopen**

North Carolina

**Fisher Phillips**

With North Carolina's Stay at Home order extended through May 8, 2020, leaders focus on testing, tracing, and trends to determine when to re-open the...

---

## **Shutting the Gate: Temporary Worker Excluded From FLSA Collective Action**

Kansas

**Barnes & Thornburg LLP**

After conditionally certifying a collective action under Section 216(b) of the Fair Labor Standards Act (FLSA), the U.S. District Court for the...

---

## **Employees Catch a (Meal) Break from the Oregon Supreme Court**

Oregon

**Littler Mendelson PC**

On April 23, 2020, the Oregon Supreme Court declined to review a ruling by the Oregon Court of Appeals in which employers were held to a standard of...

---



## **L.A. City Council Adopts Right of Recall and Citywide Worker Retention Ordinances**

### **Manatt Phelps & Phillips LLP**

On April 22, 2020, the Los Angeles City Council considered amendments to two previously proposed ordinances in response to the COVID-19 emergency...

---

## **NYC Council Considering Worker "Bill of Rights" Amid COVID-19 Relief Bills**

New York

### **Seyfarth Shaw LLP**

During its first-ever remote session, members of the New York City Council have introduced a series of bills aimed at providing relief for...

---

## **New I-9 Form Required but Verification Relaxed for Some Employers**

### **Akerman LLP**

Amidst the fast changing pace of employer benefits and obligations during the COVID-19 pandemic, the Department of Homeland Security (DHS) has...

---

## **The Next Normal: A Littler Insight on Returning to Work - Recalling Furloughed Employees and the Rehire Process**

### **Littler Mendelson PC**

After COVID-19 abates, employers may determine that they cannot return all employees to the workforce. Some employers may need to recall employees on...

---

## **Kentucky OSHA is Shutting Down Employers for Lack of Social Distancing**

Kentucky

### **Fisher Phillips**

Kentucky OSHA (KOSH) has been tasked with enforcing Governor Beshear's Executive Orders (EO) regarding essential businesses and social distancing...

---

## **U.S. Department of Labor Issues Q&A on the Families First Coronavirus Response Act**

### **Morgan, Brown & Joy LLP**

Last week, we published a client alert on the Families First Coronavirus Response Act ("FFCRA") which may be found here. On March 24, 2020, the United...

---

## **Webinar Recording: Pre-employment Background Screening and Drug Testing: Considerations for Employers in the COVID-19 Environment**

### **Seyfarth Shaw LLP**

With courts and other public records and information repositories closed, and laboratories and health care facilities prioritizing COVID-19...

---

## **Changes to Massachusetts Unemployment Benefits in the Wake of COVID-19**

### **Morgan, Brown & Joy LLP**

In March 2020, in response to the COVID-19 pandemic, the Massachusetts Executive Office of Labor and Workforce Development (EOLWD) and the Department...

---

---

## **Let's Get [Back] to Business: Private Means Private**

### **Graydon Head & Ritchey LLP**

I don't know about you, but I cannot help but sing the Mulan song in my head every time that I read the title. I get pumped up a little thinking that...

---

## **New York Employers: Engage In The Interactive Dialogue With Medical Marijuana Users**

New York

### **Jackson Lewis PC**

A New York state court denied summary judgment to an employer that terminated an employee for testing positive for marijuana, when the employee...

---

## **Proclamation suspending entry of immigrants who present risk to the U.S. labor market during the economic recovery following the COVID-19 outbreak**

### **Miller Thomson LLP**

On Wednesday, April 22, President Trump signed a proclamation (the "Proclamation") suspending entry into the U.S. of certain immigrants who present...

---

## **Updated FFCRA Guidance for Employers**

### **Bass, Berry & Sims PLC**

The following guide has been updated with the latest guidance on the employment-related provisions of the Families First Coronavirus Response Act...

---

## **Fifth Circuit Affirms Dismissal of Qui Tam Complaint Due to Lack of Materiality in Significant False Claims Act Decision**

Mississippi

### **Faegre Drinker Biddle & Reath LLP**

The U.S. Court of Appeals for the Fifth Circuit affirmed on April 15, 2020 the dismissal of a non-intervened qui tam action in United States ex rel...

---

## **Ohio Governor Unveils Industry-Specific Protocols for "Responsible Restart Ohio" Amid the COVID-19 Crisis**

Ohio

### **Duane Morris LLP**

Governor DeWine encouraged employers to use a phased approach to returning employees to the workplace, with "high-risk employees" returning last...

---

## **U.S. Department of Labor Updates Q&A on the Families First Coronavirus Response Act**

### **Morgan, Brown & Joy LLP**

Last week, we published a client alert on the United States Department of Labor's ("DOL") questions and answers to assist in the implementation of the...

---

## **Class Notice Interference On The Defense: Court Penalizes Defendants And Attorney**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In a class action lawsuit alleging multiple fraud claims, a federal court in Illinois granted the Plaintiff's motion to sanction...

---



---

## **COVID-19: Read This Before You Take the Temperatures of Your Customers, Visitors or Employees**

### **Kilpatrick Townsend & Stockton LLP**

You want to reopen your place of business, and certainly do not want to harm your customers or employees in doing so. Safety from COVID-19 in your...

---

## **Employer's Guide for Returning to the Workplace**

### **Bass, Berry & Sims PLC**

As the U.S. economy reopens in the coming weeks and months, employers are faced with the challenge of bringing employees back to work to a workplace...

---

## **District Court Finds Biometrics Data Vendor May Be Liable for Illinois BIPA Violations**

### **Holland & Knight LLP**

The U.S. District Court for the Northern District of Illinois held that a vendor of biometric time clocks could be liable for violations of Illinois'...

---

## **Interim Guidance on Site Field Work Decisions Due to Impacts of COVID-19**

### **Vedder Price PC**

Once again, recognizing that adjustments to the evolving COVID-19 situation continue, on Friday, April 10, 2020, the United States Environmental...

---

## **New California Paid Sick Leave For Food Sector Workers**

California

### **Baker McKenzie**

On April 16, 2020, California Governor Gavin Newsom signed Executive Order N-51-20 ("Order") requiring employers in the food sector to: Provide...

---

## **EEOC Updates Guidance on the ADA, the Rehabilitation Act and COVID-19**

### **Morgan, Brown & Joy LLP**

On March 18, 2020, the Equal Employment Opportunity Commission ("EEOC") issued guidance about the Americans with Disabilities Act ("ADA") and the...

---

## **New York City Council Introduces COVID-19 Bills Addressing Essential Workers and Paid Sick Leave Coverage**

New York

### **Proskauer Rose LLP**

As previously announced, the New York City Council has introduced an expansive package of COVID-19 bills that, among other things, propose sweeping...

---

## **Massachusetts Governor Issues Emergency Order Limiting On-Site Work to Essential Services and Restricting Gatherings to Maximum of 10**

Massachusetts

### **Morgan, Brown & Joy LLP**

On March 23, 2020, Massachusetts Governor Charlie Baker issued an Emergency Order requiring all businesses that do not provide "COVID-19 Essential...

---



## **The EEOC Continues to Update Guidance on Returning to Work Pandemic-Prepared**

### **Payne & Fears LLP**

The EEOC continues to update its pandemic preparedness guidance regarding the Americans with Disabilities Act (ADA), the Rehabilitation Act, and...

---

## **EEOC Offers Employers Post-COVID-19 Return-to-Work Pointers (US)**

### **Squire Patton Boggs**

Since early in the pandemic, the EEOC has been maintaining a Technical Assistance Questions and Answers page, which it updates from time to time. As...

---

## **What Businesses Can Do to Ease the Transition When Reopening Their Doors**

### **Phelps Dunbar LLP**

As governments start easing stay-at-home orders and other restrictions, businesses that closed their doors to help contain the COVID-19 spread will...

---

## **OSHA Issues Interim Enforcement Response Plan for COVID-19 Inspections**

### **Morgan, Brown & Joy LLP**

On April 13, 2020, the Occupational Safety and Health Administration (OSHA) published an Interim Enforcement Response Plan (Plan) to provide...

---

## **Preliminary Thinking on Reopening a Business: Planning for the End of Stay-at-Home**

### **Fried Frank Harris Shriver & Jacobson LLP**

Companies have begun to think about what a reopening of business will look like. The Fried Frank Coronavirus Task Force Resource Center (available...

---

## **Employer Must Show Evidence of Union's Loss of Majority Support to Withdraw Recognition**

### **Barnes & Thornburg LLP**

The National Labor Relations Board recently ruled in Kauai Veterans Express, that a Hawaii trucking company violated Section 8(a)(5) of the National...

---

## **Philadelphia Moves Forward with Fair Workweek Law Despite COVID-19 Pandemic**

[Pennsylvania](#)

### **Cozen O'Connor**

On April 21, 2020, the Mayor's Office of Labor issued a post restating the key provisions of the City of Philadelphia's new Fair Workweek law, which...

---

## **New Congressional Aid Package May Help Coops**

### **Eversheds Sutherland (US) LLP**

Lawmakers approved an additional \$320 billion in funds for the Paycheck Protection Program, for which some cooperatives may qualify. The funds may be...

---

## **Georgia Allows Most Businesses to Reopen to the Public: What Employers Need**

to Know Georgia

### **Duane Morris LLP**

Reopening the doors of your business can also mean opening the door to lawsuits from customers and employees...

---

### **Planning for Re-Opening: What Owners, Property Managers and Users of Office and Retail Properties Should Consider**

#### **Buchalter**

Now is the time to prepare for when non-essential businesses will be allowed to re-open after the various state and local COVID-19 shutdown orders...

---

### **America Reopens: What Employers Need To Be Thinking About in Light of the Guidelines**

#### **Squire Patton Boggs**

On April 16, 2020, President Trump unveiled broad new federal guidelines laying out conditions for states to begin relaxing the strict measures...

---

### **Motions to Dismiss Granted in ADA Gift Card Cases**

#### **Bryan Cave Leighton Paisner LLP**

A New York federal court has granted motions to dismiss in four separate cases alleging that the failure to offer gift cards in Braille violates the...

---

### **EPA Publishes Draft Risk Evaluation of Perchloroethylene**

#### **Bergeson & Campbell PC**

On April 27, 2020, the U.S. Environmental Protection Agency (EPA) released the draft risk evaluation of perchloroethylene. According to EPA, it...

---

### **ACC Northeast Webinar Recording: Issue Spotting: Litigation Trends in the Post COVID-19 World**

#### **Seyfarth Shaw LLP**

As we begin to focus on what the return to work will look like, as well as what the "new normal" will be, organizations of all sizes will need to be...

---

### **Trade Secret Litigation on the Rise in California: How ADR Can Help** California

#### **Seyfarth Shaw LLP**

Trade secret litigation in California is growing, in both volume and impact. The second-largest plaintiffs' verdict in 2019 was \$845 million, as...

---

### **Essential services — new obligations for B.C. employers**

#### **DLA Piper**

A new order from the Provincial Health Officer on April 14, 2020, has created new obligations for employers who are either essential...

---

### **US antitrust enforcers on high alert for collusion in labor markets during COVID-19 pandemic**

#### **DLA Piper**

As businesses continue to adapt to the ever-changing market dynamics in the



wake of the coronavirus disease 2019 (COVID-19) pandemic, the US...

---

### **Illinois Stay-at-Home Order Modified and Extended - What Do Employers Need To Know Before May 1, 2020?**

Illinois

**Little Mendelson PC**

Illinois has been under a "Stay-at-Home" Executive Order since March 20, 2020. Among its mandates, the original Stay-At-Home Order closed...

---

### **Colorado Issues Multiple Mandates For Business Operations During "Safer at Home" Phase**

Colorado

**Fisher Phillips**

The Colorado Department of Public Health issued Public Health Order 20-28 to govern the next phase of Colorado's reopening, labeled "Safer at Home."...

---

### **Essential business provide the framework for a new normal at US worksites**

**DLA Piper**

As the US economy works its way towards reopening, experiences like those at the Charmin factory will be the new normal. As they say here, these...

---

### **Court Scorches Employer, Upholds Class Arbitration Decision**

**Barnes & Thornburg LLP**

In a blistering decision, the U.S. Court of Appeals for the Fifth Circuit upheld an arbitrator's determination that class arbitration was available...

---

### **Telework remote control and monitoring of employees' health data**

**Ius Laboris**

The Portuguese Data Protection Authority (CNPD) has recently issued guidelines on the rules regarding remote control of employees on telework, and on...

---

### **Michigan's Third Shelter-In-Place Order Begins To Relax Restrictions On Businesses**

Michigan

**Fisher Phillips**

Michigan Governor Gretchen Whitmer issued Executive Order 2020-59, which extends the State's shelter-in-place order until May 15, 2020 while also...

---

### **EEOC Authorizes COVID-19 Testing Before Employees Enter the Workplace**

**Gordon Rees Scully Mansukhani**

As employers contemplate reopening the workplace, coordinating concerns of workplace safety and compliance with the Americans with Disabilities Act...

---

### **Empty Rooms - COVID-19's Impact on the Hospitality Industry**

**Cadwalader Wickersham & Taft LLP**

The ongoing COVID-19 pandemic has had an unprecedented impact on all sectors of the U.S. economy in a remarkably short period of time, but one of the...

---

### **Employment Question of the Day: April 24, 2020**

**Fredrikson & Byron PA**

Yesterday, April 23, 2020, Governor Walz issued Executive Order 20-40 "Allowing Workers in Certain Non-Critical Sectors to Return to Safe Workplaces."...

---

### **Essential Businesses In Pennsylvania, New York, And New Jersey Must Now Require Their Employees To Wear Face Masks Or Face Coverings**

**Ansa Assuncao LLP**

Essential businesses throughout Pennsylvania authorized to maintain in-person operations must now require their employees to wear face masks while on...

---

### **Unpacking Exposure Risks for Meat and Poultry Processors: New OSHA/CDC Guidance**

**Littler Mendelson PC**

While the White House plans to sign an Executive Order to keep meat and poultry processing facilities open, the Occupational Safety and Health...

---

### **Indiana Supreme Court Favors Employee Over Interpretation of "Public Policy" Exception to At-Will Employment.**

Indiana

**Ogletree Deakins**

In Perkins v. Memorial Hospital of South Bend (Case No. 20S-CT-233), a split Indiana Supreme Court ruled in favor of an employee who was discharged...

---

### **Arbitration Agreements Lacking Employer's Signature Can Be Enforceable, Says Texas Appellate Court (US)**

Texas

**Squire Patton Boggs**

On April 16, 2020, a three-judge panel of the Court of Appeals for the First District Court of Texas held that an employer could compel a former...

---

### **Amendments to New York's Wage Theft Prevention Act Includes New Notice Obligations**

New York

**Littler Mendelson PC**

On April 3, 2020, New York Governor Andrew Cuomo signed the 2020-2021 State Budget bills, which include several amendments to New York's Wage Theft...

---

### **Colorado Expands Coverage and Amount of Leave under Health Emergency Leave with Pay (HELP) Rules**

**Littler Mendelson PC**

On April 27, 2020, the Colorado Department of Labor and Employment amended its Health Emergency Leave with Pay (HELP) Rules, which require certain...

---

### **Employer's Guide for Returning to the Workplace**

**Bass, Berry & Sims PLC**

As the U.S. economy reopens in the coming weeks and months, employers are faced with the challenge of bringing employees back to work to a workplace...

---

### **COVID-19 Checklist for North Carolina Employers**

North Carolina

**Brooks Pierce McLendon Humphrey & Leonard LLP**



Brooks Pierce has been honored to have so many North Carolina employers rely on us for up-to-date guidance on personnel matters stemming from the...

---

### **[FCRA] A Bridge Too Far: Ninth Circuit Rejects Former Employee's "Novel" Interpretation of the FCRA**

**Squire Patton Boggs**

Last week, in *Luna v. Hansen & Adkins Auto Transp., Inc.*, 2020 U.S. App. LEXIS 13215 (9th Cir. Apr. 24, 2020), the Ninth Circuit rejected a former...

---

### **United States: Mitigating Employment Litigation Claims in the Complex Landscaping of COVID-19**

**Baker McKenzie**

Employers must provide employees a safe place to work under the Occupational Safety and Health Act's "General Duty Clause." This catchall safety...

---

### **Work From Home Cybersecurity Basics: Following Company Practices (United States)**

**Bryan Cave Leighton Paisner LLP**

As the Covid-19 Pandemic forces more employees than ever before to work from home ("WFH"), businesses face new and different data privacy and...

---

### **Managing Cyber Risk for Research and Higher Education Institutions During COVID-19 Pandemic**

**Quarles & Brady LLP**

With the attention on COVID-19 prevention, treatment and research, as well as remote work and remote learning, research and higher education...

---

### **New York Reverses Course On Contours Of Paid Voting Time Leave Law**

New

York

**Fisher Phillips**

New York is reverting to its pre-2019 voting leave law, as employers will now only need to provide their workers with two hours of paid voting time...

---

### **DWZ - Drinking While Zooming (And Other Telework Dilemmas)**

**Shawe Rosenthal LLP**

By now we probably all have seen the YouTube Video of poor Danny, who finished his Zoom video meeting with his colleagues and forgot to end the call...

---

### **Key considerations in designing a return to Work Plan**

**Shearman & Sterling LLP**

Although it is too early to know when America's workforce will return to offices and other places of work, it is prudent for companies to start...

---

### **President Trump Issues Executive Order Invoking Defense Production Act for Meat and Poultry Processors**

**Hogan Lovells**

Late yesterday, President Donald Trump issued an Executive Order invoking the



Defense Production Act (DPA) to protect the meat and poultry production...

---

### **Massachusetts Nonsolicitation Case Highlights Importance of Choice-of-Law Provisions** [Massachusetts](#)

#### **Ogletree Deakins**

Many employers have national and international workforces. When entering into contracts with employees, inclusion of a choice-of-law provision is...

---

### **Virginia Human Rights Act Amendment Removes Large Employee Cap; Could Open Floodgate of New Employment Discrimination Cases For Larger Virginia Employers** [Virginia](#)

#### **Hunton Andrews Kurth LLP**

On Saturday, April 11, 2020 the Virginia Values Act was signed into law. The bill's headlining purpose-- adding gender identity and sexual...

---

### **Nurseries and Garden Stores Permitted to Resume Activities With Conditions Under Executive Order 2020-59**

#### **Foster Swift Collins & Smith PC**

On April 24, Governor Gretchen Whitmer issued Executive Order 2020-59 ("EO 2020-59"), which extends Michigan's "stay-at-home" order until May 15...

---

### **Frequently Asked Questions by Public Libraries During COVID-19**

#### **Foster Swift Collins & Smith PC**

No. Based on the strict reading of Executive Order 2020-59 ("EO 2020-59"), libraries cannot provide curbside service. In fact, we do not believe EO...

---

### **New York State Amends Paid Election Leave Law, Again, to Provide Up to 2 Hours' Paid Voting Leave**

#### **Perlman & Perlman LLP**

You may recall that in 2019, New York State's voting leave law was amended to require employers to offer employees "so much working time as will...

---

### **Colorado's "Safer at Home" Order Permits Some Businesses to Reopen with Strict COVID-19 Suppression Measures** [Colorado](#)

#### **Littler Mendelson PC**

On April 27, 2020, Colorado began its phased relaxation of the statewide stay-at-home restrictions in place since March 25, 2020, with Governor Jared...

---

### **EEOC Says OK for Mandatory Employee COVID-19 Testing**

#### **Venable LLP**

Ordinarily, the Americans with Disability Act (ADA) prohibits an employer from performing medical tests on all of its employees - but these are not...

---

### **Transferring and Fostering Positivity in the Workplace** [Audio](#)

#### **Ogletree Deakins**

Joe Beachboard and Dennis Davis discuss the concept of Emotional Contagion in the workplace. They discuss six techniques for transferring positive...

---

**Employment Question of the Day: April 27, 2020** [North Dakota](#)

**Fredrikson & Byron PA**

Employers have a lot to deal with right now as they attempt to navigate numerous statutory and regulatory changes. Thinking about, and preparing for...

---

**New Virginia Whistleblower Law Alters Employment Litigation Landscape**

[Virginia](#)

**Greenberg Traurig LLP**

Virginia's new whistleblower protection law, the Fraud and Abuse Whistle Blower Protection Act (the Law), will go into effect on July 1, 2020. The...

---

**Phasing-In: Use of COVID-19 Testing as a "Return to Work" Strategy**

**Ropes & Gray LLP**

As "stay-at-home" orders approach expiration or are lifted, it appears that a return to the workplace through "phasing-in" is rapidly approaching...

---

**Digital Issues for Individuals Working at Home** [Audio](#)

**Pepper Hamilton LLP**

The Digital Planning Podcast is designed to educate individuals about all things digital in connection with estate planning, business planning and...

---

**Ninth Circuit: FCRA Does Not Require Disclosure to be Distinct in Time from Other Employment Documents**

**Jackson Lewis PC**

The Ninth Circuit recognized that Plaintiff's argument was novel but was thwarted by the statute itself. Plaintiff below, argued on behalf of a class...

---

**Opening the Doors: Return-to-Workplace Considerations During COVID-19: Part One: Navigation the Legal Risk of Return**

**Covington & Burling LLP**

Whether a company is an essential business or is expecting to reopen in the coming weeks, a number of challenges must be addressed in order to...

---

**Updated EEOC COVID-19 Guidance: The Commission Officially Sanctions Employer Use Of COVID-19 Testing**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: In its latest update to guidance for employers in the COVID-19 pandemic, the EEOC has now clarified that employers can test...

---

**Wisconsin Federal Court Allows Airline Workers' Uniform Class Claims To Take Flight** [Wisconsin](#)

**Seyfarth Shaw LLP**

Seyfarth Synopsis: The U.S. District Court for the Western District of Wisconsin recently cast doubt on employers' ability to strike the class...

---

**Illinois releases model sexual harassment training** [Illinois](#)



### **Reed Smith LLP**

On April 28, 2020, the Illinois Department of Human Rights (IDHR) released its model Sexual Harassment Prevention Training (download here), providing...

---

### **Ohio Businesses Begin Reopening May 1: What Does It Mean For Employers?**

Ohio

#### **Fisher Phillips**

Ohio Governor Mike DeWine just unveiled the first phase of a plan to gradually reopen Ohio businesses. It will not be business as usual, however, and...

---

### **Eleventh Circuit Finds Comparator Evidence Requirement Less Stringent Under the Pregnancy Discrimination Act**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April, 17, 2020, the Eleventh Circuit Court of Appeals in *Durham v. Rural/Metro Corp.*, No. 18-14687, considered a matter of...

---

### **The 'Laker Effect' Continues: Ongoing Uncertainty With PPP Borrowers' Uncertainty Certification**

#### **Lane Powell PC**

Probably the best known provision of the CARES Act is the creation of the forgivable payroll protection program (PPP) loan, but the devil truly has...

---

### **Employment Question of the Day: April 28, 2020**

#### **Fredrikson & Byron PA**

Please explain the intersection of Families First Coronavirus Response Act (FFCRA) and the Fair Labor Standards Act (FLSA), which sets the federal...

---

### **California Counties and Cities Issue Face Covering Requirements**

California

#### **Ford & Harrison LLP**

In the wake of the global coronavirus pandemic, a number of counties and cities in California have issued Orders requiring residents and visitors to...

---

### **Texas partially reopens businesses effective May 1st**

Texas

#### **Reed Smith LLP**

In the first phase of an effort to restart parts of Texas' economy, on April 27, Texas Governor Greg Abbott issued an Executive Order allowing...

---

### **Plaintiffs Prevail in Appeal of Illinois Prevailing Wage Act Case**

#### **Barnes & Thornburg LLP**

On March 26, 2020, the Appellate Court of Illinois issued a decision holding that a municipality's failure to stipulate in its contract that the...

---

### **COVID-19 Update for Georgia Employers**

Georgia

#### **Littler Mendelson PC**

Over the past month, the state of Georgia has enacted several measures, largely affecting unemployment and business operations, in response to...

---

## **What employers need to know about the CARES Act Employee Retention Payroll Tax Credit**

### **Thompson Coburn LLP**

As we previously discussed, the Coronavirus Aid, Relief, and Economic Security Act (the “CARES Act”) provides an employee retention payroll tax...

---

## **Employer Liability for COVID-19 Exposure in the Workplace** Maryland

### **Goodell DeVries Leech & Dann LLP**

As states and businesses across the United States begin to reopen, businesses need to know whether they will be deemed responsible if an employee...

---

## **Legal Considerations in Determining Whether and How to Construct Protections for Businesses from Liability in Cases Arising from Alleged Exposure to the COVID-19 Virus**

### **Seyfarth Shaw LLP**

There’s an old saying in Washington DC, at least among Capitol Hill staff, that one should never throw away their files because old issues will...

---

## **Illinois Publishes Model Sexual Harassment Prevention Training Program** Illinois

### **Proskauer Rose LLP**

On April 28, 2020, the Illinois Department of Human Rights (the “IDHR”) published its model sexual harassment prevention training program, a copy of...

---

## **Businesses Be Ready: California Temporarily Expands Sick Leave Laws**

California

### **Newmeyer Dillion**

California, Los Angeles and San Francisco all temporarily expand their sick leave laws in response to COVID-19. The supplemental sick leave laws...

---

## **Supplemental Paid Sick Leave (Immediately) Required in Unincorporated Los Angeles County, California**

### **Littler Mendelson PC**

On April 28, 2020, the Los Angeles County Board of Supervisors voted unanimously to enact an interim urgency ordinance to require employers with 500...

---

## **OSHA State Plan Agencies Issue COVID-19 Guidance (US)**

### **Squire Patton Boggs**

Over the past several months, the federal Occupational Safety and Health Administration (OSHA) has steadily issued guidance to both employers and...

---

## **New York City Council to Consider Legislation Impacting Employers** New York

### **Cozen O'Connor**

In response to the COVID-19 crisis, the New York City Council (city council or council) has introduced a package of legislation deemed the “Essential...

---

## **Illinois Department of Human Rights Releases Model Sexual Harassment**



## Training Illinois

### **Littler Mendelson PC**

In accordance with the Illinois Human Rights Act (IHRA) amendments under Public Act 101-0221 (known as the Workplace Transparency Act), all Illinois...

---

## Ohio to Reopen with its RestartOhio Program Ohio

### **Frost Brown Todd LLC**

On April 27, 2020, Governor Mike DeWine announced his plan to reopen businesses in the State of Ohio. As phase one of "Responsible RestartOhio,"...

---

## Opening the Doors: Return-to-Workplace Considerations During COVID-19 Part Two: Potential Screening Measures for Employees Returning to the Workplace

### **Covington & Burling LLP**

Whether a company is an essential business or is expecting to reopen its doors in the coming weeks, a number of challenges must be addressed in order...

---

## COVID-19 Business Liability Considerations in Reopening the Economy

### **Ropes & Gray LLP**

As governors across the country contemplate reopening their state economies, businesses may face potential liability if workers, or if customers and...

---

## 9th Circuit: Providing disclosure with employment documents does not violate FCRA

### **Buckley LLP**

On April 24, the U.S. Court of Appeals for the Ninth Circuit affirmed a district court's ruling that an employer that obtained a consumer report for...

---

## COVID-19 UPDATE: U.S. Antitrust Agencies Issue Joint Statement on COVID-19 and Competition in U.S. Labor Markets

### **Bryan Cave Leighton Paisner LLP**

In a warning to businesses, the Antitrust Division of the U.S. Department of Justice ("DOJ") and Federal Trade Commission ("FTC," collectively the...

---

## Return to Work: Key Immigration Issues for Employers

### **Akerman LLP**

As federal, state, and local government authorities pave the pathway to re-opening America in the ever-changing COVID-19 environment, employers...

---

## Opening Up Your Workplace Again

### **Masuda Funai Eifert & Mitchell Ltd**

On Thursday April 16, 2020, President Trump unveiled his "Guidelines for Opening Up America Again" (the "Guidelines"). The Guidelines are designed to...

---

## SBA Issues Supplemental Guidance on the Paycheck Protection Program As Congress Replenishes Funding for Small Business Loans

### **Faegre Drinker Biddle & Reath LLP**

On Friday, April 24, 2020, President Trump signed into law the Paycheck



Protection Program and Health Care Enhancement Act, the fourth in a series of...

---

### **Eleventh Circuit Renders Landmark Decision on ERISA Sanctions**

#### **Littler Mendelson PC**

While everyone has been focusing on COVID-19 and still getting used to homeschooling their children, the Eleventh Circuit released a long-awaited (by...

---

### **Georgia Governor Issues Executive Order Allowing Businesses to Reopen**

Georgia

#### **Ogletree Deakins**

On April 23, 2020, Georgia Governor Brian Kemp issued Executive Order (EO) No. 04.23.20.02 entitled "Reviving a Healthy Georgia" to broaden permitted...

---

### **OSHA Guidance for the Construction Industry During Coronavirus Disease 2019**

#### **Greenberg Traurig LLP**

We have issued several GT Alerts on the Occupational Safety and Health Administration's (OSHA) response to Coronavirus Disease 2019 (COVID-19). Our...

---

### **Virginia adopts a wave of new employment laws. Part 3 - Wage payment laws**

Virginia

#### **Reed Smith LLP**

As we previously reported on April 23 and April 27, 2020, in the midst of the COVID-19 pandemic dominating the news, Virginia Governor Ralph Northam...

---

### **Texas Reopens: What Businesses Need To Know**

Texas

#### **Baker McKenzie**

On April 27, 2020, Texas Governor Greg Abbott announced details of his plan to reopen Texas businesses in phases, so long as the COVID-19 outbreak...

---

### **Delaware Governor Issues Order Imposing Obligations on Businesses Regarding the Use of Face Coverings**

Delaware

#### **Ogletree Deakins**

On April 25, 2020, Delaware Governor John Carney issued the thirteenth modification of his "COVID-19 State of Emergency" declaration, imposing...

---

### **Client Alert: CDC Releases Reopening Guidance**

#### **Bowditch & Dewey LLP**

As local, state, and federal authorities begin to endorse phased reopening plans in response to the COVID-19 pandemic, employers nationwide are...

---

### **Employers must face it: Face covering requirements growing across states and municipalities**

#### **Reed Smith LLP**

As we have previously reported, several states, including New Jersey, New York, Connecticut and Pennsylvania, now require employees, customers and/or...

---

## **Pause in Immigrant Visa Processing Imposed by Presidential Proclamation - Effective April 23 for Sixty Days at Consular Posts**

**Dickinson Wright**

After numerous rumors in the past few days regarding the suspension of immigration to the United States (U.S.), President Trump's Proclamation...

---

## **COVID-19 - States Expanding Workers' Compensation Coverage For Essential Employees**

**Baker & Hostetler LLP**

In very recent days, some states have made it easier for certain workers who have contracted COVID-19 to establish a claim for workers' compensation...

---

## **Changes to Employment-Based Immigration Processing in Light of COVID-19**

**Ford & Harrison LLP**

In light of the enormous impact of the Coronavirus pandemic on U.S. employers, their workforces and the economy, the U.S...

---

## **Why, How and When Katz May "Trump" an Expired CBA When It Comes to Making Unilateral Changes — The Relationship Between MV Transportation and Raytheon Network**

**Sheppard Mullin Richter & Hampton LLP**

From time to time, employers trigger labor disputes when they make unilateral changes in working conditions. Unions objecting to such changes often...

---

## **Bay Area Counties Now Requiring Face Coverings**

**Davis Wright Tremaine LLP**

Bay Area Counties have issued Health Orders mandating that persons wear face coverings when interacting in public. Each county's orders impose...

---

## **More States and Municipalities Impose Mandatory Face Covering and Other Workplace Protections**

**Faegre Drinker Biddle & Reath LLP**

After an initial wave that saw a focus on closing or limiting "non-essential" or "non-life sustaining" businesses and limiting individual travel...

---

## **COVID-19 Washington Update: April 23, 2020**

**Kelley Drye & Warren LLP**

Today's federal government actions in response to COVID-19, includes House passage of the Paycheck Protection Program and Health Care Enhancement Act...

---

## **OSHA Issues COVID-19 Compliance Guidance for Construction Workforces**

**Ogletree Deakins**

The U.S. Occupational Safety and Health Administration (OSHA) has issued a series of tips tailored to construction work to help reduce the risk of...

---

## **5 Tips for Employers to Safeguard Against Employee Discrimination Claims**

### **Arising from COVID-19**

#### **Holland & Knight LLP**

As employers continue to navigate the coronavirus (COVID-19) pandemic and contemplate returning employees back to the workplace, these unprecedented...

---

### **U.S. COVID-19: Preparing a Reopening Plan - Five Steps to Take Right Now**

#### **Bryan Cave Leighton Paisner LLP**

As state governments and businesses look towards restarting the economy, the consensus is that as the U.S. gradually re-opens, the look and feel of...

---

### **DOL Issues More FFCRA Compliance Guidance on Paid Leaves**

#### **Dykema Gossett PLLC**

Guidance Focuses on Concurrent Leave Issues, Hours to be Paid During Leaves, and Regular Rates of Pay Applicable...

---

### **COVID-19 Washington Update: April 22, 2020**

#### **Kelley Drye & Warren LLP**

Today's federal government actions in response to the COVID-19 pandemic include: Congress Tomorrow, the U.S. House of Representatives is scheduled to...

---

### **Finding Fevers: Considerations Before Using Temperature-Detecting Cameras**

#### **Kelley Drye & Warren LLP**

Last week, the FDA approved the use of telethermographic systems (essentially, heat-sensitive cameras) to detect human temperature during the COVID-19...

---

### **10 Practical Tips for Employers to Safeguard Their Trade Secrets During COVID-19**

#### **Holland & Knight LLP**

As a result of both mandatory government restrictions and voluntary safety measures to combat the spread of coronavirus (COVID-19), many companies...

---

### **Los Angeles City Council to Require Businesses to Rehire Former Employees**

#### **Proskauer Rose LLP**

Employers who have laid off workers due to COVID-19 may soon be required to rehire the laid off workers before they can hire any new employees...

---

### **NLRB: Contract Coverage Standard Is No Defense to Unilateral Change Unless CBA 'Explicitly' Says So**

#### **Jackson Lewis PC**

Provisions in an expired collective-bargaining agreement (CBA) do not cover post-expiration unilateral changes under the National Labor Relations Act...

---

### **Putting An ENDS To It: How To Address Vaping In The Workplace**

#### **Fisher Phillips**

A few months ago, the United States Center for Disease Control (CDC) had linked 2,807 hospitalizations and 68 deaths to e-cigarette vaping associated...



---

## **EEOC Publishes Further Guidance for COVID-19 Pandemic Preparedness in Workplace**

### **Holland & Knight LLP**

The U.S. Equal Employment Opportunity Commission (EEOC) previously published pandemic guidance originally issued during the H1N1 influenza pandemic in...

---

## **Rolling Reopening: Planning for Employment-Related Issues**

### **Davis Wright Tremaine LLP**

As we approach May 2020, many federal, state, and local slow-the-spread guidelines and stay-home orders are set to expire. Although some...

---

## **Update on Federal Agency Activity - EEOC, NLRB, OSHA, and DOL - Amidst the COVID-19 Crisis (US)**

### **Squire Patton Boggs**

The COVID-19 pandemic has had a major impact on all aspects of life for all Americans and we are all still adjusting to this new "normal," which is...

---

## **CARES Act: Business Tax Provisions for Tribal-Owned Businesses**

### **Quarles & Brady LLP**

The Coronavirus Aid, Relief and Economic Security Act (CARES Act) grants many significant tax benefits to help tribal businesses stay afloat and...

---

## **DOL Issues More FFCRA Compliance Guidance on Paid Leaves**

### **Dykema Gossett PLLC**

Guidance Focuses on Concurrent Leave Issues, Hours to be Paid During Leaves, and Regular Rates of Pay Applicable Now that covered employers are...

---

## **Organ Procurement Coordinator Found Exempt Under FLSA Highly Compensated Exemption: A Case Study in the HCE**

### **Fox Rothschild LLP**

I have found a very interesting exemption case involving a rather unique job title that also is very instructive in the interpretation of the Highly...

---

## **Un-PAUSE New York: What Empire State Employers Need to Know About Reopening the Workplace**

New York

### **Ogletree Deakins**

On April 13, 2020, New York Governor Andrew Cuomo, New Jersey Governor Phil Murphy, Connecticut Governor Ned Lamont, Pennsylvania Governor Tom Wolf...

---

## **Keep a Lid on It - The Trump NLRB Reaffirms Employer Ability to Enforce Investigative Confidentiality Rules**

### **Sheppard Mullin Richter & Hampton LLP**

In Apogee Retail, 368 NLRB No. 144 (2019), the NLRB overruled the Obama Board's decision in Banner Estrella Medical Center, 362 NLRB 1108 (2015)

and...

---

**Fifth Circuit examines the job duties required for the highly-compensated employee exemption from overtime pay under the FLSA**

**Reed Smith LLP**

The Fair Labor Standards Act (FLSA) exempts certain highly-compensated employees (HCEs) from the requirement that they receive overtime pay for hours...

---

**COVID-19 Washington Update: April 22, 2020**

**Kelley Drye & Warren LLP**

Today's federal government actions in response to the COVID-19 pandemic include: Congress Tomorrow, the U.S. House of Representatives is scheduled to...

---

**Essential Information for Employers on Alabama's Unemployment Benefits and COVID-19**

**Ogletree Deakins**

The coronavirus pandemic has resulted in critical changes to workforces across the United States. In the state of Alabama, there have been more than...

---

**OFCCP Remains Active - New Scheduling Letters and Agency Directives Will Impact Audits**

**Crowell & Moring LLP**

Despite the coronavirus pandemic, the Office of Federal Contract Compliance Programs (OFCCP or "the Agency") remains busy, and there are several...

---

**4-Step Plan For Handling Confirmed COVID-19 Cases When Your Business Reopens**

**Fisher Phillips**

Businesses will soon reopen, presenting employers with new challenges as part of the next phase of the COVID-19 pandemic. With no known vaccine or...

---

**DOL issues new guidance on Families First Coronavirus Response Act (FFCRA)**

**Reed Smith LLP**

Earlier this month, the US Department of Labor (DOL) promulgated regulations to implement the recently enacted Emergency Paid Sick Leave Act (EPSLA)...

---

**OSHA State Plan Agencies Issue COVID-19 Guidance**

**Squire Patton Boggs**

Over the past several months, the federal Occupational Safety and Health Administration (OSHA) has steadily issued guidance to both employers and...

---

**Operating in the Ordinary Course in Extraordinary Circumstances** Delaware

**Weil Gotshal & Manges LLP**

As the COVID-19 pandemic continues to disrupt markets and shake the global economy, the full impact on private equity transactions remains unknown...



---

**EEOC Clarifies Today That Employers May Test Employees For COVID-19****Crowell & Moring LLP**

The EEOC today updated its online guidance regarding COVID-19 and the Americans with Disabilities Act (the ADA), stating that employers may now test...

---

**US: IRS, DOL and Treasury Issue Joint News Release****Baker McKenzie**

On Friday, March 20, 2020, the Internal Revenue Service (IRS), US Department of Labor (DOL), and US Department of the Treasury published a joint news...

---

**COVID-19 Emergency Paid Sick Leave Has Come to Bay Area****Davis Wright Tremaine LLP**

On April 17, 2020, San Francisco implemented an emergency ordinance requiring businesses with 500 or more employees to provide an additional two...

---

**Federal Reserve Releases Details of Main Street Lending Program****Troutman Sanders LLP**

On April 9, the Federal Reserve Board released term sheets for its widely anticipated Main Street Lending Program to ensure credit flows to small and...

---

**South Florida Business & Wealth, "How to Get Employer Tax Credits for Paid Sick Leave, Family Leave"****Berger Singerman LLP**

The Families First Coronavirus Response Act imposes a mandate on all private employers with fewer than 500 employees (subject to some exceptions...

---

**Client Alert: "Necessity is the Mother of Invention" - Checklist of Issues to Consider Before Reopening After COVID-19****Brouse McDowell**

We have witnessed remarkable changes in our everyday lives during the COVID-19 pandemic. Manufacturing businesses are modifying production lines...

---

**Federal Antitrust Authorities Issue Warning Against Employer Collusion to Disadvantage Essential Service Workers****Faegre Drinker Biddle & Reath LLP**

On April 13, 2020, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) (collectively, the Agencies) issued their Joint Antitrust...

---

**Beltway Buzz, April 24, 2020****Ogletree Deakins**

Despite our elected officials being out of town, there was a lot of action coming out of Congress this week...

---

**Former EEOC Attorney and Assistant U.S. Attorney Suntrease Williams-Maynard Joins Adams and Reese's Government Investigations and White Collar Defense Practice**

### **Adams and Reese LLP**

MOBILE, Ala. — Adams and Reese is pleased to announce Sontrease Williams-Maynard has joined the firm's Mobile office as Special Counsel...

---

### **Employers can test for coronavirus, EEOC says**

#### **Constangy Brooks Smith & Prophete LLP**

The Equal Employment Opportunity Commission updated its guidance on COVID-19 yesterday to say that employers could test employees fo...

---

### **COVID-19 and Returning to Work: For Employers, It's Not Too Soon to Plan a Comeback**

#### **Kelley Drye & Warren LLP**

Although the U.S. is still in the thick of the COVID-19 crisis, this is exactly when employers who are deemed "non-essential" should be developing a...

---

### **SEC Announces Largest Whistleblower Award of 2020 - Over \$27 Million**

#### **Jackson Lewis PC**

The Securities and Exchange Commission (the "SEC") announced a whistleblower award of more than \$27 million, representing the largest SEC...

---

### **Preparing for the health, legal risks when reopening your business**

#### **Adams and Reese LLP**

How is your business preparing to reopen? Adams and Reese attorney Greg Rouchell, a partner and Labor & Employment Team Leader, says in New Orleans...

---

### **What Do Eased Restrictions of Michigan's Reaffirmed Stay-At-Home Measures Mean for Your Business?**

#### **Dykema Gossett PLLC**

On April 24, 2020, Governor Whitmer reaffirmed the stay-at-home measures set forth in Executive Order 2020-42, amended the scope of that order, and...

---

### **Recent Court Case Highlights Limitations Of An "Unlimited" Vacation Policy In California**

California

#### **Fisher Phillips**

A California state court just created a controversy for those employers in the state that provide unlimited vacation policies for their exempt...

---

### **Show Me the Masks: Supplying Face Coverings and Respirators to Essential Employees**

#### **Morgan Lewis**

Employers are facing issues relating to shortages of respirators and non-surgical face coverings. The ever-evolving local, state, and federal...

---

### **OSHA's Interim Response Plan for Coronavirus Disease 2019 (COVID-19) May Have Been Issued to Guide Agency Action, but It is Just as Useful for Employers**

#### **Squire Patton Boggs**



Since the COVID-19 pandemic first hit the United States in early 2020, the US Occupational Safety and Health Administration (OSHA) has been issuing...

---

### **Immunize Your Organization Against Common HR Claims: Projects to Consider While Sheltering in Place**

**Hopkins & Carley**

In the wake of the shelter-in-place orders issued by many state and local governments, business is anything but normal for most organizations. Human...

---

### **Executive Order Relaxes Employer's Ability to Qualify for Work Share Program and Clarifies Expansions of Unemployment Benefits**

**Miller Canfield PLC**

On Thursday, April 23, 2020, Governor Whitmer issued Executive Order 2020-57. This Executive Order continues the temporary expansion of unemployment...

---

### **Navigating Employer Obligations to Provide Employees with Masks, Face Coverings**

**Jackson Lewis PC**

As the Centers for Disease Control and Prevention (CDC) continues to study COVID-19, the agency is regularly updating guidance on precautionary...

---

### **Back to Work: Practical Considerations from the U.S. Federal Reopening Guidelines**

**Bryan Cave Leighton Paisner LLP**

On April 16, the White House and the CDC released guidelines for a phased reopening of the U.S. economy. Most states and localities have been under...

---

### **Are You Ready to Reopen? Legal and Practical Issues to Consider**

**Ford & Harrison LLP**

There is mounting pressure to reopen businesses as many, particularly small ones, are struggling to survive under various stay-at-home and...

---

### **OSHA Guidance Marks Dramatic Shift in Enforcement Focus Amid COVID-19 Pandemic**

**Morgan Lewis**

The Occupational Safety and Health Administration has issued a new guidance allowing field offices flexibility in handling COVID-19-related matters...

---

### **Newsom's Executive Order Focuses On Protections for Food Service Workers**

**Fox Rothschild LLP**

It shouldn't surprise anyone that a massive component of California's economy is and has been agriculture and food service, including farming...

---

### **To Provide an N95 Mask or Not to...That is the Question Plaguing Some Employers (US)**

**Squire Patton Boggs**

One of the biggest questions plaguing employers during the COVID-19 pandemic

is whether or not to provide employees with respirators—the holy grail of...

---

### **Teamsters Union Lost Most Members in 20 Years in 2019**

#### **Jackson Lewis PC**

According to an analysis by Bloomberg Law Daily Labor Report, the Teamsters Union lost almost 65,000 members in 2019, the largest decline in the...

---

### **OSHA Issues COVID-19 Guidelines for the Construction Workforce**

#### **Smith Currie & Hancock**

During the course of COVID-19, the CDC and other government entities have provided workplace guidelines in an attempt to flatten the curve and reduce...

---

### **As America Prepares to Return to Work, EEOC Approves Testing Employees for COVID-19**

#### **Sheppard Mullin Richter & Hampton LLP**

The U.S. Equal Employment Opportunity Commission (EEOC) updated its guidance concerning COVID-19, affirming an employer's ability to medically test...

---

### **Client Alert: EEOC Releases "What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws"**

#### **Bowditch & Dewey LLP**

The U.S. Equal Employment Opportunity Commission (EEOC) has recently released Q&A guidance titled "What You Should Know About COVID-19 and the ADA...

---

### **Unemployment alphabet soup: Here's what it means**

#### **Constangy Brooks Smith & Prophete LLP**

The federal CARES Act has some very important provisions related to unemployment benefits for people who have lost their jobs, been fur...

---

### **Workforce Planning During COVID-19**

#### **Fox Rothschild LLP**

In the midst of the COVID-19 pandemic, employers face monumental decisions on how to keep their businesses alive. Given the uncertain duration of...

---

### **Integrity Tests: To Test Or Not To Test, That Is The Hiring Question**

#### **Fisher Phillips**

Employers often use tests and other selection procedures to screen applicants for hire and employees for promotion. There are many different types...

---

### **Surging Unemployment Claims Pose New Challenges to Employers - Are You Ready?**

#### **Foster Garvey**

Employers: Brace for unemployment benefit inquiries, watch for legal pitfalls, and consider federal relief programs in managing payroll and position...

---



### **Is This an "Emergency"?**

**Breazeale Sachse & Wilson LLP**

Many businesses have been in an “all hands on deck” mode for several weeks now, with no real end in sight. Employees are being asked to do whatever...

---

### **OSHA’s Interim Response Plan for COVID-19 May Have Been Issued to Guide Agency Action, but It is Just as Useful for Employers (US)**

**Squire Patton Boggs**

From our colleagues at the FrESH Law Blog comes a post analyzing the US Occupational Safety and Health Administration’s (OSHA) recent Interim...

---

### **Supreme Court to Consider Scope of CFAA**

**Akin Gump Strauss Hauer & Feld LLP**

Key Points The U.S. Supreme Court will review whether a person who is authorized to access information on a computer for certain purposes violates the...

---

### **NLRB Rejects Hospital’s Bid to Stay Representation Election based on COVID-19 Pandemic**

**Jackson Lewis PC**

In an unpublished decision, the National Labor Relations Board (NLRB) has denied an acute-care hospital’s request to stay a representation election...

---

### **Warming Up to Employee Temperature Checks: Employer Guidance From the EEOC and NYC**

New York

**Fox Rothschild LLP**

Although many New York businesses are temporarily closed due to the COVID-19 pandemic and the state’s stay-at-home orders, employers that remain open...

---

### **Restrictive Covenants in the Time of Coronavirus**

**Ogletree Deakins**

The spread of the coronavirus disease 2019 (COVID-19) has led to changes regarding many legal issues. Despite the changes, companies still need to...

---

### **EEOC Confirms Employer-Mandated COVID-19 Testing Does Not Violate the ADA**

**Hunton Andrews Kurth LLP**

On April 23, 2020, the EEOC updated its Technical Assistance Questions and Answers, “What You Should Know About COVID-19 and the ADA, the...

---

### **DOJ and FTC Warn Employers Against COVID-19-Related Business Collusion**

**Ogletree Deakins**

The United States Department of Justice’s (DOJ) Antitrust Division and the Federal Trade Commission (FTC) warned employers in a joint statement...

---

### **The COVID-19 pandemic may spur union organizing and complicate union relations: Part Two**

**Constangy Brooks Smith & Prophete LLP**



The Coronavirus pandemic has shuttered much economic activity and forced employers to make business decisions in response to a rapidly shifting legal...

---

### **What is the Impact of President Trump's Temporary Immigration Suspension?**

#### **Holland & Hart LLP**

In light of the impact of COVID-19 on the U.S. labor market, on Monday President Trump tweeted "I will be issuing a temporary suspension of..."

---

### **Musicians Reach Deal on AB5 Exemption**

#### **Fox Rothschild LLP**

California's music industry finally came to an agreement with lawmakers on pending amendments to California's Assembly Bill 5 (AB5). The amendments...

---

### **COVID-19: CARES Act Employer Payroll Retention Tax Credit**

#### **K&L Gates**

The recently passed Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") provides a tax credit for eligible employers to encourage...

---

### **Maintaining Trade Secrets Amid the COVID-19 Pandemic**

#### **Dickinson Wright**

Over the last few months, the widespread transmission of the coronavirus disease of 2019 (COVID-19 or the "coronavirus") has prompted immediate...

---

### **COVID-19 Washington Update: April 23, 2020**

#### **Kelley Drye & Warren LLP**

Today's federal government actions in response to COVID-19, includes House passage of the Paycheck Protection Program and Health Care Enhancement Act...

---

### **What Employers Should Do to Prepare their Workplaces per OSHA's COVID-19 Compliance**

#### **Haynsworth Sinkler Boyd PA**

The Occupational Safety and Health Administration (OSHA) issued numerous directives in March and April 2020 related to COVID-19...

---

### **USDOL Issues Updated FFCRA FAQs**

#### **Davis Wright Tremaine LLP**

The United States Department of Labor (USDOL) recently issued further clarification around several technical aspects of the Families First...

---

### **Update: Federal COVID-19 Relief Efforts Impact Higher Education Institutions**

#### **Vorys Sater Seymour and Pease LLP**

Our team continues to track legal developments related to the COVID-19 pandemic, specifically as they relate to colleges and universities. As you know...

---

### **Early Lawsuit Based on Violations of the FFCRA Asserts Claims Against Employer, Human Resources Consultant and CEO Individually**

### **Hall Render Killian Heath & Lyman PC**

On April 16, 2020, just weeks after the Family First Coronavirus Response Act ("FFCRA") became law on March 18, 2020, a single mother sued her...

---

### **COVID-19: What Will Our Workplaces Look Like When the Economy Reopens?**

#### **Freeborn & Peters**

"Germany Plans to Start Reopening Economy." The April 16, 2020 edition of the Wall Street Journal used this headline to introduce an article about the...

---

### **Chicago City Council Introduces COVID-19 Anti-Retaliation Ordinance, Reflecting Growing Trend**

#### **Proskauer Rose LLP**

On April 22, 2020, Chicago Mayor Lori Lightfoot, with the backing of several Aldermen, introduced the COVID-19 Anti-Retaliation Ordinance (the...

---

### **New Deadlines for Retirement Plans, Tax Filings and Paid Leave Policies**

#### **Dickinson Wright**

The Coronavirus Aid, Relief and Economic Security Act ("CARES"), and IRS and Department of Labor ("DOL") rules establish new and revised deadlines...

---

### **State COVID-19 Orders Regulating Worker Safety—Are They Preempted?** New

York

#### **Ogletree Deakins**

Almost every state has issued closure orders designating certain businesses as "essential" and allowing them to continue to operate during the...

---

### **Updated EEOC COVID-19-Related Workplace Guidance: COVID-19 Testing**

#### **Wilson Elser**

On April 23, 2020, the EEOC issued an update to its technical assistance guidance, "What You Should Know About COVID-19 and the ADA, the...

---

### **New York Relaxes Layoff Notification Requirements for Some Employers Due to COVID-19** New York

#### **Day Pitney LLP**

On April 17, New York Governor Andrew Cuomo signed Executive Order No. 202.19, which eases the notification requirements under New York's Worker...

---

### **U.S. Supreme Court Will Finally Weigh In on Scope of Computer Fraud and Abuse Act**

#### **Jackson Lewis PC**

The U.S. Supreme Court has agreed to decide whether it is a violation of the Computer Fraud and Abuse Act (CFAA) when an individual who is authorized...

---

### **Families First Coronavirus Response Act - Health emergency leave and exempted health care providers**

#### **DLA Piper**

The Secretary of Labor recently promulgated temporary regulations (the



“Regulations”) in connection with the Families First Coronavirus Response Act...

---

### **Back to Work: Georgia's - Reopening Executive Order: Risks and Guidance for Businesses**

**Bryan Cave Leighton Paisner LLP**

On April 20, 2020, Governor Brian Kemp signed an Executive Order which initiates the process of reopening businesses within the State of Georgia on...

---

### **FMCSA Extends Emergency Declaration to May 15 in Response to COVID-19, Direct Assistance Needs**

**Holland & Knight LLP**

The Federal Motor Carrier Safety Administration (FMCSA) has expanded and extended its Emergency Declaration through May 15, 2020, or until the...

---

### **Employer's After-the-Fact Discovery of Lack of Job Qualification Sinks Employee's ADA Discrimination Claim (US)**

**Squire Patton Boggs**

Sunny Anthony worked for TRAX International as a technical writer. During the course of her employment, she asked TRAX to accommodate her...

---

### **Protecting Your Company from Coronavirus-related Premises Liability Claims**

**Haynes and Boone LLP**

Businesses preparing to reopen amid the coronavirus pandemic and the essential businesses that have remained open through the pandemic should make a...

---

### **Michigan Employers Now Have More Flexibility To Implement Work Share Plans**

**Fisher Phillips**

Governor Whitmer recently expanded unemployment benefits, most notably for access to the Work-Share Program, by issuing Executive Order 2020-57. The...

---

### **What Employers Need to Know about OSHA's Reporting Requirements and Enforcement Guidance for COVID-19 Inspections**

**Haynsworth Sinkler Boyd PA**

The Occupational Safety and Health Administration (OSHA) issued Enforcement Guidance outlining Employer's reporting responsibilities related to...

---

### **EEOC Permits Employers to Test for COVID-19**

**Frankfurt Kurnit Klein & Selz PC**

This week, as parts of the nation began returning to work, the EEOC responded to an increasingly urgent question: May employers test employees for...

---

### **Commercial Litigation in the Cannabis Space: Resolving Disputes Like Every Other Industry Does**

**Duane Morris LLP**

As a commercial litigator who has handled a broad range of claims in highly regulated industries over the past 20 years — particularly in complex...

---

## **New York Enacts Permanent Paid Sick Leave Legislation**

New York

### **Duane Morris LLP**

Employees are to accrue one hour of sick leave for every 30 hours worked, beginning September 30, 2020...

---

## **Fifth Circuit Reverses Course, Concludes That “Day Rate” Pay Method Fails to Satisfy FLSA’s “Salary Basis” Test for Overtime Exemptions**

### **Jackson Lewis PC**

Upon further reflection, a panel of the U.S. Court of Appeals for the Fifth Circuit has determined that paying an employee a set amount for each day...

---

## **EEOC Says “Yes” to Return to Work COVID-19 Testing**

### **Kelley Drye & Warren LLP**

With the reopening of state economies and return-to-work on the horizon, on April 23, 2020, the EEOC issued new guidance on workplace testing for...

---

## **Yes, We Think We’re Open... Getting your Employees Back to Work During and After the COVID-19 Pandemic (Part I)**

### **Bradley Arant Boult Cummings LLP**

One of the hardest things about the COVID-19 crisis is that nobody is sure about when things will open back up and life can go back to “normal.” If...

---

## **Employers, Take Note: Virginia Enacts Broad Protections for Private-Sector Whistleblowers**

### **Ogletree Deakins**

In our previous article—What Virginia Employers Might Have Missed While Managing COVID-19: The Silent Labor and Employment Law Revolution—we detailed...

---

## **EEOC Opines on COVID-19 Testing by Employers**

### **Jackson Lewis PC**

In the past few weeks, the EEOC has updated its What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws on...

---

## **Federal and State Protections for Nonprofits Navigating the COVID-19 Pandemic**

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

The COVID-19 pandemic creates a unique set of circumstances for nonprofits. Many of them are facing similar challenges to for-profit businesses — how...

---

## **SCOTUS to Hear CFAA Case**

### **Jackson Lewis PC**

It’s not often that a case in our practice area reaches the Supreme Court of the United States, so we are genuinely excited! In *Van Buren v. United...*

---

## **Updated EEOC COVID-19-Related Workplace Guidance**

### **Wilson Elser**

On April 17, 2020, the EEOC issued updates to its recently revised technical



assistance guidance to address questions arising under the federal Equal...

---

### **EEOC Says Employers Can Require COVID-19 Testing**

**Lane Powell PC**

The EEOC has issued welcome guidance for employers who are seeking to take all steps necessary to eradicate the virus from their facilities. This...

---

### **What Employers Should Know About Bringing Employees Back into the Workplace.**

**McBrayer McGinnis Leslie & Kirkland PLLC**

By now, all businesses in the Commonwealth of Kentucky have experienced at least five weeks of interrupted operations. Some businesses have faced a...

---

### **Court Halts Enforcement of Illinois's New Workers' Compensation Rule That Presumes COVID-19 Infections Are Work-Related**

**Ogletree Deakins**

On April 13, 2020, the Illinois Workers' Compensation Commission established an emergency rule amending the Illinois Administrative Code for workers'...

---

### **COVID-19 OSHA Follow-Up: Agency Updates and Additional Recommended Employer Practices**

**Holland & Knight LLP**

The fast-moving developments in response to the novel coronavirus (COVID-19) require employers to remain diligent with following published federal...

---

### **Summary of CISA Guidance on Essential Critical Infrastructure Workforce 3.0**

**Spencer Fane LLP**

On April 17, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released version 3.0 of its guidance to help state and local...

---

### **Is a Global Pandemic a De Minimis Hardship? EEOC Guidance on COVID-19 and Religious Accommodation**

**Ogletree Deakins**

As government officials at all levels continue issuing guidance on best practices for employers to help mitigate the spread of COVID-19, some...

---

### **U.S. COVID-19: As the FFCRA Goes Live, the DOL Continues to Publish Revised and New Guidance for Employers**

**Bryan Cave Leighton Paisner LLP**

Although the federal Department of Labor ("DOL") declared April 1 - 17 to be a temporary period of non-enforcement of the Families First Coronavirus...

---

### **COVID-19 Washington Update: April 27, 2020**

**Kelley Drye & Warren LLP**

Following is an update on COVID-19-related federal government actions since our last update. Congress remains in recess, with both chambers...

---



## **What Employers Should Know About Bringing Employees Back into the Workplace, Part II**

### **McBrayer McGinnis Leslie & Kirkland PLLC**

In our first set of guidance on reopening workplaces, we focused on basics of providing a safe working environment, compliance with ADA...

---

## **5 Steps Healthcare Employers Should Take To Address COVID-19 Anxiety And Complaints Over Working Conditions**

### **Fisher Phillips**

Across the country, pockets of healthcare workers are protesting working conditions that they claim are unsafe and expose them to greater risk of...

---

## **Employee Benefits as Payroll Costs under the Paycheck Protection Program**

### **Haynes and Boone LLP**

Businesses that received a loan under the Paycheck Protection Program ("PPP") are eligible for forgiveness of that loan if, among other things, the...

---

## **U.S. COVID-19: EEOC Updates COVID-19 Guidance, Permitting Employers To Administer COVID-19 Tests and Clarifying Accommodation Obligations**

### **Bryan Cave Leighton Paisner LLP**

The U.S. Equal Employment Opportunity Commission ("EEOC") recently issued new guidance to employers regarding the COVID-19 pandemic. Notably, and in...

---

## **NLRB: Employer Right to Take Unilateral Action Under a Collective-Bargaining Agreement Does Not Survive the Expiration of the Agreement Absent Explicit Language to the Contrary**

### **Hunton Andrews Kurth LLP**

In a recent decision of first impression, the NLRB held that its contract coverage doctrine does not apply to changes to the terms and conditions of...

---

## **Business Roundtable Releases Roadmap for Resumption of Economic Activity**

### **Paul Weiss**

The coronavirus pandemic has forced the business community to implement and abide by unprecedented restrictions in an effort to maintain their...

---

## **Return-to-Work Checklist for Employers Reopening Their Businesses**

### **Dinsmore & Shohl LLP**

In anticipation of federal and state restrictions lifting as COVID-19 cases and deaths decrease, employers should start planning their employees'...

---

## **[UPDATED] Coronavirus: Federal and state governments work quickly to enable remote online notarization and SBA PPP loans to meet global crisis**

[Georgia](#)

[Maryland](#)

[Pennsylvania](#)

[Florida](#)

### **DLA Piper**

As more businesses are forced to work remotely due to the coronavirus disease 2019 (COVID-19) crisis, several federal and state governments are...

---

## **Benefits Briefs in the Time of COVID-19, Part 1: Federal Agencies Relax Summary of Benefits and Coverage ("SBC") Disclosure Deadlines**

### **Dickinson Wright**

Recent guidance from the Department of Labor ("DOL"), Health and Human Services ("HHS") and Treasury (the "Departments") provides limited enforcement...

---

## **U.S. Supreme Court Will Finally Weigh in on Scope of CFAA**

### **Jackson Lewis PC**

The United States Supreme Court recently granted a petition for certiorari in Van Buren v. United States addressing the issue of whether it is a...

---

## **Plan Now for Bringing Back Your Work Force**

### **Pierce Atwood LLP**

As hard as it may be at times to believe this, the day will soon...

---

## **San Francisco's COVID-19 Paid Sick Leave Ordinance Takes Effect**

### **Duane Morris LLP**

On April 17, 2020, Mayor Breed signed an amended version of the Public Health Emergency Leave ordinance...

---

## **EEOC Guidance Permits Employers to Test Employees for COVID-19**

### **Dinsmore & Shohl LLP**

On April 23, 2020, the Equal Employment Opportunity Commission (EEOC) released new guidance that permits employers to test employees for COVID-19. In...

---

## **Workers' Compensation Claims During the Pandemic and Mitigating the Risk**

### **Sheppard Mullin Richter & Hampton LLP**

While essential workers continue to make their way into the office amid the pandemic, many other Californians have been ordered to shelter in place...

---

## **Practically Speaking: A Series of Practical Tips for Employers in Navigating COVID-19**

### **Krieg DeVault**

No matter the line of business, every employer has been impacted by the Coronavirus of...

---

## **What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws**

### **Payne & Fears LLP**

The EEOC recently updated its guidance, What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws, including...

---

## **Connecticut Updates Safe Workplace Rules for Essential Employers and COVID-19**

### **Day Pitney LLP**



On April 24, the Connecticut Department of Economic and Community Development (DECD) updated its Safe Workplace Rules for Essential Employers. The...

---

### **Construction Industry at Core of Post-COVID-19 Debates**

Pennsylvania

**Duane Morris LLP**

Who is in the best position to sustain the loss? And what outcome is in the overall best interests of industry, economy and the public at-large...

---

### **Rocky Mountain Region COVID-19 Employment Update (CO, ID, MT, NE, NM, UT, WY) (April 28, 2020)**

**Gordon Rees Scully Mansukhani**

The Rocky Mountain Region COVID-19 Employment Update provides information about COVID-19 orders in Colorado, Idaho, Montana, Nebraska, New Mexico...

---

### **Does The FLSA "Emergency" Exception Apply To You?**

**Breazeale Sachse & Wilson LLP**

Many businesses have been in an "all hands on deck" mode for several weeks now.. Employees are being asked to do whatever is necessary to keep our...

---

### **Feds Provide COVID-19 Guidance To Meat And Poultry Processing Employers**

**Fisher Phillips**

Two federal agencies just released guidance for the meat and poultry packing industry to address the unique challenges it faces in light of COVID-19...

---

### **CDC Adds New Symptoms for COVID-19 Screening - Employers Must Adjust Accordingly**

**Dinsmore & Shohl LLP**

On April 26, 2020, the U.S. Center for Disease Control and Prevention (CDC) updated its guidance to add six new symptoms of COVID-19. Based on this...

---

### **COVID-19 Washington Update: April 27, 2020**

**Kelley Drye & Warren LLP**

Following is an update on COVID-19-related federal government actions since our last update. Congress remains in recess, with both chambers...

---

### **COVID-19 and Business Operations/Reopening, Cybersecurity from Home, and SEC Whistleblower Activity**

**Bryan Cave Leighton Paisner LLP**

The devastating impact of the Coronavirus (COVID-19) needs no introduction. BCLP has consolidated all of its client alerts regarding Coronavirus...

---

### **The Virtues And Vices Of Voluntary Attendance Policies In The COVID-19 Era**

California

**Fisher Phillips**

The COVID-19 pandemic has forced employers to scramble to find novel responses to new workplace challenges, and one such innovation has been the...

---

**To Record or Not To Record, That is the Question: Questions and Answers Regarding U.S. Federal OSHA Recordkeeping and Reporting Requirements During the COVID-19 Crisis**

**Bryan Cave Leighton Paisner LLP**

The federal Occupational Safety and Health Act and its implementing regulations require employers to record certain work-related injuries and...

---

**Back to Business After COVID-19: Addressing Disability Accommodation Requests in New York** [New York](#)

**Fox Rothschild LLP**

Though the Equal Employment Opportunity Commission (EEOC) has yet to find that a COVID-19 diagnosis, in and of itself, would be considered a...

---

**Developing Leave Policies to Keep Up with the FFCRA**

**Krieg DeVault**

Many employers that did not previously have a sick time policy or a Family and Medical Leave Act (FMLA) policy are now having to address employee...

---

**Governmental Oversight and CARES Act Funds: Recent Treasury Department Guidance**

**Dinsmore & Shohl LLP**

After the nearly \$350 billion in funds allocated to the Paycheck Protection Program (PPP) under the CARES Act were depleted in mid-April, Congress...

---

**What Mine Operators Can Expect after the Pandemic: MSHA Will Soon Push Its Regulatory Agenda**

**Fisher Phillips**

As the country begins to reopen, many mine operators are contemplating next steps for their own operations. One certainty is that the Mine Safety and...

---

**Workplace Safety and COVID-19: OSHA's Interim Enforcement Guidance and What It Means for Employers**

**Krieg DeVault**

The Occupational Safety and Health Administration (OSHA) of the U.S. Department of Labor (DOL) works to enforce the federal Occupational Safety and...

---

**The DOL and the IRS Jointly Provide Relief from Certain Timeframes Applicable to Health and Welfare and Pension Plans**

**Haynes and Boone LLP**

On April 28, 2020, the IRS and DOL issued a Final Rule extending certain timeframes under ERISA and the Internal Revenue Code for group health...

---

**Nota Bene Episode 77: Labor, Employment, and Immigration in a Pandemic World with Kelly Hensley, Denise Giraudo, and Greg Berk** [Audio](#)

**Sheppard Mullin Richter & Hampton LLP**



Furloughs. Layoffs. Loss of work visas. The state of employment in the U.S. is in flux due to the coronavirus, and employers and employees are left to...

---

### **Los Angeles County Implements Supplemental Paid Sick For COVID-19 Purposes**

**Fisher Phillips**

The Los Angeles County Board of Supervisors just unanimously approved a Supplemental Paid Sick Leave designed to fill in the gaps between the...

---

### **EEOC Issues Guidelines on COVID-19 Testing of Employees**

**Cozen O'Connor**

On April 23, 2020, the U.S. Equal Employment Opportunity Commission (EEOC) published updates to the Frequently Asked Questions (FAQ) that it...

---

### **Defense Production Act: Order Directing Continued Operation of Meat and Poultry Processing Facilities for the National Defense**

**Mayer Brown**

By Executive Order ("EO") dated April 28, 2020, President Trump invoked the authority of the Defense Production Act ("DPA") to direct that meat and...

---

### **San Francisco Amends Public Health Emergency Leave Ordinance and Issues Implementation Guidance**

**Fox Rothschild LLP**

San Francisco has amended the Public Health Emergency Leave Ordinance (PHELO) it originally passed on April 7, 2020 (as discussed in this previous...

---

### **Fifth Circuit Holds Day Rates Do Not Satisfy the Salary Basis Test**

**Holland & Knight LLP**

The U.S. Court of Appeals for the Fifth Circuit on April 20, 2020, held that a "day rate," or flat amount paid for each day actually worked, does not...

---

### **EEOC Says "Yes" to Return to Work COVID-19 Testing**

**Kelley Drye & Warren LLP**

This article was written by Barbara E. Hoey & Alison Frimmel and originally posted to Kelley Drye's Labor Days Blog. With the reopening of state...

---

### **What to Expect from OSHA's COVID-19 Enforcement Efforts**

**Vinson & Elkins LLP**

On April 13, 2020, the Occupational Safety and Health Administration (OSHA) issued its latest COVID-19-related interim guidance, describing how it...

---

### **What Employers Should Know About Furloughs, Layoffs, and WARN Act Obligations in Light of COVID-19**

**Jackson Lewis PC**

Employers struggling with the challenges presented by the COVID-19 pandemic may be contemplating reductions in force or in hours. It is important...

---



## **Taking Temperatures During COVID-19: A Practical Toolkit**

### **Sheppard Mullin Richter & Hampton LLP**

As we move into the second quarter of 2020, governments around the country are analyzing how to best open up their economies. Part of this will...

---

## **COVID-19 Update: Moving Forward - Considerations for the Re-Opening of Physical Workplaces**

### **McCarthy Tétrault LLP**

Governments and businesses have now begun to turn their minds toward the re-opening of the economy and physical workplaces. This past week, for...

---

## **Reopening America - Employers Facing Paid Leave Issues Under the FFCRA**

### **Ford & Harrison LLP**

As the "Reopening of America" begins, many employers will be faced with implementing the paid leaves provided by the Families First Coronavirus...

---

## **What We Do in the Shadows: Vampires Disregard Wage and Hour Rules for Human Familiars**

### **Ford & Harrison LLP**

As our family continues to practice social distancing, we are always on the lookout for a new comedy series to take a bit of the bite out of this new...

---

## **COVID-19 Social Media Considerations for Employers with Employees Returning to Work**

### **Holland & Knight LLP**

Even those employers with the best social media policies can be placed in difficult positions when confronted with negative social media usage by...

---

## **COVID-19 Return to Work Policies - Are You Ready?**

### **Adams and Reese LLP**

Employers of non-essential workers are gearing up for office re-openings all over the country. Employers are anxious—and rightfully so—and...

---

## **Plan Ahead, Employers: NLRB Ordering Mail Ballot Elections Because of COVID-19 Pandemic**

### **Jackson Lewis PC**

Recent representation case decisions and directions of election by National Labor Relations Board (NLRB) Regional Directors strongly suggest that...

---

## **New York City Forms Response Team To Combat Asian-American Discrimination In Response To COVID-19**

New York

### **Fisher Phillips**

The New York City Commission on Human Rights (NYCCHR) recently announced the formation of a COVID-19 Response Team to handle allegations of...

---

## **States Create Presumptions for Essential Workers to Become Eligible for**

## **Workers' Compensation Benefits During Pandemic**

### **Ogletree Deakins**

A number of states have recently passed or proposed amendments to their workers' compensation statutes (or have issued other authority) to make it...

---

## **First Steps for Return-To-Work Planning**

### **Fox Rothschild LLP**

I have been speaking with many clients about the first steps for return-to-work planning. The Covid-19 shut-downs were so quick that there wasn't...

---

## **EEOC Offers Guidance To Employers Preparing To Reopen Their Workplaces**

### **Fisher Phillips**

The Equal Employment Opportunity Commission (EEOC) has provided additional guidance for employers restarting and ramping up their businesses. The...

---

## **Workplace Reopening Preparedness: Creating a Safe Office and Wellness Policy**

### **Nelson Mullins Riley & Scarborough LLP**

Federal, state, and local COVID-19 pandemic mitigation strategies have included both government shutdowns of all but essential businesses and "social...

---

## **Environment & Climate Change**



## **Environmental Groups Sue EPA Over Relaxation of Enforcement of Environmental Laws Due to COVID-19**

### **Goldberg Segalla LLP**

On April 16, 2020 a coalition of environmental groups commenced the action National Resources Defense Council, et al. V. U.S. EPA et al., No. 20-3058...

---

## **US EPA Issues New Guidance for Hazardous Waste Cleanup & Emergency Response Sites Impacted by COVID-19**

### **Squire Patton Boggs**

On April 10, 2020, US EPA issued updated interim guidance to regional offices for dealing with the "challenges posed by the COVID-19 situation." The...

---

## **USEPA Interim Guidance on Cleanup Sites During COVID-19 and Remediation in New Jersey**

### **Porzio Bromberg & Newman PC**

On April 10, 2020, the United States Environmental Protection Agency ("EPA") issued Interim Guidance to its regional offices to evaluate ongoing...

---

## **Environmental Due Diligence in Real Estate Transactions During the COVID-19 Crisis**

### **Miller Canfield PLC**

Real property transactions (purchases, leases and foreclosures) need not be put on hold due to...

---

## **County of Maui Decided: Groundwater Discharges Require Permit . . . Sometimes**





Hawaii

### **Davis Wright Tremaine LLP**

Today, in a 6-3 opinion, the U. S. Supreme Court decided one of the more closely followed environmental disputes of recent years. In *County of Maui v...*

---

### **Supreme Court Expands the Reach of Clean Water Act Permitting Authority**

#### **Jenner & Block LLP**

On April 23, 2020, the U.S. Supreme Court issued an important decision on the reach of the Clean Water Act ("CWA"). The Court's decision in *County of...*

---

### **SCOTUS: Clean Water Act Permits Required for Some Releases into Groundwater**

#### **Beveridge & Diamond PC**

The U.S. Supreme Court held today, in a much-anticipated ruling, that the Clean Water Act's (CWA) requirement to obtain a National Pollutant...

---

### **EPA Releases Second Set of Draft Scope Documents for Remaining High-Priority Substances**

#### **Bergeson & Campbell PC**

On April 17, 2020, the U.S. Environmental Protection Agency (EPA) released the draft scope documents for the remaining seven of the 20 chemicals...

---

### **In First Month of COVID-19 Guidance, the California Regional Water Quality Control Boards Have Issued Hundreds of Approvals for Compliance Extensions Submitted by Regulated Entities**

California

#### **Hunton Andrews Kurth LLP**

On March 20, the California Water Boards issued guidance about complying with regulatory requirements during the COVID-19 shelter-in-place orders. We...

---

### **Supreme Court Reverses EPA in Key CWA Groundwater Case**

#### **Stinson LLP**

Today the U.S. Supreme Court issued its long-awaited opinion in *County of Maui v. Hawaii Wildlife Fund*, regarding whether the discharge of pollutants...

---

### **EPA Holds Calls on Plan to Reduce Burden for Certain Stakeholders Subject to TSCA Fees Rule Requirements for EPA-Initiated Risk Evaluations**

#### **Bergeson & Campbell PC**

On April 16, 2020, the U.S. Environmental Protection Agency (EPA) hosted a call on its recently announced plan to reduce the burden for certain...

---

### **NJDEP Issues General Environmental Compliance and Enforcement Alert**

#### **Manko Gold Katcher & Fox**

On April 21, 2020, in an apparent move to distance itself from EPA's approach to enforcement and compliance during the COVID-19 outbreak (the EPA...

---

### **Industry Groups Request Assistance from White House in Response to Carbon Dioxide Shortage**

### **Keller and Heckman LLP**

In an April 7 letter to Vice President Mike Pence, groups including the Beer Institute, Brewers Association, National Pork Producers Council, North...

---

### **Lockdown Has Shown Us the Environmental Cost of Transport: Will We Now Do What's Necessary to Reduce the Bill?**

#### **Bryan Cave Leighton Paisner LLP**

It is perhaps curious to write something about the future of mass transit at a time when many of us might legitimately question whether mass transit...

---

### **United States Supreme Court Announces Functional Equivalent Test to Require Permits for Discharges to Groundwater (County of Maui v. Hawaii Wildlife Fund)**

#### **Kilpatrick Townsend & Stockton LLP**

The United States Supreme Court has expanded the authority of the United States Environmental Protection Agency (EPA) to regulate discharges to...

---

### **Environmental Audit Opportunities to Consider for Return-to-Work in the Wake of COVID-19**

#### **Bracewell LLP**

As regulated companies and facilities around the country consider their approaches to partially or even fully returning to the workplace - even...

---

### **COVID-19: Environmental Agency Responses to Virus Mitigation Measures**

#### **K&L Gates**

As COVID-19 mitigation efforts have taken effect across the country, environmental protection agencies are also adjusting operations and policies to...

---

### **Are Environmental Cleanups "Essential" Under Gov. Inslee's Shelter-in-Place Order?**

[Washington](#)

#### **Davis Wright Tremaine LLP**

Across Washington State, businesses and individuals are working hard to comply with Gov. Jay Inslee's "Stay Home, Stay Healthy" Order, issued as...

---

### **EPA Issues Revised Supplemental Finding for Mercury and Air Toxics Standards and Final Risk and Technology Review**

#### **Sidley Austin LLP**

On April 16, 2020, the U.S. Environmental Protection Agency (EPA) released a prepublication final rule (along with a fact sheet and memorandum)...

---

### **San Francisco Bay Area Counties Ban Reusable Bags Due to COVID-19**

#### **Keller and Heckman LLP**

San Francisco and several other Bay Area jurisdictions have temporally banned reusable bags as part of an updated shelter in place order. By way of...

---

### **EPA Postpones SACC Meeting on Asbestos**

#### **Bergeson & Campbell PC**

The U.S. Environmental Protection Agency (EPA) has postponed the Toxic



Substances Control Act (TSCA) Science Advisory Committee on Chemicals (SACC)...

---

**SCOTUS Muddies All The Waters**

**Womble Bond Dickinson (US) LLP**

In a decision which seems likely to inject yet more uncertainty into whether the introduction of pollutants to surface waters via groundwater...

---

**Supreme Court Adopts Multifactor, Functional-Equivalent Standard to Determine When the Clean Water Act Requires a Permit for Discharges from a Point Source**  
**Mayer Brown**

Today, the Supreme Court reined in the Ninth Circuit's broad standard requiring a permit under the Clean Water Act ("CWA") for all discharges to...

---

**US EPA and the Corps Finally Publish Their Definition of "Waters of the United States" Narrowing the Scope of Federal Jurisdiction Under the Clean Water Act**  
**Squire Patton Boggs**

On April 21, 2020, the United States Environmental Protection Agency (US EPA) and the United States Army Corps of Engineers (Corps) published, in the...

---

**US EPA and US DOT Issue Final Rule Rolling Back Vehicle Emissions Standard**  
**Squire Patton Boggs**

In the midst of the COVID-19 pandemic, US EPA and the US Department of Transportation (DOT) issued the final rule rolling back greenhouse gas (GHG)...

---

**Supreme Court Holds NPDES Permits Required for Discharges Through Groundwater**

**Taft Stettinius & Hollister LLP**

Today the U.S. Supreme Court issued a long awaited decision in County of Maui, Hawaii v. Hawaii Wildlife Fund, 590 U.S. (2020), holding that point...

---

**Environmental Group's Attempt to Compel PHMSA Action Dismissed**

Montana

**Troutman Sanders LLP**

A Montana federal district court recently dismissed a challenge by an environmental group seeking to compel the Pipeline and Hazardous Materials...

---

**U.S. Supreme Court: Indirect Discharge Into Groundwater Covered Under Clean Water Act**

**Vorys Sater Seymour and Pease LLP**

On April 23, 2020, the U.S. Supreme Court, in a 6-3 decision, held that a permit is required for either "a direct discharge of pollutants from a point..."

---

**Supreme Court Establishes Permitting Standard for Discharges to Groundwater**  
**Wilmer Cutler Pickering Hale and Dorr LLP**

On April 23, 2020, the Supreme Court ruled in County of Maui v. Hawaii Wildlife Fund that a federal permit is required under the Clean Water Act...

---



**County of Maui v. Hawai'i Wildlife Fund: Supreme Court Rejects Ninth Circuit's Expansive Test for NPDES Permitting Under Clean Water Act, Requires Direct Discharges to Navigable Waters or Functional Equivalent of a Direct Discharge**  
**Hunton Andrews Kurth LLP**

Yesterday the Supreme Court of the United States issued its most significant Clean Water Act decision in more than a decade, resolving a split among...

---

**Supreme Court Decides County of Maui v. Hawaii Wildlife Fund**  
**Faegre Drinker Biddle & Reath LLP**

On April 23, 2020, the U.S. Supreme Court decided County of Maui v. Hawaii Wildlife Fund, holding that the Clean Water Act requires a permit for a...

---

**Supreme Court Decides Atlantic Richfield Co. v. Christian** Montana  
**Faegre Drinker Biddle & Reath LLP**

On April 20, 2020, the U.S. Supreme Court decided Atlantic Richfield Co. v. Christian holding that CERCLA does not strip state courts of jurisdiction...

---

**Supreme Court Holds Clean Water Act Can Apply To Groundwater**  
**Monchamp Meldrum LLP**

In a 6-3 decision penned by Justice Breyer, the United States Supreme Court held on April 23 that discharges of pollutants to groundwater that reach...

---

**EPA Finalizes Removal of Water Quality Standards Despite Pending Washington Lawsuit**  
**Beveridge & Diamond PC**

In what may be the beginning of the final chapter of a long-running saga over water quality standards in Washington State (Washington), the U.S...

---

**There is No Full and Final Settlement Under CERCLA** Montana  
**Goldberg Segalla LLP**

The U.S. Supreme Court this week ruled in Atlantic Richfield Co. v. Christian that state law claims are still valid against landowners who have...

---

**Comments on Second Batch of Draft Scope Documents Due June 8**  
**Bergeson & Campbell PC**

The U.S. Environmental Protection Agency (EPA) published a Federal Register notice on April 23, 2020, announcing the availability of the draft scope...

---

**California Argues for State Law in Appeal of Roundup Case**  
**Clyde & Co LLP**

On March 23, 2020, the California attorney general's office asked the Court of Appeals for the Ninth Circuit to reject an appeal by Bayer AG to...

---

**EPA Issues COVID-19 Enforcement Discretion Policy**  
**Jones Day**

The Environmental Protection Agency ("EPA") announced that it will not penalize certain environmental violations that are the result of the...

---

## **Clean Water Act Permit Required for “Functional Equivalent” of Direct Discharge, Supreme Court Says**

### **Sheppard Mullin Richter & Hampton LLP**

The Clean Water Act sometimes requires a permit for the indirect discharge of pollutants from a point source to navigable waters, but only when the...

---

## **Governor Newsom Relaxes Key CEQA Notice and Consultation Requirements**

California

### **Nossaman LLP**

On March 23, 2020, Governor Newsom signed Executive Order N-54-20, suspending for 60 days public agency and project proponent procedures for posting...

---

## **Supreme Court Splits the Baby: A Multifactorial Balancing Test to Determine When Clean Water Act Permits Required for Discharges to Groundwater**

### **Sidley Austin LLP**

On April 23, the U.S. Supreme Court decided *County of Maui, Hawaii v. Hawaii Wildlife Fund*, likely the most important environmental case on this...

---

## **SCOTUS Establishes “Functional Equivalent” Test for Permitting Discharges to Groundwater**

### **Troutman Sanders LLP**

The U.S. Supreme Court issued its long-awaited opinion in *County of Maui v. Hawaii Wildlife Fund*, addressing whether the Clean Water Act (CWA)...

---

## **Earth Day 2020: Fashion Brands Continue Focus on Green Marketing**

### **Kelley Drye & Warren LLP**

To celebrate the 50th Anniversary of Earth Day this week, we look at the increasingly pressing topic of green marketing in the fashion industry...

---

## **Redefining Navigable Waters: The Next Frontier of the WOTUS Saga**

### **Nossaman LLP**

In the ongoing saga of the Clean Water Act’s so-called “Waters of the United States” or WOTUS rule, the U.S. Environmental Protection Agency (EPA)...

---

## **U.S. EPA’s COVID-19 Based Discretionary Civil Enforcement Policy and Guidance on Timing of Performing Field Work**

### **Sullivan & Worcester LLP**

The COVID-19 pandemic has disrupted many business and governmental activities, and environmental compliance is no exception. In recognition of the...

---

## **Supreme Court Again Muddies Clean Water Act Standards**

### **Paul Hastings LLP**

On Thursday, April, 23, 2020, the United States Supreme Court issued the term’s most anticipated environmental decision of year, ruling that the Clean...

---



## **NJDEP Confirms Policy Regarding Site Remediation and Issues an Alert Regarding Environmental Compliance and Enforcement**

### **Porzio Bromberg & Newman PC**

Last week, we reported that Executive Order 122, carved out environmental remediation at a site as essential construction that can continue as long...

---

## **Striking Middle Ground(water), the Supreme Court Holds That Some Discharges to Groundwater Require Clean Water Act Permits**

### **Brownstein Hyatt Farber Schreck LLP**

The U.S. Supreme Court issued on April 23, 2020, a significant and controversial Clean Water Act ("CWA") decision in *County of Maui v. Hawaii...*

---

## **Recognizing the Need Spurred by Climate Change and COVID-19, New Jersey Moves Forward on Offshore Wind Workforce Development**

New Jersey

### **McCarter & English LLP**

It is an ill wind that blows nobody any good. Offshore wind certainly doesn't fit in that category. In fact, it might be said that offshore wind...

---

## **EPA Provides Temporary Amendments for CEMs Quality Assurance Requirements During COVID-19 For Specified Part 75 Sources**

### **Nelson Mullins Riley & Scarborough LLP**

In the April 22, 2020 Federal Register, EPA posted an Interim Final Rule and requested comments on the Agency amending the emissions reporting...

---

## **Supreme Court Issues New "Functional Equivalent" Test for Clean Water Act Permitting Coverage of Discharges to Groundwater**

### **Troutman Sanders LLP**

Today the U.S. Supreme Court issued its long-awaited opinion in *County of Maui v. Hawaii Wildlife Fund*, addressing whether the Clean Water Act (CWA)...

---

## **County of Maui, Hawaii v. Hawaii Wildlife Fund**

### **Haynes and Boone LLP**

The U.S. Supreme Court creates a test for when discharges to groundwater trigger NPDES permitting requirement, but its failure to include a bright...

---

## **What You Need to Know About EPA Enforcement During COVID-19**

### **Bradley Arant Boult Cummings LLP**

The United States Environmental Protection Agency (EPA) has issued three guidance documents to address changes in enforcement of...

---

## **California Curbs Recycling Requirements in the Time of COVID-19**

California

### **Manatt Phelps & Phillips LLP**

Since California Governor Gavin Newsom issued his first Emergency Declaration in response to the COVID-19 pandemic on March 4, 2020, he has issued...

---

## **Governor Approves Online-only CEQA Notice During COVID-19**

California

### **Monchamp Meldrum LLP**

While uncertainty remains regarding the CEQA statute of limitations under the Judicial Council's April 6th Emergency Order (available here), the...

---

### **USEPA Warns E-Commerce Platforms to Scrub Fake Coronavirus Disinfectant Products**

#### **Jenner & Block LLP**

As discussed in a prior post on Corporate Environmental Lawyer, on January 29, 2020, the United States Environmental Protection Agency ("USEPA")...

---

### **One Week, Two Key Supreme Court Environmental Law Opinions**

Montana

#### **Manatt Phelps & Phillips LLP**

In the course of a week, the Supreme Court has ruled on fundamental issues for two foundational statutes of federal environmental law: the...

---

### **Supreme Court Rules that Clean Water Act Covers Groundwater Discharges**

#### **White & Case LLP**

The Supreme Court ruled on April 23, 2020 that federal law can require a permit for pollutant discharges that travel through groundwater to surface...

---

### **California Executive Order Suspends Certain CEQA Noticing and Posting Requirements**

California

#### **Holland & Knight LLP**

In response to COVID-19, on April 23, California Gov. Gavin Newsom issued Executive Order N-54-20, which, among other things, suspends for 60 days...

---

### **Supreme Court Clarifies Scope of Clean Water Act Permitting Requirements**

#### **Winston & Strawn LLP**

On April 23, 2019, the Supreme Court of the United States issued its highly anticipated decision in *County of Maui v. Hawaii Wildlife Fund*. The case...

---

### **The Primacy of Federal Authority at Superfund Sites After *ARCO v. Christian Ice Miller***

Earlier this week, the Supreme Court issued an important decision delineating the scope of federal and state authority at Superfund sites in Atlantic...

---

### **Supreme Court Establishes "Functional Equivalent" Standard for Permitting Discharges to Groundwater Under the Clean Water Act**

#### **Manko Gold Katcher & Fox**

Today, the Supreme Court altered Clean Water Act jurisprudence when it vacated and remanded a closely-watched Ninth Circuit decision which pertained...

---

### **EPA Proposes to Retain Particulate Matter Standards of Importance to Industries in Arid West**

#### **Holland & Hart LLP**

On April 14, 2020, the Environmental Protection Agency (EPA) proposed to retain the current National Ambient Air Quality Standards (NAAQS) for...

---



## **Supreme Court Creates New Standard for Clean Water Act Jurisdiction Over Discharges to Groundwater**

### **Frost Brown Todd LLC**

On April 23, 2020, the U.S. Supreme Court issued its much-anticipated ruling in *County of Maui v. Hawaii Wildlife Fund* addressing whether permits are...

---

## **Supreme Court expands reach of Clean Water Act to cover some discharges to groundwater**

### **Thompson Coburn LLP**

On April 23, 2020, the United States Supreme Court adopted a new flexible standard that expands the reach of the Clean Water Act (CWA). In a 6-3...

---

## **Environment Agency reassures operators in wake of COVID-19**

### **Bryan Cave Leighton Paisner LLP**

The Environment Agency is responding to the compliance difficulties that businesses face as a result of COVID-19 with some much needed reassurance as...

---

## **Environmental Compliance Enforcement in the Wake of COVID-19**

### **Baker & Hostetler LLP**

This client alert focuses on the circumstances that could lead to criminal investigation or enforcement for environmental noncompliance during...

---

## **SCOTUS Holds Common Law Claims Seeking Restoration Require EPA's Approval if CERCLA Remediation is Ongoing**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: Consider this hypothetical. Acme Company's historic operations has contaminated its property and those of its adjacent neighbors...

---

## **DEP Issues Guidance Regarding Compliance Challenges Arising from COVID-19**

New Jersey

### **Greenbaum, Rowe, Smith & Davis LLP**

On April 21, 2020, the New Jersey Department of Environmental Protection (DEP) issued two Environmental Compliance and Enforcement Alerts providing...

---

## **SAB to Review EPA Research on Large Scale Disinfection of COVID-19 Virus**

### **Bergeson & Campbell PC**

On April 20, 2020, the U.S. Environmental Protection Agency (EPA) announced that EPA Administrator Wheeler has requested that the Science Advisory...

---

## **U.S. Supreme Court Decides Two Important Environmental Cases**

### **Ice Miller LLP**

Last week, the U.S. Supreme Court issued important decisions in two high-profile environmental cases. Both addressed the balance between federal and...

---

## **EPA Tells Platforms to Get Illegal Disinfectants Off Their Sites**

### **Frankfurt Kurnit Klein & Selz PC**



In early April, I blogged about the EPA's efforts to fight scam marketers selling bogus disinfectant products. As detailed in EPA's earlier release...

---

### **U.S. Supreme Court Requires EPA Approval of State Law Remedy for Extra Cleanup at ARCO's Anaconda Smelter CERCLA Superfund Site** Montana

#### **K&L Gates**

In *Atlantic Richfield Co. v. Christian* (Atlantic Richfield),[1] the Supreme Court of the United States (Court) held that Montana landowners could sue...

---

### **CERCLA Does not Bar State-Court Litigation that May Impact an EPA-Approved Remediation** Montana

#### **Baker McKenzie**

This week the U.S. Supreme Court continued its plain language approach to interpreting CERCLA, allowing property owners' state law claims for...

---

### **Supreme Court Ruling Sets New Test for Clean Water Act Permitting**

#### **Bergeson & Campbell PC**

On April 23, 2020, the Supreme Court ruled that pollution traveling indirectly to rivers and streams through groundwater can be covered by the Clean...

---

### **Post-COVID-19 Environmental Compliance Checklist**

#### **Thompson Hine LLP**

This checklist is intended to assist a company in assessing its environmental compliance status after COVID-19 Federal and state limitations are...

---

### **Ripple Effects of Court Decision to Vacate Army Corps Nationwide Permit for Pipelines and Other Utility Line Projects**

#### **Baker McKenzie**

On April 15, the U.S. District Court for the District of Montana held that the Army Corps of Engineers failed to comply with the Endangered Species...

---

### **Digital CEQA: New Executive Order Creates An Alternative Path For Complying With CEQA Notice, Posting And Public Review Requirements** California

#### **Sheppard Mullin Richter & Hampton LLP**

On April 23, 2020, California Governor Gavin Newsom issued Executive Order N-54-20 (EO) which, in part, addresses an outstanding question related to...

---

### **San Francisco Bay Area Counties Ban Reusable Bags Due to COVID-19; California Suspends Plastic Bag Ban**

#### **Keller and Heckman LLP**

San Francisco and several other Bay Area jurisdictions have temporally banned reusable bags as part of an updated shelter in place order. By way of...

---

### **NRC Affirms Decision Allowing SLR Applicants to Rely on License Renewal GEIS**

#### **Morgan Lewis**

The US Nuclear Regulatory Commission (NRC) has issued an order, with the four-member Commission acting in its appellate capacity, holding that power...

---

## **US Supreme Court: Clean Water Act May Regulate Discharges to Groundwater** **Morgan Lewis**

In rejecting guidance from the US Environmental Protection Agency, the Supreme Court concluded that a discharge to groundwater that reaches navigable...

---

## **How Can the Oil and Gas Industry Prepare to Deal With the Impact of COVID-19?** **Squire Patton Boggs**

The price of crude oil, which was already hammered by market conditions, took a further hit in the wake of the COVID-19 outbreak, dropping to 18-year...

---

## **SCOTUS Delivers Two Important Environmental Rulings** **McCarter & English LLP**

Amidst the COVID-19 pandemic, the U.S. Supreme Court issued last week two important decisions, one regarding the federal Superfund law and the other...

---

## **Update: Corps Seeks Stay of Montana District Court's NWP 12 Ruling** Montana **Troutman Sanders LLP**

As we previously reported, the Federal District Court for Montana vacated the U.S. Army Corps of Engineers (Corps) Nationwide Permit (NWP) 12 on April...

---

## **We Finally Have the US Supreme Court Decision in Atlantic Richfield, But Who Really Won?** **Squire Patton Boggs**

On April 20, 2020, the US Supreme Court issued its much-anticipated decision in Atlantic Richfield Co. v. Gregory Christian. In short, the Court held...

---

## **U.S. EPA and Army Corps Publish Final WOTUS Rule** **Thompson Hine LLP**

On April 21, U.S. EPA and the U.S. Department of the Army (Army Corps) published the long-awaited final "waters of the United States" rule, which...

---

## **Lions, Tigers, and Trademarks: IP Lessons from "Tiger King"** **Gordon Rees Scully Mansukhani**

Netflix's recent docu-series "Tiger King" has quarantined Americans captivated&mdash;a reported 34 million viewers binged the series within the first...

---

## **The Nation Goes the Way Montana Goes? Nationwide Permit 12 Vacatur and Injunction** **K&L Gates**

On April 15, 2020, the Montana federal district court issued an Order in Northern Plains Resource Council v. U.S. Army Corps of Engineers, No...

---

## **EPA Relaxes Part 75 Continuous Emission Monitoring Rules During the COVID-19 Pandemic** **Winston & Strawn LLP**



On April 22, 2020, EPA published an interim rule granting temporary reprieve to regulated sources from the quality-assurance monitoring and reporting...

---

### **USEPA Issues Interim COVID-19 Guidance for Environmental Cleanup Site Field Work Decisions**

#### **Quarles & Brady LLP**

George J. Marek, Cynthia A. Faur, Jacqueline M. Vidmar, Lauren R. Harpke, Michael S. Mostow, Jeremy A. Lite Stay at home orders and public health...

---

### **Flexibility for Transactional and Regulatory Requirements in the Wake of COVID-19**

#### **Squire Patton Boggs**

In a little over a couple of months, the COVID-19 outbreak has dramatically altered the landscape of business. Companies are struggling to cope with...

---

### **SCOTUS Decision Provides Narrower Test for Discharges to Groundwater**

#### **Holland & Hart LLP**

On April 23, 2020, the U.S. Supreme Court in a 6-3 decision held that the Clean Water Act (CWA) requires a permit for either a direct discharge from a...

---

### **Members of House Committee on Oversight and Reform Request EPA Briefing on March 26, 2020 Memorandum**

#### **Sidley Austin LLP**

On April 22, 2020, members of the U.S. House Committee on Oversight and Reform (Committee) issued a letter to the Environmental Protection Agency...

---

### **Environmental Protection Agency Extends PFOA/PFOS Comment Deadline to June 10, 2020**

#### **Holland & Knight LLP**

On April 17, U.S. Environmental Protection Agency (EPA) Assistant Administrator for Water David Ross issued a notice indicating the comment period for...

---

### **Update: Corps Seeks Stay of Montana District Court's NWP 12 Ruling**

Montana

#### **Troutman Sanders LLP**

As we previously reported, the Federal District Court for Montana vacated the U.S. Army Corps of Engineers ("Corps") Nationwide Permit ("NWP 12") on...

---

### **Middle Ground, or Muddy Waters? SCOTUS Issues Vague Rule in Clean Water Act Decision**

#### **Nossaman LLP**

Last week, the U.S. Supreme Court issued a long-awaited decision in *County of Maui v. Hawaii Wildlife Fund et al.*, 590 U.S. \_\_\_\_ (2020), in which it...

---

### **EPA and CalEPA guidance on field activities during COVID-19 focuses on agency communication, deadlines and flexibility**

#### **DLA Piper**

On April 10, 2020, US EPA issued supplemental guidance to its regional

administrators offering a decision-making...

---

**Prop 65: Certainty in Uncertain Times** California

**Hunton Andrews Kurth LLP**

Uncertainty. Today nearly everything we thought we knew is uncertain. It's good, then, that at least one regulatory program in California remains...

---

**Supreme Court Holds Clean Water Act Does Regulate Some Point Source Discharges to Groundwater**

**Nelson Mullins Riley & Scarborough LLP**

In a decision delivered by Justice Breyer in the case of County of Maui, Hawaii v. Hawaii Wildlife Fund, et al. No. 18-260 ("County of Maui"), a six...

---

**Additional EPA Guidance and Developments During the COVID-19 Era**

**McGuireWoods LLP**

The U.S. Environmental Protection Agency has published various guidance documents after it issued its March 26, 2020, Policy Memorandum announcing...

---

**Muddied Ground water: New Supreme Court Test Adds Confusion and Uncertainty to Clean Water Act Permitting Jurisdiction**

**K&L Gates**

On April 23, 2020, the U.S. Supreme Court announced its much-awaited decision in County of Maui v. Hawai'i Wildlife Fund on whether the Clean Water...

---

**Murky Water Ahead: SCOTUS Rules Contaminant Discharges to Groundwater "May" or "May Not" Require NPDES Permit**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: Rather than providing clarity, the Supreme Court introduced substantial uncertainty into the NPDES permitting process involving...

---

**NJDEP Proposes Significant Changes to Remediation Standards for Cleanup of Contaminated Sites** New Jersey

**Riker Danzig Scherer Hyland & Perretti LLP**

On April 6th, the New Jersey Department of Environmental Protection ("NJDEP") proposed major revisions to the existing Remediation Standards codified...

---

**U.S. Supreme Court Addresses Permit Requirements for Groundwater Discharges Under the Clean Water Act**

**Nutter McClennen & Fish LLP**

Last week, the Supreme Court addressed a longstanding issue about whether pollutants discharged to groundwater but that eventually reach a navigable...

---

**Ninth Circuit Orders EPA to Rule on NRDC Petition to Cancel Pet Use Registration for Organophosphate Pesticide**

**Beveridge & Diamond PC**

A long-running dispute between the U.S. Environmental Protection Agency (EPA) and the Natural Resources Defense Council (NRDC) moved a step closer to...



---

## **Working with Environmental Agencies When Managing Business Impacts from COVID-19**

### **Stinson LLP**

Since the COVID-19 pandemic, federal, state and local agencies have adapted their procedures to both working remotely and allowing certain...

---

## **Supreme Court: Pollutants Reaching Navigable Waters Through Groundwater May Require Permit Under Clean Water Act**

### **Greenberg Traurig LLP**

Rejecting the Trump administration's novel 2019 interpretation that the Clean Water Act never requires permits for pollutant discharges to...

---

## **NJDEP Extends Certain Site Remediation Deadlines Due to COVID-19 Pandemic**

### **McCarter & English LLP**

The New Jersey Department of Environmental Protection (NJDEP) took steps on April 24, 2020, to suspend the application of certain New Jersey Site...

---

## **Gov. Newsom Suspends Some CEQA Requirements, Threatening the Ability of Certain Projects to Proceed**

California

### **Brownstein Hyatt Farber Schreck LLP**

As the coronavirus pandemic continues, Gov. Newsom issued an Executive Order to address challenges faced by lead agencies, responsible agencies, and...

---

## **CWA Alert: High Court Establishes New "Functional Equivalent" Test for Permitting Related to Groundwater Discharge**

### **Goldberg Segalla LLP**

Last week, the United States Supreme Court provided additional guidance regarding the application of the Clean Water Act. In short, the Clean Water...

---

## **Landowners Can Seek a Cleaner Cleanup in State Court**

Montana

### **Spencer Fane LLP**

On April 20, 2020, the United States Supreme Court issued its long-awaited decision allowing 98 private landowners in Montana to pursue a restoration...

---

## **A Compilation of Updated CMS and CDC Guidance for Dialysis Facilities in Light of COVID-19**

### **Faegre Drinker Biddle & Reath LLP**

The Centers for Medicare and Medicaid Services (CMS) and the Centers for Disease Control and Prevention (CDC) have announced an array of...

---

## **Internet & Social Media**



## **Joint Agencies Issue Guidance on Prevalence of Cyberattacks Exploiting COVID-19 and Teleworking**

### **Baker & Hostetler LLP**

On Friday, April 10, 2020, the Department of Homeland Security, the



Cybersecurity and Infrastructure Agency and the United Kingdom's National Cyber...

---

### **Price Gouging Takedowns - The Online Platforms Have a Say**

#### **Proskauer Rose LLP**

Over the past month, state enforcers have declared a war on price gouging, but some of the most effective enforcers have not been the states. Online...

---

### **Will It Still be "In" When It Gets Here? Online Fashion Retailer Agrees to Largest Ever Settlement for Slow Deliveries**

#### **Hunton Andrews Kurth LLP**

On April 21, the FTC announced a record-setting \$9.3 million settlement with online retailer Fashion Nova for violating the decades-old Mail Order...

---

### **COVID-19 Update: Don't Be a Target: What Business Should Know about State Attorney General Reactions to COVID-19**

New York

Tennessee

#### **Cadwalader Wickersham & Taft LLP**

In any time of crisis, there is heightened risk for fraud and scams. While United States Attorney General Barr has warned of scams and other illegal...

---

### **Adapt to Thrive: Privacy and Data Security Considerations for Taking Business Online in Response to COVID-19**

#### **Lane Powell PC**

Shelter-in-place orders in response to the global COVID-19 outbreak have inspired businesses that rely on foot traffic and in-person meetings to find...

---

### **To Zoom or Not to Zoom—Privacy and Cybersecurity Challenges**

#### **Troutman Sanders LLP**

Wynter Deagle, Anne-Marie Dao, and Yarazel Mejorado were published in Bloomberg Law with their article "To Zoom or Not to Zoom—Privacy and...

---

### **No Disgorgement When Injunction is Sufficient Remedy**

#### **McDermott Will & Emery**

Addressing issues related to the disgorgement of profits and attorneys' fees in a trademark infringement lawsuit, the US Court of Appeals for the...

---

### **Revival of Facebook Internet Tracking Litigation Reveals Importance of CCPA Compliance and Highlights Ambiguities**

#### **Troutman Sanders LLP**

On April 9, 2020, the Ninth Circuit reversed the dismissal of several privacy and wiretap claims brought against Facebook, Inc. The action was brought...

---

### **Signing while Social Distancing, Part 2: Assignments**

#### **Harness, Dickey & Pierce, PLC**

Problems with assignments are likely to occur many years in the future when the assignor may be unavailable or uncooperative. Therefore, you...

---

## **US FINRA Issues Cybersecurity Guidance on Working Securely from Home During Covid-19**

### **Linklaters LLP**

The resilience of US firms' business operations has come under scrutiny in the light of Covid-19. In this context, the US self-regulator of...

---

## **Google to Require All Advertisers to be Verified**

### **Frankfurt Kurnit Klein & Selz PC**

Today, Google announced that it will be requiring all advertisers to be verified before they can buy ads on the Google platform. Google said that it...

---

## **Looking for Likes: Social Media Post Results in Unintended License to Share Photograph**

### **Bradley Arant Boult Cummings LLP**

A New York federal district court has dismissed a photographer's copyright infringement claims after finding that the photographer gave Instagram the...

---

## **FTC Cuts Checks to Salve Wounded Negative Option Subscribers**

### **Baker & Hostetler LLP**

Multiple defendants pay out \$488K in settlement fees...

---

## **Don't Feed the Fish: COVID-19 Phishing Scams and Malware Attacks**

### **Paul Hastings LLP**

Congratulations! Your entire workforce is now remote and your cyber training has effectively taught them that the prince in exile is not really going...

---

## **Electronic Signatures Becoming the Norm during COVID-19 Outbreak**

### **Proskauer Rose LLP**

The COVID-19 pandemic has fundamentally altered the way we live and conduct business. Most non-essential businesses have closed their offices and...

---

## **How COVID-19 Made Esports the 'Only Game in Town'**

### **Morgan Lewis**

By the second week of March, the National Basketball Association, National Hockey League, Major League Soccer, and Major League Baseball had...

---

## **Now Available — AdTech and Privacy: Managing Risk in a Complex and Evolving Digital Economy (Webinar Materials)**

### **Hogan Lovells**

On Wednesday April 15, Hogan Lovells and Ankura hosted a webinar about the impact of the GDPR and CCPA on cookies and similar AdTech tracking...

---

## **Live streaming - the US edition**

### **Reed Smith LLP**

Hot on the heels of our UK edition of the live streaming guide, our US colleagues have published a US edition, providing insights into rights...

---



## **Lessons Learned from FTC's IoT Tapplock Settlement**

### **Adams and Reese LLP**

On April 6, the Federal Trade Commission settled with smart lock maker Tapplock over allegations that it deceived consumers by falsely claiming that...

---

## **The Importance of Well-Drafted Website Terms and Conditions**

### **Klein Moynihan Turco LLP**

The United States District Court for the Southern District of New York recently issued a ruling that exemplifies the importance of well-drafted...

---

## **When Fast Fashion Slows Online Orders: Lessons Learned From \$9.3 Million FTC Settlement**

### **Akin Gump Strauss Hauer & Feld LLP**

On April 21, 2020 the FTC announced a record settlement of \$9.3 million with an online retailer in an action brought under the "Mail...

---

## **As COVID-19 Drives More Art Auctions Online, How Do Market Participants Maintain Financial Crimes Compliance?**

### **K2 Intelligence/Financial Integrity Network**

With the global economy reeling from the direct effects of the COVID-19 pandemic, no sector is spared from its impact, including the art market. As...

---

## **Mr Worldwide's Great American 'Scream' - Protection granted for Pitbull's famous yell**

### **King & Wood Mallesons**

American rapper, singer and songwriter Pitbull (Armando Christian Pérez) has successfully trade marked his tell-tale yell "EEEEEEYOOOOOO!" that...

---

## **Web-Conferencing? Don't Let Your Energy Zoom Away**

### **Holland & Hart LLP**

These days, instead of spending our days in offices, conference rooms, and courthouses, we are likely spending those days in front of laptop...

---

## **In the Crosshairs: Planned Obsolescence**

### **Linklaters LLP**

In the wake of news about Apple's EUR 25 million settlement with the French competition and consumer regulator following allegations of planned...

---

## **Remote Document Execution and Other Tax Matters Related to the Coronavirus Crisis**

### **Lewis Rice LLC**

The coronavirus pandemic and the response by federal, state, and local authorities has severely impacted nearly all individuals and businesses. These...

---

## **New FBI Alert to Healthcare Providers - Beware of COVID-19 Phishing Campaigns**

### **Akerman LLP**

Healthcare providers are under siege, not only from the COVID-19 pandemic, but also from cyber criminals. Following reports of targeted email...

---

### **Why Businesses Should Embrace Electronic Contracts and Signatures During Social Distancing**

#### **Phelps Dunbar LLP**

Due to the COVID-19 outbreak, much of Louisiana is working from home. With a drastic move toward remote working, electronic contracts and signatures...

---

### **Zooming into New Privacy Issues**

#### **Vedder Price PC**

"Should we do a Zoom?" It has taken little more than a month for the Zoom video conference platform to take its place among the likes of Google...

---

### **Validity of Electronic Signatures in Myanmar**

#### **Duane Morris LLP**

The COVID-19 pandemic impacts all aspects of our daily life. Government authorities around the world impose various measures to reduce the physical...

---

### **Cybersecurity Threat Actors Target Data of Businesses Seeking Economic Relief**

#### **Akin Gump Strauss Hauer & Feld LLP**

Cybersecurity threat actors are targeting information of businesses seeking assistance during this time of crisis. For example, last week the Small...

---

### **Remote Notarization in Missouri and Illinois During the COVID-19 Pandemic**

Illinois

Missouri

#### **Lewis Rice LLC**

In response to the COVID-19 pandemic, the governor of Illinois ordered residents to stay home and all non-essential businesses and operations to...

---

### **Episode 313: Is the international law of cyberwar a thing?**

Audio

#### **Steptoe & Johnson LLP**

In today's interview, I spar with Harriet Moynihan over the application of international law to cyberattacks, a topic on which she has written with...

---

### **Calif. Privacy Law Takeaways From 9th Circ. Facebook Case**

California

#### **Troutman Sanders LLP**

On April 9, the U.S. Court of Appeals for the Ninth Circuit reversed the dismissal of several privacy and wiretap claims brought against Facebook Inc...

---

### **Fortnite Owner, Epic Games, Formally Introduced to CCPA Through Class Action Complaint**

#### **Troutman Sanders LLP**

On April 17, a class action complaint was filed by plaintiff Heather Sweeney against Life on Air, Inc. - creator of the video chat app Houseparty -...

---

### **Hawaii is Latest State to Implement a Regulatory Sandbox to Attract**



## **Cryptocurrency Business**

### **Proskauer Rose LLP**

On March 17, 2020, the governor of Hawaii announced the Digital Currency Innovation Lab, a collaborative effort between Hawaii's Department of...

## **Virtual Mediations: My Initial Impression: Positive Impressions of Settling Cases Online**

### **Schulwolf Mediation**

COVID-19 has forced mediators to perform their services online. Just in the last month I have taken numerous webinars and reached out to my ADR...

## **When it Comes to Virtual Learning, Privacy Isn't as Easy as 2 + 2 = 4**

### **Frankfurt Kurnit Klein & Selz PC**

The creativity with which people around the world have responded, and continue to respond, to this pandemic in addressing the needs of others is...

## **COVID-19: The Risks and Rewards of Remote Videoconferencing**

### **Troutman Sanders LLP**

The past few weeks have demonstrated that companies across all industries and sectors face daily pressure as they adapt to doing business in the era...

## **Communication During a Pandemic**

### **Porzio Bromberg & Newman PC**

This article offers best practices for company communication during a pandemic, such as the current COVID-19 global emergency. The author emphasizes...

## **US Federal Court says Breach of Website's Terms is Not a Criminal Offense**

District of Columbia

### **Pearl Cohen Zedek Latzer Baratz**

The United States District Court for the District of Columbia held that a breach of a website's terms of use does not constitute an actionable...

## **Court approves \$5 billion FTC settlement with social media company**

### **Buckley LLP**

On April 23, the U.S. District Court for the District of Columbia approved a \$5 billion settlement between the FTC and a global social media company...

Legal Practice



## **5 Must-Have Contract Management Tools for Effective Remote Work**

### **CobbleStone Software**

In the face of unforeseen circumstances, many organizations allow employees to work from home. Legal professionals in a variety of industries must...

## **Seven Top Trends in COVID-19 Litigation Targeting Business Practices**

### **Pepper Hamilton LLP**

The unprecedented health emergency and closely related economic crisis created



by COVID-19 have triggered a wave of putative class action...

---

**Ethics and risk management: What will the “new normal” look like?**

**Thompson Hine LLP**

When we scheduled our daughter’s wedding for March 15 in New York City, little did we know how surreal the world would be by then. The wedding did...

---

**Internal Corporate Investigations May Deserve Work Product Protection If They Differ From The Corporation's Normal Procedures: Part II**

**McGuireWoods LLP**

Last week's Privilege Point described a court's finding that the work product doctrine protected a corporation's investigation of a gender and age...

---

**CPS issues guidance on the application of the Public Interest test during the COVID-19 crisis**

**Ropes & Gray LLP**

Coming two weeks after the release of the Interim CPS Charging Protocol (see [here](#) and [here](#) for more details) the CPS has issued Interim Guidance on...

---

**Ethics Traps for the Unwary: Don't Lose the Remote Control During COVID-19**

**Goodell DeVries Leech & Dann LLP**

Of the many impacts that COVID-19 is having on the practice of law, perhaps the most challenging is the transition to remote or virtual office...

---

**English High Court Sets out Principles for COVID-19 Adjournments and Time Extensions**

**Faegre Drinker Biddle & Reath LLP**

In a recent ruling of the English High Court, a judge has set out the principles which the English Courts should apply when considering applications...

---

**Projects & Procurement**



---

**GAO Recommends Improvements to SEC Operations**

**Cadwalader Wickersham & Taft LLP**

The GAO recommended improvements to SEC operations. The GAO advised the SEC to: conduct periodic validations of its performance management system...

---

**OFCCP Issues Three New Directives**

**Proskauer Rose LLP**

As noted in our recent posts, OFCCP remains open for business despite the COVID-19 pandemic. On April 17, 2020, OFCCP provided further evidence of...

---

**Government’s Apparent Acquiescence Doesn’t Overcome “Plain” Contract Language**

**Stinson LLP**

Despite “troubling” government conduct, the Armed Services Board of Contract Appeals (ASBCA) recently denied an appeal arising out of electrical work...

---

---

## **Critical PPP Issues for Government Contractors**

### **Bradley Arant Boult Cummings LLP**

Many federal contractors have already taken advantage of the Paycheck Protection Program (PPP), which was established by the CARES Act to help small...

---

## **Government Innovation During a Pandemic**

### **Bilzin Sumberg**

During this current COVID-19 crisis, a great deal has been written on what government is not doing (or not allowing others to do). But the same...

---

## **COVID-19: CARES Act Funding Facts and Enforcement Risks for the Healthcare Industry**

### **Bass, Berry & Sims PLC**

Under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), the federal government is delivering a significant influx of money to the...

---

## **CBCA Rejects a Claim for Increased Costs Stemming from Contractor's Efforts to Mitigate Project Impacts Due to Ebola Epidemic**

### **Smith Currie & Hancock**

In an April 22, 2020 decision, Pernix Serka Joint Venture v. Department of State, the Civilian Board of Contract Appeals (CBCA) denied a contractor's...

---

## **Bond Markets and Debt Placements**

### **Skadden Arps Slate Meagher & Flom LLP**

Project bonds have been a critical source of debt financing in the project finance space for many years. Most commonly, a project sponsor will seek to...

---

## **DoD's Joint Artificial Intelligence Center Seeks Tools to Test Artificial Intelligence**

### **Crowell & Moring LLP**

Consistent with the U.S. Department of Defense's (DoD) Artificial Intelligence (AI) Strategy, as we previously reported on here, on April 13, 2020...

---

## **COVID-19: Assessing the Impact of Force Majeure on Emerging Markets PPPs**

### **Hunton Andrews Kurth LLP**

Infrastructure projects, and public-private partnerships in particular, around the globe and in all sectors have felt the impact of the COVID-19...

---

## **False Claims for Supplements Costs Marketers \$38 Million in Deal with FTC**

### **FisherBroyles LLP**

The marketers of several supplements that claimed their drugs did any number of things, from relieving arthritis pain to improving brain function...

---

## **Do We Still Need Retainage?**

### **Bradley Arant Boult Cummings LLP**



There have been debates for years about the pros and cons of owners withholding retainage (usually 5% or 10%, depending on each state's retainage...

---

### **CARES Act May Provide Financial Relief for Contractors Impacted by COVID-19 if They Remain in a Ready State**

**Davis Wright Tremaine LLP**

The economic impact of COVID-19 has been felt across almost all industries in the United States, and Government contractors are no exception. Many do...

---

### **CARES Act Section 3610 Provides Federal Agencies Discretion to Reimburse Federal Contractors' Employee Compensation**

**Baker & Hostetler LLP**

Federal contractors have a new avenue to potentially secure financial relief from the impacts of COVID-19 on their operations under Section 3610 of...

---

### **2020 Construction Planning in the Wake of COVID-19**

**Bradley Arant Boult Cummings LLP**

The COVID-19 pandemic swiftly eroded recent gains in the U.S. and world economies and has exposed economic and societal vulnerabilities that many...

---

### **OFCCP Temporarily Relaxes Certain Affirmative Action Requirements in Federal Contracts in Response to COVID-19**

**Taft Stettinius & Hollister LLP**

On March 17, 2020, the Office of Federal Contract Compliance Programs (OFCCP) issued a temporary waiver of three areas of equal employment...

---

### **Board Determines Virus Is Excusable but Non-Compensable Delay**

**Davis Wright Tremaine LLP**

A decision just issued by the Civilian Board of Contract Appeals (CBCA) offers guidance on how the federal government may respond to COVID-19 claims...

---

### **Insurers' COVID-19 Notepad: What You Need to Know Now**

**Crowell & Moring LLP**

LH Dining LLC and Newchops Restaurant Comcast LLC moved in the U.S. District Court (E.D. Pa.) pursuant to 28 U.S.C. § 1407 to consolidate business...

---

### **Why Procurement Processes Still Matter During a Pandemic**

New York

**K2 Intelligence/Financial Integrity Network**

For government and private institutions, the COVID-19 pandemic has meant acting quickly—so quickly, in fact, that companies run the risk of...

---

### **Government Contractor Mergers & Acquisitions: What To Do With Pending Proposals?**

**DLA Piper**

Mergers and acquisitions involving Government contractors give rise to...

---

### **GSA Issues Class Deviation Regarding Implementation of Section 3610 of the**

## **CARES Act**

### **Crowell & Moring LLP**

On April 21, 2020, the General Services Administration (GSA) Office of Governmentwide Policy, issued Class Deviation CD-2020-12, effective...

---

## **NC Politics in the News** North Carolina

### **McGuireWoods Consulting LLC**

The U.S. Agriculture Department approved Friday two North Carolina requests for additional resources as part of the State's response to the COVID-19...

---

## **Webinar Recording: COVID-19's Impact on Public and Private Construction Projects** Video

### **Seyfarth Shaw LLP**

This webinar is a practical review of the impacts of COVID-19 on public and private construction contracts, including clauses covering delay, impact...

---

## **Guidance for the Federal Contractor in Dealing with a Financially-Distressed Subcontractor During and After the COVID-19 Pandemic**

### **Crowell & Moring LLP**

The ongoing COVID-19 crisis has caused unprecedented harm to nearly all industries, including those involved in federal government contracts. This...

---

## **New Jersey Shuts Down "Non-Essential" Construction Projects To Mitigate Covid-19 - "Essential" Projects Can Continue Under Certain Conditions** New

Jersey

### **Ansa Assuncao LLP**

In continuing efforts to flatten the coronavirus infection curve, New Jersey Governor Phil Murphy has ordered all "non-essential" construction...

---

## **False Claims Act and Other Potential Liability for Misuse of Paycheck Protection Program Loans**

### **Nelson Mullins Riley & Scarborough LLP**

In response to the economic crisis caused by the COVID-19 pandemic, the Coronavirus Aid, Relief, and Economic Security Act, or CARES Act, was signed...

---

## **CARES Act Loans Available for National Security Businesses**

### **Sheppard Mullin Richter & Hampton LLP**

The US Treasury Department is accepting CARES Act Title IV loan applications from national security businesses to provide liquidity to offset covered...

---

## **Bay Area Counties Allow Construction to Recommence on May 4**

### **Manatt Phelps & Phillips LLP**

Effective May 4, 2020, construction projects throughout the Bay Area may recommence, subject to specified protocols. Although Governor Newsom's...

---

## **Higher Education Federal Contractors: Is Your Supply Chain Compliant With the National Defense Authorization Act?**



### **Ogletree Deakins**

President Donald Trump signed the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA) (Pub. L. No. 115-232) into law on...

---

### **Having Access to Capital to Invest in Better Infrastructure and Growth: Critical Consideration #4** [Video](#)

#### **Epstein Becker Green**

The health care marketplace is evolving, and it takes substantial investment in infrastructure, such as IT, to stay ahead and continue be successful...

---

### **Document ... Document ... Document ... Smart steps for government contractors** **Odin Feldman & Pittleman PC**

With the Federal government issuing near-daily guidance to government contractors and rolling out much needed relief for small businesses, there is...

Public



---

### **New Problem, Old Solution: Bring Back Tax-Exempt Advance Refundings**

#### **Squire Patton Boggs**

As the world grapples with the effects of the coronavirus disease 2019 (COVID-19) pandemic, state and local governments (collectively, State and Local...

---

### **Executive Summary: Tracking Telehealth Changes State-by-State in Response to COVID-19**

#### **Manatt Phelps & Phillips LLP**

As the coronavirus pandemic continues to spread across the U.S., states, payers and providers are looking for ways to expand access to telehealth...

---

### **COVID-19: Medidas para la adquisición de medicamentos y otros insumos de la salud**

#### **Morgan & Morgan**

De Acuerdo a la Resoluci&oacute;n No. 53960 de 25 de marzo de 2020, se incluye un nuevo art&iacute;culo que establece el procedimiento bajo la...

---

### **SBA 7(a) Program Funding May Temporarily Lapse Due to CARES Act Mishap**

#### **Nelson Mullins Riley & Scarborough LLP**

With Congress set to replenish the Paycheck Protection Program (PPP) funding this week, SBA 7(a) program lenders are urging lawmakers to clarify...

---

### **Coronavirus (COVID-19) Update: Trade, Supply Chains and Defense : April 10, 2020**

#### **Squire Patton Boggs**

Countries around the world continue to enact policies aimed at mitigating the spread of COVID-19 that both recognize the importance of trade to...

---

### **FEMA Releases Temporary Final Rule on US Exports of Personal Protective**



## **Equipment**

### **Squire Patton Boggs**

The Federal Emergency Management Agency (FEMA) has released a temporary final rule on US exports of personal protective equipment (PPE). It went into...

---

## **OFAC Issues Fact Sheet on Providing Humanitarian Aid to Combat COVID-19 Under Various Sanctions Programs**

### **Thompson Hine LLP**

On April 16, 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC) stated that the United States "is committed to ensuring...

---

## **How to Obtain PPP Loan Forgiveness!: COVID-19 Transportation Update - Wednesday, April 22, 2020**

### **Windels Marx Lane & Mittendorf LLP**

The White House and Congress have reached a deal on a bill that includes nearly \$320 billion in new funding for the Paycheck Protection Program...

---

## **DOE issues guidance on the use of the CARES Act's Higher Education Emergency Relief Fund (HEERF)**

### **Nelson Mullins Riley & Scarborough LLP**

In new FAQs on Emergency Student Aid portion of HEERF and FAQs on Institutional Portion of HEERF, the US DOE explained the requirements relating to...

---

## **Business coalition DC2021 presents its COVID-19 Impact and Recovery Plan for DC**

### **Venable LLP**

Local restaurant, retail, hotel, arts, sports, and entertainment businesses join civic leaders to form an advocacy group, DC2021, to support the...

---

## **Bring Back Tax-Exempt Advance Refundings**

### **Squire Patton Boggs**

Over at our Restructuring GlobalView blog, our public finance colleagues Pedro Miranda and Pedro Hernandez make the case for bringing back tax-exempt...

---

## **Reopening economies - which level of government has the last word?**

### **Hogan Lovells**

As states begin to work together to reopen the economy, companies in all industries will soon have to wrestle with a new wave of federal, state, and...

---

## **House Passes \$484 billion Bill "3.5" to Refill the PPP and EDL Loans, Hospitals, and Testing**

### **Michael Best & Friedrich LLP**

The House of Representatives overwhelmingly passed a \$484 billion coronavirus relief bill to replenish a tapped-out small business loan program...

---

## **New Jersey Governor Signs Bill Requiring 'Title 26 Hospitals' to Report**

## **Demographic Data on COVID-19**

New Jersey

### **Jackson Lewis PC**

New Jersey Governor Phil Murphy has signed a bill requiring hospitals licensed under New Jersey Statutes Title 26 to report demographic data on...

---

## **What You Need to Know About the Latest Updates to the Paycheck Protection Program (PPP)**

### **Nossaman LLP**

This is an update to our eAlert dated April 3, 2020 entitled "Finding the Right Fit Under CARES: Understanding the SBA Loan Programs Available Under..."

---

## **Three tips for Government contractors seeking CARES Act Section 3610 assistance for paying employees or subcontractors**

### **Thompson Coburn LLP**

As many Government contractors have heard by now, Section 3610 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act includes a section...

---

## **OFAC Issues Fact Sheet on Providing Humanitarian Aid to Combat COVID-19 Under Various Sanctions Programs**

### **Thompson Hine LLP**

On April 16, 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC) stated that the United States "is committed to ensuring..."

---

## **Reopening the State of Georgia**

Georgia

### **Barnes & Thornburg LLP**

On April 20, Georgia Gov. Brian Kemp laid out his initial plan to reopen the State's economy. His plan calls for a gradual economic reopening with...

---

## **Illinois residents urged to 'stay at home'**

Illinois

### **Thompson Coburn LLP**

In an unprecedented move, Governor J.B. Pritzker extended his "stay at home" order through Saturday May 30, 2020, for residents of the state of...

---

## **Managing CARES Act Stimulus Funds: Preparing for Robust Federal Oversight**

### **Squire Patton Boggs**

On March 27, 2020, the President signed the much-anticipated Phase 3 of the coronavirus disease 2019 (COVID-19) stimulus package (the Coronavirus Aid...

---

## **COVID-19 class actions against universities**

### **Hogan Lovells**

In response to the COVID-19 pandemic, universities have had to make difficult, but important, decisions to protect the health of their students, among...

---

## **House Votes to Form COVID-19 Oversight Subcommittee**

### **Step toe & Johnson LLP**

In its brief return to work on April 23 to vote on added funding for the CARES Act,



the US House of Representatives also approved a new Select...

---

### **Congress Passes “Stimulus 3.5” to Aid Small Businesses, Hospitals, and Virus Testing**

#### **Bradley Arant Boult Cummings LLP**

Governmental Affairs Alert The House and Senate have passed the latest round of emergency stimulus measures to address the COVID-19 crisis - a \$484...

---

### **California’s Newsom on Reopening State: ‘There Is No Light Switch, There Is No Date’**

California

#### **Manatt Phelps & Phillips LLP**

As promised, California Governor Gavin Newsom provided an update on reopening the California economy in his daily press conference: There is no...

---

### **No Private Right of Action to Enforce CARES Act; Expect Claims Under State Consumer Protection Laws**

#### **McGuireWoods LLP**

As previously reported, the U.S. District Court for the District of Maryland denied multiple motions brought by a number of small business owners...

---

### **Litigation During the Pandemic: Remote Depositions**

#### **Cozen O'Connor**

No one knows how long we will be living in this COVID-19-inspired Twilight Zone Episode. Estimates vary widely over how long shelter in place rules...

---

### **COVID-19 Washington Update: April 21, 2020**

#### **Kelley Drye & Warren LLP**

Today, the Senate passed a \$484 billion interim emergency funding bill, with House passage expected Thursday. See more below on today’s federal...

---

### **Impacts of COVID-19 on U.S. Infrastructure Projects**

#### **Nossaman LLP**

As the COVID-19 pandemic continues, both the public and private sectors have been working to understand the market’s response and search for...

---

### **Congress Funds \$310B for Paycheck Protection Program, \$60B for Economic Injury Disaster Loans**

#### **McGuireWoods LLP**

The U.S. House of Representatives passed the Paycheck Protection Program and Health Care Enhancement Act (PPP Enhancement Act) by 388 to 5 on April...

---

### **Connecticut and New Jersey Executive Orders on COVID-19 Business Closures**

Connecticut

New Jersey

#### **Davis Wright Tremaine LLP**

As we reported on Friday, March 20, all non-essential businesses across New York State are under orders from Governor Cuomo to keep 100 percent of...

---

**COVID-19 Giveaways: Avoiding the Pitfalls of Charitable Promotions and Marketing****Thompson Hine LLP**

Many organizations have substantially increased their charitable contributions, corporate giving and philanthropy to assist those affected by the...

---

**Federal Aid Plan for PPP and Hospitals Announced****Michael Best & Friedrich LLP**

Congress and the White House Announce Deal Congressional leaders and the White House have agreed to Phase 3.5 of COVID-19 Response. This deal will...

---

**Lessons Learned from Post-9/11 and Anthrax Experiences to be Applied to Covid-19 in the Food Industry****Hogan Lovells**

As we face huge challenges from COVID-19, I am reminded daily of the parallels we faced in the 9/11 aftermath and related Anthrax incident nearly 20...

---

**Attorney General's Office Issues Opinion on the Definition of "Effective Date" as Used in Business and Professions Code Section 805****Nossaman LLP**

At the request of the Medical Board of California, on April 17, 2020, the Office of the Attorney General issued California Opinion of the Attorney...

---

**DOE Requests Input on Fusion Public-Private Partnership Program****Hogan Lovells**

Fusion holds the potential to revolutionize energy generation around the globe, and innovators in the private sector have been working hard to make...

---

**COVID-19 Litigation And Government Investigations in the U.S.: What We Are Seeing Now, And What the Future Holds****Goodwin Procter LLP**

The emergence of COVID-19 has led to increased litigation and government activity across all industries, and this trend is only likely to accelerate...

---

**President Trump Signs Second Emergency Stimulus Bill Allocating Additional Funding for Paycheck Protection Program****Greenbaum, Rowe, Smith & Davis LLP**

A short while ago, President Trump signed the Paycheck Protection Program and Health Care Enhancement Act into law. The legislation allocates \$484...

---

**Managing Outdoor Race Season in Uncertain Times****Ansa Assuncao LLP**

The breaking of winter brings warmer weather and, in usual times, the first 5K, half/full marathon, and even 100-mile super-marathon (yes, you read...

---

**COVID-19: Congress Approves Interim Emergency Relief Package**



### **Pierce Atwood LLP**

On Friday, April 24, 2020, President Trump signed another emergency relief package (CARES Act II) totaling close to \$500 billion, the bulk of which...

---

### **New Federal Stimulus Legislation Provides Funding for Small Businesses, Healthcare Providers, and Coronavirus Testing**

#### **Ogletree Deakins**

On April 24, 2020, President Trump signed the Paycheck Protection Program and Health Care Enhancement Act, which will allocate over \$480 billion in...

---

### **Alaska Issues COVID-19 Mandates to Clarify Restrictions on Religious Gatherings and to Address Non-urgent and Elective Medical Procedures**

Alaska

#### **Ogletree Deakins**

Alaska has joined a growing number of states addressing the thorny issue of the size and density of religious gatherings during the COVID-19 health...

---

### **House Passes a \$484 Billion Relief Package; Treasury and the SBA Release New Guidelines for PPP Loans**

#### **Morrison & Foerster LLP**

On Thursday, April 23, 2020, the U.S. House of Representatives voted in favor of the \$484 billion relief package that passed in the Senate earlier...

---

### **Davidson County (TN) Extends Safer-At-Home Order And Unveils Roadmap For Reopening Nashville**

Tennessee

#### **Fisher Phillips**

Though the statewide Safer at Home Order is set to expire on April 30, some counties in Tennessee - including Davidson County - have extended their...

---

### **HHS Announces Further Allocations of \$100 Billion CARES Act Provider Relief Fund; Warns of "Significant" Anti-Fraud and Auditing Work**

#### **Bass, Berry & Sims PLC**

On Wednesday, April 22, the U.S. Department of Health and Human Services (HHS) issued a press release announcing additional allocations from the \$100...

---

### **US Education Policy Update: Governor's Emergency Education Relief Fund - Charter School Grants - and More**

#### **Squire Patton Boggs**

The following update includes two latest funding announcements on the GEER Fund (the Governor's Emergency Education Relief Fund) and for charter...

---

### **Consider COVID Attitude Changes, Part 4: More Polarization on Science**

#### **Holland & Hart LLP**

After a brief time when it seemed that Americans were coming together in favor of social isolation to slow the spread of the novel coronavirus, it...

---

### **Mashpee Wampanoag Tribe Seeks Reservation Protection from Federal Court**

#### **Barnes & Thornburg LLP**



The Mashpee Wampanoag Tribe, also known as the People of the First Light, has inhabited present-day Massachusetts and Eastern Rhode Island for...

---

**Regulatory Takings and Executive Power to Seize Property** [Audio](#)

**Pepper Hamilton LLP**

Troutman Sanders and Pepper Hamilton are producing a series of podcasts to discuss litigation topics that have been brought to the forefront by the...

---

**United Technologies/Raytheon Highlights Key Issues in Aerospace and Defense Industry Merger Review**

**McDermott Will & Emery**

The DOJ Antitrust Division's (DOJ) recent challenge to the United Technologies (UTC)/Raytheon (RTN) merger highlights a few key considerations for...

---

**The Pendulum Swings: Record Fine Imposed by UK Sanctions Monitor, but Only After Reduction on Review**

**Greenberg Traurig LLP**

The UK's sanctions monitor, the Office of Financial Sanctions Implementation (OFSI), has issued its biggest fine to date, imposing a total financial...

---

**Considerations for Colleges and Universities Facing Class Action Refund Lawsuits From Students**

**Faegre Drinker Biddle & Reath LLP**

COVID-19 has forced colleges and universities to move from traditional in-person classroom instruction to online learning. Just as students, faculty...

---

**Maryland Governor Announces Three-Stage Plan for Reopening the State**

[Maryland](#)

**Duane Morris LLP**

On Friday afternoon, Maryland Governor Larry Hogan announced a three-stage plan to reopen the State called "Maryland Strong: Roadmap to Recovery,"...

---

**Commercial Real Estate Finance COVID-19 Impact Series: Retail and Shopping Center Landlords**

**Frost Brown Todd LLC**

The ongoing COVID-19 pandemic continues to impact all areas of the economy, however, retail shopping center owners (often referred to below as...

---

**EPA Announces Its Continued Efforts to Provide Critical Information on Safe Disinfectant Use During COVID-19 Crisis**

**Bergeson & Campbell PC**

On April 23, 2020, the U.S. Environmental Protection Agency (EPA) announced it is continuing efforts to provide critical information on surface...

---

**Department of Health & Human Services Clarifies Broad Scope of Immunity Protection Under the PREP Act**

**Duane Morris LLP**

While the declaration defined “Covered Persons” and “Covered Countermeasures,” there were numerous requests for more clarity on the scope of the...

---

### **Senate Approves \$310 Billion in Additional Funding for the Paycheck Protection Program**

**Paul Weiss**

On April 21, 2020, the Senate passed the “Paycheck Protection Program and Health Care Enhancement Act”[1] to provide up to \$484 billion in additional...

---

### **PPPHCEA Expands the PPP, EIDL and the Number of Acronyms We Need to Master**

**Lane Powell PC**

On April 22, the Senate approved a new stimulus bill and the House followed with their approval. On April 23, President Trump has indicated he will...

---

### **U.S. Importers Can Postpone Duty Payments for 90 Days, But Relief Limited**

**Stinson LLP**

On April 19, U.S. Customs and Border Protection (CBP) announced the rollout of a 90-day duty deferral program for importers experiencing significant...

---

### **Congress Passes Additional \$100 Billion in Aid for Public Health and Social Services Emergency Fund**

**Bass, Berry & Sims PLC**

On April 21, the U.S. Senate approved an additional \$100 billion in funding for the Public Health and Social Services Emergency Fund established under...

---

### **COVID-19: Daily Report for Life Sciences and Health Care Companies**

**Hogan Lovells**

The Daily Report is a compilation of COVID-19 (coronavirus) news briefs from around the world to help life sciences and health care companies stay...

---

### **North Carolina General Assembly — Coronavirus (COVID-19) Update**

**Carolina**

**McGuireWoods Consulting LLC**

The North Carolina General Assembly will reconvene Tuesday, April 28 at 12:00. Due to the COVID-19 pandemic, the upcoming session will look different...

---

### **Georgia Issues Guidelines for Reopening Sectors of Its Economy**

**Fox Rothschild LLP**

On Monday, April 20, 2020 Georgia Gov. Brian Kemp issued an Executive Order that set the state on a path to begin reopening some of the businesses...

---

### **New/Updated Terms and Conditions and Hall Render Briefing Document**

**Hall Render Killian Heath & Lyman PC**

HHS published a new Terms and Conditions document that is specific to payments that started being distributed on Friday, April 24 from the CARES Act...



---

## **NC Outlines Three-Phase Approach to Reopen State** North Carolina

### **Fox Rothschild LLP**

North Carolina Gov. Roy Cooper officially extended the State's stay-at-home order through May 8, 2020, which includes closures of dine-in restaurants...

---

## **NC Governor Cooper Extends Statewide "Stay at Home" Order and Order Closing Schools** North Carolina

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

North Carolina Governor Roy Cooper took additional executive action this week related to the COVID-19 virus and its impact on the state...

---

## **Banking litigation in the next decade: A look ahead**

### **Linklaters LLP**

Banking litigation in the next decade: a look ahead Foreword The start of a new decade seems a good time to take stock of the likely sources of...

---

## **Texas Developments, Week of April 20, 2020** Texas

### **Frost Brown Todd LLC**

On April 17, 2020, Texas Governor Greg Abbott issued several Executive Orders to "Open Texas." This means they will begin a process of "safely and...

---

## **U.S. Department of Education Releases Additional Details on CARES Act Emergency Assistance for Higher Education Institutions and Students**

### **Faegre Drinker Biddle & Reath LLP**

On Tuesday, April 21, 2020, the U.S. Department of Education (ED) released additional information regarding emergency assistance for higher education...

---

## **COVID-19: Federal Reserve Board to publish CARES Act borrower information. Does more oversight follow?**

### **Hogan Lovells**

On April 23, the Federal Reserve Board issued a vow to report information every month regarding the participants of lending and liquidity facilities...

---

## **DOJ Continues Expedited Approval of COVID-19 Related Competitor Collaborations**

### **Crowell & Moring LLP**

Earlier this week, the U.S. Department of Justice issued a business review letter approving a competitor collaboration intended to accelerate and...

---

## **Private Student Loan Servicers Enter Agreement with Multiple States for Relief Options**

### **Troutman Sanders LLP**

Multiple states have come together to enact initiatives aimed at prohibiting private student loan servicers from certain activities that will remain...

---

## **UPDATE: NCAA Rejects Blanket Waiver of Minimum Sports Requirement in**

## **Midst of COVID-19**

### **Jackson Lewis PC**

The NCAA Division I Council has rejected the efforts of the leaders of five Division I Conferences (the American Athletic, Mountain West...

---

## **Department of Education Releases FAQs on CARES ACT Funding for Universities**

### **Vorys Sater Seymour and Pease LLP**

Our team continues to track legal developments related to the COVID-19 pandemic, specifically as they relate to colleges and universities. As you know...

---

## **PA Law Allows Municipal Governments to Hold Virtual Meetings for Zoning and Land Development Applications**

[Pennsylvania](#)

### **Pepper Hamilton LLP**

On April 20, Pennsylvania Gov. Tom Wolf signed into law Act 15 of 2020 (previously SB 841), which expressly authorizes municipal...

---

## **COVID-19: PA Announces May 1 reopening for Golf Courses, Marinas and Privately Owned Camp Grounds**

### **Duane Morris LLP**

As of May 1, PA will allow golf courses and marinas and privately owned campgrounds to re-open...

---

## **COVID-19: NY announces Phased Approach for Re-Opening**

[New York](#)

### **Duane Morris LLP**

On April 27th, Governor Cuomo outlined a phased plan to re-open New York starting with construction and manufacturing. Based on CDC recommendations...

---

## **ARRC Proposes New York State Legislation to Facilitate LIBOR-to-SOFR Transition**

[New York](#)

### **Paul Hastings LLP**

The Alternative Reference Rates Committee (the "ARRC") recently proposed statutory language for consideration by the New York State legislature...

---

## **Massachusetts Enacts Emergency Regulation on CORI Verifications**

[Massachusetts](#)

### **Littler Mendelson PC**

On April 9, 2020, the Massachusetts' Department of Criminal Justice Information Systems (DCJIS) passed an Emergency Regulation to address the social...

---

## **South Carolina Joins States Proposing Legislation to Mandate Insurers Pay COVID-19 Losses**

### **Wilson Elser**

On April 8, 2020, a bipartisan group of three South Carolina state senators introduced Senate Bill 1188, which would provide coverage for loss of...

---

## **Governor Baker's Emergency Order Closing Adult-Use Marijuana Establishments**



## **Survives Constitutional Challenge in BLS** Massachusetts

### **Nutter McClennen & Fish LLP**

To help slow the spread of the COVID-19 pandemic, Governor Baker has ordered businesses to suspend physical operations unless he deems them...

---

## **COVID-19: NJ Announces 6-Point Plan and Methodology for ReOpening the State - "The Road Back"** New Jersey

### **Duane Morris LLP**

Gov. Murphy announces NJ's 6-point reopening plan called "The Road Back: Restoring Economic Health Through Public Health." The Governor also...

---

## **Second Emergency Stimulus Bill Provides \$100 Billion in Additional Funding to Further Support COVID-19 Treatment and Testing**

### **Greenbaum, Rowe, Smith & Davis LLP**

The Paycheck Protection Program and Health Care Enhancement Act (the Act), a second round of emergency economic stimulus funding that was signed into...

---

## **COVID-19: Colorado Transitions to "Safer at Home"** Colorado

### **Wilmer Cutler Pickering Hale and Dorr LLP**

Colorado's stay-at-home order expired on Sunday, April 26. It has been replaced by a new order, issued April 26, reflecting the State's transition...

---

## **Colorado issues new "safer at home" executive order** Colorado

### **Buckley LLP**

On April 26, the Colorado governor issued an Executive Order that provides new requirements for social distancing and remote work. Among other things...

---

## **Massachusetts Legislature Passes Legislation Allowing Use of Virtual Notarization During COVID-19 Pandemic** Massachusetts

### **Nelson Mullins Riley & Scarborough LLP**

After some delay, on April 23, 2020, the Massachusetts Senate and House passed emergency legislation that allows for notaries public to use electronic...

---

## **Sixth Circuit Holds Due Process Guarantees Right To Access Literacy**

### **Squire Patton Boggs**

A Sixth Circuit panel held last week, in *Gary B. V. Whitmer*, that the Fourteenth Amendment's Due Process Clause guarantees a "right to access to..."

---

## **Maryland Governor Outlines Phased Reopening Plan Post-COVID-19 Shutdown**

Maryland

### **Jackson Lewis PC**

Maryland Governor Larry Hogan has introduced the Maryland Strong: Roadmap to Recovery, a three-stage plan for the state to restart its economy and...

---

## **Nevada State and Local Governments Make Licensing and Permit Accommodations to Help Businesses Amid the COVID-19 Crisis**



### **Dickinson Wright**

Like many other states in response to the widespread transmission of COVID-19, Nevada has banned business operations for non-essential businesses and...

---

### **COVID-19 Response: US financial services regulatory**

#### **White & Case LLP**

In response to the global COVID-19 crisis, US financial regulators at the state level are taking important actions that affect US and non-US...

---

### **OFAC Issues Guidance on COVID-19-Related Exports and Compliance Challenges**

#### **Baker & Hostetler LLP**

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has issued guidance on humanitarian exports and compliance challenges...

---

### **Client Alert: Virtual Notarization and Witnessing of Your Documents During COVID-19 Emergency**

Massachusetts

#### **Bowditch & Dewey LLP**

On April 27, 2020, Massachusetts enacted An Act Providing for Virtual Notarization to Address Challenges Related to COVID-19. This emergency virtual...

---

### **COVID-19: Distressed Debt and Tax - Part I - Lender and Debt Holder Considerations**

#### **K&L Gates**

In response to the economic havoc resulting from the onset of the coronavirus ("COVID-19") pandemic, Congress has enacted wide-ranging legislation to...

---

### **Memphis Extends Safer-At-Home Order And Issues New Guidelines For Essential Businesses**

Tennessee

#### **Fisher Phillips**

Memphis Mayor Jim Strickland recently issued an update to the March 23 Safer at Home Executive Order. While most Tennessee counties plan for...

---

### **North Carolina extends stay at home order**

North Carolina

#### **Buckley LLP**

On April 23, North Carolina Governor Roy Cooper issued an Executive Order extending his prior stay at home order (previously discussed here) until...

---

### **In updated COVID-19 FAQ, Indiana Department of Local Government Finance clarifies application of interest to late property tax payments; No change (yet) to 2020 assessment notice & appeal deadlines; Abatement compliance extended; Waiver of penalties on special assessments and fees**

Indiana

#### **Faegre Drinker Biddle & Reath LLP**

On April 24th, the Indiana Department of Local Government Finance updated its FAQ covering topics related to "COVID-19 & Executive Orders," as those...

---

## **The IRS Provides Tax Relief for Individuals and Businesses Affected by COVID-19-Related Travel Disruptions**

### **Kramer Levin Naftalis & Frankel LLP**

In recognition of the disruption of travel plans resulting from the global outbreak of COVID-19 (the COVID-19 Emergency), the Internal Revenue Service...

---

## **New Illinois Stay at Home Order Announced for May** Illinois

### **Ropes & Gray LLP**

On April 23, 2020, Governor J.B. Pritzker announced that he will sign a modified stay at home Executive Order (the "Order") to go into effect on May...

---

## **CARES Act funds: Significant new USED guidance includes surprises**

### **Thompson Coburn LLP**

Yesterday, the U.S. Department of Education issued significant new guidance to institutions of higher education regarding their receipt and use of...

---

イリノイ州の外出禁止令が延長されたことにより イリノイ州を拠点とする必要不可欠(essential)なビジネスおよび製造会社に及ぼされる影響 Illinois

### **Masuda Funai Eifert & Mitchell Ltd**

2020年4月23日 イリノイ州のJ.B.プリツカー知事は 現在出されている 外出禁止令(stay-at-home...

---

## **Covid-19 coronavirus: an overview of U.S federal legislation phase 4**

### **Allen & Overy LLP**

Congress passed the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") in late March 2020. The CARES Act included a Paycheck Protection...

---

## **President Trump Signs Bill to Provide Additional COVID-19-Related Small Business Funding**

### **Cadwalader Wickersham & Taft LLP**

Congress adopted and President Donald Trump signed into law an act to provide additional funding under the Paycheck Protection Program and to provide...

---

## **Real Estate Development in the Time of Coronavirus: Massachusetts - Update 4/28/20** Massachusetts

### **Pierce Atwood LLP**

On April 28, 2020, Massachusetts Governor Charlie Baker extended his previous order...

---

## **COVID-19: NJ names 21 Member COVID Taskforce** New Jersey

### **Duane Morris LLP**

NJ has officially announced the 21 members of its COVID Taskforce. According to Governor Murphy, the NJ taskforce "is composed of experts in a...

---

## **Congress approves extension for PPP and EIDL programs**

### **McBrayer McGinnis Leslie & Kirkland PLLC**



After the initial funding for the Payroll Protection Program (PPP) and the Economic Injury Disaster Loan program (EIDL) were exhausted, Congress...

---

**Virginia outlines student loan servicer requirements** Virginia

**Buckley LLP**

On April 22, the Virginia legislature enacted SB 77, which requires entities servicing student loans in the Commonwealth to be licensed by the State...

---

**Betsy DeVos Refuses to Request Much-Needed Waivers from the IDEA and Section 504**

**Nelson Mullins Riley & Scarborough LLP**

U.S. Secretary of Education Betsy DeVos has submitted a recommendation to Congress that states and local educational agencies (LEAs) not receive any...

---

**U.S. - Coronavirus (Legal) Immunity - The Risky Business of Re-Opening**

**Bryan Cave Leighton Paisner LLP**

In the midst of unprecedented business and court closures, the Coronavirus (COVID-19) pandemic has already caused a flood of litigation. Businesses...

---

**New Threat on the Horizon for Schools, Colleges, and Universities: Class Action Lawsuits for Return of Tuition**

**Krieg DeVault**

COVID-19 has caused tremendous disruption and expense for colleges and universities, and other tuition-based education institutions, leading to...

---

**Higher Education Institutions Should Prepare for Fallout from COVID-19**

**Akin Gump Strauss Hauer & Feld LLP**

Universities across the country have shuttered their campuses and moved classes online in reaction to the novel coronavirus...

---

**What to Expect From the New Congressional Coronavirus Subcommittee**

**US Squire Patton Boggs**

On April 23, 2020, the US House of Representatives voted to establish a new investigative subcommittee of the Committee on Oversight and Reform...

---

**COVID-19: HHS Clarifies Scope of PREP Act COVID-19 Declaration in Advisory Opinion**

**Michael Best & Friedrich LLP**

On April 14, 2020, the Department of Health and Human Services (HHS) General Counsel issued an Advisory Opinion clarifying the scope of liability...

---

**COVID-19 Washington Update: April 28, 2020**

**Kelley Drye & Warren LLP**

Following is a synopsis of today's federal government actions in response to COVID-19. Congress Today, House leaders reversed plans to return to...

---

**COVID-19: Expert Soundbite - The Geopolitical Consequences of the Pandemic**

Audio

### **Squire Patton Boggs**

Our global Public Policy Practice meets several times a week to examine the profound and transformative effect of the coronavirus disease 2019...

---

### **As Independent Schools throughout the Country Navigate the Rough Seas of the COVID-19 Global Pandemic, Does the Federal Financial Assistance Available to Them through the CARES Act PPP Loan Program an**

#### **Breazeale Sachse & Wilson LLP**

As Independent Schools throughout the Country Navigate the Rough Seas of the COVID-19 Global Pandemic, Does the Federal Financial Assistance...

---

### **Client Alert: State Announces Schedule for Reopening Businesses**

#### **Brouse McDowell**

On Monday, the Governor announced the State's plan for allowing businesses to reopen. This morning, the criteria were amended to revise the mask...

---

### **New Jersey Director of Emergency Management Eases Restrictions on Certain Businesses**

New Jersey

#### **Jackson Lewis PC**

The New Jersey State Director of Emergency Management has issued an Order designating additional businesses as "essential retail" and permitting auto...

---

### **Illinois to Modify and Extend Stay at Home Order Until May 30, 2020**

Illinois

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On Thursday, April 23, 2020, Governor J.B. Pritzker announced that he expected to sign an order modifying and extending the...

---

### **New Jersey's Post-COVID-19 'Road Back' Plan Full of Red Lights**

New Jersey

#### **Jackson Lewis PC**

New Jersey Governor Phil Murphy has released The Road Back: Restoring Economic Health Through Public Health, outlining six principles or milestones...

---

### **COVID-19: Massachusetts Allows Remote Notarization**

Massachusetts

#### **Pierce Atwood LLP**

On April 27, 2020, Massachusetts Governor Charlie Baker signed into law an emergency measure to authorize Massachusetts notaries public to use...

---

### **Higher education third party provider viability risk during COVID-19**

#### **MinterEllison**

Nowadays, many universities partner with third parties in the private sector to enrol and deliver (or assist in the delivery of) courses to students...

---

### **How Illinois-Based Japanese Essential Businesses and Manufacturing Companies Will Be Affected under the Illinois Extended Stay-at-Home Order**

Illinois

#### **Masuda Funai Eifert & Mitchell Ltd**



Illinois Governor J.B. Pritzker announced on April 23, 2020, that the Illinois stay-at-home order will be extended to May 30, 2020. The standing...

---

### **Louisiana Extends Statewide Stay-At-Home Order While Loosening Business Restrictions**

Louisiana

#### **Fisher Phillips**

Governor Jon Bel Edwards just extended Louisiana's statewide stay-at-home order through May 15 while also providing a Lifeline to some businesses...

---

### **Texas Unveils Phase One of Plan to Reopen Businesses**

Texas

#### **Fox Rothschild LLP**

On April 27, Texas Gov. Greg Abbott announced a multi-phase plan to reopen businesses. Phase One of the plan, set forth in an executive order...

---

### **Ohio House Members Release Guidelines for Re-Opening Ohio Businesses**

Ohio

#### **Dinsmore & Shohl LLP**

On April 27, 2020, members of the Ohio House of Representatives released the Open Ohio Responsibly Framework. This framework contains recommended...

---

### **New York Remote Notarization**

New York

#### **Haynes and Boone LLP**

In light of the social distancing orders put in place in response to the COVID-19 pandemic, Governor Andrew Cuomo signed Executive Order 202.7 on...

---

### **Introduction to United States Space Force Acquisitions**

#### **Davis Wright Tremaine LLP**

After becoming law in December 2019, the National Defense Authorization Act (NDAA) for Fiscal Year 2020 formally established the Space Force as the...

---

### **Considerations for schools and Universities that manufacture or supply ppe**

#### **Squire Patton Boggs**

In the ultimate act of service learning, many universities and schools have shifted their focus during the COVID-19 crisis to manufacturing personal...

---

### **Texas Allows More Elective Procedures, But Questions Remain**

Texas

#### **Seyfarth Shaw LLP**

On April 17, 2020, Texas Governor, Gregg Abbot signed Executive Order GA-15 which extended, with some modifications, Executive Order GA-09 which...

---

### **Virginia General Assembly Permits Local Governments to Meet Electronically**

Virginia

#### **McGuireWoods LLP**

The Virginia General Assembly recently authorized public bodies — including local boards and commissions — to meet electronically during the state of...

---

### **Illinois Governor Extends COVID-19 Stay-at-Home Order with Some**



## **Modifications** Illinois

### **Duane Morris LLP**

On April 23, 2020, Illinois Governor JB Pritzker announced that he is extending the state's stay-at-home order with modifications. This new order...

---

## **Alaska Issues First Phase of 'Reopen Alaska Responsibly' Plan** Alaska

### **Ogletree Deakins**

On April 22, 2020, Alaska Governor Mike Dunleavy, Alaska Department of Health and Social Services Commissioner Adam Crum, and Dr. Anne Zink, Chief...

---

## **The CARES Act: What Does It Mean for Your School District?**

### **Squire Patton Boggs**

The federal government approved the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) on March 27, 2020, as part of its efforts to...

---

## **COVID-19 Mexico Update: "Essential Activities" and Federal & State Enforcement Through April 29, 2020**

### **Wilmer Cutler Pickering Hale and Dorr LLP**

A joint client alert update by WilmerHale and Creel García-Cuellar Aiza & Enriquez.1 This publication updates our April 8, 2020, client alert...

---

## **Proposed California Legislation Seeks to Expand Eviction Protections Including Rent Reduction** California

### **Procopio Cory Hargreaves & Savitch LLP**

The California Legislature is currently considering two COVID-19 response bills aimed at protecting both residential and commercial tenants regarding...

---

## **Ohio Launches "Responsible RestartOhio" Plan** Ohio

### **Thompson Hine LLP**

On April 27, Ohio Governor Mike DeWine announced details of the Responsible RestartOhio plan, which will phase in a relaxing of the Amended...

---

## **Georgia Executive Orders Permits Re-Opening of Businesses** Georgia

### **Greenberg Traurig LLP**

Georgia Governor Brian Kemp recently issued two Executive Orders: (1) Executive Order 04.20.20.01; and (2) Executive Order 04.23.20.02 (herein...

---

## **Illinois Department of Financial and Professional Regulation issues guidance to student borrowers** Illinois

### **Buckley LLP**

The Illinois Department of Financial and Professional Regulation has issued responses to Frequently Asked Questions regarding the expansion of...

---

## **Campaign Finance Violation for Unregistered Political Committee Upheld in Washington State, but \$18 Million Penalty Must Still Pass Excessive Fine Test**

Washington

### **Covington & Burling LLP**

In one of the most watched campaign finance disclosure enforcement cases, last week, the Washington State Supreme Court upheld a trial court's...

---

### **CFIUS Filing Fees Go Into Effect May 1, 2020**

#### **Thompson Hine LLP**

On April 29, 2020, the U.S. Department of the Treasury's Office of Investment Security published an interim rule in the Federal Register that...

---

### **House Bill 197 Provisions Regarding School Leadership Evaluations, Education Metrics and Distance Learning**

#### **Taft Stettinius & Hollister LLP**

On April 20, 2020, Ohio Governor, Mike DeWine announced that the March 14, 2020 statewide order directing all of Ohio's public, community, and...

---

### **State Lobbyist and Campaign Finance Filing Changes Related to COVID-19**

#### **Covington & Burling LLP**

As states grapple with the effects of the COVID-19 crisis, many have opted to make changes to campaign finance and lobbying reporting due dates and...

---

### **Cayuga Nation Prevails in Long-Running Litigation Over Gaming Rights**

#### **Jenner & Block LLP**

On March 24, The Cayuga Nation vindicated its sovereign right to game under the Indian Gaming Regulatory Act (IGRA) when a New York federal judge ruled...

---

### **COVID-19: Governor Mills Establishes Four-Stage Plan to Reopen Maine's Economy; Extends Statewide Stay-At-Home Order**

Maine

#### **Pierce Atwood LLP**

On Tuesday, April 28, 2020, Maine Governor Janet Mills extended the statewide stay-at-home order through May 31, 2020, and announced a four-part plan...

---

### **COVID-19: Massachusetts Governor Extends Non-Essential Business Closures to May 18, 2020**

Massachusetts

#### **Pierce Atwood LLP**

On April 28, 2020, Massachusetts Governor Charlie Baker announced the second extension of Massachusetts' non-essential business closure order, now in...

---

### **West Virginia Reopening Plan Depends on Percentage of Positive Cases**

West

Virginia

#### **Frost Brown Todd LLC**

Governor Jim Justice's vision for reopening West Virginia was applauded by lawmakers from across the political spectrum as it provides a...

---

### **Compliance Notes - Vol. 1, Issue 1**

#### **Nossaman LLP**

Here, we are expanding upon our eAlerts (where we provide substantive analysis on key issues), to deliver a periodic digest of the headlines...



---

## **ReOpen DC Advisory Group Mission and Leadership**

### **Venable LLP**

The Group has 11 committees that will follow the Johns Hopkins' "Public Health Principles for a Phased Reopening during COVID-19: Guidance for...

---

## **U.S. Army Corps Asks Federal Court to Stay Decision Vacating NWP 12, Indicates It Will Appeal**

### **Fredrikson & Byron PA**

On April 27, 2020, the U.S. Army Corps of Engineers filed a motion asking a Montana federal court to partially stay its April 15, 2020, decision...

---

## **Kentucky Tax Talk: Budget Focuses on Pandemic Relief**

Kentucky

### **Frost Brown Todd LLC**

The commonwealth's primary concerns have drastically changed since the start of the 2020 General Assembly's regular session in January. Whether it was...

---

## **Congress Increases Funding for Coronavirus Relief Programs**

### **Vinson & Elkins LLP**

The U.S. Congress passed legislation to increase funding for coronavirus relief programs on Thursday, April 23, 2020. The \$483.4 billion package adds...

---

## **FARA: using anti-propaganda laws in the fight against corruption**

### **Raedas**

As the spread of the coronavirus limits travel and shuts archives, investigators are looking to pandemic-proof repositories of evidence. One such...

---

## **Andrew Yang Sues New York State Board of Elections for Canceling Democratic Primary**

New York

### **Steptoe & Johnson LLP**

On Monday, the New York State Board of Elections voted to cancel New York's democratic presidential primary, which it had originally postponed from...

---

## **A (Cloudy) CARES 2.0 Crystal Ball**

### **Hogan Lovells**

With an interim relief measure, the Paycheck Protection Program (PPP) and Health Care Enhancement Act, now signed into law, the jockeying over a CARES...

---

## **Courts Consider the Constitutionality of PPP Loans Under the CARES Act, Government Shutdown Orders, and Signature Requirements for Getting on the Ballot**

### **Seyfarth Shaw LLP**

As the pandemic continues, courts are addressing COVID-19-related constitutional challenges. The most recent cases address the eligibility...

---

## **Client Alert: The Mask is Back**

### **Brouse McDowell**

After the State of Ohio revised its internet postings yesterday, we advised our clients of where each industry scheduled for reopening stood as of...

---

### **Impact of COVID-19 Shutdown on Club Dues**

#### **Greenberg Traurig LLP**

Most golf and social clubs have either shut down or curtailed operations in response to the Coronavirus Disease 2019 (COVID-19) crisis. Some members...

---

### **Department of Education Releases CARES Act Funds**

#### **Step toe & Johnson LLP**

Last week, the Department of Education (Department) released details and guidance regarding its distribution of funds appropriated to institutions of...

---

### **Today in Washington - April 29, 2020: COVID-19 Updates**

Washington

#### **Hall Render Killian Heath & Lyman PC**

The Health Resources and Services Administration will host a webinar for health care providers on the agency's COVID-19 Uninsured Program Portal...

---

### **Paycheck Protection Program Update: More Funds but More Clarity on Economic Uncertainty-Make Sure Your Certification is Accurate**

#### **Kilpatrick Townsend & Stockton LLP**

Applications for the Paycheck Protection Program (PPP) are once again being accepted by lenders after Congress authorized another \$310 billion in...

---

### **IP Watchdog, "Emergency Distance Learning and Fair Use"**

#### **Berger Singerman LLP**

"[A] teacher creates a transformative work, which falls into the protective bubble of Fair Use, when they craft a message, enhance their students'...

---

### **CARES Act Relief Fund Payments to Health Care Providers: Key Requirements and Compliance Risks**

#### **Faegre Drinker Biddle & Reath LLP**

On April 10, 2020, the federal government began distributing \$30 billion of the \$100 billion in funds that the Coronavirus Aid, Relief, and Economic...

---

### **HHS Provides Additional Guidance on Uninsured Funding and Application for the Remainder of General Distribution Funds**

#### **Ropes & Gray LLP**

On April 27th, the Health Resources & Services Administration (HRSA) launched its portal for reimbursement of uninsured COVID-19 testing and...

---

### **Providers Can Now Access Additional \$20 Billion via CARES Act Relief Portal**

#### **Gordon Rees Scully Mansukhani**

All providers with a Medicare billing tax identification number may now apply for a grant from the Phase II CARES Act Provider Relief Fund via the...





## Global

### Employment & Labor



**Business as unusual - What role can business play in shaping a fair and lasting recovery?**

**Freshfields Bruckhaus Deringer**

How we recover from the crisis will shape our societies for many generations. How business responds to this challenge will define their future...

**COVID-19 Summary of Government Financial Support Europe and Middle East**  
**Squire Patton Boggs**

The federal state will provide a guarantee of €50 billion for certain loans issued by financial institutions in Belgium...

**Australia: Competition and Consumer Commission**

**Global Competition Review**

As Australia's competition regulator, the Australian Competition and Consumer Commission (ACCC) is tasked with protecting competitive processes by...

**CMS Expert Guide to Government Support for Employers and Workers**

**CMS Legal**

During previous economic crises, Germany came up with a social instrument called Kurzarbeit ("short-time working") to sustain businesses and save jobs...

**Todos os olhos em mim: dicas práticas para compliance durante e após um período de crise**

**Paul Hastings LLP**

Diretores de compliance, advogados internos e outros gatekeepers corporativos sabem que, mesmo quando a economia está em expansão, a implementação de...

**Our guide to the top 10 employment issues facing the hospitality & leisure industry during COVID-19**

**DLA Piper**

As with other sectors, hotels and establishments have an obligation to ensure a safe workplace for their employees, which includes taking steps to...

**Keeping the Lights on During the Coronavirus Pandemic: Lessons from Around the Globe**

**Baker McKenzie**

COVID-19 and government responses to the growing pandemic are creating unprecedented and rapidly evolving challenges. In the coming days, businesses...



**ENSafrica**

Africa: The African Development Bank Group (AfDB) is ready to provide fast, flexible and effective responses to lessen the severe economic and social...

**Environment & Climate Change**



**World IP Day 2020 - Innovate for a Green Future**

**UDL Intellectual Property**

This year, World Intellectual Property Day (26 April 2020) celebrates innovation for a greener future and seeks to put IP at the heart of efforts to...

**Law and Climate Change: the Paris Agreement grounds plans for a third runway at Heathrow Airport**

**Squire Patton Boggs**

The fight against climate change has increased in the last years. The latest development was in the English Court of Appeal, which handed down a...

**The Future of CORSIA Amidst COVID-19**

**Baker McKenzie**

The balance between promoting greater global connectivity via air travel and protecting the environment against increasing emissions has been a...

**The Latest Court Challenge in a Steady Line of Leading Youth-Led Climate Cases**

**Hausfeld LLP**

Youth climate activists are boldly bringing climate mitigation cases in courts around the world, challenging the inadequacy of respective...

**From the plastics present to a sustainable future**

**Clarivate Analytics**

As part of eXXpedition Round the World, I spent 10 days at sea analyzing the waters to make the unseen seen: microplastics in our oceans. These tiny...

**Modern trends and challenges for supply chains: emerging technologies and environmental consciousness**

**Reed Smith LLP**

Clients are always on the lookout for commercial advice that helps to manage modern trends and current challenges. In the transportation and...

**Ciudades: principal causa del cambio climático y a la vez solución para su mitigación**

**Terraqui**

La integración del cambio climático en la planificación urbana: desarrollo urbano compacto, asentamientos adecuados y resilientes, infraestructura...

**How hard rock and acid might be the answer to greener power**

**Griffith Hack**

The theme of this years' World IP Day is "innovate for a greener future". Griffith Hack is proud of our collaboration with the many organisations and...

## Internet & Social Media



### **FSB consults on cyber-attack response and recovery**

#### **K&L Gates**

The Financial Stability Board (FSB) issued a consultation on a toolkit of measures designed to help ensure firms and regulators are well prepared to...

### **New opportunities for esports growth in Poland**

#### **DLA Piper**

The current pandemic is causing a massive shift in how we spend our free time and what options are available for sport enthusiasts. Since almost...

### **ICANN responds to COVID-19**

#### **Hogan Lovells**

The Internet Corporation for Assigned Names and Numbers (ICANN) recently announced that registrants unable to renew their domain names when they...

### **WIPO panel finds that Danish start-up Acubit engaged in reverse domain name hijacking**

#### **AWA**

Technology start-up Acubit claimed that Danish trademark rules and practice should assign domain names to the relevant trademark owner. A panel from...

### **How COVID-19 has impacted the adtech industry**

#### **Bristows**

As we are all well aware, the impact of the coronavirus is being felt acutely across a broad spectrum of economic sectors and on a global scale...

## Legal Practice



### **COVID-19 Pressure Points: Force majeure considerations in a potential "second wave" of COVID-19**

#### **Herbert Smith Freehills LLP**

As many countries contemplate an easing of COVID-19 lockdown restrictions following a downturn in cases, scientists and politicians are warning of...

### **How to reach out and support your clients**

#### **Globe Law and Business**

This is an unprecedented time for lawyers, for clients and for everyone. Whilst many lawyers may hesitate to pick up the phone for fear of being too...

## Legal Tech



### **COVID-19: Managing the Security Risks of a Remote Workforce**



## **K2 Intelligence/Financial Integrity Network**

As COVID-19 remains prevalent, working remotely has become the new normal. This means that many organizations will have people working from home for...

### **Projects & Procurement**



#### **Coronavirus (COVID-19) updates**

##### **ENSafrica**

Africa: In a statement issued on 13 April 2020, the International Monetary Fund (IMF) Executive Board announced that it has approved relief on debt...

#### **ESG - Risks and opportunities in the Infrastructure investment cycle**

##### **Linklaters LLP**

97%1 of infrastructure companies2 with core and non-core infrastructure assets are exposed to environmental, social and governance (ESG) risks that...

#### **Project Finance Arrangements in General**

##### **L&L Partners (Formerly Luthra & Luthra Law Offices)**

Project finance is a way to finance large infrastructure projects that might otherwise be too expensive or speculative to be carried on a corporate...

#### **Multilateral Lenders and Regional Development Banks**

##### **Veirano Advogados**

Multilateral development banks and regional development banks (MDBs) are international financial institutions created by a group of countries with the...

#### **International: COVID-19 Effects on Large Project Transactions - Summary of Conference Call**

##### **Baker McKenzie**

The importance of China as a hub of global trade has increased substantially since the 2002-2003 SARS epidemic and the COVID-19 disruption to supply...

#### **Projects Global Insight Issue 3, 2020**

##### **DLA Piper**

Contributing to a sustainable future is more important than ever during these uncertain and testing times. Infrastructure and public services are...

#### **Export Credit Agencies and Insurers**

##### **Mayer Brown**

Export credit agencies (ECAs) are national government-owned or affiliated entities that support exports of goods and services from their own countries...

#### **Core Project Agreements**

##### **Morgan Lewis**

To fully appreciate project agreements, it is important to understand their significant role in a project finance transaction, which is essentially a...



## **COVID-19: IP Strategies for Universities and Nonprofits During the Pandemic - Mitigating Patent Infringement Risks When Making PPE and Other Health-Related Supplies**

**K&L Gates**

The rapid emergence of COVID-19 — and the limited and diminishing supply of healthcare resources needed to treat patients and protect healthcare...

---

## **Consider COVID Attitude Changes, Part 3: Higher Levels of Xenophobia**

**Holland & Hart LLP**

What's in a name? In the current pandemic, do you prefer to call it the "coronavirus," or the "Chinese-" or "Wuhan-Virus"? In addition to that choice...

---

## **GBP1 million target hit for Hope and Homes for Children**

**Allen & Overy LLP**

Discover how the money we've raised for our Global Charity Partner is being used to end institutionalisation and how we're extending our partnership...

---

## **COVID-19: Public Health Orders**

**King & Wood Mallesons**

The table below provides a current snapshot of the material restrictions on businesses, venues and movement that have been imposed by the Australian...

---

## **Women leaders are setting an example**

**DLA Piper**

It turns out women leaders are perfectly suited to lead the way in this crisis with a combination of decisiveness, practicality and empathy...

---

## **COVID-19: government response guide for Africa**

**DLA Piper**

As African governments take drastic action to help businesses weather the storm from COVID-19, we have produced a guide to help lay out the measures...

---

## **Driving Research & Development in a Downturn**

**Ellis Terry**

In challenging times, the natural reaction of many businesses is to minimise expenditure in an attempt to ride out the storm. Research and...

---

## **Other top stories**

**COVID-19 Guide for Attorneys and GCs**

---

**Five Interesting Force Majeure Cases from Around the Country**

---

**Preparing For Re-Entry: Key Considerations For Returning Employees To The Workplace Amid The COVID-19 Crisis**

---

**COVID-19: Executing Simple Agreements and Deeds Remotely Under English Law**



---

**Employment-related COVID-19 Litigation Has Begun**

---

**Texas Governor Issues Executive Orders to Reopen Business for Retail and Healthcare Employers**

---

**Employee furlough considerations**

---

**ESG, Capital Access, and the Future of the Oil & Gas Industry**

---

**COVID-19 and the World of Commercial Leases: Force Majeure and Related Common Law Doctrines**

---

**Second Circuit Invokes Standard Contract Provisions to Limit the Use of Agency and Estoppel to Bind Non-Signatories to Arbitration**

---

## **International developments**

**When is talking to your lawyer not a privilege? CAA v Jet2 and RBI v ACE & Ashurst**

---

**Canada Emergency Wage Subsidy Calculator**

---

**COVID-19 and temporary updates to electronic signing**

---

**Job Retention Scheme heads in wrong Direction, with respect (UK)**

---

**Cambodia Legal Update: Ministry of Tourism Issues Notification on Government's Additional Measures Towards Certain Tourism Enterprises Seriously Impacted by COVID-19**

---

**Are Contractors Playing with Fire? Construction Projects and 'Uncertified Revenue'**

---

**International tracker - COVID-19 Restrictions**

---

**Can Private Employers Pay Reduced Salary during Lockdown**

---

**COVID-19 Update #41: Serbia/Montenegro/Bosnia and Herzegovina**

---

**COVID-19 impact on the Hong Kong private education market**

---

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law

[Contact Lexology](#)

[About Lexology](#)



© 2006-2020 Law Business Research



**From:** [CLA Public Section](#)  
**To:** [John Nagel](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, May 01, 2020 2:46:16 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive \(972,542 articles\)](#)



[North America](#) | [Global](#)

**USA**

[North America](#)

Construction



**Pennsylvania 'Builds' Towards Reopening Its Economy: Restrictions Eased On Construction, Motor Vehicle Sales, and Curbside Alcohol Pickup** [Pennsylvania](#)

**Seyfarth Shaw LLP**

On April 20, 2020, Governor Tom Wolf announced his administration's first, limited reopening of Pennsylvania's economy since his March 19 business...

**Pennsylvania Governor Paves Way to Reopen Construction on May 1**

[Pennsylvania](#)

**Pepper Hamilton LLP**

On April 20, Pennsylvania Gov. Tom Wolf amended his March 19, 2020 Order Regarding the Closure of All Businesses That Are Not Life Sustaining. Under...

**Dispute Boards: Another Potential Means of Resolving COVID-19 Disputes**

**Dechert LLP**

COVID-19 has caused a widespread evaluation of how existing therapies could assist in treating this new pathogen. This OnPoint does something similar...

**Recent Court Decision Affects Enforceability of Pay-When-Paid Clauses**

[California](#)

### **Procopio Cory Hargreaves & Savitch LLP**

Construction contracts are exchanged so routinely that it is not uncommon for contractors to give the documents a quick glance or not even read them...

---

### **Washington State Reopens Some Construction, with Restrictions** Washington

#### **Cozen O'Connor**

On April 24, 2020, Washington Governor, Jay Inslee, signed an addendum to Proclamation 20-25 that allows a limited restart to construction projects...

---

### **Do We Still Need Retainage?**

#### **Bradley Arant Boult Cummings LLP**

There have been debates for years about the pros and cons of owners withholding retainage (usually 5% or 10%, depending on each state's retainage...

---

### **Construction Resumes on Pennsylvania in May 1** Pennsylvania

#### **Cozen O'Connor**

On April 22, Governor Wolf unveiled a plan to gradually reopen Pennsylvania's economy after almost a month of shuttering all businesses that were not...

---

### **2020 Construction Planning in the Wake of COVID-19**

#### **Bradley Arant Boult Cummings LLP**

The COVID-19 pandemic swiftly eroded recent gains in the U.S. and world economies and has exposed economic and societal vulnerabilities that many...

---

### **A Short Primer on Force Majeure and Related Defenses, Including Discussion on Their Applicability to the COVID-19 Pandemic**

#### **Akerman LLP**

The current COVID-19 pandemic may result in debtors asserting payment defenses to loans and other contractual obligations based on force majeure...

---

### **Inconsistent Forum Selection Language Affected Enforcement** New Jersey

#### **Commonsense Construction Law LLC**

Courts typically enforce forum-selection clauses unless there is a public policy reason not to do so. A New Jersey appellate court has refused to...

---

### **Webinar Recording: COVID-19's Impact on Public and Private Construction Projects** Video

#### **Seyfarth Shaw LLP**

This webinar is a practical review of the impacts of COVID-19 on public and private construction contracts, including clauses covering delay, impact...

---

### **Guidance for the Federal Contractor in Dealing with a Financially-Distressed Subcontractor During and After the COVID-19 Pandemic**

#### **Crowell & Moring LLP**

The ongoing COVID-19 crisis has caused unprecedented harm to nearly all industries, including those involved in federal government contracts. This...

---



## **New Jersey Shuts Down “Non-Essential” Construction Projects To Mitigate Covid-19 - “Essential” Projects Can Continue Under Certain Conditions**

New

Jersey

### **Ansa Assuncao LLP**

In continuing efforts to flatten the coronavirus infection curve, New Jersey Governor Phil Murphy has ordered all “non-essential” construction...

## **Pennsylvania Construction Projects Can Soon Resume After COVID-19 Shutdown**

Pennsylvania

### **Fisher Phillips**

Pennsylvania Governor Tom Wolf recently announced that construction industry businesses in the state will be permitted to resume operations on May 1...

## **New York’s Phased Plan to Reopen begins with Construction Industry**

New York

### **Cozen O'Connor**

On April 26, 2020, Governor Cuomo broadly described New York’s plan to reopen the state beginning on May 15. Like many other states, New York plans...

## **Bay Area Counties Allow Construction to Recommence on May 4**

### **Manatt Phelps & Phillips LLP**

Effective May 4, 2020, construction projects throughout the Bay Area may recommence, subject to specified protocols. Although Governor Newsom’s...

## **Employee Benefits & Pensions**



## **IRS Extends Filing Deadlines for Employee Benefit Plans**

### **Faegre Drinker Biddle & Reath LLP**

In response to the COVID-19 pandemic, the IRS has issued Notice 2020-23, which automatically extends the deadlines for certain filing obligations...

## **Ninth Circuit Reverses Denial of Longshore Act Benefits to California Widows**

California

### **Goldberg Segalla LLP**

Two widows of California shipyard workers, whose husbands were allegedly exposed to asbestos and died as a result, sought compensation under the...

## **Tax-Qualified Deferred Compensation Plan Sponsors: Considerations for Administration During the COVID-19 Pandemic**

### **McCarter & English LLP**

This Alert discusses certain considerations for tax-qualified retirement plan (in particular, 401(k) and 403(b) Plan) sponsors and fiduciaries in...

## **ERISA Settlements - The Non-Monetary Concessions Continue to Mount**

### **Thompson Hine LLP**

In a prior post, we commented on the growing trend of fiduciaries making non-monetary concessions to settle ERISA fee litigation cases. We observed...

## **Cutting Costs in a COVID-19 World - Reducing or Suspending Company Contributions to a 401(k) or 403(b) Plan**

### **Faegre Drinker Biddle & Reath LLP**

In response to the current economic crisis caused by COVID-19, many companies are considering cost-savings measures to improve their companies'...

---

## **Defined Benefit Plan Annual Funding Notices Have Not Been Delayed**

### **Haynes and Boone LLP**

Although the CARES Act permitted the DOL to delay the deadline for distributing defined benefit plan Annual Funding Notices ("AFNs"), the DOL has not...

---

## **IRS Releases FAQs on Federal Tax Consequences of Payroll Support for Air Carriers and Contractors under CARES Act**

### **Covington & Burling LLP**

The Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") authorizes the Treasury Department to provide payments to passenger air carriers...

---

## **United States: Important Implications Coronavirus Aid, Relief, and Economic Security Act in US**

### **Baker McKenzie**

Coronavirus-Related Distributions. The Act would allow participants in eligible retirement plans to take distributions in 2020 of up to USD 100,000...

---

## **Why an ESOP? Advantages to Employer of Deductible Cash Dividends to ESOP Participants**

### **Hall Benefits Law**

An Employee Stock Ownership Program or ESOP is a way for owners to share the wealth and success of a company with employees. It is often used for...

---

## **Retirement Plan Participant QRDOs**

### **Hall Benefits Law**

Benefits attorneys like to focus on businesses and benefit plan structures for employees. However, there is an overlap between benefits law, family...

---

## **Relief . . . Just a Little Bit - IRS Notice 2020-23: Limited Extensions of Form 5500**

### **Holland & Hart LLP**

In the midst of everything going on, we wanted to point out a few "under the radar" implications of IRS Notice 2020-23. The Notice, issued on April...

---

## **Considerations for Angel and VC Funded Startups and Emerging Growth Companies Considering a Loan under the Paycheck Protection Program**

### **Procopio Cory Hargreaves & Savitch LLP**

What are the eligibility criteria most likely to be of concern to emerging growth companies funded by angel or institutional investors considering...

---

## **Webinar Recording: WARN, Furloughs, and RIFs: Obligations and Best Practices**



## **when considering COVID-19 Workforce Reductions**

Video

### **Seyfarth Shaw LLP**

Is this the time to hold tightly to your current workforce or let some of them go? This remains the No. 1 question on nearly every US employer's mind...

---

## **San Francisco Unveils Plan To Allow Employees to Use Employer Healthcare Funds For Food, Rent, And Utilities During The COVID-19 Pandemic**

### **Fisher Phillips**

Mayor Breed just announced a plan to allow employees in San Francisco to now use funds their employers have contributed in compliance with San...

---

## **IRS and PBGC Issue Relief Extending Certain Employee Benefit Plan Deadlines Due to COVID-19 Pandemic**

### **McCarter & English LLP**

On April 9, 2020, the IRS released Notice 2020-23, which postpones (automatically, without the need for the taxpayer to file for an extension) numer...

---

## **IRS Repurposes Military and Disaster Relief For COVID-19 Deadline Extensions**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 9, 2020, the IRS issued Notice 2020-23, extending federal tax filing deadlines and payment obligations to July 15, 2020...

---

## **Employee Retirement Plans: Cost-Saving Measures and Increasing Employee Monetary Access During COVID-19**

### **Akerman LLP**

With today's uncertainties, employers are addressing their own short term cash needs as well as their employees'/former employees' ability to support...

---

## **Illinois Withdraws Emergency COVID-19 Workers' Compensation Rule**

Illinois

### **Duane Morris LLP**

The Illinois Workers' Compensation Commission has withdrawn its April 16, 2020, emergency rule that would have established that all first responders...

---

## **Client Alert: National Emergency Enables Tax-Free Employee Relief Fund**

### **Bowditch & Dewey LLP**

Once the President declared the COVID-19 pandemic a national emergency on March 13, 2020, in addition to opening access to billions of federal dollars...

---

## **COVID-19 and Retirement Plan Partial Terminations**

### **Greenberg Traurig LLP**

Among the longer-term considerations for employer layoff and furlough decisions is the impact on a single employer pension, profit sharing, or 401(k)...

---

## **Cafeteria Plan Considerations During a Pandemic**

### **Foster Swift Collins & Smith PC**

Many employers sponsor a Code Section 125 cafeteria plan that allows eligible employees to pay for certain health and welfare benefits on a pretax...



---

## **State and Local Tax Responses to COVID-19: Nexus and Apportionment Relief for Employers With Telecommuting Employees [Updated April 22, 2020]**

**Baker McKenzie**

Many employees continue to telecommute due to the COVID-19 outbreak. As discussed in our previous blog post on state tax nexus and apportionment...

---

## **US DOL Provides More Guidance On Pandemic Unemployment Assistance: Restrictions on Eligibility, Summer Break Limitations, Gig Worker Benefits, and More (US)**

**Squire Patton Boggs**

As most everyone now knows, among other things, the massive \$2 trillion-plus CARES Act created multiple federal unemployment compensation programs...

---

## **Tri-Agency FAQs Clarify Group Health Plan Obligations under FFCRA and CARES Act**

**McDermott Will & Emery**

Earlier this month, the Departments of Labor (DOL), Health and Human Services (HHS) and the Treasury jointly issued an FAQ (found here, as updated...

---

## **IRS FAQs on Retention Credit Highlight Aggregation Concerns and Narrow Potential Eligibility**

**Covington & Burling LLP**

Late Wednesday, the IRS released extensive new guidance in the form of Frequently Asked Questions ("FAQs") on the IRS website addressing various...

---

## **The CARES Act Impact: Retirement Plans**

**Hall Render Killian Heath & Lyman PC**

This is the first in a series of articles covering the employee benefits provisions of the Coronavirus Aid, Relief, and Economic Security Act ("CARES...

---

## **ERISA Claims for Cross-Marketing Participant Data Hit a Snag**

**Thompson Hine LLP**

The Seventh Circuit has issued its decision in the much-anticipated case of *Divane v. Northwestern*. The district court below had refused to allow...

---

## **Benefits Briefs in the Time of COVID-19, Part 2: Temporary Expansion of Educational Assistance Programs to Cover Employees' Student Loan Debt**

**Dickinson Wright**

The CARES Act gives employers a way to pay employees' student loan debt on a pre-tax basis during a portion of 2020 through an educational assistance...

---

## **California Provides COVID-19 Paid Sick Leave for Food Sector Workers (US)**

California

**Squire Patton Boggs**

In a move that mirrors the efforts of several local California communities to fill gaps not otherwise addressed by the federal Families First...

---

## **IRS Released New FAQs on Employee Retention Credit**

### **Covington & Burling LLP**

On April 29, 2020, the IRS released new FAQs providing significant guidance on the employee retention credit. We are still analyzing the guidance...

---

## **Wisconsin Employers Making the Best of the Worst: Implementing a Work-Share Program**

[Wisconsin](#)

### **Littler Mendelson PC**

The unprecedented economic conditions brought about by the COVID-19 pandemic have forced many Wisconsin employers to implement layoffs, partial...

---

## **Rolling Over Required Minimum Distributions Already Taken in 2020**

### **Holland & Knight LLP**

To prevent individuals from being forced to liquidate assets in their retirement accounts at greatly reduced values to fund a Required Minimum...

---

## **I Think a Change, a Change Would Do You Good . . . Modifying Deferred Compensation Plan Contributions and Elections During the Pandemic**

### **Holland & Hart LLP**

In response to the unprecedented worldwide COVID-19 pandemic, businesses are turning to cash flow issues resulting from the abrupt economic downturn...

---

## **The CARES Act Contains Changes to Retirement Plan Withdrawal Rules - What Are They? [Part I]**

### **Hall Benefits Law**

Over the past few weeks, the 2019 Novel Coronavirus (or "Coronavirus") has hit businesses (and employees) financially across the U.S. in an...

---

## **SECURE Act Impacts Decision to Name Trust as Beneficiary of Retirement Plan**

### **Lewis Rice LLC**

Signed into law on December 20, 2019, and effective for those individuals who die after December 31, 2019, the SECURE Act made a number of changes...

---

## **Employment & Labor**



## **UPDATED: Emergency legislation and measures around the world (COVID-19)**

### **Lexology PRO**

A list of key recent emergency legislation and measures implemented by nations across the world in response to COVID-19.

---

## **Open for business: how 'essential' businesses can keep their workplace healthy and safe**

### **McDermott Will & Emery**

Most states have issued some form of 'shelter in place' or 'stay at home' order to flatten the curve of COVID-19. As a result, many business...

---

## **IRS Concludes No Statute of Limitations Shields Employers from ACA Liability -**



## **Impacts on Family Businesses**

### **Davis Wright Tremaine LLP**

On February 21, 2020, the Internal Revenue Service (IRS) released a memo to address whether the Employer Shared Responsibility Payment (ESRP) imposed...

---

## **Virginia Increases its Minimum Wage to \$12.00 per Hour by 2023** Virginia

### **Littler Mendelson PC**

On April 22, 2020, during a special legislative session, the Virginia General Assembly voted to approve Governor Ralph Northam's proposed amendment...

---

## **Trade Secret Litigation: Activity on the Rise**

### **Seyfarth Shaw LLP**

As a special feature of our blog—guest postings by experts, clients, and other professionals—please enjoy this blog entry from Neil Eisgruber...

---

## **NEWARK POLICE ISSUE SUMMONSES TO MANUFACTURERS FOR VIOLATING GOVERNOR MURPHY'S EXECUTIVE ORDERS 104, 107, AND 108** New Jersey

### **Porzio Bromberg & Newman PC**

On behalf of manufacturing and logistic companies, Alan Zakin, representing NJMEP, contacted the Attorney General and Governor's office. They were...

---

## **Coronavirus (COVID-19) | Summary of Key International Tax Measures**

### **Hogan Lovells**

This Hogan Lovells Global Tax Practice guide gives You a summary of key measures to date for MNEs In China, France, Germany, Italy, Luxembourg, Mexico...

---

## **COVID-19 Update: CISA Updates Critical Infrastructure Workers Guidance to Provide Additional Recommendations for Government and Businesses and Clarify Scope of Food and Agriculture Sector**

### **Hogan Lovells**

The Department of Homeland Security's (DHS's) Cybersecurity & Infrastructure Security Agency (CISA) revised its interim guidance identifying critical...

---

## **Employment Question of the Day: April 20, 2020**

### **Fredrikson & Byron PA**

My company was either ineligible for, or did not receive, a loan under the Small Business Administration's Paycheck Protection Program (PPP). Is...

---

## **Defendant Seeks Rehearing En Banc On Seventh Circuit's Decision Rejecting Bristol-Myers Squibb In Rule 23 Class Actions**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The battle continues over the applicability of the U.S. Supreme Court's decision in Bristol-Myers Squibb v. Superior Court, 137 S...

---

## **COVID-19: Walking the Line Between Worker Safety and Privacy** Audio

### **Sidley Austin LLP**

The COVID-19 pandemic poses unprecedented challenges for employers. Businesses must walk the line between keeping workers safe and respecting their...

---

### **New York Employers Must Prepare To Provide Sick Leave Benefits in Accordance With New Statewide Sick Leave Law**

New York

### **Kramer Levin Naftalis & Frankel LLP**

As part of its approval of the state budget, New York State recently enacted a paid sick leave law that will apply to all private employers in New...

---

### **Lessons Learned From Walmart: Best Practices For Employers Regarding COVID-19 Preparation and Communication**

### **Porzio Bromberg & Newman PC**

The first COVID-19-related wrongful death lawsuit against an employer has been filed, specifically in Illinois state court, against Walmart[1]. The...

---

### **Unemployment Assistance and the CARES Act: Minimizing Liability for Withdrawing Job Offers**

### **Ogletree Deakins**

Employers across the country are making difficult decisions due to the COVID-19 crisis. The economic downturn has affected current employees in a...

---

### **DOJ and FTC Issue Joint Statement Regarding COVID-19 and Antitrust Violations**

### **Sheppard Mullin Richter & Hampton LLP**

The Department of Justice ("DOJ") and the Federal Trade Commission ("FTC") recently issued a joint statement (the "COVID-19 Statement") regarding...

---

### **All Non-Essential Employees Across New York State Required to Stay Home**

New York

### **Davis Wright Tremaine LLP**

At a press conference on March 20, 2020, New York Governor Andrew Cuomo announced what is effectively a state-wide shutdown, requiring 100 percent of...

---

### **Coronavirus (COVID-19) Update: States & Municipalities**

### **Squire Patton Boggs**

State and municipal governments and other public entities are struggling to navigate unprecedented uncertainty and mounting financial demands. An...

---

### **COVID-19: Planning Ahead at a (Social) Distance—Considerations for Emerging Companies**

### **Wilmer Cutler Pickering Hale and Dorr LLP**

COVID-19 continues to spread at an alarming rate, causing rippling effects throughout our daily lives and profoundly impacting our health, wellness...

---

### **OSHA Issues COVID-19 Guidance for the Construction Workforce**

### **Seyfarth Shaw LLP**



Seyfarth Synopsis: The Occupational Safety and Health Administration (OSHA) has issued an alert listing safety tips (Guidance) employers can follow...

---

### **Employment issues to consider as businesses get ready to re-open after covid-19**

#### **Thompson Hine LLP**

After weeks (if not months) of state "stay-at-home" and "shelter-in-place" orders, social distancing mandates and telework, there may be light at the...

---

### **The Ties That Bind: NLRB Division Of Advice Rebukes Union Limitations On Employees' Right to Resign Membership**

#### **Fisher Phillips**

A recently released Advice Memorandum from the National Labor Relations Board's Division of Advice found unlawful a union's attempt to restrict...

---

### **Minnesota Update: The Latest COVID-19 Developments Impacting Minnesota Employers**

[Minnesota](#)

#### **Littler Mendelson PC**

Note: Because the COVID-19 situation is dynamic, including with new governmental measures each day, employers should consult with counsel for the...

---

### **Bankruptcy is Not a "Get Out of Jail Free" Card: Enforcing Trade Secret Rights and Restrictive Covenants Against Financially Troubled Wrongdoers**

#### **Seyfarth Shaw LLP**

We have previously written about the effects of COVID-19 on the way we currently work, as well as how businesses need to adapt to protect their trade...

---

### **Proposed NYC Essential Workers Bill of Rights Provides Just Cause Termination and Premium Pay for Essential Workers, Sick Leave for Independent Contractors**

[New York](#)

#### **Littler Mendelson PC**

On April 22, 2020, the New York City Council introduced a series of bills in response to the COVID-19 crisis that is ravaging the city. In addition...

---

### **San Franciscans Ordered to Wear Face Masks - Who Pays For Them While At Work?**

#### **Fisher Phillips**

San Francisco has ordered individuals to wear face coverings when they are shopping, taking transit, getting healthcare, or working in a job that...

---

### **San Francisco, San Jose Mandate New COVID-19 Paid Sick Leave Benefits**

#### **McGuireWoods LLP**

As previously reported, in response to the Families First Coronavirus Response Act (FFCRA), California's governor and a growing number of California...

---

### **Tribal Businesses Eligible for Loans / Tax Credits Under the CARES Act**



### **Quarles & Brady LLP**

The Coronavirus Aid, Relief and Economic Security Act (CARES Act) establishes many significant loan programs and tax benefits to help tribal-owned...

---

### **Los Angeles Implements Multiple Employment-Related Measures Responding to COVID-19 Crisis (US)**

#### **Squire Patton Boggs**

Ordinances and Executive Orders require paid sick leave, provide additional protections for grocery, drug store, and food delivery employees, and...

---

### **South Carolina Unemployment Notice Requirements Updated**

South Carolina

#### **Jackson Lewis PC**

South Carolina's Department of Employment and Workforce (DEW) issued a notice effective April 16, 2020, requiring all employers to provide employees...

---

### **Employer Fears of Messing Up During COVID-19 Pandemic**

#### **Bradley Arant Boult Cummings LLP**

Even in pandemic-free times, the world of labor laws and employment regulations is at best confusing to an employer, and at worst...

---

### **NOL Changes and Opportunities in the CARES Act and Revenue Procedure 2020-24**

#### **Pepper Hamilton LLP**

In order to get cash into the hands of taxpayers during the international pandemic caused by COVID-19, Congress enacted the Coronavirus Aid, Relief...

---

### **Mask Up! New York "Essential" Businesses and Nonprofit Organizations Must Provide Face Masks to Public-Facing Employees**

New York

#### **Perlman & Perlman LLP**

All New York "essential" businesses, including nonprofit organizations, must provide face coverings to their employees when in direct contact with...

---

### **Connecticut Extends Time to Comply with Mandatory Sexual Harassment Prevention Training**

Connecticut

#### **Jackson Lewis PC**

Recognizing employers have challenges in ensuring employees complete Connecticut's new mandatory sexual harassment training requirements during the...

---

### **Updated "Stay-at-Home" Order: Executive Order 2020-59**

#### **Foster Swift Collins & Smith PC**

As expected, Governor Whitmer's newest order, Executive Order 2020-59 ("EO 2020-59"), extends Michigan's "stay-at-home" order until May 15, 2020. EO...

---

### **Attendance Bonuses During COVID-19 Rebuilding Can Lead To Unintended Legal Consequences**

#### **Fisher Phillips**

As the nation's political leaders discuss the easing of the various shelter-in-place orders in an effort to re-start the economy, businesses have...

---

### **GAO Set To Launch Flurry of COVID-19 Related Audits**

#### **Covington & Burling LLP**

The Government Accountability Office ("GAO"), often referred to as Congress' watchdog, is ramping up its oversight activities in preparation for an...

---

### **Buchalter Client Alert COVID-19: Takeaways from the DOL's Latest FFCRA FAQs**

#### **Buchalter**

Earlier this week, the US Department of Labor (DOL) added to their long list of Frequently Asked Questions (FAQs) to the Families First Coronavirus...

---

### **West Virginia Supreme Court Upholds Right-to-Work Law** West Virginia

#### **Dinsmore & Shohl LLP**

The Supreme Court of Appeals of West Virginia upheld the constitutionality of the Workplace Freedom Act in a 5-0 decision, with one justice...

---

### **AG Sues China over COVID-19 | Layoffs in AG's Office | FTC Settles with Rent-to-Own Payment Plan Co**

#### **Cozen O'Connor**

Cozen O'Connor Member and former Virginia AG Jerry Kilgore participated in the opening panel for the Attorney General Allianc...

---

### **2020 is hereby incorporated by reference—Maximizing deal value through thoughtful disclosure**

#### **Eversheds Sutherland (US) LLP**

When the last of the cool spring days are behind us, stay-at-home orders are lifted, and M&A activity begins to resume in earnest, the high of the...

---

### **Facing Your Face Mask Duties - A List of Statewide Orders, as of April 22, 2020**

#### **Little Mendelson PC**

Governors and public health officials across the country have implemented stringent measures to help contain the spread of COVID-19, such as stay at...

---

### **Texas Begins Reopening Businesses; Employers May Be Required To Provide Face Coverings** Texas

#### **Fisher Phillips**

Texas Governor Greg Abbott issued a series of Executive Orders on April 17 aimed at beginning the process of reopening the State's businesses. In...

---

### **Smile when you say that!**

#### **Constangy Brooks Smith & Prophete LLP**

Online snark can be an unfair labor practice. If you're going to joke on Twitter about what you'll do to employees if they unionize, be sure to add...

---

### **5 Steps To Reopen Your Workplace, According To CDC's Latest Guidance**



### **Fisher Phillips**

The Centers for Disease Controls and Prevention (CDC) just released guidance to assist employers in making decisions regarding reopening during the...

---

### **Texas employers who do not participate in workers' compensation face heightened workplace liability risks as employees return from COVID-19 quarantine**

Texas

#### **Reed Smith LLP**

Texas employers who have opted out of workers' compensation coverage may face significantly increased workplace risks in the weeks and months ahead...

---

### **Webinar Recording: Coronavirus & Remote Work Force: Best Practices for Protecting Trade Secrets and Intellectual Capital**

Video

#### **Seyfarth Shaw LLP**

Enacting a remote work policy or expanding an existing policy to include remote work at all levels within an organization can have consequences for...

---

### **This Won't Hurt a Bit: Employee Temperature and Health Screenings - A List of Statewide Orders, as of April 23, 2020**

#### **Littler Mendelson PC**

Governors and public health officials across the country have implemented stringent measures to help contain the spread of COVID-19, such as stay at...

---

### **Fluctuating Workweek + Incentive Pay = No Problem—DOL Sends Final Rule to White House**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The U.S. Department of Labor's Wage & Hour Division has entered the final phase of issuing a new rule concerning the fluctuating...

---

### **Department of Labor Provides Further Guidance Regarding Unemployment Under the CARES Act**

#### **Ice Miller LLP**

The U.S. Department of Labor ("DOL") provided additional guidance related to the massive expansion to unemployment benefits under the Coronavirus Aid...

---

### **Employment Law Update: A Guide for Employers and Parents Regarding School and Childcare Center Closures**

#### **Greenbaum, Rowe, Smith & Davis LLP**

New Jersey Governor Phil Murphy recently announced that New Jersey primary and secondary schools (kindergarten through 12th grade) will be closed...

---

### **California grants additional paid sick leave rights to food sector workers**

California

#### **Hogan Lovells**

California food sector workers now have the right to additional paid sick leave, even if they work for large employers exempted from the federal...

---

## **The Anticipated Rise in At-Home Work Injury Claims During the Coronavirus Pandemic**

Mississippi

Texas

### **Foster Swift Collins & Smith PC**

We remain in the midst of a worldwide pandemic. The federal government and all 50 states have declared states of emergency. In an effort to mitigate...

---

## **COVID-19 and Cross-Border Furloughs and RIFs**

### **Vinson & Elkins LLP**

During the last month, we have been talking a lot about the legal challenges involved in laying off or furloughing workers in the United States. How...

---

## **Employment Law Update: EEOC Issues New Guidance on Accommodation Requests; Expands “Undue Hardship” Definition; Provides Guidance for Employers on Employees Returning to Work**

### **Greenbaum, Rowe, Smith & Davis LLP**

On April 17, 2020, the U.S. Equal Employment Opportunity Commission (EEOC) issued updated guidance for employers navigating the complex issues...

---

## **COVID-19 Emergency Local Paid Sick Leave Chart (California)**

California

### **Davis Wright Tremaine LLP**

This summary is for general information only. It is not a full analysis of the matters presented and should not be relied on as legal advice. In...

---

## **Law on COVID19 in Poland - Handbook**

### **Baker McKenzie**

Among other things, new set of regulations contains solutions regarding the remote operation of companies. There are, however, no changes in the...

---

## **Prior Ruling on What Constitutes a Litigation “Emergency” May Not Be a Unicorn After All**

### **Seyfarth Shaw LLP**

As we previously reported, as a result of the COVID-19 crisis, courts across the country are adjourning most appearances, including trials, and...

---

## **New York Issues Guidance On Face Masks For Essential Business Employees**

New York

### **Fisher Phillips**

Governor Cuomo recently issued an Executive Order directing essential businesses to provide face coverings to their employees when in direct contact...

---

## **New York Challenges U.S. Department of Labor’s Final Rule on FFCRA**

New York

### **Ogletree Deakins**

On April 14, 2020, the State of New York filed a lawsuit against the U.S. Department of Labor (DOL) seeking declaratory and injunctive relief in the...

---

## **Protecting Trade Secrets During the Pandemic**

### **Paul Hastings LLP**



As more employees are furloughed and laid-off during the COVID-19 pandemic, now is the ideal time to update your trade secret protection program...

---

### **Facemasks Are the Rule in the Connecticut Workplace**

Connecticut

#### **Ogletree Deakins**

On April 17, 2020, Governor Ned Lamont issued Executive Order 7BB requiring state residents “who [are] unable to or [do] not maintain a safe social...

---

### **COVID-19: Clarification measures to the JobKeeper Rules announced**

#### **MinterEllison**

On 24 April 2020 Treasury announced a number of measures which will be enacted to clarify the operation of the JobKeeper rules. We discuss these...

---

### **New Paid Supplemental Sick Leave for California Food Sector Employers**

California

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 16, 2020, California Governor Gavin Newsom issued Executive Order N-51-20, requiring employers of Food Sector Workers to...

---

### **Virginia Continues Sweeping Employment Reforms**

Virginia

#### **McGuireWoods LLP**

Although Virginia's recent amendments to its Human Rights Act have garnered the most media attention, Gov. Ralph Northam has also signed or proposed...

---

### **Force Majeure in the Age of COVID-19: A Force to be Reckoned With**

New Jersey

#### **Greenbaum, Rowe, Smith & Davis LLP**

As the COVID-19 pandemic continues to wreak havoc on our social, legal, financial, real estate, and healthcare systems, the widespread disruptions...

---

### **COVID-19 Compliance Conversations (VIDEO)**

Video

#### **Bass, Berry & Sims PLC**

In this Episode, Lindsey Fetzer and John Kelly provide a brief overview of compliance considerations related to conducting internal investigations...

---

### **Minnesota Legislative Update: COVID-19 Testing Agreement Initiated**

Minnesota

#### **Faegre Drinker Biddle & Reath LLP**

Governor Walz announced an agreement with the University of Minnesota and the Mayo Clinic to expand the State's ability to test for COVID-19. The...

---

### **[FCRA] No Solace for the Solis's: Empty FCRA Allegation Ends in Dismissal**

#### **Squire Patton Boggs**

In a consumer loan agreement that went south, Citibank wins dismissal of Fair Credit Reporting Act (“FCRA”) allegations levied by pro se Plaintiffs...

---

### **EEOC Provides Updated Guidance on COVID-19 Testing**

#### **Ogletree Deakins**



Employers continuing to operate as essential businesses under the various state closure orders, or that are now beginning to plan to reopen or return...

---

### **COVID-19 in California: Bay Area Counties Join Others in Mandating Face Coverings**

California

**Morgan Lewis**

Several counties and cities in California are requiring individuals to wear cloth face coverings, including those working in or visiting...

---

### **States expand workers' compensation law for "front-line" workers in response to COVID-19**

**Hogan Lovells**

Employers should be aware of recent changes in state workers' compensation laws which expand protections for "front-line" workers in response to the...

---

### **A Leadership Invitation on Inclusion & Belonging During the COVID-19 Pandemic**

**Seyfarth Shaw LLP**

For weeks, leaders in our profession have been living, breathing, and reacting to COVID-19. Thank you for your continued leadership as things change...

---

### **OSHA Issues Temporary Guidance on Using Enforcement Discretion During the Coronavirus Pandemic**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: The Occupational Safety and Health Administration (OSHA) has issued Interim Guidance to advise compliance safety and health...

---

### **COVID-19: Employers Have Options to Provide Relief to Employees and Their Communities**

**Wilmer Cutler Pickering Hale and Dorr LLP**

As the COVID-19 pandemic spreads, the economy has struggled significantly under its new burdens. The impact both domestically and globally has been...

---

### **Employment and compensation**

**Baker McKenzie**

Yes. Pursuant to the National Health emergency declared on March 12, 2020, employees have to notify employers if they have COVID- 19 symptoms...

---

### **DOT and FMCSA Guidance for Managing Disruptions to Regulated Drug and Alcohol Testing Due to COVID-19**

**Ansa Assuncao LLP**

On March 23, the Department of Transportation ("DOT") issued guidance for conducting DOT-required drug and alcohol testing in safety-sensitive...

---

### **Minnesota Executive Order: Some Business May Reopen with 'Non-Critical Exempt' Workers**

Minnesota

**Jackson Lewis PC**

Minnesota State Governor Tim Walz has issued Emergency Executive Order 20-

40, Allowing Workers in Certain Non-Critical Sectors to Return to Safe...

---

### **NLRB Affirms that Employers May Prohibit Employees from Discussing Ongoing Investigations**

**Vorys Sater Seymour and Pease LLP**

Hard to believe these days, but non-Covid-19-related developments do still pop up from time-to-time. Last week, the NLRB gave us one on an issue the...

---

### **What Colorado Employers Need To Know About New Face Covering Requirement**

Colorado

**Fisher Phillips**

Colorado Governor Jared Polis just issued a new Executive Order: "Ordering Workers in Critical Businesses and Critical Government Functions to Wear..."

---

### **Michigan's Newest Stay-At-Home Order: Amendments Employers Need to Know**

Michigan

**Miller Canfield PLC**

On April 24, 2020, Michigan Governor Gretchen Whitmer signed Executive Order 2020-59 (the "Order"). The Order rescinds Executive Order 2020-42 and...

---

### **Don't Forget the Basics When Reopening Your Retail Business: A 5-Point Plan**

**Fisher Phillips**

The COVID-19 coronavirus pandemic that closed hundreds of thousands of business around the country is unprecedented. Fortunately, many retailers were...

---

### **OSHA Issues COVID-19 Guidance for Package Delivery Employers**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: OSHA has issued a COVID-19 guidance for package delivery employers. OSHA offers recommendations to help reduce employees' risk of...

---

### **In the Trenches: Operating During the Crisis: Main Street Lending Program Webinar**

Video

**Nelson Mullins Riley & Scarborough LLP**

Nelson Mullins attorneys held a discussion on Tuesday, April 21 at 11 a.m. On all aspects of the new Main Street Lending Program — a \$600 billion...

---

### **Conducting Trade Secret and Restrictive Covenant Investigations Remotely**

**Seyfarth Shaw LLP**

One of the first things a company should do when it suspects that its trade secrets have been compromised or that an employee has violated...

---

### **New Permitting Requirements Proposed for Construction Projects in the City of Boston**

Massachusetts

**Seyfarth Shaw LLP**

The City of Boston has proposed new safety protocols for construction work deemed essential during the ongoing health emergency caused by the...



---

## **What comes next: Reopening the workplace after COVID-19**

### **Reed Smith LLP**

In light of the COVID-19 pandemic, many U.S. businesses remain shuttered or operating at reduced levels. While the ultimate decision to allow...

---

## **COVID-19: New York State Governor Andrew Cuomo Press Conference Weekly Highlights**

New York

### **Manatt Phelps & Phillips LLP**

Governor Andrew Cuomo provides daily press briefings on the status of New York State's COVID-19 response and expected executive actions. The Manatt...

---

## **Strategies For Developing A Return To Work Action Plan**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: While most of the country is subject to shutdown orders, federal and local leaders are contemplating when and how to bring people...

---

## **Non-Compete Agreements and Restrictive Covenants During COVID-19**

### **Crowell & Moring LLP**

Are non-competes still enforceable in middle of the unprecedented economic disruption caused by COVID-19? Many employers have reacted to the business...

---

## **The Roots Of The CROWN Act: What Employers Need To Know About Hairstyle Discrimination Laws**

### **Fisher Phillips**

Curly, straight, natural, relaxed, braids, dreads, Afro, or weave. Hair in the workplace is a controversial issue that has been flooding the media in...

---

## **Los Angeles Mayor Expands Social Distancing Protocols**

California

### **Barnes & Thornburg LLP**

Los Angeles businesses must adhere to an emergency order issued by Mayor Eric Garcetti regarding providing face coverings. Effective April 16, Mayor...

---

## **Avoiding Employee Complaints and OSHA Inspections When Reopening the Workplace**

### **McGuireWoods LLP**

Since the COVID-19 crisis began, employees have submitted unsafe workplace complaints to the U.S. Occupational Safety and Health Administration...

---

## **Pennsylvania Supreme Court Narrows Independent Contractor Test Under State's Unemployment Law**

Pennsylvania

### **Littler Mendelson PC**

On April 22, 2020, the Pennsylvania Supreme Court issued a decision affecting the classification of independent contractors for purposes of the state...

---

## **Alabama Implements New Strategies as UI Claims Overwhelm Current Structure**

Alabama

### **Ogletree Deakins**

On April 21, 2020, Alabama Governor Kay Ivey held a press conference that addressed business concerns surrounding the COVID-19 pandemic and included...

---

### **Assessing the Pros and Cons of Class Action Waivers in Employment Arbitration Agreements**

#### **Davis Wright Tremaine LLP**

Last year, the U.S. Supreme Court held in *Epic Systems v. Lewis* that class action waivers in arbitration agreements between employers and employees...

---

### **Guidance for Employers Returning to Work; COVID Infections as Worker's Compensation Injuries, and More**

#### **Clingen Callow & McLean LLC**

Many of our clients are operating in a limited fashion pursuant to one of the many exemptions set forth in Governor Pritzker's stay at home order...

---

### **New COVID-19 Stimulus Measure Provides More Aid for Small Businesses, Health Care Providers, and Testing**

#### **Epstein Becker Green**

On the heels of its passage by the U.S. Senate two days earlier, the Paycheck Protection Program and Health Care Enhancement Act (the "Act") was...

---

### **Michigan: Gradual Reopening of Businesses**

Michigan

#### **Jackson Lewis PC**

To gradually reopen businesses in the state while continuing to slow the spread of COVID-19 in Michigan, Governor Gretchen Whitmer's Executive Order...

---

### **Return to Work Post-Coronavirus Checklist**

#### **Cozen O'Connor**

Monitor federal, state, and local closure orders, re-opening guidelines, industry practices, and geographic considerations...

---

### **Contractors Performing COVID-19 Relief Work Should Start Preparing for Whistleblower Complaints Now**

#### **Venable LLP**

Congress has responded to the recent COVID-19 pandemic with relief spending at historic levels, including federal funds that are enabling agencies to...

---

### **COVID-19: Daily Report for Life Sciences and Health Care Companies (10 - 17 April 2020)**

#### **Hogan Lovells**

The Daily Report is a compilation of COVID-19 (coronavirus) news briefs from around the world to help life sciences and health care companies stay...

---

### **The Government's Friendly Reminder for Employers in Times of Crisis: No**



## **COVID-19 Exception to Antitrust Law Exists**

### **Baker & Hostetler LLP**

The pandemic has resulted in worker layoffs, furloughs, and terminations erasing nearly overnight the nation's record low unemployment and ballooning...

---

## **What Does Governor Hogan's Roadmap to Recovery Mean for Maryland Employers?**

Maryland

### **Shawe Rosenthal LLP**

On April 24, 2020, Governor Hogan issued "Maryland Strong: Roadmap to Recovery," his plan for reopening the state as the COVID-19 pandemic crisis...

---

## **Kentucky Launches 'Healthy at Work' Plan for Reopening Economy Safely**

Kentucky

### **Jackson Lewis PC**

Kentucky Governor Andy Beshear is urging a gradual, phased re-opening of the economy — not just on a statewide basis, but on an individual business...

---

## **Employers: Are You Following Michigan's New Mandatory Employee Safety Requirements?**

Michigan

### **Dickinson Wright**

Coronavirus continues to impose hardships on lives around the globe. Employers of American workers have to adjust to constantly-evolving laws and...

---

## **Now More Than Ever, California Employers Need To Stay Abreast Of Working Time and Control Issues**

California

### **Fisher Phillips**

The California appellate courts, and the California Supreme Court, continue to weigh in on significant and compelling wage and hour issues that...

---

## **ERISA Rules Every ESOP Fiduciary Needs to Know to Avoid Breach Claims**

### **Hall Benefits Law**

Employee Stock Ownership Plan (ESOP) fiduciaries are governed by ERISA rules just as administrators of other qualified retirement and benefit plans...

---

## **A Checklist for Loan Forgiveness Under the Payroll Protection Program**

### **Bowditch & Dewey LLP**

With some necessary preparedness and a bit of luck, some U.S. small businesses were able to obtain some financial relief last week thanks to SBA loans...

---

## **President Trump Announces Suspension of Immigration Due to COVID-19, Details Not Yet Available**

### **Greenberg Traurig LLP**

Late on April 20, President Trump tweeted his intention to issue an Executive Order (EO) that "temporarily" suspends immigration into the United...

---

## **COVID-19: PA Construction Guidance - May 1, 2020 Return to Work**



### **Duane Morris LLP**

As the construction industry prepares to resume work, the Wolf Administration today issued guidance for all construction businesses and employees to...

---

### **Executive Order Provides California Food Sector Workers With COVID-19 Supplemental Paid Sick Leave**

#### **Davis Wright Tremaine LLP**

On April 16, 2020, California Governor Newsom signed Executive Order N-51-20, requiring qualifying "hiring entities" to provide two weeks of...

---

### **Potential Pitfalls of Temperature Screenings** California

#### **Cozen O'Connor**

A few short weeks ago, employer-mandated temperature checks would have been considered an overbroad medical exam under the Americans with...

---

### **COVID-19 Washington Update: April 24, 2020**

#### **Kelley Drye & Warren LLP**

Today's federal government actions in response to COVID-19, includes enactment of the Paycheck Protection Program and Health Care Enhancement Act...

---

### **EEOC Issues Technical Assistance on COVID-19 Workplace Issues**

#### **Davis Wright Tremaine LLP**

The Equal Employment Opportunity Commission (EEOC) has issued updated technical assistance to help employers address a number of workplace issues...

---

### **Delaware Employers Must Supply Face Coverings, Hand Sanitizer** Delaware

#### **Fox Rothschild LLP**

Businesses and individuals in Delaware are required to take additional protective measures in workplaces and public settings under Gov. John Carney's...

---

### **Pennsylvania Set to Reopen Construction Sites on May 1, with New COVID-19 Measures** Pennsylvania

#### **Greenberg Traurig LLP**

Pennsylvania construction sites are allowed to return-to-work as of May 1, pursuant to a new order issued April 24, 2020, by Gov. Tom Wolf. Pursuant...

---

### **Virginia Employers Get Ready: New Laws Dramatically Expand Employee Protections and Employer Liability in the Commonwealth** Virginia

#### **Proskauer Rose LLP**

In the wake of Virginia voting in Democratic majorities in both houses of the state legislature last year, the Virginia legislature has passed, and...

---

### **EEOC states that employers may administer COVID-19 tests before permitting employees to enter the workplace**

#### **Hogan Lovells**

In an important development for critical workforces that continue to operate, as

well as businesses planning to reopen, the Equal Employment...

---

**Returning to Work in Arizona: What Employers Need to Do to Prepare** Arizona

**Ogletree Deakins**

On March 30, 2020, Arizona Governor Doug Ducey issued the "Stay Home, Stay Healthy, Stay Connected" order. The order, which went into effect on March...

---

**U.S. Department of Labor Issues Families First Coronavirus Response Act Notice**  
**Morgan, Brown & Joy LLP**

As set forth in our prior alert, and the text of the new Families First Coronavirus Response Act ("FFCRA"), on March 25, 2020, the United States...

---

**Seyfarth Policy Matters Newsletter - April 23, 2020** New York

**Seyfarth Shaw LLP**

Congress Replenishes Paycheck Protection Program (PPP) Through its Phase Four Coronavirus Relief Package. On Tuesday, via unanimous consent, the...

---

**Furloughs as a Response to Coronavirus**

**Morgan, Brown & Joy LLP**

As employers face seemingly endless employment-related decisions as a result of the novel coronavirus (COVID-19) pandemic, many have asked about...

---

**Strong Whistleblower Protections Are Vital During Covid-19**

**Katz Marshall & Banks LLP**

During the coronavirus pandemic, we are now more than ever relying on our governments and health-care providers to take unprecedented action to save...

---

**U.S. Department of Labor Issues Regulations on the Families First Coronavirus Response Act**

**Morgan, Brown & Joy LLP**

Over the past few weeks, MJB has published several client alerts relative to COVID-19 and the Families First Coronavirus Response Act ("FFCRA") which...

---

**Current State of Loan Forgiveness Under the Paycheck Protection Program**

**Lowenstein Sandler LLP**

Now that many clients have received (or are about to receive) the proceeds of Paycheck Protection Program (PPP) loans, we have been fielding many...

---

**Coronavirus Continues to Spread: What Employers Should Do**

**Morgan, Brown & Joy LLP**

On February 13, 2020 we published a Client Alert entitled "Coronavirus: Employer Considerations" that can be found here. We are continuing to monitor...

---

**FERC Reaffirms Obligations Requiring Public Utilities to Address Excess and Deficient Income Taxes Resulting from Tax Act Changes**

**Troutman Sanders LLP**

On April 16, 2020, FERC addressed the American Public Power Association



("APPA") and Exelon Corporation and its public utility subsidiaries...

---

### **Coronavirus Aid, Relief, and Economic Security Act (CARES Act)**

#### **Morgan, Brown & Joy LLP**

On March 27, 2020, the U.S. House of Representatives approved and President Trump signed into law the Coronavirus Aid, Relief, and Economic Security...

---

### **San Francisco Grocery, Drug, And Restaurant Employees - And On-Demand Delivery Contractors - Receive New COVID-19 Protections**

#### **Fisher Phillips**

The San Francisco Board of Supervisors just passed the Grocery Store, Drug Store, Restaurant, and On-Demand Delivery Services Employee Protections...

---

### **California Cities Require Employers to Provide COVID-19 Sick Leave** California

#### **Pepper Hamilton LLP**

Client Alert Three California cities — Los Angeles, San Francisco and San Jose — have recently enacted paid sick leave laws in response to the...

---

### **Out of Sight is Not Out of Mind - Monitoring Workers Working From Home**

#### **Jackson Lewis PC**

Just over a month ago, we provided a high-level checklist to help organizations think about critical issues as employees begin working from home to...

---

### **Today in Washington - April 27, 2020: COVID-19 Updates** Washington

#### **Hall Render Killian Heath & Lyman PC**

Today, the Health Resources and Services Administration ("HRSA") launched a new COVID-19 Uninsured Program Portal so health care providers who have...

---

### **It Is A Global Pandemic, But Is It An FLSA Emergency?** California

#### **Seyfarth Shaw LLP**

Employees under heightened demands to care for their health and families are using time off and sick leave in record numbers. This has left many...

---

### **Illinois to extend stay-at-home order, require face masks May 1** Illinois

#### **Reed Smith LLP**

On April 23, 2020, Illinois Governor J.B. Pritzker announced he will be extending the state stay-at-home order through May 31, 2020. While the new...

---

### **COVID-19 Update: FDA Issues Guidance for Food and Agriculture Sector Businesses on the Use of Masks and What to Do if a Worker is Exposed to or Tests Positive for COVID-19**

#### **Hogan Lovells**

This post summarizes two recent documents the U.S. Food and Drug Administration (FDA) issued for the Food and Agriculture Sector in response to the...

---

### **Ninth Circuit Holds Employers May Provide a Standalone Background Check**

## **Disclosure Concurrently With Other Documents**

### **Littler Mendelson PC**

On April 24, 2020, the Ninth Circuit held that the Fair Credit Reporting Act (FCRA) permits an employer to provide job applicants with a background...

---

## **Employment Question of the Day: April 23, 2020**

### **Fredrikson & Byron PA**

Under Internal Revenue Code (IRC) Section 139, employers may provide non-taxable financial assistance to their employees impacted by a qualified...

---

## **Opening the Doors: Return-to-Workplace Considerations During COVID-19, Part Three: General Workplace Safety Precautions**

### **Covington & Burling LLP**

Whether a company is an essential business or is expecting to reopen its doors in the coming weeks, a number of challenges must be addressed in order...

---

## **A Contractor's Guide for Maintaining OSHA Compliance in the Wake of COVID-19**

### **Gordon Rees Scully Mansukhani**

The U.S. Occupational Safety and Health Administration ("OSHA") requires construction employers to provide a safe workplace for employees...

---

## **The Next Normal: A Littler Insight on Returning to Work - Privacy and Data Security Implications of Employee Screening**

### **Littler Mendelson PC**

By April 30, 2020, the stay-at-home orders imposed in at least 15 U.S. states will have expired. Although the governors of some of these states are...

---

## **COVID-19 Update: Practical Considerations for Employers as They Prepare for a Return to the Workplace**

### **Paul Weiss**

As state and local governments modify stay-at-home directives and non-essential worker restrictions over the coming weeks, employers must consider...

---

## **COVID-19 RIF Checklist: Key Issues to Consider in Reductions in Force**

### **Holland & Knight LLP**

The COVID-19 crisis has demonstrated that even historically successful organizations may be forced to reduce employee headcount to maintain...

---

## **Human Rights Agencies Issue Discrimination / Harassment Guidance Amidst COVID-19 Concerns**

New York

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The U.S. Equal Employment Opportunity Commission ("EEOC"), the New York State Division of Human Rights (the "Division") and the...

---

## **Georgia Employers Receive Guidance On Governor's Back-To-Business Order**

Georgia

### **Fisher Phillips**



As expected, Governor Brian Kemp issued a detailed Executive Order to begin to re-open businesses throughout the state in the hopes that the worst of...

---

### **A Busy Month for the Paycheck Protection Program**

#### **Jenner & Block LLP**

Earlier this month, the Small Business Administration (SBA) launched the Paycheck Protection Program (PPP), Congress's headline-making small business...

---

### **Virginia Minimum Wage Increase Will Take Effect on May 1, 2021** Virginia

#### **Jackson Lewis PC**

Virginia's legislation raising the hourly minimum wage has cleared its final hurdle and is set to take effect on May 1, 2021. As originally passed by...

---

### **Recent Wrongful Death Lawsuit Reveals Liability Theories for COVID-19 Exposure**

#### **Ansa Assuncao LLP**

A wrongful death lawsuit recently filed by the estate of a Walmart Inc. employee in Illinois provides a glimpse of emerging liability theories for...

---

### **Ohio Workers' Compensation System Approves \$1.6B Distribution for State Fund Employers (US)** Ohio

#### **Squire Patton Boggs**

By the end of the April, many Ohio employers with state funded workers' compensation coverage will receive a dividend from the Ohio Bureau of Workers'...

---

米国政府の支援による給与保護プログラム（PPP）の増額資金に基づくローン申込みに  
おける注意点－日系企業にありがちなミスを回避するには

#### **Masuda Funai Eifert & Mitchell Ltd**

米国政府は 給与保護プログラム(Paycheck Protection Program)（ PPP ）によ  
り提供されるローンを通じて さらに米国の中小企業を支援するために追加資  
金を投じると発表しました 中小...

---

### **COVID-19 Furloughs and Layoffs: Are you triggering pension fund withdrawal liability?**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In these uncertain economic times, temporary furloughs and long-term layoffs have become the norm. One concern expressed by...

---

### **Considerations for Returning Employees to Work During COVID-19** Audio

#### **Ogletree Deakins**

As state and local governments begin to lift restrictions related to the COVID-19 pandemic, employers are preparing for the various permutations of...

---

### **EEOC Says Employers Can Administer COVID-19 Tests Before Employees Can Come to Work**



### **Littler Mendelson PC**

In guidance issued on April 23, 2020, the Equal Employment Opportunity Commission (EEOC) stated that employers may choose to administer COVID-19...

---

### **COVID-19 Update: CDC and OSHA Release Interim Guidance for Meat and Poultry Processing Workers and Employers**

#### **Hogan Lovells**

The Centers for Disease Control and Prevention (CDC) and Occupational Safety and Health Administration (OSHA) have issued Interim Guidance on COVID-19...

---

### **Covid-19 pandemic pushes the boundaries of employment law as U.S. sports come to a halt**

#### **Linklaters LLP**

The National Basketball Association (NBA) is credited with triggering the suspension of professional and collegiate sports across the United States...

---

### **New CDC Guidance for COVID-19 Exposed Employees of Essential Businesses**

#### **DLA Piper**

With expanded testing available, employers are increasingly faced with employees who may have been exposed to COVID-19, but want to continue working...

---

### **Los Angeles City Council Moves Forward With Right of Recall and Worker Retention Ordinances**

#### **Davis Wright Tremaine LLP**

On April 22, 2020, the Los Angeles City Council amended and moved forward with two controversial draft ordinances aimed at regulating the order of...

---

### **Georgia Pushes Forward: Latest Order Offers Detailed Reopening Steps and A Preview for Other States**

Georgia

#### **Littler Mendelson PC**

On April 23, 2020, Governor Brian Kemp signed an Executive Order (Order) relaxing the statewide Shelter in Place Order issued on April 2, 2020, and...

---

### **North Carolina Announces Three-Phase Plan to Reopen**

North Carolina

#### **Fisher Phillips**

With North Carolina's Stay at Home order extended through May 8, 2020, leaders focus on testing, tracing, and trends to determine when to re-open the...

---

### **Shutting the Gate: Temporary Worker Excluded From FLSA Collective Action**

Kansas

#### **Barnes & Thornburg LLP**

After conditionally certifying a collective action under Section 216(b) of the Fair Labor Standards Act (FLSA), the U.S. District Court for the...

---

### **Employees Catch a (Meal) Break from the Oregon Supreme Court**

Oregon

### **Littler Mendelson PC**

On April 23, 2020, the Oregon Supreme Court declined to review a ruling by the Oregon Court of Appeals in which employers were held to a standard of...

---

### **L.A. City Council Adopts Right of Recall and Citywide Worker Retention Ordinances**

#### **Manatt Phelps & Phillips LLP**

On April 22, 2020, the Los Angeles City Council considered amendments to two previously proposed ordinances in response to the COVID-19 emergency...

---

### **NYC Council Considering Worker “Bill of Rights” Amid COVID-19 Relief Bills**

New York

#### **Seyfarth Shaw LLP**

During its first-ever remote session, members of the New York City Council have introduced a series of bills aimed at providing relief for...

---

### **New I-9 Form Required but Verification Relaxed for Some Employers**

#### **Akerman LLP**

Amidst the fast changing pace of employer benefits and obligations during the COVID-19 pandemic, the Department of Homeland Security (DHS) has...

---

### **The Next Normal: A Littler Insight on Returning to Work - Recalling Furloughed Employees and the Rehire Process**

#### **Littler Mendelson PC**

After COVID-19 abates, employers may determine that they cannot return all employees to the workforce. Some employers may need to recall employees on...

---

### **Kentucky OSHA is Shutting Down Employers for Lack of Social Distancing**

Kentucky

#### **Fisher Phillips**

Kentucky OSHA (KOSH) has been tasked with enforcing Governor Beshear's Executive Orders (EO) regarding essential businesses and social distancing...

---

### **COVID-19: Read This Before You Take the Temperatures of Your Customers, Visitors or Employees**

#### **Kilpatrick Townsend & Stockton LLP**

You want to reopen your place of business, and certainly do not want to harm your customers or employees in doing so. Safety from COVID-19 in your...

---

### **Employer's Guide for Returning to the Workplace**

#### **Bass, Berry & Sims PLC**

As the U.S. economy reopens in the coming weeks and months, employers are faced with the challenge of bringing employees back to work to a workplace...

---

### **District Court Finds Biometrics Data Vendor May Be Liable for Illinois BIPA Violations**

#### **Holland & Knight LLP**



The U.S. District Court for the Northern District of Illinois held that a vendor of biometric time clocks could be liable for violations of Illinois'...

---

### **Interim Guidance on Site Field Work Decisions Due to Impacts of COVID-19**

#### **Vedder Price PC**

Once again, recognizing that adjustments to the evolving COVID-19 situation continue, on Friday, April 10, 2020, the United States Environmental...

---

### **New California Paid Sick Leave For Food Sector Workers** California

#### **Baker McKenzie**

On April 16, 2020, California Governor Gavin Newsom signed Executive Order N-51-20 ("Order") requiring employers in the food sector to: Provide...

---

### **EEOC Updates Guidance on the ADA, the Rehabilitation Act and COVID-19**

#### **Morgan, Brown & Joy LLP**

On March 18, 2020, the Equal Employment Opportunity Commission ("EEOC") issued guidance about the Americans with Disabilities Act ("ADA") and the...

---

### **New York City Council Introduces COVID-19 Bills Addressing Essential Workers and Paid Sick Leave Coverage** New York

#### **Proskauer Rose LLP**

As previously announced, the New York City Council has introduced an expansive package of COVID-19 bills that, among other things, propose sweeping...

---

### **Massachusetts Governor Issues Emergency Order Limiting On-Site Work to Essential Services and Restricting Gatherings to Maximum of 10** Massachusetts

#### **Morgan, Brown & Joy LLP**

On March 23, 2020, Massachusetts Governor Charlie Baker issued an Emergency Order requiring all businesses that do not provide "COVID-19 Essential...

---

### **The EEOC Continues to Update Guidance on Returning to Work Pandemic-Prepared**

#### **Payne & Fears LLP**

The EEOC continues to update its pandemic preparedness guidance regarding the Americans with Disabilities Act (ADA), the Rehabilitation Act, and...

---

### **EEOC Offers Employers Post-COVID-19 Return-to-Work Pointers (US)**

#### **Squire Patton Boggs**

Since early in the pandemic, the EEOC has been maintaining a Technical Assistance Questions and Answers page, which it updates from time to time. As...

---

### **What Businesses Can Do to Ease the Transition When Reopening Their Doors**

#### **Phelps Dunbar LLP**

As governments start easing stay-at-home orders and other restrictions,

businesses that closed their doors to help contain the COVID-19 spread will...

---

### **OSHA Issues Interim Enforcement Response Plan for COVID-19 Inspections**

**Morgan, Brown & Joy LLP**

On April 13, 2020, the Occupational Safety and Health Administration (OSHA) published an Interim Enforcement Response Plan (Plan) to provide...

---

### **Preliminary Thinking on Reopening a Business: Planning for the End of Stay-at-Home**

**Fried Frank Harris Shriver & Jacobson LLP**

Companies have begun to think about what a reopening of business will look like. The Fried Frank Coronavirus Task Force Resource Center (available...

---

### **Employer Must Show Evidence of Union's Loss of Majority Support to Withdraw Recognition**

**Barnes & Thornburg LLP**

The National Labor Relations Board recently ruled in Kauai Veterans Express, that a Hawaii trucking company violated Section 8(a)(5) of the National...

---

### **Philadelphia Moves Forward with Fair Workweek Law Despite COVID-19**

**Pandemic** [Pennsylvania](#)

**Cozen O'Connor**

On April 21, 2020, the Mayor's Office of Labor issued a post restating the key provisions of the City of Philadelphia's new Fair Workweek law, which...

---

### **New Congressional Aid Package May Help Coops**

**Eversheds Sutherland (US) LLP**

Lawmakers approved an additional \$320 billion in funds for the Paycheck Protection Program, for which some cooperatives may qualify. The funds may be...

---

### **Georgia Allows Most Businesses to Reopen to the Public: What Employers Need to Know**

[Georgia](#)

**Duane Morris LLP**

Reopening the doors of your business can also mean opening the door to lawsuits from customers and employees...

---

### **Planning for Re-Opening: What Owners, Property Managers and Users of Office and Retail Properties Should Consider**

**Buchalter**

Now is the time to prepare for when non-essential businesses will be allowed to re-open after the various state and local COVID-19 shutdown orders...

---

### **America Reopens: What Employers Need To Be Thinking About in Light of the Guidelines**

**Squire Patton Boggs**

On April 16, 2020, President Trump unveiled broad new federal guidelines laying



out conditions for states to begin relaxing the strict measures...

---

### **Motions to Dismiss Granted in ADA Gift Card Cases**

#### **Bryan Cave Leighton Paisner LLP**

A New York federal court has granted motions to dismiss in four separate cases alleging that the failure to offer gift cards in Braille violates the...

---

### **EPA Publishes Draft Risk Evaluation of Perchloroethylene**

#### **Bergeson & Campbell PC**

On April 27, 2020, the U.S. Environmental Protection Agency (EPA) released the draft risk evaluation of perchloroethylene. According to EPA, it...

---

### **ACC Northeast Webinar Recording: Issue Spotting: Litigation Trends in the Post COVID-19 World**

#### **Seyfarth Shaw LLP**

As we begin to focus on what the return to work will look like, as well as what the "new normal" will be, organizations of all sizes will need to be...

---

### **Trade Secret Litigation on the Rise in California: How ADR Can Help** California

#### **Seyfarth Shaw LLP**

Trade secret litigation in California is growing, in both volume and impact. The second-largest plaintiffs' verdict in 2019 was \$845 million, as...

---

### **Essential services — new obligations for B.C. employers**

#### **DLA Piper**

A new order from the Provincial Health Officer on April 14, 2020, has created new obligations for employers who are either essential...

---

### **US antitrust enforcers on high alert for collusion in labor markets during COVID-19 pandemic**

#### **DLA Piper**

As businesses continue to adapt to the ever-changing market dynamics in the wake of the coronavirus disease 2019 (COVID-19) pandemic, the US...

---

### **Illinois Stay-at-Home Order Modified and Extended - What Do Employers Need To Know Before May 1, 2020?** Illinois

#### **Littler Mendelson PC**

Illinois has been under a "Stay-at-Home" Executive Order since March 20, 2020. Among its mandates, the original Stay-At-Home Order closed...

---

### **Colorado Issues Multiple Mandates For Business Operations During "Safer at Home" Phase** Colorado

#### **Fisher Phillips**

The Colorado Department of Public Health issued Public Health Order 20-28 to govern the next phase of Colorado's reopening, labeled "Safer at Home."...

---

### **Essential business provide the framework for a new normal at US worksites**



### **DLA Piper**

As the US economy works its way towards reopening, experiences like those at the Charmin factory will be the new normal. As they say here, these...

---

### **Court Scorches Employer, Upholds Class Arbitration Decision**

#### **Barnes & Thornburg LLP**

In a blistering decision, the U.S. Court of Appeals for the Fifth Circuit upheld an arbitrator's determination that class arbitration was available...

---

### **Telework remote control and monitoring of employees' health data**

#### **Ius Laboris**

The Portuguese Data Protection Authority (CNPD) has recently issued guidelines on the rules regarding remote control of employees on telework, and on...

---

### **Michigan's Third Shelter-In-Place Order Begins To Relax Restrictions On Businesses**

Michigan

#### **Fisher Phillips**

Michigan Governor Gretchen Whitmer issued Executive Order 2020-59, which extends the State's shelter-in-place order until May 15, 2020 while also...

---

### **EEOC Authorizes COVID-19 Testing Before Employees Enter the Workplace**

#### **Gordon Rees Scully Mansukhani**

As employers contemplate reopening the workplace, coordinating concerns of workplace safety and compliance with the Americans with Disabilities Act...

---

### **Empty Rooms - COVID-19's Impact on the Hospitality Industry**

#### **Cadwalader Wickersham & Taft LLP**

The ongoing COVID-19 pandemic has had an unprecedented impact on all sectors of the U.S. economy in a remarkably short period of time, but one of the...

---

### **Employment Question of the Day: April 24, 2020**

#### **Fredrikson & Byron PA**

Yesterday, April 23, 2020, Governor Walz issued Executive Order 20-40 "Allowing Workers in Certain Non-Critical Sectors to Return to Safe Workplaces."...

---

### **Essential Businesses In Pennsylvania, New York, And New Jersey Must Now Require Their Employees To Wear Face Masks Or Face Coverings**

#### **Ansa Assuncao LLP**

Essential businesses throughout Pennsylvania authorized to maintain in-person operations must now require their employees to wear face masks while on...

---

### **Unpacking Exposure Risks for Meat and Poultry Processors: New OSHA/CDC Guidance**

#### **Little Mendelson PC**

While the White House plans to sign an Executive Order to keep meat and poultry processing facilities open, the Occupational Safety and Health...

---

## **Indiana Supreme Court Favors Employee Over Interpretation of “Public Policy” Exception to At-Will Employment.**

Indiana

### **Ogletree Deakins**

In *Perkins v. Memorial Hospital of South Bend* (Case No. 20S-CT-233), a split Indiana Supreme Court ruled in favor of an employee who was discharged...

---

## **Arbitration Agreements Lacking Employer’s Signature Can Be Enforceable, Says Texas Appellate Court (US)**

Texas

### **Squire Patton Boggs**

On April 16, 2020, a three-judge panel of the Court of Appeals for the First District Court of Texas held that an employer could compel a former...

---

## **Amendments to New York’s Wage Theft Prevention Act Includes New Notice Obligations**

New York

### **Littler Mendelson PC**

On April 3, 2020, New York Governor Andrew Cuomo signed the 2020-2021 State Budget bills, which include several amendments to New York’s Wage Theft...

---

## **Colorado Expands Coverage and Amount of Leave under Health Emergency Leave with Pay (HELP) Rules**

### **Littler Mendelson PC**

On April 27, 2020, the Colorado Department of Labor and Employment amended its Health Emergency Leave with Pay (HELP) Rules, which require certain...

---

## **Employer’s Guide for Returning to the Workplace**

### **Bass, Berry & Sims PLC**

As the U.S. economy reopens in the coming weeks and months, employers are faced with the challenge of bringing employees back to work to a workplace...

---

## **COVID-19 Checklist for North Carolina Employers**

North Carolina

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

Brooks Pierce has been honored to have so many North Carolina employers rely on us for up-to-date guidance on personnel matters stemming from the...

---

## **[FCRA] A Bridge Too Far: Ninth Circuit Rejects Former Employee’s “Novel” Interpretation of the FCRA**

### **Squire Patton Boggs**

Last week, in *Luna v. Hansen & Adkins Auto Transp., Inc.*, 2020 U.S. App. LEXIS 13215 (9th Cir. Apr. 24, 2020), the Ninth Circuit rejected a former...

---

## **United States: Mitigating Employment Litigation Claims in the Complex Landscaping of COVID-19**

### **Baker McKenzie**

Employers must provide employees a safe place to work under the Occupational Safety and Health Act’s “General Duty Clause.” This catchall safety...

---



## **Work From Home Cybersecurity Basics: Following Company Practices (United States)**

### **Bryan Cave Leighton Paisner LLP**

As the Covid-19 Pandemic forces more employees than ever before to work from home ("WFH"), businesses face new and different data privacy and...

---

## **Managing Cyber Risk for Research and Higher Education Institutions During COVID-19 Pandemic**

### **Quarles & Brady LLP**

With the attention on COVID-19 prevention, treatment and research, as well as remote work and remote learning, research and higher education...

---

## **New York Reverses Course On Contours Of Paid Voting Time Leave Law** New

York

### **Fisher Phillips**

New York is reverting to its pre-2019 voting leave law, as employers will now only need to provide their workers with two hours of paid voting time...

---

## **DWZ - Drinking While Zooming (And Other Telework Dilemmas)**

### **Shawe Rosenthal LLP**

By now we probably all have seen the YouTube Video of poor Danny, who finished his Zoom video meeting with his colleagues and forgot to end the call...

---

## **Key considerations in designing a return to Work Plan**

### **Shearman & Sterling LLP**

Although it is too early to know when America's workforce will return to offices and other places of work, it is prudent for companies to start...

---

## **President Trump Issues Executive Order Invoking Defense Production Act for Meat and Poultry Processors**

### **Hogan Lovells**

Late yesterday, President Donald Trump issued an Executive Order invoking the Defense Production Act (DPA) to protect the meat and poultry production...

---

## **Massachusetts Nonsolicitation Case Highlights Importance of Choice-of-Law Provisions** Massachusetts

### **Ogletree Deakins**

Many employers have national and international workforces. When entering into contracts with employees, inclusion of a choice-of-law provision is...

---

## **Virginia Human Rights Act Amendment Removes Large Employee Cap; Could Open Floodgate of New Employment Discrimination Cases For Larger Virginia Employers** Virginia

### **Hunton Andrews Kurth LLP**

On Saturday, April 11, 2020 the Virginia Values Act was signed into law. The bill's headlining purpose-- adding gender identity and sexual...

---

## **Nurseries and Garden Stores Permitted to Resume Activities With Conditions Under Executive Order 2020-59**

### **Foster Swift Collins & Smith PC**

On April 24, Governor Gretchen Whitmer issued Executive Order 2020-59 ("EO 2020-59"), which extends Michigan's "stay-at-home" order until May 15...

---

## **Frequently Asked Questions by Public Libraries During COVID-19**

### **Foster Swift Collins & Smith PC**

No. Based on the strict reading of Executive Order 2020-59 ("EO 2020-59"), libraries cannot provide curbside service. In fact, we do not believe EO...

---

## **Proclamation suspending entry of immigrants who present risk to the U.S. labor market during the economic recovery following the COVID-19 outbreak**

### **Miller Thomson LLP**

On Wednesday, April 22, President Trump signed a proclamation (the "Proclamation") suspending entry into the U.S. of certain immigrants who present...

---

## **Supplemental Paid Sick Leave (Immediately) Required in Unincorporated Los Angeles County, California**

### **Little Mendelson PC**

On April 28, 2020, the Los Angeles County Board of Supervisors voted unanimously to enact an interim urgency ordinance to require employers with 500...

---

## **New York State Amends Paid Election Leave Law, Again, to Provide Up to 2 Hours' Paid Voting Leave**

### **Perlman & Perlman LLP**

You may recall that in 2019, New York State's voting leave law was amended to require employers to offer employees "so much working time as will...

---

## **Updated FFCRA Guidance for Employers**

### **Bass, Berry & Sims PLC**

The following guide has been updated with the latest guidance on the employment-related provisions of the Families First Coronavirus Response Act...

---

## **OSHA State Plan Agencies Issue COVID-19 Guidance (US)**

### **Squire Patton Boggs**

Over the past several months, the federal Occupational Safety and Health Administration (OSHA) has steadily issued guidance to both employers and...

---

## **Fifth Circuit Affirms Dismissal of Qui Tam Complaint Due to Lack of Materiality in Significant False Claims Act Decision**

Mississippi

### **Faegre Drinker Biddle & Reath LLP**

The U.S. Court of Appeals for the Fifth Circuit affirmed on April 15, 2020 the dismissal of a non-intervened qui tam action in United States ex rel...

---



## **New York City Council to Consider Legislation Impacting Employers** New York

**Cozen O'Connor**

In response to the COVID-19 crisis, the New York City Council (city council or council) has introduced a package of legislation deemed the "Essential...

---

## **Colorado's "Safer at Home" Order Permits Some Businesses to Reopen with Strict COVID-19 Suppression Measures** Colorado

**Little Mendelson PC**

On April 27, 2020, Colorado began its phased relaxation of the statewide stay-at-home restrictions in place since March 25, 2020, with Governor Jared...

---

## **Ohio Governor Unveils Industry-Specific Protocols for "Responsible Restart Ohio" Amid the COVID-19 Crisis** Ohio

**Duane Morris LLP**

Governor DeWine encouraged employers to use a phased approach to returning employees to the workplace, with "high-risk employees" returning last...

---

## **U.S. Department of Labor Updates Q&A on the Families First Coronavirus Response Act**

**Morgan, Brown & Joy LLP**

Last week, we published a client alert on the United States Department of Labor's ("DOL") questions and answers to assist in the implementation of the...

---

## **Illinois Department of Human Rights Releases Model Sexual Harassment Training** Illinois

**Little Mendelson PC**

In accordance with the Illinois Human Rights Act (IHRA) amendments under Public Act 101-0221 (known as the Workplace Transparency Act), all Illinois...

---

## **EEOC Says OK for Mandatory Employee COVID-19 Testing**

**Venable LLP**

Ordinarily, the Americans with Disability Act (ADA) prohibits an employer from performing medical tests on all of its employees - but these are not...

---

## **Transferring and Fostering Positivity in the Workplace** Audio

**Ogletree Deakins**

Joe Beachboard and Dennis Davis discuss the concept of Emotional Contagion in the workplace. They discuss six techniques for transferring positive...

---

## **Class Notice Interference On The Defense: Court Penalizes Defendants And Attorney**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: In a class action lawsuit alleging multiple fraud claims, a federal court in Illinois granted the Plaintiff's motion to sanction...

---

## **Ohio to Reopen with its RestartOhio Program** Ohio



### **Frost Brown Todd LLC**

On April 27, 2020, Governor Mike DeWine announced his plan to reopen businesses in the State of Ohio. As phase one of “Responsible RestartOhio,”...

---

### **Employment Question of the Day: April 27, 2020** North Dakota

#### **Fredrikson & Byron PA**

Employers have a lot to deal with right now as they attempt to navigate numerous statutory and regulatory changes. Thinking about, and preparing for...

---

### **Opening the Doors: Return-to-Workplace Considerations During COVID-19 Part Two: Potential Screening Measures for Employees Returning to the Workplace**

#### **Covington & Burling LLP**

Whether a company is an essential business or is expecting to reopen its doors in the coming weeks, a number of challenges must be addressed in order...

---

### **New Virginia Whistleblower Law Alters Employment Litigation Landscape**

Virginia

#### **Greenberg Traurig LLP**

Virginia's new whistleblower protection law, the Fraud and Abuse Whistle Blower Protection Act (the Law), will go into effect on July 1, 2020. The...

---

### **COVID-19 Business Liability Considerations in Reopening the Economy**

#### **Ropes & Gray LLP**

As governors across the country contemplate reopening their state economies, businesses may face potential liability if workers, or if customers and...

---

### **Phasing-In: Use of COVID-19 Testing as a “Return to Work” Strategy**

#### **Ropes & Gray LLP**

As “stay-at-home” orders approach expiration or are lifted, it appears that a return to the workplace through “phasing-in” is rapidly approaching...

---

### **Digital Issues for Individuals Working at Home** Audio

#### **Pepper Hamilton LLP**

The Digital Planning Podcast is designed to educate individuals about all things digital in connection with estate planning, business planning and...

---

### **9th Circuit: Providing disclosure with employment documents does not violate FCRA**

#### **Buckley LLP**

On April 24, the U.S. Court of Appeals for the Ninth Circuit affirmed a district court's ruling that an employer that obtained a consumer report for...

---

### **Ninth Circuit: FCRA Does Not Require Disclosure to be Distinct in Time from Other Employment Documents**

#### **Jackson Lewis PC**

The Ninth Circuit recognized that Plaintiff's argument was novel but was thwarted by the statute itself. Plaintiff below, argued on behalf of a class...

---

## **U.S. Department of Labor Issues Q&A on the Families First Coronavirus Response Act**

### **Morgan, Brown & Joy LLP**

Last week, we published a client alert on the Families First Coronavirus Response Act ("FFCRA") which may be found here. On March 24, 2020, the United...

---

## **Opening the Doors: Return-to-Workplace Considerations During COVID-19: Part One: Navigation the Legal Risk of Return**

### **Covington & Burling LLP**

Whether a company is an essential business or is expecting to reopen in the coming weeks, a number of challenges must be addressed in order to...

---

## **COVID-19 UPDATE: U.S. Antitrust Agencies Issue Joint Statement on COVID-19 and Competition in U.S. Labor Markets**

### **Bryan Cave Leighton Paisner LLP**

In a warning to businesses, the Antitrust Division of the U.S. Department of Justice ("DOJ") and Federal Trade Commission ("FTC," collectively the...

---

## **Return to Work: Key Immigration Issues for Employers**

### **Akerman LLP**

As federal, state, and local government authorities pave the pathway to re-opening America in the ever-changing COVID-19 environment, employers...

---

## **Updated EEOC COVID-19 Guidance: The Commission Officially Sanctions Employer Use Of COVID-19 Testing**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In its latest update to guidance for employers in the COVID-19 pandemic, the EEOC has now clarified that employers can test...

---

## **Opening Up Your Workplace Again**

### **Masuda Funai Eifert & Mitchell Ltd**

On Thursday April 16, 2020, President Trump unveiled his "Guidelines for Opening Up America Again" (the "Guidelines"). The Guidelines are designed to...

---

## **Webinar Recording: Pre-employment Background Screening and Drug Testing: Considerations for Employers in the COVID-19 Environment**

### **Seyfarth Shaw LLP**

With courts and other public records and information repositories closed, and laboratories and health care facilities prioritizing COVID-19...

---

## **Wisconsin Federal Court Allows Airline Workers' Uniform Class Claims To Take Flight**

Wisconsin

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The U.S. District Court for the Western District of Wisconsin recently cast doubt on employers' ability to strike the class...

---



---

## **SBA Issues Supplemental Guidance on the Paycheck Protection Program As Congress Replenishes Funding for Small Business Loans**

### **Faegre Drinker Biddle & Reath LLP**

On Friday, April 24, 2020, President Trump signed into law the Paycheck Protection Program and Health Care Enhancement Act, the fourth in a series of...

---

## **Changes to Massachusetts Unemployment Benefits in the Wake of COVID-19**

### **Morgan, Brown & Joy LLP**

In March 2020, in response to the COVID-19 pandemic, the Massachusetts Executive Office of Labor and Workforce Development (EOLWD) and the Department...

---

## **Eleventh Circuit Renders Landmark Decision on ERISA Sanctions**

### **Littler Mendelson PC**

While everyone has been focusing on COVID-19 and still getting used to homeschooling their children, the Eleventh Circuit released a long-awaited (by...

---

## **Let's Get [Back] to Business: Private Means Private**

### **Graydon Head & Ritchey LLP**

I don't know about you, but I cannot help but sing the Mulan song in my head every time that I read the title. I get pumped up a little thinking that...

---

## **Illinois releases model sexual harassment training** Illinois

### **Reed Smith LLP**

On April 28, 2020, the Illinois Department of Human Rights (IDHR) released its model Sexual Harassment Prevention Training ([download here](#)), providing...

---

## **New York Employers: Engage In The Interactive Dialogue With Medical Marijuana Users** New York

### **Jackson Lewis PC**

A New York state court denied summary judgment to an employer that terminated an employee for testing positive for marijuana, when the employee...

---

## **Ohio Businesses Begin Reopening May 1: What Does It Mean For Employers?**

Ohio

### **Fisher Phillips**

Ohio Governor Mike DeWine just unveiled the first phase of a plan to gradually reopen Ohio businesses. It will not be business as usual, however, and...

---

## **Georgia Governor Issues Executive Order Allowing Businesses to Reopen**

Georgia

### **Ogletree Deakins**

On April 23, 2020, Georgia Governor Brian Kemp issued Executive Order (EO) No. 04.23.20.02 entitled "Reviving a Healthy Georgia" to broaden permitted...

---

## **Eleventh Circuit Finds Comparator Evidence Requirement Less Stringent Under**

## **the Pregnancy Discrimination Act**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April, 17, 2020, the Eleventh Circuit Court of Appeals in *Durham v. Rural/Metro Corp.*, No. 18-14687, considered a matter of...

---

## **OSHA Guidance for the Construction Industry During Coronavirus Disease 2019**

### **Greenberg Traurig LLP**

We have issued several GT Alerts on the Occupational Safety and Health Administration's (OSHA) response to Coronavirus Disease 2019 (COVID-19). Our...

---

## **The 'Laker Effect' Continues: Ongoing Uncertainty With PPP Borrowers' Uncertainty Certification**

### **Lane Powell PC**

Probably the best known provision of the CARES Act is the creation of the forgivable payroll protection program (PPP) loan, but the devil truly has...

---

## **Virginia adopts a wave of new employment laws. Part 3 - Wage payment laws**

Virginia

### **Reed Smith LLP**

As we previously reported on April 23 and April 27, 2020, in the midst of the COVID-19 pandemic dominating the news, Virginia Governor Ralph Northam...

---

## **Employment Question of the Day: April 28, 2020**

### **Fredrikson & Byron PA**

Please explain the intersection of Families First Coronavirus Response Act (FFCRA) and the Fair Labor Standards Act (FLSA), which sets the federal...

---

## **Texas Reopens: What Businesses Need To Know**

Texas

### **Baker McKenzie**

On April 27, 2020, Texas Governor Greg Abbott announced details of his plan to reopen Texas businesses in phases, so long as the COVID-19 outbreak...

---

## **California Counties and Cities Issue Face Covering Requirements**

California

### **Ford & Harrison LLP**

In the wake of the global coronavirus pandemic, a number of counties and cities in California have issued Orders requiring residents and visitors to...

---

## **Texas partially reopens businesses effective May 1st**

Texas

### **Reed Smith LLP**

In the first phase of an effort to restart parts of Texas' economy, on April 27, Texas Governor Greg Abbott issued an Executive Order allowing...

---

## **Plaintiffs Prevail in Appeal of Illinois Prevailing Wage Act Case**

### **Barnes & Thornburg LLP**

On March 26, 2020, the Appellate Court of Illinois issued a decision holding that a municipality's failure to stipulate in its contract that the...



---

## **Delaware Governor Issues Order Imposing Obligations on Businesses Regarding the Use of Face Coverings**

Delaware

### **Ogletree Deakins**

On April 25, 2020, Delaware Governor John Carney issued the thirteenth modification of his "COVID-19 State of Emergency" declaration, imposing...

---

## **COVID-19 Update for Georgia Employers**

Georgia

### **Littler Mendelson PC**

Over the past month, the state of Georgia has enacted several measures, largely affecting unemployment and business operations, in response to...

---

## **Client Alert: CDC Releases Reopening Guidance**

### **Bowditch & Dewey LLP**

As local, state, and federal authorities begin to endorse phased reopening plans in response to the COVID-19 pandemic, employers nationwide are...

---

## **What employers need to know about the CARES Act Employee Retention Payroll Tax Credit**

### **Thompson Coburn LLP**

As we previously discussed, the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") provides an employee retention payroll tax...

---

## **Employer Liability for COVID-19 Exposure in the Workplace**

Maryland

### **Goodell DeVries Leech & Dann LLP**

As states and businesses across the United States begin to reopen, businesses need to know whether they will be deemed responsible if an employee...

---

## **Legal Considerations in Determining Whether and How to Construct Protections for Businesses from Liability in Cases Arising from Alleged Exposure to the COVID-19 Virus**

### **Seyfarth Shaw LLP**

There's an old saying in Washington DC, at least among Capitol Hill staff, that one should never throw away their files because old issues will...

---

## **Illinois Publishes Model Sexual Harassment Prevention Training Program**

Illinois

### **Proskauer Rose LLP**

On April 28, 2020, the Illinois Department of Human Rights (the "IDHR") published its model sexual harassment prevention training program, a copy of...

---

## **Businesses Be Ready: California Temporarily Expands Sick Leave Laws**

California

### **Newmeyer Dillion**

California, Los Angeles and San Francisco all temporarily expand their sick leave laws in response to COVID-19. The supplemental sick leave laws...

---

## **Paid sick leave and handwashing for the food sector: new Californian rules**



California

### **Ius Laboris**

California Governor Gavin Newsom has issued an Executive Order requiring employers in the food sector to provide their employees with paid sick leave...

---

### **May an Employer Require Its Employees to Use a Contact Tracing App?**

#### **Jenner & Block LLP**

Businesses around the United States are beginning to reopen and more and more will reopen in the coming months. There is, however, no vaccine for the...

---

### **COVID-19 Likely Responsible for Hike in OSHA "Fatality/Catastrophe"**

#### **Investigations at Healthcare Facilities**

#### **Ogletree Deakins**

Compared to the first three weeks of April in 2019, April 1, 2020, through April 21, 2020, had a 720 percent increase in healthcare facility...

---

### **The Families First Coronavirus Response Act**

#### **Morgan, Brown & Joy LLP**

On March 18, 2020, the United States Senate approved, and President Trump signed into law, a revised version of a novel coronavirus relief measure, H...

---

### **Employment Question of the Day: April 22, 2020 - Part 1**

#### **Fredrikson & Byron PA**

Some employers may be ready to recall employees furloughed during the prior four to five weeks. The COVID-19 pandemic is not over, but maybe funds...

---

### **Re-Opening for Business: Is Your Workplace Ready?**

#### **Akerman LLP**

Employers face a myriad of issues in thinking through whether and how to re-open for business after mandatory closures, or how to thoughtfully phase...

---

### **The Reopening Playbook: What US Employers Should Be Thinking About Right Now**

#### **Baker McKenzie**

With signs that the virus is peaking in the US, and with some state Shelter-in-Place Orders scheduled to be lifted in the coming weeks, employers are...

---

### **What You Need To Know About Kentucky OSHA's Proposed Injury and Illness Reporting Rule Change**

Kentucky

#### **Fisher Phillips**

The Kentucky Labor Cabinet's Department of Workplace Standards released its proposed amendments to its injury and illness recordkeeping and reporting...

---

### **Is the Future U.S. Workplace a Work Share Program?**

#### **Littler Mendelson PC**

In response to COVID-19 and the current economic downturn, employers across the country have experienced a dramatic decline in business and a lack of...

---

## **COVID-19: Re-Opening Issues Checklist**

### **Kilpatrick Townsend & Stockton LLP**

The fluidity of the COVID-19 situation will require businesses to consider a myriad of issues as they navigate the decision as to whether, when, and...

---

## **Updated EEOC Guidance Allows Employee COVID-19 Testing**

### **Barnes & Thornburg LLP**

How far is too far? That is a question most employers are struggling with as they work to maintain workplaces free from COVID-19 and ensure the...

---

## **Business lookouts during covid-19 (part 1)**

### **ProLegal Law Chambers**

Businesses are experiencing unprecedented challenges and market disruption due to Covid-19 pandemic and consequential economic meltdown seems...

---

## **Los Angeles COVID-19 Guidance: Week in Review (April 27, 2020)**

### **Manatt Phelps & Phillips LLP**

On April 22, 2020, the City Council passed Right of Recall and Worker Retention ordinances. The Mayor has indicated that he supports both and will...

---

## **CFAA Battle Heading to the Supreme Court**

### **Seyfarth Shaw LLP**

While it can be hard to remember in a world dominated by COVID-19 headlines, the wheels of justice have not stopped turning at the Supreme Court—even...

---

## **Counting to 500 Under the PPP**

### **Lane Powell PC**

The SBA has again updated their PPP loan FAQs to add FAQ 36. This FAQ, issued Sunday, April 26, provides guidance on how to count employees to...

---

## **Gardeners, Golfers, and Boaters Rejoice! Michigan Extends “Stay Home, Stay Safe” Order but Provides for the Reopening of Certain Businesses and Recreational Activities**

[Michigan](#)

### **Littler Mendelson PC**

On April 24, 2020, Michigan Governor Whitmer issued an Executive Order extending her April 3, 2020 Stay Home, Stay Safe Order through May 15, 2020...

---

## **More Paid Sick Leave in Massachusetts? Bill Would Add Up to 80 Hours of Emergency Leave**

[Massachusetts](#)

### **Fisher Phillips**

The Massachusetts legislature is considering expanding the State’s generous paid sick leave statute to add up to 80 hours of emergency paid sick...

---

## **The Duty to Bargain During the COVID-19 Pandemic**

### **Morgan, Brown & Joy LLP**

In response to the COVID-19 pandemic and its severe nationwide impact to the



economy, employers have had to make many difficult and time-sensitive...

---

### **Massachusetts Department of Unemployment Assistance Announces Implementation of CARES Act and Pandemic Unemployment Assistance**

Massachusetts

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: With the advent of the CARES Act, the Commonwealth of Massachusetts has taken steps to implement Pandemic Unemployment Assistance...

---

### **The Next Normal: A Littler Insight on Returning to Work - Some Lessons from Asia**

#### **Littler Mendelson PC**

The COVID-19 pandemic has had an unprecedented impact on individuals and businesses across the globe. Governments closed their Borders, issued health...

---

### **COVID-19 weekly round-up (20-26 April 2020)**

#### **Lexology PRO**

With new economic data heralding a potential global recession of a kind not seen since the 1930s and possible falls in gross domestic product of...

---

### **Protecting Trade Secrets Without Breaking the Bank (Or Even Negatively Affecting Profits)**

#### **Seyfarth Shaw LLP**

As a result of the COVID-19 crisis, and the effective shut down of most of the US economy over the past several weeks (and for the foreseeable...

---

### **Antitrust Enforcers on Alert for Anticompetitive Conduct Targeting Health Care and Frontline Workers**

#### **Morrison & Foerster LLP**

As much of the U.S. battles COVID-19 by self-quarantining, others fight on the front lines by providing healthcare services, maintaining supply...

---

### **COVID-19: U.S. Employer Checklist: Re-opening Strategies and Return to Work Policies After COVID-19 Outbreak**

#### **K&L Gates**

The following PDF document is a list of suggested practices for businesses to consider during the reopening process. For additional industry-specific...

---

### **EEOC Releases Guidance on ADA Issues and COVID-19 for Employers**

#### **McBrayer McGinnis Leslie & Kirkland PLLC**

On April 17, 2020, the EEOC published updated guidance for employers on how to comply with ADA and other antidiscrimination laws and regulations in...

---

### **Virginia adopts a wave of new employment laws. Part 2 - Worker classification and clampdown on restrictive covenants**

Virginia

#### **Reed Smith LLP**

As we previously reported on April 23, 2020, in the midst of the COVID-19 pandemic that is dominating the news, Virginia Governor Ralph Northam...

---

**San Jose + San Francisco Enact Temporary Emergency Paid Sick Leave Requirements for Employers Not Covered by FFCRA**

**Cooley LLP**

As mentioned in previous Cooley alerts, the federal Families First Coronavirus Response Act (FFCRA) requires private employers with fewer than 500...

---

**Best Practices for Commercial Property Owners/ Operators: Phase One of Reopening the Economy**

**Wilson Elser**

The Federal Coronavirus Task Force issued a three-stage plan last week to reopen the economy, where authorities in each state - not the federal...

---

**NYC Council Proposes Bills Providing Just Cause Discharge Requirements and Premium Pay for Essential Businesses and Expanding Paid Sick Time**

New York

**Davis Wright Tremaine LLP**

On April 22, 2020, the New York City Council referred three bills to committee: two of which would greatly affect the employment practices of...

---

**Reopening Amid COVID-19: Understanding Employees' Protest Rights**

**Fox Rothschild LLP**

With some state and local shutdown orders imposed on nonessential businesses in response to the COVID-19 pandemic set to expire, many employers are...

---

**Federal Stimulus Package Makes Loans Available to Tribal Business Concerns to Help Keep People Employed**

**Quarles & Brady LLP**

Tribal enterprises owned in whole or in part by Federally recognized Indian tribes may be eligible to receive some relief in the form of low-interest...

---

**California Requires COVID-19 Supplemental Paid Sick Leave for Food Sector Workers**

California

**Barnes & Thornburg LLP**

California's Gov. Gavin Newsom has issued Executive Order N-51-20, which requires hiring entities to provide up to 80 hours of supplemental paid sick...

---

**Developments in workplace discrimination guidance in the wake of covid-19**

New

Jersey

**Shearman & Sterling LLP**

Many employers have been forced to consider employee layoffs, furloughs or salary reductions as a way to manage some of the financial hardship...

---

**U.S. COVID-19: New CDC Guidance Allows Potentially-Exposed "Critical Infrastructure Workers" to Remain at Work - with Precautions**

**Bryan Cave Leighton Paisner LLP**



The Centers for Disease Control and Prevention ("CDC") recently issued guidance applicable to "critical infrastructure workers," and safety...

---

### **New York City Commission on Human Rights Forms COVID-19 Response Team**

New York

#### **Littler Mendelson PC**

On April 19, 2020, the New York City Commission on Human Rights (the "Commission") announced that it has formed a COVID-19 response team to handle...

---

### **Updated EEOC COVID-19 Guidance: The Commission Adds New Q&A To Help Employers Understand Their EEO Obligations In These Trying Times**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The EEOC recently released updated guidance for employers trying to navigate the federal anti-discrimination laws in the COVID-19...

---

### **The CARES Act: What Midsize Business Owners and Not-For-Profit Organizations Need To Know**

#### **Cahill Gordon & Reindel LLP**

On March 27, 2020, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act (H.R. 748) (the "CARES Act"). The CARES Act...

---

### **COVID-19-Inspired Changes to New Jersey Family Leave Act**

New Jersey

#### **Davis Wright Tremaine LLP**

On Tuesday, April 14, 2020, New Jersey Governor Phil Murphy signed S2374 into law, extending New Jersey's Family Leave Act to provide job-protected...

---

### **Expect More Employment Discrimination Claims Under New Virginia Values Act**

Virginia

#### **Quarles & Brady LLP**

On April 11, 2020, Virginia Governor Ralph Northam signed into law the Virginia Values Act. This law likely will fundamentally change how...

---

### **CARES Act Offers Assistance to Help Federal Contractors Who Offer Employees Paid Leave**

#### **Hunton Andrews Kurth LLP**

CARES Act Offers Assistance to Help Federal Contractors Who Offer Employees Paid Leave The COVID-19 pandemic is a crisis of both public health and...

---

### **SBA Releases Additional Interim Final Rule Implementing the Paycheck Protection Program; Announces Lapse in PPP and EIDL Appropriations**

#### **Kramer Levin Naftalis & Frankel LLP**

On April 14, the Small Business Administration (SBA) issued an interim final rule, effective immediately, regarding the implementation of the Paycheck...

---

### **Pennsylvania Orders Additional Worker Safety Measures to Combat COVID-19**

Pennsylvania

### **Seyfarth Shaw LLP**

Secretary of the Department of Health Dr. Rachel Levine signed an order on April 15, 2020, later approved by Governor Wolf, that significantly...

---

### **Small Business Coverage Under the Paid Leave Provisions of the FFRCA**

#### **Holland & Hart LLP**

As covered elsewhere in this site, under the FFRCA, all private employers that employ fewer than 500 employees must comply with the emergency paid...

---

### **Key Takeaways for Employers from DOJ/FTC on Antitrust Enforcement Amid COVID-19 Pandemic**

#### **Bass, Berry & Sims PLC**

On April 13, the Antitrust Division of the Department of Justice (DOJ) and the Bureau of Competition of the Federal Trade Commission (FTC)...

---

### **An Updated Practical Guide for Small Businesses to Obtain a Paycheck Protection Loan Under CARES Act**

#### **Manatt Phelps & Phillips LLP**

On April 2, 2020 and April 4, 2020, the Small Business Administration (SBA) issued unusual interim final rules (the Rules) providing further detail...

---

### **Virginia adopts a wave of new employment laws. Part 1 - Expansive discrimination and retaliation protections**

Virginia

#### **Reed Smith LLP**

In the midst of the COVID-19 pandemic that is dominating the news, Virginia Governor Ralph Northam signed into law a slew of bills passed by the...

---

### **Major Tax Changes in the CARES Act**

#### **Roberts & Holland LLP**

The COVID-19 pandemic has disrupted economic life throughout the United States (as it has all over the globe), and Federal, state, and local...

---

### **DC expands COVID-19 related leave requirements**

Washington

#### **Hogan Lovells**

The Mayor of the District of Columbia recently signed two emergency laws that expand obligations of employers to provide leave to employees for...

---

### **Employment Question of the Day: April 22, 2020 - Part 2**

#### **Fredrikson & Byron PA**

Many states have greatly expanded the availability of unemployment compensation benefits to furloughed employees as a result of the economic downturn...

---

### **CARES Act Programs Available to Small Businesses**

#### **Kilpatrick Townsend & Stockton LLP**

The CARES Act provides several programs to assist small businesses impacted by the COVID-19 pandemic, including favorable loan terms, significant...



---

## **Pennsylvania Governor Announces Three-Phase System for Reopening the Commonwealth**

[Pennsylvania](#)

### **Duane Morris LLP**

Governor Wolf stated he plans to begin easing some restrictions on May 8 in certain areas of Pennsylvania that have had a minimal COVID-19 impact...

---

## **A Reminder to Cover Up: When Face Mask Use May Be Required in the Workplace (US)**

### **Squire Patton Boggs**

As employers begin to plan for reopening their businesses after government-imposed shutdown orders, or plan for the return of more workers to their...

---

## **Should Employers Require Employees to Wear Facemasks?**

### **Morrison & Foerster LLP**

As employers begin considering return to work strategies, many are wondering whether they should permit or require individuals to wear facemasks at...

---

## **Work-from-Home Fails**

### **Ford & Harrison LLP**

The COVID-19 situation has left us all scrambling to maintain our professional lives as much as possible. We're coming up with alternate work...

---

## **The Next Normal: A Littler Insight on Returning to Work - Safety and Health**

### **Littler Mendelson PC**

Over a roughly two-month period, COVID-19 has completely upended work as we know it. Businesses across the globe have struggled to function with...

---

## **Summary of CARES Act and FFCRA Tax Credit and Payroll Tax Relief**

### **Troutman Sanders LLP**

The payroll and tax credit programs under the Coronavirus Aid, Relief and Economic Security (CARES) Act and the Families First Coronavirus Response...

---

## **Employers must face it: Face covering requirements growing across states and municipalities**

### **Reed Smith LLP**

As we have previously reported, several states, including New Jersey, New York, Connecticut and Pennsylvania, now require employees, customers and/or...

---

## **U.S. COVID-19: Preparing a Reopening Plan - Five Steps to Take Right Now**

### **Bryan Cave Leighton Paisner LLP**

As state governments and businesses look towards restarting the economy, the consensus is that as the U.S. gradually re-opens, the look and feel of...

---

## **DOL Issues More FFCRA Compliance Guidance on Paid Leaves**

### **Dykema Gossett PLLC**

Guidance Focuses on Concurrent Leave Issues, Hours to be Paid During Leaves,

and Regular Rates of Pay Applicable...

---

**COVID-19 Washington Update: April 22, 2020**

**Kelley Drye & Warren LLP**

Today's federal government actions in response to the COVID-19 pandemic include: Congress Tomorrow, the U.S. House of Representatives is scheduled to...

---

**Finding Fevers: Considerations Before Using Temperature-Detecting Cameras**

**Kelley Drye & Warren LLP**

Last week, the FDA approved the use of telethermographic systems (essentially, heat-sensitive cameras) to detect human temperature during the COVID-19...

---

**10 Practical Tips for Employers to Safeguard Their Trade Secrets During COVID-19**

**Holland & Knight LLP**

As a result of both mandatory government restrictions and voluntary safety measures to combat the spread of coronavirus (COVID-19), many companies...

---

**Los Angeles City Council to Require Businesses to Rehire Former Employees**

**Proskauer Rose LLP**

Employers who have laid off workers due to COVID-19 may soon be required to rehire the laid off workers before they can hire any new employees...

---

**NLRB: Contract Coverage Standard Is No Defense to Unilateral Change Unless CBA 'Explicitly' Says So**

**Jackson Lewis PC**

Provisions in an expired collective-bargaining agreement (CBA) do not cover post-expiration unilateral changes under the National Labor Relations Act...

---

**Putting An ENDS To It: How To Address Vaping In The Workplace**

**Fisher Phillips**

A few months ago, the United States Center for Disease Control (CDC) had linked 2,807 hospitalizations and 68 deaths to e-cigarette vaping associated...

---

**EEOC Publishes Further Guidance for COVID-19 Pandemic Preparedness in Workplace**

**Holland & Knight LLP**

The U.S. Equal Employment Opportunity Commission (EEOC) previously published pandemic guidance originally issued during the H1N1 influenza pandemic in...

---

**Rolling Reopening: Planning for Employment-Related Issues**

**Davis Wright Tremaine LLP**

As we approach May 2020, many federal, state, and local slow-the-spread guidelines and stay-home orders are set to expire. Although some...

---



## **Update on Federal Agency Activity - EEOC, NLRB, OSHA, and DOL - Amidst the COVID-19 Crisis (US)**

### **Squire Patton Boggs**

The COVID-19 pandemic has had a major impact on all aspects of life for all Americans and we are all still adjusting to this new “normal,” which is...

---

## **CARES Act: Business Tax Provisions for Tribal-Owned Businesses**

### **Quarles & Brady LLP**

The Coronavirus Aid, Relief and Economic Security Act (CARES Act) grants many significant tax benefits to help tribal businesses stay afloat and...

---

## **DOL Issues More FFCRA Compliance Guidance on Paid Leaves**

### **Dykema Gossett PLLC**

Guidance Focuses on Concurrent Leave Issues, Hours to be Paid During Leaves, and Regular Rates of Pay Applicable Now that covered employers are...

---

## **Organ Procurement Coordinator Found Exempt Under FLSA Highly Compensated Exemption: A Case Study in the HCE**

### **Fox Rothschild LLP**

I have found a very interesting exemption case involving a rather unique job title that also is very instructive in the interpretation of the Highly...

---

## **Un-PAUSE New York: What Empire State Employers Need to Know About Reopening the Workplace**

New York

### **Ogletree Deakins**

On April 13, 2020, New York Governor Andrew Cuomo, New Jersey Governor Phil Murphy, Connecticut Governor Ned Lamont, Pennsylvania Governor Tom Wolf...

---

## **Keep a Lid on It - The Trump NLRB Reaffirms Employer Ability to Enforce Investigative Confidentiality Rules**

### **Sheppard Mullin Richter & Hampton LLP**

In Apogee Retail, 368 NLRB No. 144 (2019), the NLRB overruled the Obama Board's decision in Banner Estrella Medical Center, 362 NLRB 1108 (2015) and...

---

## **Fifth Circuit examines the job duties required for the highly-compensated employee exemption from overtime pay under the FLSA**

### **Reed Smith LLP**

The Fair Labor Standards Act (FLSA) exempts certain highly-compensated employees (HCEs) from the requirement that they receive overtime pay for hours...

---

## **COVID-19 Washington Update: April 22, 2020**

### **Kelley Drye & Warren LLP**

Today's federal government actions in response to the COVID-19 pandemic include: Congress Tomorrow, the U.S. House of Representatives is scheduled

to...

---

## **Essential Information for Employers on Alabama's Unemployment Benefits and COVID-19**

### **Ogletree Deakins**

The coronavirus pandemic has resulted in critical changes to workforces across the United States. In the state of Alabama, there have been more than...

---

## **OFCCP Remains Active - New Scheduling Letters and Agency Directives Will Impact Audits**

### **Crowell & Moring LLP**

Despite the coronavirus pandemic, the Office of Federal Contract Compliance Programs (OFCCP or "the Agency") remains busy, and there are several...

---

## **4-Step Plan For Handling Confirmed COVID-19 Cases When Your Business Reopens**

### **Fisher Phillips**

Businesses will soon reopen, presenting employers with new challenges as part of the next phase of the COVID-19 pandemic. With no known vaccine or...

---

## **DOL issues new guidance on Families First Coronavirus Response Act (FFCRA)**

### **Reed Smith LLP**

Earlier this month, the US Department of Labor (DOL) promulgated regulations to implement the recently enacted Emergency Paid Sick Leave Act (EPSLA)...

---

## **OSHA State Plan Agencies Issue COVID-19 Guidance**

### **Squire Patton Boggs**

Over the past several months, the federal Occupational Safety and Health Administration (OSHA) has steadily issued guidance to both employers and...

---

## **Operating in the Ordinary Course in Extraordinary Circumstances**

Delaware

### **Weil Gotshal & Manges LLP**

As the COVID-19 pandemic continues to disrupt markets and shake the global economy, the full impact on private equity transactions remains unknown...

---

## **EEOC Clarifies Today That Employers May Test Employees For COVID-19**

### **Crowell & Moring LLP**

The EEOC today updated its online guidance regarding COVID-19 and the Americans with Disabilities Act (the ADA), stating that employers may now test...

---

## **US: IRS, DOL and Treasury Issue Joint News Release**

### **Baker McKenzie**

On Friday, March 20, 2020, the Internal Revenue Service (IRS), US Department of Labor (DOL), and US Department of the Treasury published a joint news...

---

## **COVID-19 Emergency Paid Sick Leave Has Come to Bay Area**

### **Davis Wright Tremaine LLP**



On April 17, 2020, San Francisco implemented an emergency ordinance requiring businesses with 500 or more employees to provide an additional two...

---

### **Federal Reserve Releases Details of Main Street Lending Program**

#### **Troutman Sanders LLP**

On April 9, the Federal Reserve Board released term sheets for its widely anticipated Main Street Lending Program to ensure credit flows to small and...

---

### **South Florida Business & Wealth, "How to Get Employer Tax Credits for Paid Sick Leave, Family Leave"**

#### **Berger Singerman LLP**

The Families First Coronavirus Response Act imposes a mandate on all private employers with fewer than 500 employees (subject to some exceptions...

---

### **Client Alert: "Necessity is the Mother of Invention" - Checklist of Issues to Consider Before Reopening After COVID-19**

#### **Brouse McDowell**

We have witnessed remarkable changes in our everyday lives during the COVID-19 pandemic. Manufacturing businesses are modifying production lines...

---

### **Federal Antitrust Authorities Issue Warning Against Employer Collusion to Disadvantage Essential Service Workers**

#### **Faegre Drinker Biddle & Reath LLP**

On April 13, 2020, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) (collectively, the Agencies) issued their Joint Antitrust...

---

### **Beltway Buzz, April 24, 2020**

#### **Ogletree Deakins**

Despite our elected officials being out of town, there was a lot of action coming out of Congress this week...

---

### **Former EEOC Attorney and Assistant U.S. Attorney Suntrease Williams-Maynard Joins Adams and Reese's Government Investigations and White Collar Defense Practice**

#### **Adams and Reese LLP**

MOBILE, Ala. — Adams and Reese is pleased to announce Suntrease Williams-Maynard has joined the firm's Mobile office as Special Counsel...

---

### **Employers can test for coronavirus, EEOC says**

#### **Constangy Brooks Smith & Prophete LLP**

The Equal Employment Opportunity Commission updated its guidance on COVID-19 yesterday to say that employers could test employees fo...

---

### **COVID-19 and Returning to Work: For Employers, It's Not Too Soon to Plan a Comeback**

#### **Kelley Drye & Warren LLP**

Although the U.S. is still in the thick of the COVID-19 crisis, this is exactly when

employers who are deemed “non-essential” should be developing a...

---

**SEC Announces Largest Whistleblower Award of 2020 - Over \$27 Million**  
**Jackson Lewis PC**

The Securities and Exchange Commission (the “SEC”) announced a whistleblower award of more than \$27 million, representing the largest SEC...

---

**Preparing for the health, legal risks when reopening your business**  
**Adams and Reese LLP**

How is your business preparing to reopen? Adams and Reese attorney Greg Rouchell, a partner and Labor & Employment Team Leader, says in New Orleans...

---

**What Do Eased Restrictions of Michigan’s Reaffirmed Stay-At-Home Measures Mean for Your Business?**

**Dykema Gossett PLLC**

On April 24, 2020, Governor Whitmer reaffirmed the stay-at-home measures set forth in Executive Order 2020-42, amended the scope of that order, and...

---

**Recent Court Case Highlights Limitations Of An “Unlimited” Vacation Policy In California**

California

**Fisher Phillips**

A California state court just created a controversy for those employers in the state that provide unlimited vacation policies for their exempt...

---

**Show Me the Masks: Supplying Face Coverings and Respirators to Essential Employees**

**Morgan Lewis**

Employers are facing issues relating to shortages of respirators and non-surgical face coverings. The ever-evolving local, state, and federal...

---

**OSHA’s Interim Response Plan for Coronavirus Disease 2019 (COVID-19) May Have Been Issued to Guide Agency Action, but It is Just as Useful for Employers**

**Squire Patton Boggs**

Since the COVID-19 pandemic first hit the United States in early 2020, the US Occupational Safety and Health Administration (OSHA) has been issuing...

---

**Immunize Your Organization Against Common HR Claims: Projects to Consider While Sheltering in Place**

**Hopkins & Carley**

In the wake of the shelter-in-place orders issued by many state and local governments, business is anything but normal for most organizations. Human...

---

**Executive Order Relaxes Employer’s Ability to Qualify for Work Share Program and Clarifies Expansions of Unemployment Benefits**

**Miller Canfield PLC**

On Thursday, April 23, 2020, Governor Whitmer issued Executive Order 2020-57.



This Executive Order continues the temporary expansion of unemployment...

---

### **Navigating Employer Obligations to Provide Employees with Masks, Face Coverings**

**Jackson Lewis PC**

As the Centers for Disease Control and Prevention (CDC) continues to study COVID-19, the agency is regularly updating guidance on precautionary...

---

### **Back to Work: Practical Considerations from the U.S. Federal Reopening Guidelines**

**Bryan Cave Leighton Paisner LLP**

On April 16, the White House and the CDC released guidelines for a phased reopening of the U.S. economy. Most states and localities have been under...

---

### **Are You Ready to Reopen? Legal and Practical Issues to Consider**

**Ford & Harrison LLP**

There is mounting pressure to reopen businesses as many, particularly small ones, are struggling to survive under various stay-at-home and...

---

### **OSHA Guidance Marks Dramatic Shift in Enforcement Focus Amid COVID-19 Pandemic**

**Morgan Lewis**

The Occupational Safety and Health Administration has issued a new guidance allowing field offices flexibility in handling COVID-19-related matters...

---

### **Newsom's Executive Order Focuses On Protections for Food Service Workers**

**Fox Rothschild LLP**

It shouldn't surprise anyone that a massive component of California's economy is and has been agriculture and food service, including farming...

---

### **To Provide an N95 Mask or Not to...That is the Question Plaguing Some Employers (US)**

**Squire Patton Boggs**

One of the biggest questions plaguing employers during the COVID-19 pandemic is whether or not to provide employees with respirators—the holy grail of...

---

### **Teamsters Union Lost Most Members in 20 Years in 2019**

**Jackson Lewis PC**

According to an analysis by Bloomberg Law Daily Labor Report, the Teamsters Union lost almost 65,000 members in 2019, the largest decline in the...

---

### **OSHA Issues COVID-19 Guidelines for the Construction Workforce**

**Smith Currie & Hancock**

During the course of COVID-19, the CDC and other government entities have provided workplace guidelines in an attempt to flatten the curve and reduce...

---

### **As America Prepares to Return to Work, EEOC Approves Testing Employees for**

## **COVID-19**

### **Sheppard Mullin Richter & Hampton LLP**

The U.S. Equal Employment Opportunity Commission (EEOC) updated its guidance concerning COVID-19, affirming an employer's ability to medically test...

---

### **Client Alert: EEOC Releases "What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws"**

#### **Bowditch & Dewey LLP**

The U.S. Equal Employment Opportunity Commission (EEOC) has recently released Q&A guidance titled "What You Should Know About COVID-19 and the ADA..."

---

### **Unemployment alphabet soup: Here's what it means**

#### **Constangy Brooks Smith & Prophete LLP**

The federal CARES Act has some very important provisions related to unemployment benefits for people who have lost their jobs, been fur...

---

### **Workforce Planning During COVID-19**

#### **Fox Rothschild LLP**

In the midst of the COVID-19 pandemic, employers face monumental decisions on how to keep their businesses alive. Given the uncertain duration of...

---

### **Integrity Tests: To Test Or Not To Test, That Is The Hiring Question**

#### **Fisher Phillips**

Employers often use tests and other selection procedures to screen applicants for hire and employees for promotion. There are many different types...

---

### **Surging Unemployment Claims Pose New Challenges to Employers - Are You Ready?**

#### **Foster Garvey**

Employers: Brace for unemployment benefit inquiries, watch for legal pitfalls, and consider federal relief programs in managing payroll and position...

---

### **Is This an "Emergency"?**

#### **Breazeale Sachse & Wilson LLP**

Many businesses have been in an "all hands on deck" mode for several weeks now, with no real end in sight. Employees are being asked to do whatever...

---

### **OSHA's Interim Response Plan for COVID-19 May Have Been Issued to Guide Agency Action, but It is Just as Useful for Employers (US)**

#### **Squire Patton Boggs**

From our colleagues at the FrESH Law Blog comes a post analyzing the US Occupational Safety and Health Administration's (OSHA) recent Interim...

---

### **Supreme Court to Consider Scope of CFAA**

#### **Akin Gump Strauss Hauer & Feld LLP**



Key Points The U.S. Supreme Court will review whether a person who is authorized to access information on a computer for certain purposes violates the...

---

### **NLRB Rejects Hospital's Bid to Stay Representation Election based on COVID-19 Pandemic**

**Jackson Lewis PC**

In an unpublished decision, the National Labor Relations Board (NLRB) has denied an acute-care hospital's request to stay a representation election...

---

### **Warming Up to Employee Temperature Checks: Employer Guidance From the EEOC and NYC**

New York

**Fox Rothschild LLP**

Although many New York businesses are temporarily closed due to the COVID-19 pandemic and the state's stay-at-home orders, employers that remain open...

---

### **Restrictive Covenants in the Time of Coronavirus**

**Ogletree Deakins**

The spread of the coronavirus disease 2019 (COVID-19) has led to changes regarding many legal issues. Despite the changes, companies still need to...

---

### **EEOC Confirms Employer-Mandated COVID-19 Testing Does Not Violate the ADA**

**Hunton Andrews Kurth LLP**

On April 23, 2020, the EEOC updated its Technical Assistance Questions and Answers, "What You Should Know About COVID-19 and the ADA, the..."

---

### **DOJ and FTC Warn Employers Against COVID-19-Related Business Collusion**

**Ogletree Deakins**

The United States Department of Justice's (DOJ) Antitrust Division and the Federal Trade Commission (FTC) warned employers in a joint statement...

---

### **The COVID-19 pandemic may spur union organizing and complicate union relations: Part Two**

**Constangy Brooks Smith & Prophete LLP**

The Coronavirus pandemic has shuttered much economic activity and forced employers to make business decisions in response to a rapidly shifting legal...

---

### **What is the Impact of President Trump's Temporary Immigration Suspension?**

**Holland & Hart LLP**

In light of the impact of COVID-19 on the U.S. labor market, on Monday President Trump tweeted "I will be issuing a temporary suspension of..."

---

### **Musicians Reach Deal on AB5 Exemption**

**Fox Rothschild LLP**

California's music industry finally came to an agreement with lawmakers on pending amendments to California's Assembly Bill 5 (AB5). The amendments...

---

## **COVID-19: CARES Act Employer Payroll Retention Tax Credit**

### **K&L Gates**

The recently passed Coronavirus Aid, Relief, and Economic Security Act (the “CARES Act”) provides a tax credit for eligible employers to encourage...

---

## **Maintaining Trade Secrets Amid the COVID-19 Pandemic**

### **Dickinson Wright**

Over the last few months, the widespread transmission of the coronavirus disease of 2019 (COVID-19 or the “coronavirus”) has prompted immediate...

---

## **COVID-19 Washington Update: April 23, 2020**

### **Kelley Drye & Warren LLP**

Today’s federal government actions in response to COVID-19, includes House passage of the Paycheck Protection Program and Health Care Enhancement Act...

---

## **EEOC Opines on COVID-19 Testing by Employers**

### **Jackson Lewis PC**

In the past few weeks, the EEOC has updated its What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws on...

---

## **Federal and State Protections for Nonprofits Navigating the COVID-19 Pandemic**

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

The COVID-19 pandemic creates a unique set of circumstances for nonprofits. Many of them are facing similar challenges to for-profit businesses — how...

---

## **SCOTUS to Hear CFAA Case**

### **Jackson Lewis PC**

It’s not often that a case in our practice area reaches the Supreme Court of the United States, so we are genuinely excited! In *Van Buren v. United...*

---

## **Updated EEOC COVID-19-Related Workplace Guidance**

### **Wilson Elser**

On April 17, 2020, the EEOC issued updates to its recently revised technical assistance guidance to address questions arising under the federal Equal...

---

## **EEOC Says Employers Can Require COVID-19 Testing**

### **Lane Powell PC**

The EEOC has issued welcome guidance for employers who are seeking to take all steps necessary to eradicate the virus from their facilities. This...

---

## **What Employers Should Know About Bringing Employees Back into the Workplace.**

### **McBrayer McGinnis Leslie & Kirkland PLLC**

By now, all businesses in the Commonwealth of Kentucky have experienced at least five weeks of interrupted operations. Some businesses have faced a...

---



## **Court Halts Enforcement of Illinois's New Workers' Compensation Rule That Presumes COVID-19 Infections Are Work-Related**

**Ogletree Deakins**

On April 13, 2020, the Illinois Workers' Compensation Commission established an emergency rule amending the Illinois Administrative Code for workers'...

---

## **COVID-19 OSHA Follow-Up: Agency Updates and Additional Recommended Employer Practices**

**Holland & Knight LLP**

The fast-moving developments in response to the novel coronavirus (COVID-19) require employers to remain diligent with following published federal...

---

## **Summary of CISA Guidance on Essential Critical Infrastructure Workforce 3.0**

**Spencer Fane LLP**

On April 17, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released version 3.0 of its guidance to help state and local...

---

## **Is a Global Pandemic a De Minimis Hardship? EEOC Guidance on COVID-19 and Religious Accommodation**

**Ogletree Deakins**

As government officials at all levels continue issuing guidance on best practices for employers to help mitigate the spread of COVID-19, some...

---

## **U.S. COVID-19: As the FFCRA Goes Live, the DOL Continues to Publish Revised and New Guidance for Employers**

**Bryan Cave Leighton Paisner LLP**

Although the federal Department of Labor ("DOL") declared April 1 - 17 to be a temporary period of non-enforcement of the Families First Coronavirus...

---

## **COVID-19 Washington Update: April 27, 2020**

**Kelley Drye & Warren LLP**

Following is an update on COVID-19-related federal government actions since our last update. Congress remains in recess, with both chambers...

---

## **What Employers Should Know About Bringing Employees Back into the Workplace, Part II**

**McBrayer McGinnis Leslie & Kirkland PLLC**

In our first set of guidance on reopening workplaces, we focused on basics of providing a safe working environment, compliance with ADA...

---

## **5 Steps Healthcare Employers Should Take To Address COVID-19 Anxiety And Complaints Over Working Conditions**

**Fisher Phillips**

Across the country, pockets of healthcare workers are protesting working conditions that they claim are unsafe and expose them to greater risk of...

---

## **Workers' Compensation Claims During the Pandemic and Mitigating the Risk**

### **Sheppard Mullin Richter & Hampton LLP**

While essential workers continue to make their way into the office amid the pandemic, many other Californians have been ordered to shelter in place...

---

### **Practically Speaking: A Series of Practical Tips for Employers in Navigating COVID-19**

#### **Krieg DeVault**

No matter the line of business, every employer has been impacted by the Coronavirus of...

---

### **What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws**

#### **Payne & Fears LLP**

The EEOC recently updated its guidance, What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws, including...

---

### **Connecticut Updates Safe Workplace Rules for Essential Employers and COVID-19**

#### **Day Pitney LLP**

On April 24, the Connecticut Department of Economic and Community Development (DECD) updated its Safe Workplace Rules for Essential Employers. The...

---

### **Construction Industry at Core of Post-COVID-19 Debates**

[Pennsylvania](#)

#### **Duane Morris LLP**

Who is in the best position to sustain the loss? And what outcome is in the overall best interests of industry, economy and the public at-large...

---

### **Rocky Mountain Region COVID-19 Employment Update (CO, ID, MT, NE, NM, UT, WY) (April 28, 2020)**

#### **Gordon Rees Scully Mansukhani**

The Rocky Mountain Region COVID-19 Employment Update provides information about COVID-19 orders in Colorado, Idaho, Montana, Nebraska, New Mexico...

---

### **Does The FLSA "Emergency" Exception Apply To You?**

#### **Breazeale Sachse & Wilson LLP**

Many businesses have been in an "all hands on deck" mode for several weeks now.. Employees are being asked to do whatever is necessary to keep our...

---

### **Feds Provide COVID-19 Guidance To Meat And Poultry Processing Employers**

#### **Fisher Phillips**

Two federal agencies just released guidance for the meat and poultry packing industry to address the unique challenges it faces in light of COVID-19...

---

### **CDC Adds New Symptoms for COVID-19 Screening - Employers Must Adjust Accordingly**

#### **Dinsmore & Shohl LLP**



On April 26, 2020, the U.S. Center for Disease Control and Prevention (CDC) updated its guidance to add six new symptoms of COVID-19. Based on this...

---

#### **COVID-19 Washington Update: April 27, 2020**

##### **Kelley Drye & Warren LLP**

Following is an update on COVID-19-related federal government actions since our last update. Congress remains in recess, with both chambers...

---

#### **COVID-19 and Business Operations/Reopening, Cybersecurity from Home, and SEC Whistleblower Activity**

##### **Bryan Cave Leighton Paisner LLP**

The devastating impact of the Coronavirus (COVID-19) needs no introduction. BCLP has consolidated all of its client alerts regarding Coronavirus...

---

#### **The Virtues And Vices Of Voluntary Attendance Policies In The COVID-19 Era**

California

##### **Fisher Phillips**

The COVID-19 pandemic has forced employers to scramble to find novel responses to new workplace challenges, and one such innovation has been the...

---

#### **To Record or Not To Record, That is the Question: Questions and Answers Regarding U.S. Federal OSHA Recordkeeping and Reporting Requirements During the COVID-19 Crisis**

##### **Bryan Cave Leighton Paisner LLP**

The federal Occupational Safety and Health Act and its implementing regulations require employers to record certain work-related injuries and...

---

#### **Back to Business After COVID-19: Addressing Disability Accommodation Requests in New York**

New York

##### **Fox Rothschild LLP**

Though the Equal Employment Opportunity Commission (EEOC) has yet to find that a COVID-19 diagnosis, in and of itself, would be considered a...

---

#### **Developing Leave Policies to Keep Up with the FFCRA**

##### **Krieg DeVault**

Many employers that did not previously have a sick time policy or a Family and Medical Leave Act (FMLA) policy are now having to address employee...

---

#### **Governmental Oversight and CARES Act Funds: Recent Treasury Department Guidance**

##### **Dinsmore & Shohl LLP**

After the nearly \$350 billion in funds allocated to the Paycheck Protection Program (PPP) under the CARES Act were depleted in mid-April, Congress...

---

#### **What Mine Operators Can Expect after the Pandemic: MSHA Will Soon Push Its Regulatory Agenda**

##### **Fisher Phillips**

As the country begins to reopen, many mine operators are contemplating next steps for their own operations. One certainty is that the Mine Safety and...

---

### **Workplace Safety and COVID-19: OSHA's Interim Enforcement Guidance and What It Means for Employers**

**Krieg DeVault**

The Occupational Safety and Health Administration (OSHA) of the U.S. Department of Labor (DOL) works to enforce the federal Occupational Safety and...

---

### **The DOL and the IRS Jointly Provide Relief from Certain Timeframes Applicable to Health and Welfare and Pension Plans**

**Haynes and Boone LLP**

On April 28, 2020, the IRS and DOL issued a Final Rule extending certain timeframes under ERISA and the Internal Revenue Code for group health...

---

### **Nota Bene Episode 77: Labor, Employment, and Immigration in a Pandemic World with Kelly Hensley, Denise Giraudo, and Greg Berk**

[Audio](#)

**Sheppard Mullin Richter & Hampton LLP**

Furloughs. Layoffs. Loss of work visas. The state of employment in the U.S. is in flux due to the coronavirus, and employers and employees are left to...

---

### **NLRB: Employer Right to Take Unilateral Action Under a Collective-Bargaining Agreement Does Not Survive the Expiration of the Agreement Absent Explicit Language to the Contrary**

**Hunton Andrews Kurth LLP**

In a recent decision of first impression, the NLRB held that its contract coverage doctrine does not apply to changes to the terms and conditions of...

---

### **Business Roundtable Releases Roadmap for Resumption of Economic Activity**

**Paul Weiss**

The coronavirus pandemic has forced the business community to implement and abide by unprecedented restrictions in an effort to maintain their...

---

### **Los Angeles County Implements Supplemental Paid Sick For COVID-19 Purposes**

**Fisher Phillips**

The Los Angeles County Board of Supervisors just unanimously approved a Supplemental Paid Sick Leave designed to fill in the gaps between the...

---

### **Return-to-Work Checklist for Employers Reopening Their Businesses**

**Dinsmore & Shohl LLP**

In anticipation of federal and state restrictions lifting as COVID-19 cases and deaths decrease, employers should start planning their employees'...

---

### **EEOC Issues Guidelines on COVID-19 Testing of Employees**

**Cozen O'Connor**



On April 23, 2020, the U.S Equal Employment Opportunity Commission (EEOC) published updates to the Frequently Asked Questions (FAQ) that it...

---

### **Reopening America - Employers Facing Paid Leave Issues Under the FFCRA** **Ford & Harrison LLP**

As the "Reopening of America" begins, many employers will be faced with implementing the paid leaves provided by the Families First Coronavirus...

---

### **Defense Production Act: Order Directing Continued Operation of Meat and Poultry Processing Facilities for the National Defense** **Mayer Brown**

By Executive Order ("EO") dated April 28, 2020, President Trump invoked the authority of the Defense Production Act ("DPA") to direct that meat and...

---

### **[UPDATED] Coronavirus: Federal and state governments work quickly to enable remote online notarization and SBA PPP loans to meet global crisis**

[Georgia](#)

[Maryland](#)

[Pennsylvania](#)

[Florida](#)

### **DLA Piper**

As more businesses are forced to work remotely due to the coronavirus disease 2019 (COVID-19) crisis, several federal and state governments are...

---

### **What We Do in the Shadows: Vampires Disregard Wage and Hour Rules for Human Familiars**

#### **Ford & Harrison LLP**

As our family continues to practice social distancing, we are always on the lookout for a new comedy series to take a bit of the bite out of this new...

---

### **Benefits Briefs in the Time of COVID-19, Part 1: Federal Agencies Relax Summary of Benefits and Coverage ("SBC") Disclosure Deadlines**

#### **Dickinson Wright**

Recent guidance from the Department of Labor ("DOL"), Health and Human Services ("HHS") and Treasury (the "Departments") provides limited enforcement...

---

### **COVID-19 Social Media Considerations for Employers with Employees Returning to Work**

#### **Holland & Knight LLP**

Even those employers with the best social media policies can be placed in difficult positions when confronted with negative social media usage by...

---

### **San Francisco Amends Public Health Emergency Leave Ordinance and Issues Implementation Guidance**

#### **Fox Rothschild LLP**

San Francisco has amended the Public Health Emergency Leave Ordinance (PHELO) it originally passed on April 7, 2020 (as discussed in this previous...

---

### **U.S. Supreme Court Will Finally Weigh in on Scope of CFAA**

### **Jackson Lewis PC**

The United States Supreme Court recently granted a petition for certiorari in *Van Buren v. United States* addressing the issue of whether it is a...

---

### **Plan Now for Bringing Back Your Work Force**

#### **Pierce Atwood LLP**

As hard as it may be at times to believe this, the day will soon...

---

### **San Francisco's COVID-19 Paid Sick Leave Ordinance Takes Effect**

#### **Duane Morris LLP**

On April 17, 2020, Mayor Breed signed an amended version of the Public Health Emergency Leave ordinance...

---

### **COVID-19 Return to Work Policies - Are You Ready?**

#### **Adams and Reese LLP**

Employers of non-essential workers are gearing up for office re-openings all over the country. Employers are anxious—and rightfully so—

---

### **EEOC Guidance Permits Employers to Test Employees for COVID-19**

#### **Dinsmore & Shohl LLP**

On April 23, 2020, the Equal Employment Opportunity Commission (EEOC) released new guidance that permits employers to test employees for COVID-19. In...

---

### **Plan Ahead, Employers: NLRB Ordering Mail Ballot Elections Because of COVID-19 Pandemic**

#### **Jackson Lewis PC**

Recent representation case decisions and directions of election by National Labor Relations Board (NLRB) Regional Directors strongly suggest that...

---

### **Fifth Circuit Holds Day Rates Do Not Satisfy the Salary Basis Test**

#### **Holland & Knight LLP**

The U.S. Court of Appeals for the Fifth Circuit on April 20, 2020, held that a "day rate," or flat amount paid for each day actually worked, does not...

---

### **New York City Forms Response Team To Combat Asian-American Discrimination In Response To COVID-19**

New York

#### **Fisher Phillips**

The New York City Commission on Human Rights (NYCCHR) recently announced the formation of a COVID-19 Response Team to handle allegations of...

---

### **Employee Benefits as Payroll Costs under the Paycheck Protection Program**

#### **Haynes and Boone LLP**

Businesses that received a loan under the Paycheck Protection Program ("PPP") are eligible for forgiveness of that loan if, among other things, the...

---



## **EEOC Says “Yes” to Return to Work COVID-19 Testing**

### **Kelley Drye & Warren LLP**

This article was written by Barbara E. Hoey & Alison Frimmel and originally posted to Kelley Drye's Labor Days Blog. With the reopening of state...

---

## **U.S. COVID-19: EEOC Updates COVID-19 Guidance, Permitting Employers To Administer COVID-19 Tests and Clarifying Accommodation Obligations**

### **Bryan Cave Leighton Paisner LLP**

The U.S. Equal Employment Opportunity Commission (“EEOC”) recently issued new guidance to employers regarding the COVID-19 pandemic. Notably, and in...

---

## **What to Expect from OSHA’s COVID-19 Enforcement Efforts**

### **Vinson & Elkins LLP**

On April 13, 2020, the Occupational Safety and Health Administration (OSHA) issued its latest COVID-19-related interim guidance, describing how it...

---

## **States Create Presumptions for Essential Workers to Become Eligible for Workers’ Compensation Benefits During Pandemic**

### **Ogletree Deakins**

A number of states have recently passed or proposed amendments to their workers’ compensation statutes (or have issued other authority) to make it...

---

## **First Steps for Return-To-Work Planning**

### **Fox Rothschild LLP**

I have been speaking with many clients about the first steps for return-to-work planning. The Covid-19 shut-downs were so quick that there wasn't...

---

## **EEOC Offers Guidance To Employers Preparing To Reopen Their Workplaces**

### **Fisher Phillips**

The Equal Employment Opportunity Commission (EEOC) has provided additional guidance for employers restarting and ramping up their businesses. The...

---

## **Workplace Reopening Preparedness: Creating a Safe Office and Wellness Policy**

### **Nelson Mullins Riley & Scarborough LLP**

Federal, state, and local COVID-19 pandemic mitigation strategies have included both government shutdowns of all but essential businesses and “social...

---

## **What Employers Should Know About Furloughs, Layoffs, and WARN Act Obligations in Light of COVID-19**

### **Jackson Lewis PC**

Employers struggling with the challenges presented by the COVID-19 pandemic may be contemplating reductions in force or in hours. It is important...

---

## **Taking Temperatures During COVID-19: A Practical Toolkit**

### **Sheppard Mullin Richter & Hampton LLP**

As we move into the second quarter of 2020, governments around the country are analyzing how to best open up their economies. Part of this will...

---

## **COVID-19 Update: Moving Forward - Considerations for the Re-Opening of Physical Workplaces**

### **McCarthy Tétrault LLP**

Governments and businesses have now begun to turn their minds toward the re-opening of the economy and physical workplaces. This past week, for...

---

## **What Employers Should Do to Prepare their Workplaces per OSHA's COVID-19 Compliance**

### **Haynsworth Sinkler Boyd PA**

The Occupational Safety and Health Administration (OSHA) issued numerous directives in March and April 2020 related to COVID-19...

---

## **USDOL Issues Updated FFCRA FAQs**

### **Davis Wright Tremaine LLP**

The United States Department of Labor (USDOL) recently issued further clarification around several technical aspects of the Families First...

---

## **Update: Federal COVID-19 Relief Efforts Impact Higher Education Institutions**

### **Vorys Sater Seymour and Pease LLP**

Our team continues to track legal developments related to the COVID-19 pandemic, specifically as they relate to colleges and universities. As you know...

---

## **Early Lawsuit Based on Violations of the FFCRA Asserts Claims Against Employer, Human Resources Consultant and CEO Individually**

### **Hall Render Killian Heath & Lyman PC**

On April 16, 2020, just weeks after the Family First Coronavirus Response Act ("FFCRA") became law on March 18, 2020, a single mother sued her...

---

## **COVID-19: What Will Our Workplaces Look Like When the Economy Reopens?**

### **Freeborn & Peters**

"Germany Plans to Start Reopening Economy." The April 16, 2020 edition of the Wall Street Journal used this headline to introduce an article about the...

---

## **Chicago City Council Introduces COVID-19 Anti-Retaliation Ordinance, Reflecting Growing Trend**

### **Proskauer Rose LLP**

On April 22, 2020, Chicago Mayor Lori Lightfoot, with the backing of several Aldermen, introduced the COVID-19 Anti-Retaliation Ordinance (the...

---

## **New Deadlines for Retirement Plans, Tax Filings and Paid Leave Policies**

### **Dickinson Wright**

The Coronavirus Aid, Relief and Economic Security Act ("CARES"), and IRS and Department of Labor ("DOL") rules establish new and revised deadlines...

---

## **State COVID-19 Orders Regulating Worker Safety—Are They Preempted?**

York

New



### **Ogletree Deakins**

Almost every state has issued closure orders designating certain businesses as “essential” and allowing them to continue to operate during the...

---

### **Updated EEOC COVID-19-Related Workplace Guidance: COVID-19 Testing**

#### **Wilson Elser**

On April 23, 2020, the EEOC issued an update to its technical assistance guidance, “What You Should Know About COVID-19 and the ADA, the...

---

### **New York Relaxes Layoff Notification Requirements for Some Employers Due to COVID-19**

New York

#### **Day Pitney LLP**

On April 17, New York Governor Andrew Cuomo signed Executive Order No. 202.19, which eases the notification requirements under New York's Worker...

---

### **U.S. Supreme Court Will Finally Weigh In on Scope of Computer Fraud and Abuse Act**

#### **Jackson Lewis PC**

The U.S. Supreme Court has agreed to decide whether it is a violation of the Computer Fraud and Abuse Act (CFAA) when an individual who is authorized...

---

### **Families First Coronavirus Response Act - Health emergency leave and exempted health care providers**

#### **DLA Piper**

The Secretary of Labor recently promulgated temporary regulations (the “Regulations”) in connection with the Families First Coronavirus Response Act...

---

### **Back to Work: Georgia's - Reopening Executive Order: Risks and Guidance for Businesses**

#### **Bryan Cave Leighton Paisner LLP**

On April 20, 2020, Governor Brian Kemp signed an Executive Order which initiates the process of reopening businesses within the State of Georgia on...

---

### **FMCSA Extends Emergency Declaration to May 15 in Response to COVID-19, Direct Assistance Needs**

#### **Holland & Knight LLP**

The Federal Motor Carrier Safety Administration (FMCSA) has expanded and extended its Emergency Declaration through May 15, 2020, or until the...

---

### **Employer's After-the-Fact Discovery of Lack of Job Qualification Sinks Employee's ADA Discrimination Claim (US)**

#### **Squire Patton Boggs**

Sunny Anthony worked for TRAX International as a technical writer. During the course of her employment, she asked TRAX to accommodate her...

---

### **Protecting Your Company from Coronavirus-related Premises Liability Claims**

#### **Haynes and Boone LLP**

Businesses preparing to reopen amid the coronavirus pandemic and the essential businesses that have remained open through the pandemic should make a...

---

### **Michigan Employers Now Have More Flexibility To Implement Work Share Plans** **Fisher Phillips**

Governor Whitmer recently expanded unemployment benefits, most notably for access to the Work-Share Program, by issuing Executive Order 2020-57. The...

---

### **What Employers Need to Know about OSHA's Reporting Requirements and Enforcement Guidance for COVID-19 Inspections**

**Haynsworth Sinkler Boyd PA**

The Occupational Safety and Health Administration (OSHA) issued Enforcement Guidance outlining Employer's reporting responsibilities related to...

---

### **EEOC Permits Employers to Test for COVID-19**

**Frankfurt Kurnit Klein & Selz PC**

This week, as parts of the nation began returning to work, the EEOC responded to an increasingly urgent question: May employers test employees for...

---

### **Commercial Litigation in the Cannabis Space: Resolving Disputes Like Every Other Industry Does**

**Duane Morris LLP**

As a commercial litigator who has handled a broad range of claims in highly regulated industries over the past 20 years — particularly in complex...

---

### **New York Enacts Permanent Paid Sick Leave Legislation**

New York

**Duane Morris LLP**

Employees are to accrue one hour of sick leave for every 30 hours worked, beginning September 30, 2020...

---

### **Fifth Circuit Reverses Course, Concludes That "Day Rate" Pay Method Fails to Satisfy FLSA's "Salary Basis" Test for Overtime Exemptions**

**Jackson Lewis PC**

Upon further reflection, a panel of the U.S. Court of Appeals for the Fifth Circuit has determined that paying an employee a set amount for each day...

---

### **EEOC Says "Yes" to Return to Work COVID-19 Testing**

**Kelley Drye & Warren LLP**

With the reopening of state economies and return-to-work on the horizon, on April 23, 2020, the EEOC issued new guidance on workplace testing for...

---

### **Yes, We Think We're Open... Getting your Employees Back to Work During and After the COVID-19 Pandemic (Part I)**

**Bradley Arant Boult Cummings LLP**

One of the hardest things about the COVID-19 crisis is that nobody is sure about when things will open back up and life can go back to "normal." If...

---



## **Employers, Take Note: Virginia Enacts Broad Protections for Private-Sector Whistleblowers**

### **Ogletree Deakins**

In our previous article—What Virginia Employers Might Have Missed While Managing COVID-19: The Silent Labor and Employment Law Revolution—we detailed...

---

## **Pause in Immigrant Visa Processing Imposed by Presidential Proclamation - Effective April 23 for Sixty Days at Consular Posts**

### **Dickinson Wright**

After numerous rumors in the past few days regarding the suspension of immigration to the United States (U.S.), President Trump's Proclamation...

---

## **COVID-19 - States Expanding Workers' Compensation Coverage For Essential Employees**

### **Baker & Hostetler LLP**

In very recent days, some states have made it easier for certain workers who have contracted COVID-19 to establish a claim for workers' compensation...

---

## **Changes to Employment-Based Immigration Processing in Light of COVID-19**

### **Ford & Harrison LLP**

In light of the enormous impact of the Coronavirus pandemic on U.S. employers, their workforces and the economy, the U.S...

---

## **Why, How and When Katz May "Trump" an Expired CBA When It Comes to Making Unilateral Changes — The Relationship Between MV Transportation and Raytheon Network**

### **Sheppard Mullin Richter & Hampton LLP**

From time to time, employers trigger labor disputes when they make unilateral changes in working conditions. Unions objecting to such changes often...

---

## **Bay Area Counties Now Requiring Face Coverings**

### **Davis Wright Tremaine LLP**

Bay Area Counties have issued Health Orders mandating that persons wear face coverings when interacting in public. Each county's orders impose...

---

## **More States and Municipalities Impose Mandatory Face Covering and Other Workplace Protections**

### **Faegre Drinker Biddle & Reath LLP**

After an initial wave that saw a focus on closing or limiting "non-essential" or "non-life sustaining" businesses and limiting individual travel...

---

## **COVID-19 Washington Update: April 23, 2020**

### **Kelley Drye & Warren LLP**

Today's federal government actions in response to COVID-19, includes House passage of the Paycheck Protection Program and Health Care Enhancement Act...

---

---

## **OSHA Issues COVID-19 Compliance Guidance for Construction Workforces**

### **Ogletree Deakins**

The U.S. Occupational Safety and Health Administration (OSHA) has issued a series of tips tailored to construction work to help reduce the risk of...

---

## **5 Tips for Employers to Safeguard Against Employee Discrimination Claims Arising from COVID-19**

### **Holland & Knight LLP**

As employers continue to navigate the coronavirus (COVID-19) pandemic and contemplate returning employees back to the workplace, these unprecedented...

---

Law Department Management



## **Courtroom Attire in the Coronavirus World**

### **Graydon Head & Ritchey LLP**

I attended a hearing in Hamilton County Juvenile court yesterday via Zoom. As you can see from the photo, my attire was bit of a mixed bag. Coat and...

---

## **5 Must-Have Contract Management Tools for Effective Remote Work**

### **CobbleStone Software**

In the face of unforeseen circumstances, many organizations allow employees to work from home. Legal professionals in a variety of industries must...

---

## **Former Political Consultant, South Carolina State Government Affairs Manager for JUUL Labs LaJoia Broughton Joins Adams and Reese in Columbia**

### **Adams and Reese LLP**

COLUMBIA, S.C. — Adams and Reese is pleased to announce LaJoia Broughton has joined the firm's Government Relations practice and Columbia office as a...

---

## **More Courts Attempt to Move Civil Cases Forward Despite the COVID-19 Pandemic**

### **Seyfarth Shaw LLP**

We continue to track the impact of COVID-19 on court operations and parties in civil litigation across the country. (You can read our most recent...

---

## **Extensions of Court Orders Regarding Impact of COVID-19 in Massachusetts**

Massachusetts

### **Nutter McClennen & Fish LLP**

Yesterday, the Supreme Judicial Court issued an order updating the status of operations of the state courts. This order confirms that the judiciary...

---

Legal Tech



## **English High Court Sets out Principles for COVID-19 Adjournments and Time Extensions**

### **Faegre Drinker Biddle & Reath LLP**

In a recent ruling of the English High Court, a judge has set out the principles



which the English Courts should apply when considering applications...

Public



### **Considerations for Colleges and Universities Facing Class Action Refund Lawsuits From Students**

**Faegre Drinker Biddle & Reath LLP**

COVID-19 has forced colleges and universities to move from traditional in-person classroom instruction to online learning. Just as students, faculty...

### **COVID-19: Daily Report for Life Sciences and Health Care Companies**

**Hogan Lovells**

The Daily Report is a compilation of COVID-19 (coronavirus) news briefs from around the world to help life sciences and health care companies stay...

### **North Carolina General Assembly — Coronavirus (COVID-19) Update**

North

Carolina

**McGuireWoods Consulting LLC**

The North Carolina General Assembly will reconvene Tuesday, April 28 at 12:00. Due to the COVID-19 pandemic, the upcoming session will look different...

### **Georgia Issues Guidelines for Reopening Sectors of Its Economy**

Georgia

**Fox Rothschild LLP**

On Monday, April 20, 2020 Georgia Gov. Brian Kemp issued an Executive Order that set the state on a path to begin reopening some of the businesses...

### **New/Updated Terms and Conditions and Hall Render Briefing Document**

**Hall Render Killian Heath & Lyman PC**

HHS published a new Terms and Conditions document that is specific to payments that started being distributed on Friday, April 24 from the CARES Act...

### **NC Outlines Three-Phase Approach to Reopen State**

North Carolina

**Fox Rothschild LLP**

North Carolina Gov. Roy Cooper officially extended the State's stay-at-home order through May 8, 2020, which includes closures of dine-in restaurants...

### **NC Governor Cooper Extends Statewide "Stay at Home" Order and Order Closing Schools**

North Carolina

**Brooks Pierce McLendon Humphrey & Leonard LLP**

North Carolina Governor Roy Cooper took additional executive action this week related to the COVID-19 virus and its impact on the state...

### **Banking litigation in the next decade: A look ahead**

**Linklaters LLP**

Banking litigation in the next decade: a look ahead Foreword The start of a new decade seems a good time to take stock of the likely sources of...

## **Texas Developments, Week of April 20, 2020**

Texas

### **Frost Brown Todd LLC**

On April 17, 2020, Texas Governor Greg Abbott issued several Executive Orders to “Open Texas.” This means they will begin a process of “safely and...

---

### **U.S. Department of Education Releases Additional Details on CARES Act Emergency Assistance for Higher Education Institutions and Students**

#### **Faegre Drinker Biddle & Reath LLP**

On Tuesday, April 21, 2020, the U.S. Department of Education (ED) released additional information regarding emergency assistance for higher education...

---

### **COVID-19: Federal Reserve Board to publish CARES Act borrower information. Does more oversight follow?**

#### **Hogan Lovells**

On April 23, the Federal Reserve Board issued a vow to report information every month regarding the participants of lending and liquidity facilities...

---

### **DOJ Continues Expedited Approval of COVID-19 Related Competitor Collaborations**

#### **Crowell & Moring LLP**

Earlier this week, the U.S. Department of Justice issued a business review letter approving a competitor collaboration intended to accelerate and...

---

### **Private Student Loan Servicers Enter Agreement with Multiple States for Relief Options**

#### **Troutman Sanders LLP**

Multiple states have come together to enact initiatives aimed at prohibiting private student loan servicers from certain activities that will remain...

---

### **UPDATE: NCAA Rejects Blanket Waiver of Minimum Sports Requirement in Midst of COVID-19**

#### **Jackson Lewis PC**

The NCAA Division I Council has rejected the efforts of the leaders of five Division I Conferences (the American Athletic, Mountain West...

---

### **Department of Education Releases FAQs on CARES ACT Funding for Universities**

#### **Vorys Sater Seymour and Pease LLP**

Our team continues to track legal developments related to the COVID-19 pandemic, specifically as they relate to colleges and universities. As you know...

---

### **PA Law Allows Municipal Governments to Hold Virtual Meetings for Zoning and Land Development Applications**

Pennsylvania

#### **Pepper Hamilton LLP**

On April 20, Pennsylvania Gov. Tom Wolf signed into law Act 15 of 2020 (previously SB 841), which expressly authorizes municipal...

---



## **COVID-19: PA Announces May 1 reopening for Golf Courses, Marinas and Privately Owned Camp Grounds**

**Duane Morris LLP**

As of May 1, PA will allow golf courses and marinas and privately owned campgrounds to re-open...

---

## **COVID-19: NY announces Phased Approach for Re-Opening** New York

**Duane Morris LLP**

On April 27th, Governor Cuomo outlined a phased plan to re-open New York starting with construction and manufacturing. Based on CDC recommendations...

---

## **ARRC Proposes New York State Legislation to Facilitate LIBOR-to-SOFR Transition** New York

**Paul Hastings LLP**

The Alternative Reference Rates Committee (the "ARRC") recently proposed statutory language for consideration by the New York State legislature...

---

## **California Curbs Recycling Requirements in the Time of COVID-19** California

**Manatt Phelps & Phillips LLP**

Since California Governor Gavin Newsom issued his first Emergency Declaration in response to the COVID-19 pandemic on March 4, 2020, he has issued...

---

## **Massachusetts Enacts Emergency Regulation on CORI Verifications**

Massachusetts

**Littler Mendelson PC**

On April 9, 2020, the Massachusetts' Department of Criminal Justice Information Systems (DCJIS) passed an Emergency Regulation to address the social...

---

## **South Carolina Joins States Proposing Legislation to Mandate Insurers Pay COVID-19 Losses**

**Wilson Elser**

On April 8, 2020, a bipartisan group of three South Carolina state senators introduced Senate Bill 1188, which would provide coverage for loss of...

---

## **Governor Baker's Emergency Order Closing Adult-Use Marijuana Establishments Survives Constitutional Challenge in BLS** Massachusetts

**Nutter McClennen & Fish LLP**

To help slow the spread of the COVID-19 pandemic, Governor Baker has ordered businesses to suspend physical operations unless he deems them...

---

## **COVID-19: NJ Announces 6-Point Plan and Methodology for ReOpening the State - "The Road Back"** New Jersey

**Duane Morris LLP**

Gov. Murphy announces NJ's 6-point reopening plan called "The Road Back: Restoring Economic Health Through Public Health." The Governor also...

---

## **Second Emergency Stimulus Bill Provides \$100 Billion in Additional Funding to**

## **Further Support COVID-19 Treatment and Testing**

### **Greenbaum, Rowe, Smith & Davis LLP**

The Paycheck Protection Program and Health Care Enhancement Act (the Act), a second round of emergency economic stimulus funding that was signed into...

---

## **COVID-19: Colorado Transitions to “Safer at Home”**

Colorado

### **Wilmer Cutler Pickering Hale and Dorr LLP**

Colorado's stay-at-home order expired on Sunday, April 26. It has been replaced by a new order, issued April 26, reflecting the State's transition...

---

## **Colorado issues new “safer at home” executive order**

Colorado

### **Buckley LLP**

On April 26, the Colorado governor issued an Executive Order that provides new requirements for social distancing and remote work. Among other things...

---

## **Massachusetts Legislature Passes Legislation Allowing Use of Virtual Notarization During COVID-19 Pandemic**

Massachusetts

### **Nelson Mullins Riley & Scarborough LLP**

After some delay, on April 23, 2020, the Massachusetts Senate and House passed emergency legislation that allows for notaries public to use electronic...

---

## **Sixth Circuit Holds Due Process Guarantees Right To Access Literacy**

### **Squire Patton Boggs**

A Sixth Circuit panel held last week, in *Gary B. V. Whitmer*, that the Fourteenth Amendment's Due Process Clause guarantees a “right to access to...

---

## **Maryland Governor Outlines Phased Reopening Plan Post-COVID-19 Shutdown**

Maryland

### **Jackson Lewis PC**

Maryland Governor Larry Hogan has introduced the Maryland Strong: Roadmap to Recovery, a three-stage plan for the state to restart its economy and...

---

## **Nevada State and Local Governments Make Licensing and Permit Accommodations to Help Businesses Amid the COVID-19 Crisis**

### **Dickinson Wright**

Like many other states in response to the widespread transmission of COVID-19, Nevada has banned business operations for non-essential businesses and...

---

## **COVID-19 Response: US financial services regulatory**

### **White & Case LLP**

In response to the global COVID-19 crisis, US financial regulators at the state level are taking important actions that affect US and non-US...

---

## **OFAC Issues Guidance on COVID-19-Related Exports and Compliance Challenges**

### **Baker & Hostetler LLP**

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)



has issued guidance on humanitarian exports and compliance challenges...

---

**Client Alert: Virtual Notarization and Witnessing of Your Documents During COVID-19 Emergency** [Massachusetts](#)

**Bowditch & Dewey LLP**

On April 27, 2020, Massachusetts enacted An Act Providing for Virtual Notarization to Address Challenges Related to COVID-19. This emergency virtual...

---

**COVID-19: Distressed Debt and Tax - Part I - Lender and Debt Holder Considerations**

**K&L Gates**

In response to the economic havoc resulting from the onset of the coronavirus ("COVID-19") pandemic, Congress has enacted wide-ranging legislation to...

---

**Memphis Extends Safer-At-Home Order And Issues New Guidelines For Essential Businesses** [Tennessee](#)

**Fisher Phillips**

Memphis Mayor Jim Strickland recently issued an update to the March 23 Safer at Home Executive Order. While most Tennessee counties plan for...

---

**North Carolina extends stay at home order** [North Carolina](#)

**Buckley LLP**

On April 23, North Carolina Governor Roy Cooper issued an Executive Order extending his prior stay at home order (previously discussed here) until...

---

**In updated COVID-19 FAQ, Indiana Department of Local Government Finance clarifies application of interest to late property tax payments; No change (yet) to 2020 assessment notice & appeal deadlines; Abatement compliance extended; Waiver of penalties on special assessments and fees** [Indiana](#)

**Faegre Drinker Biddle & Reath LLP**

On April 24th, the Indiana Department of Local Government Finance updated its FAQ covering topics related to "COVID-19 & Executive Orders," as those...

---

**The IRS Provides Tax Relief for Individuals and Businesses Affected by COVID-19-Related Travel Disruptions**

**Kramer Levin Naftalis & Frankel LLP**

In recognition of the disruption of travel plans resulting from the global outbreak of COVID-19 (the COVID-19 Emergency), the Internal Revenue Service...

---

**New Illinois Stay at Home Order Announced for May** [Illinois](#)

**Ropes & Gray LLP**

On April 23, 2020, Governor J.B. Pritzker announced that he will sign a modified stay at home Executive Order (the "Order") to go into effect on May...

---

**CARES Act funds: Significant new USED guidance includes surprises**

### **Thompson Coburn LLP**

Yesterday, the U.S. Department of Education issued significant new guidance to institutions of higher education regarding their receipt and use of...

---

イリノイ州の外出禁止令が延長されたことにより イリノイ州を拠点とする必要不可欠(essential)なビジネスおよび製造会社に及ぼされる影響 [Illinois](#)

### **Masuda Funai Eifert & Mitchell Ltd**

2020年4月23日 イリノイ州のJ.B.プリツカー知事は 現在出されている 外出禁止令(stay-at-home...

---

### **Covid-19 coronavirus: an overview of U.S federal legislation phase 4**

#### **Allen & Overy LLP**

Congress passed the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") in late March 2020. The CARES Act included a Paycheck Protection...

---

### **President Trump Signs Bill to Provide Additional COVID-19-Related Small Business Funding**

#### **Cadwalader Wickersham & Taft LLP**

Congress adopted and President Donald Trump signed into law an act to provide additional funding under the Paycheck Protection Program and to provide...

---

### **Real Estate Development in the Time of Coronavirus: Massachusetts - Update 4/28/20** [Massachusetts](#)

#### **Pierce Atwood LLP**

On April 28, 2020, Massachusetts Governor Charlie Baker extended his previous order...

---

### **COVID-19: NJ names 21 Member COVID Taskforce** [New Jersey](#)

#### **Duane Morris LLP**

NJ has officially announced the 21 members of its COVID Taskforce. According to Governor Murphy, the NJ taskforce "is composed of experts in a...

---

### **Congress approves extension for PPP and EIDL programs**

#### **McBrayer McGinnis Leslie & Kirkland PLLC**

After the initial funding for the Payroll Protection Program (PPP) and the Economic Injury Disaster Loan program (EIDL) were exhausted, Congress...

---

### **Virginia outlines student loan servicer requirements** [Virginia](#)

#### **Buckley LLP**

On April 22, the Virginia legislature enacted SB 77, which requires entities servicing student loans in the Commonwealth to be licensed by the State...

---

### **Why Procurement Processes Still Matter During a Pandemic** [New York](#)

#### **K2 Intelligence/Financial Integrity Network**

For government and private institutions, the COVID-19 pandemic has meant



acting quickly—so quickly, in fact, that companies run the risk of...

---

### **Betsy DeVos Refuses to Request Much-Needed Waivers from the IDEA and Section 504**

#### **Nelson Mullins Riley & Scarborough LLP**

U.S. Secretary of Education Betsy DeVos has submitted a recommendation to Congress that states and local educational agencies (LEAs) not receive any...

---

### **U.S. - Coronavirus (Legal) Immunity - The Risky Business of Re-Opening**

#### **Bryan Cave Leighton Paisner LLP**

In the midst of unprecedented business and court closures, the Coronavirus (COVID-19) pandemic has already caused a flood of litigation. Businesses...

---

### **New Threat on the Horizon for Schools, Colleges, and Universities: Class Action Lawsuits for Return of Tuition**

#### **Krieg DeVault**

COVID-19 has caused tremendous disruption and expense for colleges and universities, and other tuition-based education institutions, leading to...

---

### **Higher Education Institutions Should Prepare for Fallout from COVID-19**

#### **Akin Gump Strauss Hauer & Feld LLP**

Universities across the country have shuttered their campuses and moved classes online in reaction to the novel coronavirus...

---

### **What to Expect From the New Congressional Coronavirus Subcommittee US**

#### **Squire Patton Boggs**

On April 23, 2020, the US House of Representatives voted to establish a new investigative subcommittee of the Committee on Oversight and Reform...

---

### **COVID-19: HHS Clarifies Scope of PREP Act COVID-19 Declaration in Advisory Opinion**

#### **Michael Best & Friedrich LLP**

On April 14, 2020, the Department of Health and Human Services (HHS) General Counsel issued an Advisory Opinion clarifying the scope of liability...

---

### **The Pendulum Swings: Record Fine Imposed by UK Sanctions Monitor, but Only After Reduction on Review**

#### **Greenberg Traurig LLP**

The UK's sanctions monitor, the Office of Financial Sanctions Implementation (OFSI), has issued its biggest fine to date, imposing a total financial...

---

### **COVID-19 Washington Update: April 28, 2020**

#### **Kelley Drye & Warren LLP**

Following is a synopsis of today's federal government actions in response to COVID-19. Congress Today, House leaders reversed plans to return to...

---

### **COVID-19: Expert Soundbite - The Geopolitical Consequences of the Pandemic**

Audio

### **Squire Patton Boggs**

Our global Public Policy Practice meets several times a week to examine the profound and transformative effect of the coronavirus disease 2019...

---

### **NC Politics in the News** North Carolina

#### **McGuireWoods Consulting LLC**

The U.S. Agriculture Department approved Friday two North Carolina requests for additional resources as part of the State's response to the COVID-19...

---

### **As Independent Schools throughout the Country Navigate the Rough Seas of the COVID-19 Global Pandemic, Does the Federal Financial Assistance Available to Them through the CARES Act PPP Loan Program an**

#### **Breazeale Sachse & Wilson LLP**

As Independent Schools throughout the Country Navigate the Rough Seas of the COVID-19 Global Pandemic, Does the Federal Financial Assistance...

---

### **Client Alert: State Announces Schedule for Reopening Businesses**

#### **Brouse McDowell**

On Monday, the Governor announced the State's plan for allowing businesses to reopen. This morning, the criteria were amended to revise the mask...

---

### **New Jersey Director of Emergency Management Eases Restrictions on Certain Businesses** New Jersey

#### **Jackson Lewis PC**

The New Jersey State Director of Emergency Management has issued an Order designating additional businesses as "essential retail" and permitting auto...

---

### **Illinois to Modify and Extend Stay at Home Order Until May 30, 2020** Illinois

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On Thursday, April 23, 2020, Governor J.B. Pritzker announced that he expected to sign an order modifying and extending the...

---

### **New Jersey's Post-COVID-19 'Road Back' Plan Full of Red Lights** New Jersey

#### **Jackson Lewis PC**

New Jersey Governor Phil Murphy has released The Road Back: Restoring Economic Health Through Public Health, outlining six principles or milestones...

---

### **COVID-19: Massachusetts Allows Remote Notarization** Massachusetts

#### **Pierce Atwood LLP**

On April 27, 2020, Massachusetts Governor Charlie Baker signed into law an emergency measure to authorize Massachusetts notaries public to use...

---

### **Higher education third party provider viability risk during COVID-19**

#### **MinterEllison**

Nowadays, many universities partner with third parties in the private sector to enrol and deliver (or assist in the delivery of) courses to students...



---

## How Illinois-Based Japanese Essential Businesses and Manufacturing Companies Will Be Affected under the Illinois Extended Stay-at-Home Order

Illinois

### Masuda Funai Eifert & Mitchell Ltd

Illinois Governor J.B. Pritzker announced on April 23, 2020, that the Illinois stay-at-home order will be extended to May 30, 2020. The standing...

---

## Louisiana Extends Statewide Stay-At-Home Order While Loosening Business Restrictions

Louisiana

### Fisher Phillips

Governor Jon Bel Edwards just extended Louisiana's statewide stay-at-home order through May 15 while also providing a Lifeline to some businesses...

---

## Texas Unveils Phase One of Plan to Reopen Businesses

Texas

### Fox Rothschild LLP

On April 27, Texas Gov. Greg Abbott announced a multi-phase plan to reopen businesses. Phase One of the plan, set forth in an executive order...

---

## Ohio House Members Release Guidelines for Re-Opening Ohio Businesses

Ohio

### Dinsmore & Shohl LLP

On April 27, 2020, members of the Ohio House of Representatives released the Open Ohio Responsibly Framework. This framework contains recommended...

---

## New York Remote Notarization

New York

### Haynes and Boone LLP

In light of the social distancing orders put in place in response to the COVID-19 pandemic, Governor Andrew Cuomo signed Executive Order 202.7 on...

---

## Introduction to United States Space Force Acquisitions

### Davis Wright Tremaine LLP

After becoming law in December 2019, the National Defense Authorization Act (NDAA) for Fiscal Year 2020 formally established the Space Force as the...

---

## Considerations for schools and Universities that manufacture or supply ppe

### Squire Patton Boggs

In the ultimate act of service learning, many universities and schools have shifted their focus during the COVID-19 crisis to manufacturing personal...

---

## Texas Allows More Elective Procedures, But Questions Remain

Texas

### Seyfarth Shaw LLP

On April 17, 2020, Texas Governor, Gregg Abbot signed Executive Order GA-15 which extended, with some modifications, Executive Order GA-09 which...

---

## Virginia General Assembly Permits Local Governments to Meet Electronically

Virginia

### **McGuireWoods LLP**

The Virginia General Assembly recently authorized public bodies — including local boards and commissions — to meet electronically during the state of...

---

### **Illinois Governor Extends COVID-19 Stay-at-Home Order with Some Modifications** Illinois

#### **Duane Morris LLP**

On April 23, 2020, Illinois Governor JB Pritzker announced that he is extending the state's stay-at-home order with modifications. This new order...

---

### **Alaska Issues First Phase of 'Reopen Alaska Responsibly' Plan** Alaska

#### **Ogletree Deakins**

On April 22, 2020, Alaska Governor Mike Dunleavy, Alaska Department of Health and Social Services Commissioner Adam Crum, and Dr. Anne Zink, Chief...

---

### **The CARES Act: What Does It Mean for Your School District?**

#### **Squire Patton Boggs**

The federal government approved the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) on March 27, 2020, as part of its efforts to...

---

### **COVID-19 Mexico Update: "Essential Activities" and Federal & State Enforcement Through April 29, 2020**

#### **Wilmer Cutler Pickering Hale and Dorr LLP**

A joint client alert update by WilmerHale and Creel García-Cuellar Aiza & Enriquez.1 This publication updates our April 8, 2020, client alert...

---

### **Proposed California Legislation Seeks to Expand Eviction Protections Including Rent Reduction** California

#### **Procopio Cory Hargreaves & Savitch LLP**

The California Legislature is currently considering two COVID-19 response bills aimed at protecting both residential and commercial tenants regarding...

---

### **Ohio Launches "Responsible RestartOhio" Plan** Ohio

#### **Thompson Hine LLP**

On April 27, Ohio Governor Mike DeWine announced details of the Responsible RestartOhio plan, which will phase in a relaxing of the Amended...

---

### **Georgia Executive Orders Permits Re-Opening of Businesses** Georgia

#### **Greenberg Traurig LLP**

Georgia Governor Brian Kemp recently issued two Executive Orders: (1) Executive Order 04.20.20.01; and (2) Executive Order 04.23.20.02 (herein...

---

### **Illinois Department of Financial and Professional Regulation issues guidance to student borrowers** Illinois

#### **Buckley LLP**

The Illinois Department of Financial and Professional Regulation has issued



responses to Frequently Asked Questions regarding the expansion of...

---

### **When it Comes to Virtual Learning, Privacy Isn't as Easy as $2 + 2 = 4$**

#### **Frankfurt Kurnit Klein & Selz PC**

The creativity with which people around the world have responded, and continue to respond, to this pandemic in addressing the needs of others is...

---

### **Campaign Finance Violation for Unregistered Political Committee Upheld in Washington State, but \$18 Million Penalty Must Still Pass Excessive Fine Test**

[Washington](#)

#### **Covington & Burling LLP**

In one of the most watched campaign finance disclosure enforcement cases, last week, the Washington State Supreme Court upheld a trial court's...

---

### **CFIUS Filing Fees Go Into Effect May 1, 2020**

#### **Thompson Hine LLP**

On April 29, 2020, the U.S. Department of the Treasury's Office of Investment Security published an interim rule in the Federal Register that...

---

### **House Bill 197 Provisions Regarding School Leadership Evaluations, Education Metrics and Distance Learning**

#### **Taft Stettinius & Hollister LLP**

On April 20, 2020, Ohio Governor, Mike DeWine announced that the March 14, 2020 statewide order directing all of Ohio's public, community, and...

---

### **State Lobbyist and Campaign Finance Filing Changes Related to COVID-19**

#### **Covington & Burling LLP**

As states grapple with the effects of the COVID-19 crisis, many have opted to make changes to campaign finance and lobbying reporting due dates and...

---

### **Cayuga Nation Prevails in Long-Running Litigation Over Gaming Rights**

#### **Jenner & Block LLP**

On March 24, The Cayuga Nation vindicated its sovereign right to game under the Indian Gaming Regulatory Act (IGRA) when a New York federal judge ruled...

---

### **COVID-19: Governor Mills Establishes Four-Stage Plan to Reopen Maine's Economy; Extends Statewide Stay-At-Home Order**

[Maine](#)

#### **Pierce Atwood LLP**

On Tuesday, April 28, 2020, Maine Governor Janet Mills extended the statewide stay-at-home order through May 31, 2020, and announced a four-part plan...

---

### **COVID-19: Massachusetts Governor Extends Non-Essential Business Closures to May 18, 2020**

[Massachusetts](#)

#### **Pierce Atwood LLP**

On April 28, 2020, Massachusetts Governor Charlie Baker announced the second extension of Massachusetts' non-essential business closure order, now in...

---

## **West Virginia Reopening Plan Depends on Percentage of Positive Cases** West

Virginia

### **Frost Brown Todd LLC**

Governor Jim Justice's vision for reopening West Virginia was applauded by lawmakers from across the political spectrum as it provides a...

---

## **Compliance Notes - Vol. 1, Issue 1**

### **Nossaman LLP**

Here, we are expanding upon our eAlerts (where we provide substantive analysis on key issues), to deliver a periodic digest of the headlines...

---

## **ReOpen DC Advisory Group Mission and Leadership**

### **Venable LLP**

The Group has 11 committees that will follow the Johns Hopkins' "Public Health Principles for a Phased Reopening during COVID-19: Guidance for...

---

## **U.S. Army Corps Asks Federal Court to Stay Decision Vacating NWP 12, Indicates It Will Appeal**

### **Fredrikson & Byron PA**

On April 27, 2020, the U.S. Army Corps of Engineers filed a motion asking a Montana federal court to partially stay its April 15, 2020, decision...

---

## **Kentucky Tax Talk: Budget Focuses on Pandemic Relief** Kentucky

### **Frost Brown Todd LLC**

The commonwealth's primary concerns have drastically changed since the start of the 2020 General Assembly's regular session in January. Whether it was...

---

## **Congress Increases Funding for Coronavirus Relief Programs**

### **Vinson & Elkins LLP**

The U.S. Congress passed legislation to increase funding for coronavirus relief programs on Thursday, April 23, 2020. The \$483.4 billion package adds...

---

## **FARA: using anti-propaganda laws in the fight against corruption**

### **Raedas**

As the spread of the coronavirus limits travel and shuts archives, investigators are looking to pandemic-proof repositories of evidence. One such...

---

## **Andrew Yang Sues New York State Board of Elections for Canceling Democratic Primary** New York

### **Steptoe & Johnson LLP**

On Monday, the New York State Board of Elections voted to cancel New York's democratic presidential primary, which it had originally postponed from...

---

## **A (Cloudy) CARES 2.0 Crystal Ball**

### **Hogan Lovells**

With an interim relief measure, the Paycheck Protection Program (PPP) and Health Care Enhancement Act, now signed into law, the jockeying over a



CARES...

---

**Courts Consider the Constitutionality of PPP Loans Under the CARES Act, Government Shutdown Orders, and Signature Requirements for Getting on the Ballot**

**Seyfarth Shaw LLP**

As the pandemic continues, courts are addressing COVID-19-related constitutional challenges. The most recent cases address the eligibility...

---

**Client Alert: The Mask is Back**

**Brouse McDowell**

After the State of Ohio revised its internet postings yesterday, we advised our clients of where each industry scheduled for reopening stood as of...

---

**Impact of COVID-19 Shutdown on Club Dues**

**Greenberg Traurig LLP**

Most golf and social clubs have either shut down or curtailed operations in response to the Coronavirus Disease 2019 (COVID-19) crisis. Some members...

---

**Department of Education Releases CARES Act Funds**

**Step toe & Johnson LLP**

Last week, the Department of Education (Department) released details and guidance regarding its distribution of funds appropriated to institutions of...

---

**Today in Washington - April 29, 2020: COVID-19 Updates**

Washington

**Hall Render Killian Heath & Lyman PC**

The Health Resources and Services Administration will host a webinar for health care providers on the agency's COVID-19 Uninsured Program Portal...

---

**Paycheck Protection Program Update: More Funds but More Clarity on Economic Uncertainty-Make Sure Your Certification is Accurate**

**Kilpatrick Townsend & Stockton LLP**

Applications for the Paycheck Protection Program (PPP) are once again being accepted by lenders after Congress authorized another \$310 billion in...

---

**Coronavirus (COVID-19) Update: Trade, Supply Chains and Defense : April 10, 2020**

**Squire Patton Boggs**

Countries around the world continue to enact policies aimed at mitigating the spread of COVID-19 that both recognize the importance of trade to...

---

**FEMA Releases Temporary Final Rule on US Exports of Personal Protective Equipment**

**Squire Patton Boggs**

The Federal Emergency Management Agency (FEMA) has released a temporary final rule on US exports of personal protective equipment (PPE). It went into...

---

## **OFAC Issues Fact Sheet on Providing Humanitarian Aid to Combat COVID-19 Under Various Sanctions Programs**

### **Thompson Hine LLP**

On April 16, 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC) stated that the United States "is committed to ensuring...

---

## **How to Obtain PPP Loan Forgiveness!: COVID-19 Transportation Update - Wednesday, April 22, 2020**

### **Windels Marx Lane & Mittendorf LLP**

The White House and Congress have reached a deal on a bill that includes nearly \$320 billion in new funding for the Paycheck Protection Program...

---

## **DOE issues guidance on the use of the CARES Act's Higher Education Emergency Relief Fund (HEERF)**

### **Nelson Mullins Riley & Scarborough LLP**

In new FAQs on Emergency Student Aid portion of HEERF and FAQs on Institutional Portion of HEERF, the US DOE explained the requirements relating to...

---

## **Business coalition DC2021 presents its COVID-19 Impact and Recovery Plan for DC**

### **Venable LLP**

Local restaurant, retail, hotel, arts, sports, and entertainment businesses join civic leaders to form an advocacy group, DC2021, to support the...

---

## **Bring Back Tax-Exempt Advance Refundings**

### **Squire Patton Boggs**

Over at our Restructuring GlobalView blog, our public finance colleagues Pedro Miranda and Pedro Hernandez make the case for bringing back tax-exempt...

---

## **Reopening economies - which level of government has the last word?**

### **Hogan Lovells**

As states begin to work together to reopen the economy, companies in all industries will soon have to wrestle with a new wave of federal, state, and...

---

## **House Passes \$484 billion Bill "3.5" to Refill the PPP and EDL Loans, Hospitals, and Testing**

### **Michael Best & Friedrich LLP**

The House of Representatives overwhelmingly passed a \$484 billion coronavirus relief bill to replenish a tapped-out small business loan program...

---

## **New Jersey Governor Signs Bill Requiring 'Title 26 Hospitals' to Report Demographic Data on COVID-19**

New Jersey

### **Jackson Lewis PC**

New Jersey Governor Phil Murphy has signed a bill requiring hospitals licensed under New Jersey Statutes Title 26 to report demographic data on...

---



## **What You Need to Know About the Latest Updates to the Paycheck Protection Program (PPP)**

### **Nossaman LLP**

This is an update to our eAlert dated April 3, 2020 entitled "Finding the Right Fit Under CARES: Understanding the SBA Loan Programs Available Under..."

---

## **Three tips for Government contractors seeking CARES Act Section 3610 assistance for paying employees or subcontractors**

### **Thompson Coburn LLP**

As many Government contractors have heard by now, Section 3610 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act includes a section...

---

## **OFAC Issues Fact Sheet on Providing Humanitarian Aid to Combat COVID-19 Under Various Sanctions Programs**

### **Thompson Hine LLP**

On April 16, 2020, the Department of the Treasury's Office of Foreign Assets Control (OFAC) stated that the United States "is committed to ensuring..."

---

## **Reopening the State of Georgia**

Georgia

### **Barnes & Thornburg LLP**

On April 20, Georgia Gov. Brian Kemp laid out his initial plan to reopen the State's economy. His plan calls for a gradual economic reopening with...

---

## **Illinois residents urged to 'stay at home'**

Illinois

### **Thompson Coburn LLP**

In an unprecedented move, Governor J.B. Pritzker extended his "stay at home" order through Saturday May 30, 2020, for residents of the state of...

---

## **Managing CARES Act Stimulus Funds: Preparing for Robust Federal Oversight**

### **Squire Patton Boggs**

On March 27, 2020, the President signed the much-anticipated Phase 3 of the coronavirus disease 2019 (COVID-19) stimulus package (the Coronavirus Aid...

---

## **COVID-19 class actions against universities**

### **Hogan Lovells**

In response to the COVID-19 pandemic, universities have had to make difficult, but important, decisions to protect the health of their students, among...

---

## **House Votes to Form COVID-19 Oversight Subcommittee**

### **Step toe & Johnson LLP**

In its brief return to work on April 23 to vote on added funding for the CARES Act, the US House of Representatives also approved a new Select...

---

## **Are Environmental Cleanups "Essential" Under Gov. Inslee's Shelter-in-Place Order?**

Washington

### **Davis Wright Tremaine LLP**

Across Washington State, businesses and individuals are working hard to comply with Gov. Jay Inslee's "Stay Home, Stay Healthy" Order, issued as...

---

#### **Government Innovation During a Pandemic**

##### **Bilzin Sumberg**

During this current COVID-19 crisis, a great deal has been written on what government is not doing (or not allowing others to do). But the same...

---

#### **Congress Passes "Stimulus 3.5" to Aid Small Businesses, Hospitals, and Virus Testing**

##### **Bradley Arant Boult Cummings LLP**

Governmental Affairs Alert The House and Senate have passed the latest round of emergency stimulus measures to address the COVID-19 crisis - a \$484...

---

#### **California's Newsom on Reopening State: 'There Is No Light Switch, There Is No Date'**

California

##### **Manatt Phelps & Phillips LLP**

As promised, California Governor Gavin Newsom provided an update on reopening the California economy in his daily press conference: There is no...

---

#### **No Private Right of Action to Enforce CARES Act; Expect Claims Under State Consumer Protection Laws**

##### **McGuireWoods LLP**

As previously reported, the U.S. District Court for the District of Maryland denied multiple motions brought by a number of small business owners...

---

#### **Litigation During the Pandemic: Remote Depositions**

##### **Cozen O'Connor**

No one knows how long we will be living in this COVID-19-inspired Twilight Zone Episode. Estimates vary widely over how long shelter in place rules...

---

#### **COVID-19 Washington Update: April 21, 2020**

##### **Kelley Drye & Warren LLP**

Today, the Senate passed a \$484 billion interim emergency funding bill, with House passage expected Thursday. See more below on today's federal...

---

#### **Impacts of COVID-19 on U.S. Infrastructure Projects**

##### **Nossaman LLP**

As the COVID-19 pandemic continues, both the public and private sectors have been working to understand the market's response and search for...

---

#### **Congress Funds \$310B for Paycheck Protection Program, \$60B for Economic Injury Disaster Loans**

##### **McGuireWoods LLP**

The U.S. House of Representatives passed the Paycheck Protection Program and Health Care Enhancement Act (PPP Enhancement Act) by 388 to 5 on April...



---

## Connecticut and New Jersey Executive Orders on COVID-19 Business Closures

Connecticut

New Jersey

### Davis Wright Tremaine LLP

As we reported on Friday, March 20, all non-essential businesses across New York State are under orders from Governor Cuomo to keep 100 percent of...

---

## COVID-19 Giveaways: Avoiding the Pitfalls of Charitable Promotions and Marketing

### Thompson Hine LLP

Many organizations have substantially increased their charitable contributions, corporate giving and philanthropy to assist those affected by the...

---

## Federal Aid Plan for PPP and Hospitals Announced

### Michael Best & Friedrich LLP

Congress and the White House Announce Deal Congressional leaders and the White House have agreed to Phase 3.5 of COVID-19 Response. This deal will...

---

## Lessons Learned from Post-9/11 and Anthrax Experiences to be Applied to Covid-19 in the Food Industry

### Hogan Lovells

As we face huge challenges from COVID-19, I am reminded daily of the parallels we faced in the 9/11 aftermath and related Anthrax incident nearly 20...

---

## Attorney General's Office Issues Opinion on the Definition of "Effective Date" as Used in Business and Professions Code Section 805

### Nossaman LLP

At the request of the Medical Board of California, on April 17, 2020, the Office of the Attorney General issued California Opinion of the Attorney...

---

## DOE Requests Input on Fusion Public-Private Partnership Program

### Hogan Lovells

Fusion holds the potential to revolutionize energy generation around the globe, and innovators in the private sector have been working hard to make...

---

## COVID-19 Litigation And Government Investigations in the U.S.: What We Are Seeing Now, And What the Future Holds

### Goodwin Procter LLP

The emergence of COVID-19 has led to increased litigation and government activity across all industries, and this trend is only likely to accelerate...

---

## President Trump Signs Second Emergency Stimulus Bill Allocating Additional Funding for Paycheck Protection Program

### Greenbaum, Rowe, Smith & Davis LLP

A short while ago, President Trump signed the Paycheck Protection Program and Health Care Enhancement Act into law. The legislation allocates \$484...

---

## **IP Watchdog, "Emergency Distance Learning and Fair Use"**

### **Berger Singerman LLP**

"[A] teacher creates a transformative work, which falls into the protective bubble of Fair Use, when they craft a message, enhance their students'...

---

## **Managing Outdoor Race Season in Uncertain Times**

### **Ansa Assuncao LLP**

The breaking of winter brings warmer weather and, in usual times, the first 5K, half/full marathon, and even 100-mile super-marathon (yes, you read...

---

## **COVID-19: Congress Approves Interim Emergency Relief Package**

### **Pierce Atwood LLP**

On Friday, April 24, 2020, President Trump signed another emergency relief package (CARES Act II) totaling close to \$500 billion, the bulk of which...

---

## **New Federal Stimulus Legislation Provides Funding for Small Businesses, Healthcare Providers, and Coronavirus Testing**

### **Ogletree Deakins**

On April 24, 2020, President Trump signed the Paycheck Protection Program and Health Care Enhancement Act, which will allocate over \$480 billion in...

---

## **Alaska Issues COVID-19 Mandates to Clarify Restrictions on Religious Gatherings and to Address Non-urgent and Elective Medical Procedures**

Alaska

### **Ogletree Deakins**

Alaska has joined a growing number of states addressing the thorny issue of the size and density of religious gatherings during the COVID-19 health...

---

## **House Passes a \$484 Billion Relief Package; Treasury and the SBA Release New Guidelines for PPP Loans**

### **Morrison & Foerster LLP**

On Thursday, April 23, 2020, the U.S. House of Representatives voted in favor of the \$484 billion relief package that passed in the Senate earlier...

---

## **Davidson County (TN) Extends Safer-At-Home Order And Unveils Roadmap For Reopening Nashville**

Tennessee

### **Fisher Phillips**

Though the statewide Safer at Home Order is set to expire on April 30, some counties in Tennessee - including Davidson County - have extended their...

---

## **HHS Announces Further Allocations of \$100 Billion CARES Act Provider Relief Fund; Warns of "Significant" Anti-Fraud and Auditing Work**

### **Bass, Berry & Sims PLC**

On Wednesday, April 22, the U.S. Department of Health and Human Services (HHS) issued a press release announcing additional allocations from the \$100...

---

## **US Education Policy Update: Governor's Emergency Education Relief Fund - Charter School Grants - and More**



### **Squire Patton Boggs**

The following update includes two latest funding announcements on the GEER Fund (the Governor's Emergency Education Relief Fund) and for charter...

---

### **Consider COVID Attitude Changes, Part 4: More Polarization on Science**

#### **Holland & Hart LLP**

After a brief time when it seemed that Americans were coming together in favor of social isolation to slow the spread of the novel coronavirus, it...

---

### **Senate Approves \$310 Billion in Additional Funding for the Paycheck Protection Program**

#### **Paul Weiss**

On April 21, 2020, the Senate passed the "Paycheck Protection Program and Health Care Enhancement Act"[1] to provide up to \$484 billion in additional...

---

### **United Technologies/Raytheon Highlights Key Issues in Aerospace and Defense Industry Merger Review**

#### **McDermott Will & Emery**

The DOJ Antitrust Division's (DOJ) recent challenge to the United Technologies (UTC)/Raytheon (RTN) merger highlights a few key considerations for...

---

### **PPPHCEA Expands the PPP, EIDL and the Number of Acronyms We Need to Master**

#### **Lane Powell PC**

On April 22, the Senate approved a new stimulus bill and the House followed with their approval. On April 23, President Trump has indicated he will...

---

### **U.S. Importers Can Postpone Duty Payments for 90 Days, But Relief Limited**

#### **Stinson LLP**

On April 19, U.S. Customs and Border Protection (CBP) announced the rollout of a 90-day duty deferral program for importers experiencing significant...

---

### **Congress Passes Additional \$100 Billion in Aid for Public Health and Social Services Emergency Fund**

#### **Bass, Berry & Sims PLC**

On April 21, the U.S. Senate approved an additional \$100 billion in funding for the Public Health and Social Services Emergency Fund established under...

---

### **EPA Announces Its Continued Efforts to Provide Critical Information on Safe Disinfectant Use During COVID-19 Crisis**

#### **Bergeson & Campbell PC**

On April 23, 2020, the U.S. Environmental Protection Agency (EPA) announced it is continuing efforts to provide critical information on surface...

---

### **Maryland Governor Announces Three-Stage Plan for Reopening the State**

Maryland

#### **Duane Morris LLP**

On Friday afternoon, Maryland Governor Larry Hogan announced a three-stage plan to reopen the State called “Maryland Strong: Roadmap to Recovery,”...

---

**Commercial Real Estate Finance COVID-19 Impact Series: Retail and Shopping Center Landlords**

**Frost Brown Todd LLC**

The ongoing COVID-19 pandemic continues to impact all areas of the economy, however, retail shopping center owners (often referred to below as...

---

**New Problem, Old Solution: Bring Back Tax-Exempt Advance Refundings**

**Squire Patton Boggs**

As the world grapples with the effects of the coronavirus disease 2019 (COVID-19) pandemic, state and local governments (collectively, State and Local...

---

**Executive Summary: Tracking Telehealth Changes State-by-State in Response to COVID-19**

**Manatt Phelps & Phillips LLP**

As the coronavirus pandemic continues to spread across the U.S., states, payers and providers are looking for ways to expand access to telehealth...

---

**COVID-19: Medidas para la adquisición de medicamentos y otros insumos de la salud**

**Morgan & Morgan**

De Acuerdo a la Resolución No. 53960 de 25 de marzo de 2020, se incluye un nuevo artículo que establece el procedimiento bajo la...

---

**SBA 7(a) Program Funding May Temporarily Lapse Due to CARES Act Mishap**

**Nelson Mullins Riley & Scarborough LLP**

With Congress set to replenish the Paycheck Protection Program (PPP) funding this week, SBA 7(a) program lenders are urging lawmakers to clarify...

---

**Department of Health & Human Services Clarifies Broad Scope of Immunity Protection Under the PREP Act**

**Duane Morris LLP**

While the declaration defined “Covered Persons” and “Covered Countermeasures,” there were numerous requests for more clarity on the scope of the...

---

**Mashpee Wampanoag Tribe Seeks Reservation Protection from Federal Court**

**Barnes & Thornburg LLP**

The Mashpee Wampanoag Tribe, also known as the People of the First Light, has inhabited present-day Massachusetts and Eastern Rhode Island for...

---

**Regulatory Takings and Executive Power to Seize Property** [Audio](#)

**Pepper Hamilton LLP**

Troutman Sanders and Pepper Hamilton are producing a series of podcasts to discuss litigation topics that have been brought to the forefront by the...



---

## **HHS Provides Additional Guidance on Uninsured Funding and Application for the Remainder of General Distribution Funds**

### **Ropes & Gray LLP**

On April 27th, the Health Resources & Services Administration (HRSA) launched its portal for reimbursement of uninsured COVID-19 testing and...

---

## **Providers Can Now Access Additional \$20 Billion via CARES Act Relief Portal**

### **Gordon Rees Scully Mansukhani**

All providers with a Medicare billing tax identification number may now apply for a grant from the Phase II CARES Act Provider Relief Fund via the...

---

## **CARES Act Relief Fund Payments to Health Care Providers: Key Requirements and Compliance Risks**

### **Faegre Drinker Biddle & Reath LLP**

On April 10, 2020, the federal government began distributing \$30 billion of the \$100 billion in funds that the Coronavirus Aid, Relief, and Economic...

---



## **Global**

### **Construction**



## **The FIDIC Yellow Book Subcontract: Opportunities in Asia?**

### **White & Case LLP**

Late last year, the Fédération Internationale Des Ingénieurs-Conseils<sup>1</sup> ("FIDIC") launched the First Edition Conditions of Subcontract for Plant and...

---

## **Core Project Agreements**

### **Morgan Lewis**

To fully appreciate project agreements, it is important to understand their significant role in a project finance transaction, which is essentially a...

---

### **Employment & Labor**



## **ESG - Risks and opportunities in the Infrastructure investment cycle**

### **Linklaters LLP**

97%<sup>1</sup> of infrastructure companies<sup>2</sup> with core and non-core infrastructure assets are exposed to environmental, social and governance (ESG) risks that...

---

## **Business as unusual - What role can business play in shaping a fair and lasting recovery?**

### **Freshfields Bruckhaus Deringer**

How we recover from the crisis will shape our societies for many generations. How business responds to this challenge will define their future...

---

## **COVID-19 Summary of Government Financial Support Europe and Middle East** **Squire Patton Boggs**

The federal state will provide a guarantee of €50 billion for certain loans issued by financial institutions in Belgium...

---

## **Australia: Competition and Consumer Commission**

### **Global Competition Review**

As Australia's competition regulator, the Australian Competition and Consumer Commission (ACCC) is tasked with protecting competitive processes by...

---

## **CMS Expert Guide to Government Support for Employers and Workers**

### **CMS Legal**

During previous economic crises, Germany came up with a social instrument called Kurzarbeit ("short-time working") to sustain businesses and save jobs...

---

## **Todos os olhos em mim: dicas práticas para compliance durante e após um período de crise**

### **Paul Hastings LLP**

Diretores de compliance, advogados internos e outros gatekeepers corporativos sabem que, mesmo quando a economia está em expansão, a implementação de...

---

## **Our guide to the top 10 employment issues facing the hospitality & leisure industry during COVID-19**

### **DLA Piper**

As with other sectors, hotels and establishments have an obligation to ensure a safe workplace for their employees, which includes taking steps to...

---

## **Keeping the Lights on During the Coronavirus Pandemic: Lessons from Around the Globe**

### **Baker McKenzie**

COVID-19 and government responses to the growing pandemic are creating unprecedented and rapidly evolving challenges. In the coming days, businesses...

---

## **Africa Business in Brief - ISSUE 349 | 26 APR 2020**

### **ENSafrica**

Africa: The African Development Bank Group (AfDB) is ready to provide fast, flexible and effective responses to lessen the severe economic and social...

---

Law Department Management



## **COVID-19: Managing the Security Risks of a Remote Workforce**

### **K2 Intelligence/Financial Integrity Network**

As COVID-19 remains prevalent, working remotely has become the new normal. This means that many organizations will have people working from home for...

---



## **A Guide to Cybersecurity to Address CFIUS Considerations**

### **K2 Intelligence/Financial Integrity Network**

Investors and deal makers are taking note: The Committee on Foreign Investment in the United States (CFIUS, or the Committee) will focus on foreign...

---

## **FATF upgrades U.S. customer due diligence regime**

### **K2 Intelligence/Financial Integrity Network**

On March 31st the Financial Action Task Force (FATF) - the global AML/CFT standard-setting body and watchdog- announced that it has upgraded...

---

## **How to reach out and support your clients**

### **Globe Law and Business**

This is an unprecedented time for lawyers, for clients and for everyone. Whilst many lawyers may hesitate to pick up the phone for fear of being too...

---

Public



## **COVID-19: IP Strategies for Universities and Nonprofits During the Pandemic - Mitigating Patent Infringement Risks When Making PPE and Other Health-Related Supplies**

### **K&L Gates**

The rapid emergence of COVID-19 — and the limited and diminishing supply of healthcare resources needed to treat patients and protect healthcare...

---

## **Consider COVID Attitude Changes, Part 3: Higher Levels of Xenophobia**

### **Holland & Hart LLP**

What's in a name? In the current pandemic, do you prefer to call it the "coronavirus," or the "Chinese-" or "Wuhan-Virus"? In addition to that choice...

---

## **GBP1 million target hit for Hope and Homes for Children**

### **Allen & Overy LLP**

Discover how the money we've raised for our Global Charity Partner is being used to end institutionalisation and how we're extending our partnership...

---

## **COVID-19: Public Health Orders**

### **King & Wood Mallesons**

The table below provides a current snapshot of the material restrictions on businesses, venues and movement that have been imposed by the Australian...

---

## **Women leaders are setting an example**

### **DLA Piper**

It turns out women leaders are perfectly suited to lead the way in this crisis with a combination of decisiveness, practicality and empathy...

---

## **COVID-19: government response guide for Africa**

### **DLA Piper**

As African governments take drastic action to help businesses weather the storm

from COVID-19, we have produced a guide to help lay out the measures...

---

## **Driving Research & Development in a Downturn**

### **Ellis Terry**

In challenging times, the natural reaction of many businesses is to minimise expenditure in an attempt to ride out the storm. Research and...

---

## **Other top stories**

**COVID-19 Guide for Attorneys and GCs**

---

**Five Interesting Force Majeure Cases from Around the Country**

---

**Preparing For Re-Entry: Key Considerations For Returning Employees To The Workplace Amid The COVID-19 Crisis**

---

**COVID-19: Executing Simple Agreements and Deeds Remotely Under English Law**

---

**Employment-related COVID-19 Litigation Has Begun**

---

**Texas Governor Issues Executive Orders to Reopen Business for Retail and Healthcare Employers**

---

**Employee furlough considerations**

---

**ESG, Capital Access, and the Future of the Oil & Gas Industry**

---

**COVID-19 and the World of Commercial Leases: Force Majeure and Related Common Law Doctrines**

---

**Second Circuit Invokes Standard Contract Provisions to Limit the Use of Agency and Estoppel to Bind Non-Signatories to Arbitration**

---

---

## **International developments**

**Indirect and consequential loss exclusions: English law holds the line for now**

---

**Canada Emergency Wage Subsidy Calculator**

---

**Cambodia Legal Update: Ministry of Tourism Issues Notification on Government's Additional Measures Towards Certain Tourism Enterprises Seriously Impacted by COVID-19**

---

**Are Contractors Playing with Fire? Construction Projects and 'Uncertified Revenue'**

---

**Cyprus corrects halloumi trade mark mishap**

---

**JobKeeper - new rules for calculating a decline in turnover for service entities**

---

**International tracker - COVID-19 Restrictions**

---

**First-step analysis: risk & compliance management in China**

---

**Can Private Employers Pay Reduced Salary during Lockdown**

---

**COVID-19 impact on the Hong Kong private education market**

---



[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law  
[Contact Lexology](#)

[About Lexology](#)



© 2006-2020 Law Business Research

**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of April 20, 2020  
**Date:** Monday, April 27, 2020 10:18:37 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of April 20, 2020](#)

04/27/2020 06:27 AM EDT

Original release date: April 27, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ios_and_macos_and_mojave_and_tvos	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. An attacker in a privileged network position may be able to intercept network traffic.	2020-04-17	<a href="#">7.5</a>	<a href="#">CVE-2019-6203</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A type confusion vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code read/write on the system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7081</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A use-after-free vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to code execution on a system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7082</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A heap overflow vulnerability in the Autodesk FBX-SDK versions 2019.2 and earlier may lead to arbitrary code execution on a system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7085</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A buffer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code execution on a system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7080</a> <a href="#">MISC</a>
evenroute -- iqrouter	IQrouter through 3.3.1, when unconfigured, has multiple remote code execution vulnerabilities in the web-panel because of Bash Shell Metacharacter Injection.	2020-04-21	<a href="#">7.5</a>	<a href="#">CVE-2020-11963</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, there is a root user without a password, which allows attackers to gain full remote access via SSH.	2020-04-21	<a href="#">7.5</a>	<a href="#">CVE-2020-11965</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, the Lua function reset_password in the web-panel allows remote attackers to change the root password arbitrarily.	2020-04-21	<a href="#">7.5</a>	<a href="#">CVE-2020-11966</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, remote attackers can control the device (restart network, reboot, upgrade, reset) because of Incorrect Access Control.	2020-04-21	<a href="#">9</a>	<a href="#">CVE-2020-11967</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In onOpActiveChanged and related methods of AppOpsControllerImpl.java, there is a possible way to display an app overlaying other apps			

google -- android	without the notification icon that it's overlaying. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144092031	2020-04-17	9.3	<a href="#">CVE-2020-0080</a> MISC
google -- android	In finalize of AssetManager.java, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144028297	2020-04-17	7.2	<a href="#">CVE-2020-0081</a> MISC
google -- android	In ExternalVibration of ExternalVibration.java, there is a possible activation of an arbitrary intent due to unsafe deserialization. This could lead to local escalation of privilege to system_server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140417434	2020-04-17	7.2	<a href="#">CVE-2020-0082</a> MISC
google -- android	In rw_t2t_extract_default_locks_info of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310721	2020-04-17	10	<a href="#">CVE-2020-0071</a> MISC
google -- android	In rw_t2t_update_lock_attributes of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-148159613	2020-04-17	10	<a href="#">CVE-2020-0070</a> MISC
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310271	2020-04-17	10	<a href="#">CVE-2020-0072</a> MISC
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147309942	2020-04-17	10	<a href="#">CVE-2020-0073</a> MISC
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService mishandles OTA Provisioning on V40 and G7 devices. The LG ID is LVE-SMP-190006 (July 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20777</a> CONFIRM
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. A stack-based buffer overflow in the logging tool could allow an attacker to gain privileges. The LG ID is LVE-SMP-200005 (April 2020).	2020-04-17	7.5	<a href="#">CVE-2020-11873</a> CONFIRM
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. Unprivileged applications can execute shell commands via the connectivity service. The LG ID is LVE-SMP-190008 (August 2019).	2020-04-17	7.2	<a href="#">CVE-2019-20773</a> CONFIRM
	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1			

lg -- multiple_mobile_devices	software. Certain security settings, related to whether packages are verified and accepted only from known sources, are mishandled. The LG ID is LVE-SMP-190002 (April 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20780</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. LG Advanced Flash (LAF) has a buffer overflow. The LG ID is LVE-SMP-190001 (March 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20782</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Backup subsystem does not properly restrict operations or validate their input. The LG ID is LVE-SMP-190004 (June 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20778</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Account subsystem allows authorization bypass. The LG ID is LVE-SMP-190007 (August 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20772</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10.0 (MTK chipsets) software. The MTK kernel does not properly implement exception handling, allowing an attacker to gain privileges. The LG ID is LVE-SMP-200001 (February 2020).	2020-04-17	7.2	<a href="#">CVE-2020-11875</a> <a href="#">CONFIRM</a>
mitel_networks -- mivoice_connect	A remote code execution vulnerability in UCB component of Mitel MiVoice Connect before 19.1 SP1 could allow an unauthenticated remote attacker to execute arbitrary scripts due to insufficient validation of URL parameters. A successful exploit could allow an attacker to gain access to sensitive information.	2020-04-17	7.5	<a href="#">CVE-2020-10211</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by a hardcoded password. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-23	7.5	<a href="#">CVE-2018-21137</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020-04-23	7.5	<a href="#">CVE-2018-21132</a> <a href="#">CONFIRM</a>
pion -- dtls	handleIncomingPacket in conn.go in Pion DTLS before 1.5.2 lacks a check for application data with epoch 0, which allows remote attackers to inject arbitrary unencrypted data after handshake completion.	2020-04-19	7.5	<a href="#">CVE-2019-20786</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
webkitgtk -- webkitgtk_and_wpe_webkit	A use-after-free issue exists in WebKitGTK before 2.28.1 and WPE WebKit before 2.28.1 via crafted web content that allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash).	2020-04-17	7.5	<a href="#">CVE-2020-11793</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	In the media-library-assistant plugin before 2.82 for WordPress, Remote Code Execution can occur via the tax_query, meta_query, or date_query parameter in mla_gallery via an admin.	2020-04-20	7.5	<a href="#">CVE-2020-11928</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- dynamo_bim	An improper signature validation vulnerability in Autodesk Dynamo BIM versions 2.5.1 and 2.5.0 may lead to code execution through maliciously crafted DLL files.	2020-04-17	4.4	<a href="#">CVE-2020-7079</a> <a href="#">MISC</a>



autodesk -- fbx_software_development	A NULL pointer dereference vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	2020-04-17	4.3	<a href="#">CVE-2020-7084</a> MISC
autodesk -- fbx_software_development	An integer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	2020-04-17	4.3	<a href="#">CVE-2020-7083</a> MISC
bitrock -- installbuilder_autoupdate_tool	InstallBuilder AutoUpdate tool and regular installers enabling <checkForUpdates> built with versions earlier than 19.11 are vulnerable to Billion laughs attack (denial-of-service).	2020-04-20	5	<a href="#">CVE-2020-3946</a> CONFIRM
byobu_apport -- byobu_apport	Byobu Apport hook may disclose sensitive information since it automatically uploads the local user's .screenrc which may contain private hostnames, usernames and passwords. This issue affects: byobu	2020-04-17	5	<a href="#">CVE-2019-7306</a> MISC MISC
evenroute -- iqrouter	In IQrouter through 3.3.1, the Lua function diag_set_password in the web-panel allows remote attackers to change the root password arbitrarily.	2020-04-21	5	<a href="#">CVE-2020-11964</a> MISC MISC
evenroute -- iqrouter	In the web-panel in IQrouter through 3.3.1, remote attackers can read system logs because of Incorrect Access Control.	2020-04-21	5	<a href="#">CVE-2020-11968</a> MISC MISC
ftpdmin -- ftpdmin	A buffer overflow vulnerability in FTPDMIN 0.96 allows attackers to crash the server via a crafted packet.	2020-04-17	5	<a href="#">CVE-2020-10813</a> MISC MISC
google -- android	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-9 Android-10 Android ID: A-144506242	2020-04-17	4.6	<a href="#">CVE-2020-0079</a> MISC
google -- android	In releaseSecureStops of DrmPlugin.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-9 Android-10 Android ID: A-144766455	2020-04-17	4.6	<a href="#">CVE-2020-0078</a> MISC
google -- android	In get_auth_result of the FPC IRIS TrustZone app, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-146056878	2020-04-17	4.6	<a href="#">CVE-2020-0076</a> MISC
google -- android	There is a possible disclosure of RAM using a shared crypto key due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-140879284	2020-04-17	4.9	<a href="#">CVE-2019-2056</a> MISC
huawei -- taurus_al00b_smartphones	Huawei smartphones Taurus-AL00B with versions earlier than 10.0.0.205(C00E201R7P2) have an improper authentication vulnerability. The software insufficiently validate the user's identity when a user wants to do certain operation. An attacker can trick user into installing a malicious application to exploit this vulnerability. Successful exploit may cause some information disclosure.	2020-04-20	4.3	<a href="#">CVE-2020-9070</a> CONFIRM CONFIRM
bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 170880.	2020-04-17	4.3	<a href="#">CVE-2019-4644</a> XF CONFIRM

bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 could allow an authenticated user perform actions they are not authorized to by modifying request parameters. IBM X-Force ID: 163490.	2020-04-17	5.5	<a href="#">CVE-2019-4446</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
bm -- tririga_application_platform	IBM TRIRIGA Application Platform 3.5.3 and 3.6.1 discloses sensitive information in error messages that could aid an attacker formulate future attacks. IBM X-Force ID: 175993.	2020-04-17	5	<a href="#">CVE-2020-4277</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
lg -- g3_devices	An issue was discovered in LG PC Suite for LG G3 and earlier (aka LG PC Suite v5.3.27 and earlier). DLL Hijacking can occur via a Trojan horse DLL in the current working directory. The LG ID is LVE-MOT-190001 (November 2019).	2020-04-17	4.4	<a href="#">CVE-2019-20769</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9.0 software. The HAL service has a buffer overflow that leads to arbitrary code execution. The LG ID is LVE-SMP-190013 (September 2019).	2020-04-17	4.6	<a href="#">CVE-2019-20770</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0 and 8.1 software for the DTAG carrier. RILD in the radio layer uses an uninitialized variable. The LG ID is LVE-SMP-180013 (January 2019).	2020-04-17	4.6	<a href="#">CVE-2019-20785</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService allows unconfirmed configuration changes via a modified OMACP message. The LG ID is LVE-SMP-190006 (August 2019).	2020-04-17	5	<a href="#">CVE-2019-20771</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (North America CDMA) software. The LTE protocol implementation allows a bypass of AKA (Authentication and Key Agreement). The LG ID is LVE-SMP-180014 (February 2019).	2020-04-17	6.4	<a href="#">CVE-2019-20783</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9, and 10 software. Attackers can bypass Factory Reset Protection (FRP). The LG ID is LVE-SMP-200004 (March 2020).	2020-04-17	5	<a href="#">CVE-2020-11874</a> <a href="#">CONFIRM</a>
libming -- libming	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (2 bytes) in the function decompileIF() in decompile.c.	2020-04-19	6.4	<a href="#">CVE-2020-11895</a> <a href="#">MISC</a>
libming -- libming	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (8 bytes) in the function decompileIF() in decompile.c.	2020-04-19	6.4	<a href="#">CVE-2020-11894</a> <a href="#">MISC</a>
netgear -- d6100_devices	NETGEAR D6100 devices before 1.0.0.50_0.0.50 are affected by command injection.	2020-04-21	4.6	<a href="#">CVE-2017-18792</a> <a href="#">CONFIRM</a>
netgear -- d6220_and__d6100_devices	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.28 and D6100 before 1.0.0.50_0.0.50.	2020-04-21	4.6	<a href="#">CVE-2017-18795</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWN2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-23	5.8	<a href="#">CVE-2017-18734</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and	2020-04-21	4.6	<a href="#">CVE-2017-18805</a> <a href="#">CONFIRM</a>

	WNDAP360 before 3.7.4.0.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R7800 before 1.0.2.36, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	2020-04-22	5.2	<a href="#">CVE-2017-18770</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	2020-04-20	4.6	<a href="#">CVE-2017-18850</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-21	5.2	<a href="#">CVE-2018-21147</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	4.6	<a href="#">CVE-2017-18779</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JR6150 before 1.0.1.12, JNR1010v2 before 1.1.0.44, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	6.8	<a href="#">CVE-2017-18782</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6220 before V1.1.0.50, R7800 before V1.0.2.36, WNDR3400v3 before 1.0.1.14, and WNDR3700v5 before V1.1.0.48.	2020-04-23	5.8	<a href="#">CVE-2017-18739</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	4.3	<a href="#">CVE-2017-18783</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNDR2010v5 before 1.1.0.44, JR6150 before 1.0.1.12, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-	6.8	<a href="#">CVE-2017-18781</a>

	1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	22		<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6300v2 before 1.0.4.8_10.0.77, R6400 before 1.0.1.24, R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, R8500 before 1.0.2.100, and D6100 before 1.0.0.50_0.0.50.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18794</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D8500 through 1.0.3.28, R6400 through 1.0.1.22, R6400v2 through 1.0.2.18, R8300 through 1.0.2.94, R8500 through 1.0.2.94, and R6100 through 1.0.1.12.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18851</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6400 before 1.0.1.24, R6700 before 1.0.1.26, R6900 before 1.0.1.28, R7000 before 1.0.9.10, R7000P before 1.0.1.16, R6900P before 1.0.1.16, and R7800 before 1.0.2.36.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18796</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2017-18835</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6100 before V1.0.0.55, D7800 before V1.0.1.24, EX6150v2 before 1.0.0.48, R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before V1.0.3.16, R7800 before V1.0.2.36, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.48.	2020-04-22	<a href="#">4.6</a>	<a href="#">CVE-2017-18773</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2017-18834</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6100 before V1.0.0.55, D7000 before V1.0.1.50, D7800 before V1.0.1.24, JNR1010v2 before 1.1.0.40, JWNDR2010v5 before 1.1.0.40, R6100 before 1.0.1.12, R6220 before 1.1.0.50, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.40, WNR2000v5 before 1.0.0.42, WNR2020 before 1.1.0.40, and WNR2050 before 1.1.0.40.	2020-04-22	<a href="#">4.6</a>	<a href="#">CVE-2017-18776</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2017-18833</a> <a href="#">CONFIRM</a>



	before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before 1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96, DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6150v2 before 1.0.1.54, EX6100v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.18, R6900P before 1.3.0.8, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R8000 before 1.0.4.4_1.1.42, R7900P before 1.1.5.14, R8000P before 1.1.5.14, R8300 before 1.0.2.110, R8500 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.14, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	2020-04-22	4.6	<a href="#">CVE-2017-18788</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	4.3	<a href="#">CVE-2017-18784</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.50, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.48, and D7000 before 1.0.1.50.	2020-04-21	4.6	<a href="#">CVE-2017-18801</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.6	<a href="#">CVE-2017-18838</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before 1.0.3.16, R7800 before 1.0.2.32, EX6200v2 before 1.0.1.50, and D7800 before 1.0.1.22.	2020-04-21	4.6	<a href="#">CVE-2017-18802</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15,			

netgear -- multiple_devices	M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18830 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.46, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.46, and D7000 before 1.0.1.50.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18841 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects R6400 before 1.0.1.14, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	2020-04-23	<a href="#">4.3</a>	<a href="#">CVE-2017-18745 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18837 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.0.36, AC1450 before 1.0.0.36, R7300 before 1.0.0.54, and R8500 before 1.0.2.94.	2020-04-20	<a href="#">6.8</a>	<a href="#">CVE-2017-18848 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18829 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R7300 before 1.0.0.54, R8500 before 1.0.2.94, DGN2200v1 before 1.0.0.55, and D2200D/D2200DW-1FRNAS before 1.0.0.32.	2020-04-20	<a href="#">6.8</a>	<a href="#">CVE-2017-18842 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18826 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18822 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and WNDAP360 before 3.7.4.0.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18806 CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow. This affects R6250 before 1.0.4.12, R6400v2 before 1.0.2.32, R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	2020-04-20	4.6	<a href="#">CVE-2017-18846</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF and authentication bypass. This affects R7300DST before 1.0.0.54, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and WNDR3400v3 before 1.0.1.14.	2020-04-20	6.8	<a href="#">CVE-2017-18852</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	2020-04-20	4.6	<a href="#">CVE-2017-18849</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6100 before 1.0.1.12, R7500 before 1.0.0.108, WNDR3700v4 before 1.0.2.86, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.42.	2020-04-22	6.8	<a href="#">CVE-2017-18775</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R7100LG before 1.0.0.32, R7300DST before 1.0.0.52, R8300 before 1.0.2.94, and R8500 before 1.0.2.100.	2020-04-23	5.8	<a href="#">CVE-2017-18733</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	2020-04-23	5.8	<a href="#">CVE-2017-18744</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6100 before 1.0.1.14, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, R7500 before 1.0.0.110, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	5.8	<a href="#">CVE-2017-18764</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, and WNR2000v5 before 1.0.0.58.	2020-04-22	5.2	<a href="#">CVE-2017-18754</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated	2020-04-		<a href="#">CVE-2018-</a>

	attacker. This affects WC7500 before 6.5.3.9, WC7520 before 6.5.3.9, WC7600v1 before 6.5.3.9, and WC7600v2 before 6.5.3.9.	22	<a href="#">5.8</a>	<a href="#">21123 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21121 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-22	<a href="#">6</a>	<a href="#">CVE-2018-21120 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.58, D7800 before 1.0.1.42, R6100 before 1.0.1.28, R7500 before 1.0.0.130, R7500v2 before 1.0.3.36, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, and WNDR4500v3 before 1.0.0.56.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21113 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, R8500 before 1.0.2.74, and WNR2000v2 before 1.2.0.8.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2017-18772 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D3600 before 1.0.0.68, D6000 before 1.0.0.68, D6100 before 1.0.0.57, R6100 before 1.0.1.16, R6900P before 1.2.0.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2017-18762 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18750 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6400 before 1.0.1.14, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300 before 1.0.0.56, R7800 before 1.0.2.36, R7900 before 1.0.2.10, R8000 before 1.0.3.24, R8300 before 1.0.2.74, and R8500 before 1.0.2.74.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18767 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX6150v2 before 1.0.1.54, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R6900P before 1.2.0.22, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R6100 before 1.0.1.16, WNDR4300v2 before 1.0.0.48,	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18738 CONFIRM</a>



	WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21150 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, and R9000 before 1.0.4.12.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21112 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, EX6150v2 before 1.0.1.70, EX6100v2 before 1.0.1.70, EX6200v2 before 1.0.1.64, EX7300 before 1.0.2.136, EX6400 before 1.0.2.136, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.4.12, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21114 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18737 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-21	<a href="#">5.2</a>	<a href="#">CVE-2018-21148 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-21	<a href="#">5.2</a>	<a href="#">CVE-2018-21146 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6200v2 before 1.0.3.14, R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.1.1.20, R7000 before 1.0.7.10, R7000P/R6900P before 1.0.0.56, R7100LG before 1.0.0.30, R7900 before 1.0.1.14, R8000 before 1.0.3.22, R8500 before 1.0.2.74, and D8500 before 1.0.3.28.	2020-04-21	<a href="#">5</a>	<a href="#">CVE-2017-18799 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18732 CONFIRM</a>
	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.4.8, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000P before 1.0.0.86, R6900P			

netgear -- multiple_devices	before 1.0.0.56, R7300 before 1.0.0.54, R8300 before 1.0.2.106, R8500 before 1.0.2.106, DGN2200v4 before 1.0.0.86, DGND2200Bv4 before 1.0.0.86, R6050 before 1.0.0.86, JR6150 before 1.0.1.10, R6220 before 1.1.0.50, and WNDR3700v5 before V1.1.0.48.	2020-04-22	<a href="#">6.8</a>	<a href="#">CVE-2017-18755</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18758</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, and R6900v2 before 1.2.0.4.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18735</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, and WNDR3700v5 before 1.1.0.48.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18736</a> <a href="#">CONFIRM</a>
netgear -- r6700_and_r6800_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700v2 before 1.1.0.42 and R6800 before 1.1.0.42.	2020-04-21	<a href="#">4.3</a>	<a href="#">CVE-2017-18800</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by command injection. This affects R7800 before 1.0.2.16 and R9000 before 1.0.2.4.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18804</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21101</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.36 are affected by command injection.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18793</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21110</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21108</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21109</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21107</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21103</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21106</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21105</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21104</a> <a href="#">CONFIRM</a>
netgear -- r8000_devices	NETGEAR R8000 devices before 1.0.4.2 are affected by a stack-based buffer overflow by an authenticated user.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18761</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R8300 before 1.0.2.104 and R8500 before 1.0.2.104.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18759</a> <a href="#">CONFIRM</a>

netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18808</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WAC505 before 5.0.5.4 and WAC510 before 5.0.5.4.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21119</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by unauthenticated firmware downgrade. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020-04-23	<a href="#">6.4</a>	<a href="#">CVE-2018-21131</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by authentication bypass.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21118</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers via the traceroute handler.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21117</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21116</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21115</a> <a href="#">CONFIRM</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the sessionLocation parameter for the login page is vulnerable to cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5730</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the UI Framework Error Page reflects arbitrary, user-supplied input back to the browser, which can result in XSS. Any page that is able to trigger a UI Framework Error is susceptible to this issue.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5729</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the export functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows the export of potentially sensitive information.	2020-04-17	<a href="#">5.8</a>	<a href="#">CVE-2020-5733</a> <a href="#">MISC</a>
openmrs -- openmrs	OpenMRS 2.9 and prior copies "Referrer" header values into an html element named "redirectUrl" within many webpages (such as login.htm). There is insufficient validation for this parameter, which allows for the possibility of cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5728</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the app parameter for the ActiveVisit's page is vulnerable to cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5731</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the import functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows unauthenticated users to use a feature typically restricted to administrators.	2020-04-17	<a href="#">5.8</a>	<a href="#">CVE-2020-5732</a> <a href="#">MISC</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is an open redirection when using back parameter. The impacts can be many, and vary from the theft of information and credentials to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">5.8</a>	<a href="#">CVE-2020-5270</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.6.0.0 and 1.7.6.5, there is a reflected XSS with 'date_from' and 'date_to' parameters in the dashboard page. This problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5271</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.4.0 and 1.7.6.5, there is a reflected XSS when uploading a wrong file. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5286</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.1.0 and 1.7.6.5, there is a reflected XSS on AdminCarts page with `cartBox` parameter The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5276</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is a reflected XSS with `back` parameter. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5285</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.5.4.0 and 1.7.6.5, there is a reflected XSS on Exception page The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5278</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is a reflected XSS on Search page with `alias` and `search` parameters. The problem is patched in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5272</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminFeatures page by using the `id_feature` parameter. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5269</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminAttributesGroups page. The problem is patched in 1.7.6.5.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5265</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop before version 1.7.6.5, there is a reflected XSS while running the security compromised page. It allows anyone to execute arbitrary action. The problem is patched in the 1.7.6.5.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5264</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
svg2png -- svg2png	svg2png 4.1.1 allows XSS with resultant SSRF via JavaScript inside an SVG document.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-11887</a> <a href="#">MISC</a>
wordpress -- wordpress	The GTranslate plugin before 2.8.52 for WordPress has Reflected XSS via a crafted link. This requires use of the hreflang tags feature within a sub-domain or sub-directory paid option.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-11930</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In f2fs_xattr_generic_list of xattr.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation.Product: Android. Versions: Android kernel. Android ID: A-120551147.	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0067</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	In crus_afe_get_param of msm-cirrus-playback.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: Android. Versions: Android kernel. Android ID: A-139354541	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0068</a> <a href="#">CONFIRM</a>
google -- android	In authorize_enroll of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146055840	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0077</a> <a href="#">MISC</a>
	In set_shared_key of the FPC IRIS TrustZone			



google -- android	app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel/Android ID: A-146057864	2020-04-17	2.1	<a href="#">CVE-2020-0075</a> <a href="#">MISC</a>
huawei -- honor_v20_smartphones	Huawei smartphones Honor V20 with versions earlier than 10.0.0.179(C636E3R4P3), versions earlier than 10.0.0.180(C185E3R3P3), versions earlier than 10.0.0.180(C432E10R3P4) have an information disclosure vulnerability. The device does not sufficiently validate the identity of smart wearable device in certain specific scenario, the attacker need to gain certain information in the victim's smartphone to launch the attack, successful exploit could cause information disclosure.	2020-04-20	2.9	<a href="#">CVE-2020-1803</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 173308.	2020-04-17	3.5	<a href="#">CVE-2019-4749</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (MTK chipsets) software. Interaction of GPS with 911 emergency calls is mishandled. The LG ID is LVE-SMP-180012 (January 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20784</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A TrustZone trusted application can crash via crafted input. The LG ID is LVE-SMP-190003 (May 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20779</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. A TZ trusted application can crash via crafted input. The LG ID is LVE-SMP-190005 (July 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20776</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9.0 (Qualcomm SDM450, SDM845, SM6150, and SM8150 chipsets) software. Weak encryption leads to local information disclosure. The LG ID is LVE-SMP-190010 (August 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20775</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A system service allows local retrieval of the user's password. The LG ID is LVE-SMP-190009 (August 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20774</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-21	3.3	<a href="#">CVE-2018-21140</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-23	2.1	<a href="#">CVE-2018-21136</a> <a href="#">CONFIRM</a>
netgear -- dst6501_and_wnr2000_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects DST6501 before 1.1.0.6 and WNR2000v2 before 1.2.0.8.	2020-04-22	3.3	<a href="#">CVE-2017-18766</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by directory traversal. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before	2020-04-20	2.1	<a href="#">CVE-2017-18824</a> <a href="#">CONFIRM</a>

	12.0.2.15.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18828</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by administrative password disclosure. This affects D6220 before V1.0.0.28, D6400 before V1.0.0.60, D8500 before V1.0.3.29, DGN2200v4 before 1.0.0.82, DGN2200Bv4 before 1.0.0.82, R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	2020-04-22	2.1	<a href="#">CVE-2017-18777</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	2.1	<a href="#">CVE-2017-18840</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18831</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	2020-04-20	2.1	<a href="#">CVE-2017-18843</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400v2 before 1.0.2.32, R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	2020-04-20	2.1	<a href="#">CVE-2017-18847</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18827</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.42, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	2020-04-22	3.3	<a href="#">CVE-2017-18763</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-21	3.5	<a href="#">CVE-2017-18821</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18832</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	2.1	<a href="#">CVE-2017-18823</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	2020-04-23	3.3	<a href="#">CVE-2017-18747</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18825</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	2.1	<a href="#">CVE-2017-18836</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	2020-04-20	2.1	<a href="#">CVE-2017-18844</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18839</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by XSS. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before			

netgear -- multiple_devices	1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96, DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6100v2 before 1.0.1.54, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, R6700v2 before 1.2.0.12, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.18, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R7900P before 1.1.5.14, R8000 before 1.0.4.4, R8000P before 1.1.5.14, R8500 before 1.0.2.110, R8300 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.8, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.42, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	2020-04-22	3.5	<a href="#">CVE-2017-18785</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	2.1	<a href="#">CVE-2017-18780</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D7000 before 1.0.1.52, D7000v2 before 1.0.0.38, D7800 before 1.0.1.24, D8500 before 1.0.3.29, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300v1 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	2.1	<a href="#">CVE-2017-18778</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6250 before V1.0.4.8, R6400 before V1.0.1.22, R6400v2 before V1.0.2.32, R7100LG before V1.0.0.32, R7300 before V1.0.0.52, R8300 before V1.0.2.94, R8500 before V1.0.2.100, D6220	2020-04-22	2.1	<a href="#">CVE-2017-18789</a> <a href="#">CONFIRM</a>



	before V1.0.0.28, D6400 before V1.0.0.60, and D8500 before V1.0.3.29.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-21	<a href="#">2.7</a>	<a href="#">CVE-2018-21141 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, D7000 before 1.0.1.50, and D1500 before 1.0.0.25.	2020-04-21	<a href="#">2.1</a>	<a href="#">CVE-2017-18798 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects GS110EMX before 1.0.0.9, GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	2020-04-22	<a href="#">3.3</a>	<a href="#">CVE-2018-21122 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX6200v2 before 1.0.1.50, EX7000 before 1.0.0.56, JR6150 before 1.0.1.18, R6050 before 1.0.1.10J, R6100 before 1.0.1.16, R6150 before 1.0.1.10, R6220 before 1.1.0.50, R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.26, R6700v2 before 1.2.0.4, R6800 before 1.0.1.10, R6900 before 1.0.1.26, R6900P before 1.0.0.58, R6900v2 before 1.2.0.4, R7000 before 1.0.9.6, R7000P before 1.0.0.58, R7100LG before 1.0.0.32, R7300 before 1.0.0.54, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.40, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR4300v1 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR3500Lv2 before 1.2.0.44.	2020-04-22	<a href="#">2.1</a>	<a href="#">CVE-2017-18769 CONFIRM</a>
netgear -- r6700_and_r6800_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38 and R6800 before 1.1.0.38.	2020-04-20	<a href="#">2.1</a>	<a href="#">CVE-2017-18845 CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.30 are affected by incorrect configuration of security settings.	2020-04-21	<a href="#">2.1</a>	<a href="#">CVE-2017-18803 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18807 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18820 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18816 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18815 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18814 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18810 CONFIRM</a>

tenable -- tenable.sc	Stored XSS in Tenable.Sc before 5.14.0 could allow an authenticated remote attacker to craft a request to execute arbitrary script code in a user's browser session. Updated input validation techniques have been implemented to correct this issue.	2020-04-17	3.5	<a href="#">CVE-2020-5737</a> <a href="#">MISC</a>
-----------------------	---	------------	-----	---

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Source CVSS Published Score Info
abb -- system_800xa_base	Weak Registry permissions in ABB System 800xA Base allow low privileged users to read and modify registry settings related to control system functionality, allowing an authenticated attacker to cause system functions to stop or malfunction.	<a href="#">CVE-2020-5474</a> yes calculated <a href="#">MISC</a>
abb -- system_800xa_information_manager	The installations for ABB System 800xA Information Manager versions 5.1, 6.0 to 6.0.3.2 and 6.1 wrongly contain an auxiliary component. An attacker is able to use this for an XSS-like attack to an authenticated local user, which might lead to execution of arbitrary code.	<a href="#">CVE-2020-5477</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	The Configuration pages in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway for user profiles and services transfer the password in plaintext (although hidden when displayed).	<a href="#">CVE-2019-19107</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	The web server in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows access to different endpoints of the application without authenticating by accessing a specific uniform resource locator (URL) , violating the access-control (ACL) rules. This issue allows obtaining sensitive information that may aid in further attacks and privilege escalation.	<a href="#">CVE-2019-19104</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	Improper implementation of Access Control in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows an unauthorized user to access data marked as restricted, such as viewing or editing user profiles and application settings.	<a href="#">CVE-2019-19106</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	The backup function in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway saves the current settings and configuration of the application, including credentials of existing user accounts and other configuration's credentials in plaintext.	<a href="#">CVE-2019-19105</a> yes calculated <a href="#">MISC</a>
admidio -- admidio	SQL Injection was discovered in Admidio before version 3.3.13. The main cookie parameter is concatenated into a SQL query without any input validation/sanitization, thus an attacker without logging in, can send a GET request with arbitrary SQL queries appended to the cookie parameter and execute SQL queries. The vulnerability impacts the confidentiality of the system. This has been patched in version 3.3.13.	<a href="#">CVE-2020-11004</a> yes calculated <a href="#">MISC</a> <a href="#">CONFIRM</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	<a href="#">CVE-2020-12131</a> yes calculated <a href="#">MISC</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	<a href="#">CVE-2020-12130</a> yes calculated <a href="#">MISC</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	<a href="#">CVE-2020-12129</a> yes calculated <a href="#">MISC</a>
anchor-cms -- anchor-cms	Anchor 0.12.7 allows admins to cause XSS via crafted post content.	<a href="#">CVE-2020-12071</a> yes calculated <a href="#">MISC</a>
atlassian -- confluence_server	The attachment-uploading feature in Atlassian Confluence Server from version 6.14.0 through version 6.14.3, and version 6.15.0 before version 6.15.5 allows remote attackers to achieve stored cross-site- scripting (SXSS) via a malicious attachment with a modified `mimeType`	<a href="#">CVE-2019-21102</a> yes calculated <a href="#">MISC</a>

	parameter.	
b&r_automation -- automation_runtime	An authentication weakness in the SNMP service in B&R Automation Runtime versions 2.96, 3.00, 3.01, 3.06 to 3.10, 4.00 to 4.63, 4.72 and above allows unauthenticated users to modify the configuration of B&R products via SNMP.	<a href="#">CVE-2019-10818</a> Calculated CONFIRM
beaker -- beaker	Beaker before 0.8.9 allows a sandbox escape, enabling system access and code execution. This occurs because Electron context isolation is not used, and therefore an attacker can conduct a prototype-pollution attack against the Electron internal messaging API.	<a href="#">CVE-2020-14079</a> Calculated MISC
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.5 allows remote attackers to obtain sensitive files via Local File Inclusion.	<a href="#">CVE-2020-12112</a> Calculated MISC
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.4 allows XSS via closed captions because dangerouslySetInnerHTML in React is used.	<a href="#">CVE-2020-14113</a> Calculated MISC
bitcoin-abe -- bitcoin-abe	Abe (aka bitcoin-abe) through 0.7.2, and 0.8pre, allows XSS in __call__ in abe.py because the PATH_INFO environment variable is mishandled during a PageNotFound exception.	<a href="#">CVE-2020-14944</a> Calculated MISC
bitdefender -- antivirus_free	A vulnerability in the improper handling of junctions in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects: Bitdefender Antivirus Free versions prior to 1.0.17.	<a href="#">CVE-2020-1099</a> Calculated MISC
bson -- bson	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.	<a href="#">CVE-2020-12135</a> Calculated MISC
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shifts_btrfs_ioctl_fd_replace() calls fdget(oldfd), then without further checks passes the resulting file* into shifts_real_fdget(), which casts file->private_data, a void* that points to a filesystem-dependent type, to a "struct shifts_file_info *". As the private_data is not required to be a pointer, an attacker can use this to cause a denial of service or possibly execute arbitrary code.	<a href="#">CVE-2019-15792</a> Calculated MISC
canonical -- ubuntu	Appport creates a world writable lock file with root ownership in the world writable /var/lock/appport directory. If the appport/ directory does not exist (this is not uncommon as /var/lock is a tmpfs), it will create the directory, otherwise it will simply continue execution using the existing directory. This allows for a symlink attack if an attacker were to create a symlink at /var/lock/appport, changing appport's lock file location. This file could then be used to escalate privileges, for example. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	<a href="#">CVE-2020-8531</a> Calculated CONFIRM
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shifts_btrfs_ioctl_fd_replace() installs an fd referencing a file from the lower filesystem without taking an additional reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a refcount underflow.	<a href="#">CVE-2019-15791</a> Calculated MISC
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into init_user_ns, whereas they should have been translated into the s_user_ns for the lower filesystem. This resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts s_user_ns. A local attacker could use this to possibly bypass discretionary access control permissions.	<a href="#">CVE-2019-15793</a> Calculated MISC
	Overlayfs in the Linux kernel and shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both	<a href="#">CVE-2019-</a>

canonical -- ubuntu	replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points. On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patches change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount underflow.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
canonical -- ubuntu	Time-of-check Time-of-use Race Condition vulnerability on crash report ownership change in Apport allows for a possible privilege escalation opportunity. If fs.protected_symlinks is disabled, this can be exploited between the os.open and os.chown calls when the Apport cron script clears out crash files of size 0. A symlink with the same name as the deleted file can then be created upon which chown will be called, changing the file owner to root. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
ceph -- ceph	An issue was discovered in Ceph through 13.2.9. A POST request with an invalid tagging XML can crash the RGW process by triggering a NULL pointer exception.	<a href="#">CVE-2020-12059</a> MISC MISC MISC MISC MISC
ceph -- ceph	A path traversal flaw was found in the Ceph dashboard implemented in upstream versions v14.2.5, v14.2.6, v15.0.0 of Ceph storage and has been fixed in versions 14.2.7 and 15.1.0. An unauthenticated attacker could use this flaw to cause information disclosure on the host machine running the Ceph dashboard.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
ceph -- object_gateway	A flaw was found in the Ceph Object Gateway, where it supports request sent by an anonymous user in Amazon S3. This flaw could lead to potential XSS attacks due to the lack of proper neutralization of untrusted input.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
contiki-ng -- contiki-ng_and_contiki	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. A buffer overflow is present due to an integer underflow during 6LoWPAN fragment processing in the face of truncated fragments in os/net/ipv6/sicslowpan.c. This results in accesses of unmapped memory, crashing the application. An attacker can cause a denial-of-service via a crafted 6LoWPAN frame.	<a href="#">CVE-2019-9183</a> CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
contiki-ng -- contiki-ng_and_contiki	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. An out of bounds write is present in the data section during 6LoWPAN fragment re-assembly in the face of forged fragment offsets in os/net/ipv6/sicslowpan.c.	<a href="#">CVE-2019-9183</a> CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
d-link -- dir-615_devices	The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism and conduct brute-force attacks.	<a href="#">CVE-2019-17525</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A cfm UDP service listening on port 65002 allows remote, unauthenticated exfiltration of administrative credentials.	<a href="#">CVE-2020-9275</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The device can be reset to its default configuration by accessing an unauthenticated URL.	<a href="#">CVE-2020-9278</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A hard-coded account allows management-interface login with high privileges. The logged-in user can perform critical tasks and take full control of the device.	<a href="#">CVE-2020-9279</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. Authentication can be bypassed when accessing cgi modules. This allows one to perform administrative tasks (e.g., modify the admin password) with no authentication.	<a href="#">CVE-2020-9277</a> MISC MISC MISC MISC MISC



		<a href="#">MISC</a>
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The function do_cgi(), which processes cgi requests supplied to the device's web servers, is vulnerable to a remotely exploitable stack-based buffer overflow. Unauthenticated exploitation is possible by combining this vulnerability with CVE-2020-9277.	<a href="#">CVE-2020-9276</a> MISC Calculated
dong_joo_cho -- file_transfer_ifamily	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the .etc/ path.	<a href="#">CVE-2020-12128</a> MISC Calculated
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit.	<a href="#">CVE-2020-5869</a> MISC Calculated
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer.	<a href="#">CVE-2020-5870</a> MISC Calculated
f5 -- big-iq	In BIG-IQ 6.0.0-7.0.0, a remote access vulnerability has been discovered that may allow a remote user to execute shell commands on affected systems using HTTP requests to the BIG-IQ user interface.	<a href="#">CVE-2020-5868</a> MISC Calculated
f5 -- nginx_controller	In versions of NGINX Controller prior to 3.2.0, communication between NGINX Controller and NGINX Plus instances skip TLS verification by default.	<a href="#">CVE-2020-5864</a> CONFIRM
f5 -- nginx_controller	In versions prior to 3.3.0, the NGINX Controller Agent installer script 'install.sh' uses HTTP instead of HTTPS to check and install packages	<a href="#">CVE-2020-5867</a> CONFIRM
f5 -- nginx_controller	In versions of NGINX Controller prior to 3.3.0, the helper.sh script, which is used optionally in NGINX Controller to change settings, uses sensitive items as command-line arguments.	<a href="#">CVE-2020-5866</a> CONFIRM
f5 -- nginx_controller	In versions prior to 3.3.0, the NGINX Controller is configured to communicate with its Postgres database server over unencrypted channels, making the communicated data vulnerable to interception via man-in-the-middle (MITM) attacks.	<a href="#">CVE-2020-5865</a> CONFIRM
fifthplay -- s.a.m.i	Fifthplay S.A.M.I before 2019.3_HP2 allows unauthenticated stored XSS via a POST request.	<a href="#">CVE-2020-13132</a> MISC Calculated
flexera -- flexnet_publisher	A Denial of Service vulnerability related to stack exhaustion has been identified in FlexNet Publisher lmadm.exe 11.16.2. Because the message reading function calls itself recursively given a certain condition in the received message, an unauthenticated remote attacker can repeatedly send messages of that type to cause a stack exhaustion condition.	<a href="#">CVE-2019-8961</a> CONFIRM
flexera -- flexnet_publisher	A Denial of Service vulnerability related to command handling has been identified in FlexNet Publisher lmadm.exe version 11.16.2. The message reading function used in lmadm.exe can, given a certain message, call itself again and then wait for a further message. With a particular flag set in the original message, but no second message received, the function eventually return an unexpected value which leads to an exception being thrown. The end result can be process termination.	<a href="#">CVE-2019-8960</a> CONFIRM
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of vertices in U3D objects. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10568.	<a href="#">CVE-2020-14905</a> MISC Calculated
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction	

foxit -- phantompdf	is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the AddWatermark command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9942.	<a href="#">CVE-2020-04909</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the GetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9944.	<a href="#">CVE-2020-04911</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the OCRAndExportToExcel command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9946.	<a href="#">CVE-2020-04913</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10461.	<a href="#">CVE-2020-04901</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10463.	<a href="#">CVE-2020-04903</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10193.	<a href="#">CVE-2020-04897</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10190.	<a href="#">CVE-2020-04894</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the SetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9945.	<a href="#">CVE-2020-04912</a> 11/16/2020 Notated MISC
	This vulnerability allows remote attackers to execute arbitrary code on	

foxit -- phantompdf	affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the DuplicatePages command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9828.	<a href="#">CVE-2020-04889</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the ConvertToPDF command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9829.	<a href="#">CVE-2020-04890</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Save command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9831.	<a href="#">CVE-2020-04891</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10189.	<a href="#">CVE-2020-04893</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Export command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9865.	<a href="#">CVE-2020-04908</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10191.	<a href="#">CVE-2020-04895</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10192.	<a href="#">CVE-2020-04896</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10195.	<a href="#">CVE-2020-04898</a> Notated MISC
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a	<a href="#">CVE-2020-</a>

foxit -- phantompdf	malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10462.	<a href="#">CVE-2020-04902</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10464.	<a href="#">CVE-2020-04904</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the RotatePage command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9943.	<a href="#">CVE-2020-04910</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the CombineFiles command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9830.	<a href="#">CVE-2020-04892</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10132.	<a href="#">CVE-2020-04899</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the resetForm method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10614.	<a href="#">CVE-2020-04906</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10142.	<a href="#">CVE-2020-04900</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of widgets in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10650.	<a href="#">CVE-2020-04907</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
	Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. This bug is similar to CVE-2020-5260(GHSA-qm7j-c969-7j4q). The fix for that bug still left the door open for an exploit where <code>_some_credential</code> is leaked (but the attacker cannot control which one). Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that are considered illegal as of the recently	<a href="#">CVE-</a>



git -- git	published Git versions can cause Git to send a "blank" pattern to helpers, missing hostname and protocol fields. Many helpers will interpret this as matching <code>_any_</code> URL, and will return some unspecified stored password, leaking the password to an attacker's server. The vulnerability can be triggered by feeding a malicious URL to <code>'git clone'</code> . However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The root of the problem is in Git itself, which should not be feeding blank input to helpers. However, the ability to exploit the vulnerability in practice depends on which helpers are in use. Credential helpers which are known to trigger the vulnerability: - Git's "store" helper - Git's "cache" helper - the "osxkeychain" helper that ships in Git's "contrib" directory Credential helpers which are known to be safe even with vulnerable versions of Git: - Git Credential Manager for Windows Any helper not in this list should be assumed to trigger the vulnerability.	<a href="#">2020-11008</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">2020-11008</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">GENTOO</a>
gitlab -- gitlab	An issue was discovered in GitLab 10.7.0 and later through 12.9.2. A Workhorse bypass could lead to job artifact uploads and file disclosure (Exposure of Sensitive Information) via request smuggling.	<a href="#">CVE-2020-14506</a> <a href="#">2020-14506</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and_enterprise_editions	An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 12.7.9, 12.8.x before 12.8.9, and 12.9.x before 12.9.3. A Workhorse bypass could lead to NuGet package and file disclosure (Exposure of Sensitive Information) via request smuggling.	<a href="#">CVE-2020-14505</a> <a href="#">2020-14505</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and_enterprise_editions	An issue was discovered in GitLab CE and EE 8.15 through 12.9.2. Members of a group could still have access after the group is deleted.	<a href="#">CVE-2020-145649</a> <a href="#">2020-145649</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
gnome -- evolution	An issue was discovered in GNOME Evolution before 3.35.91. By using the proprietary (non-RFC6068) "mailto?attach=..." parameter, a website (or other source of mailto links) can make Evolution attach local files or directories to a composed email message without showing a warning to the user, as demonstrated by an attach=. value.	<a href="#">CVE-2020-145879</a> <a href="#">2020-145879</a> <a href="#">MISC</a> <a href="#">Calculated</a>
gnu -- gnu_mailman	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code.	<a href="#">CVE-2020-146887</a> <a href="#">2020-146887</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- google_earth_pro	A vulnerability in the windows installer of Google Earth Pro versions prior to 7.3.3 allows an attacker using DLL h jacking to insert malicious local files to execute unauthenticated remote code on the targeted system.	<a href="#">CVE-2020-14895</a> <a href="#">2020-14895</a> <a href="#">MISC</a> <a href="#">Calculated</a>
grafana_labs -- grafana	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	<a href="#">CVE-2020-172245</a> <a href="#">2020-172245</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">MISC</a>
hcl -- appscan_enterprise	"HCL AppScan Enterprise uses hard-coded credentials which can be exploited by attackers to get unauthorized access to application's encrypted files."	<a href="#">CVE-2019-14327</a> <a href="#">2019-14327</a> <a href="#">MISC</a> <a href="#">Calculated</a>
hcl -- connections	"HCL Connections is vulnerable to possible information leakage and could disclose sensitive information via stack trace to a local user."	<a href="#">CVE-2020-14085</a> <a href="#">2020-14085</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
helm -- helm	There is an information disclosure vulnerability in Helm from version 3.1.0 and before version 3.2.0. 'lookup' is a Helm template function introduced in Helm v3. It is able to lookup resources in the cluster to check for the existence of specific resources and get details about them. This can be used as part of the process to render templates. The documented behavior of 'helm template' states that it does not attach to a remote cluster. However, a the recently added 'lookup' template function circumvents this restriction and connects to the cluster even during 'helm template' and 'helm install update delete rollback --dry-run'. The user is	<a href="#">CVE-2020-14013</a> <a href="#">2020-14013</a> <a href="#">MISC</a>

	not notified of this behavior. Running `helm template` should not make calls to a cluster. This is different from `install`, which is presumed to have access to a cluster in order to load resources into Kubernetes. Helm 2 is unaffected by this vulnerability. A malicious chart author could inject a `lookup` into a chart that, when rendered through `helm template`, performs unannounced lookups against the cluster a user's `KUBECONFIG` file points to. This information can then be disclosed via the output of `helm template`. This issue has been fixed in Helm 3.2.0	MISC 2020-04-15 Not Calculated CONFIRM
hp -- j/h-series_nonstop_systems	This document describes a security vulnerability in Blade Maintenance Entity, Integrated Maintenance Entity and Maintenance Entity products. All J/H-series NonStop systems have a security vulnerability associated with an open UDP port 17185 on the Maintenance LAN which could result in information disclosure, denial-of-service attacks or local memory corruption against the affected system and a complete control of the system may also be possible. This vulnerability exists only if one gains access to the Maintenance LAN to which Blade Maintenance Entity, Integrated Maintenance Entity or Maintenance Entity product is connected. **Workaround:** Block the UDP port 17185(In the Maintenance LAN Network Switch/Firewall). Fix: Install following SPRs, which are already available: * T1805A01^AAI (Integrated Maintenance Entity) * T4805A01^AAZ (Blade Maintenance Entity). These SPRs are also usable with the following RVUs: * J06.19.00 ? J06.23.01. No fix planned for the following RVUs: J06.04.00 ? J06.18.01. No fix planned for H-Series NonStop systems. No fix planned for the product T2805 (Maintenance Entity).	CVE-2020-0431 Not Calculated MISC
hp -- onboard_administrator	A potential security vulnerability has been identified in HPE Onboard Administrator. The vulnerability could be remotely exploited to allow Reflected Cross Site Scripting. HPE has made the following software updates and mitigation information to resolve the vulnerability in HPE Onboard Administrator. * OA 4.95 (Linux and Windows).	CVE-2020-0432 Not Calculated MISC
hp -- uiot	A unauthorized remote access vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	CVE-2020-0433 Not Calculated MISC
hp -- uiot	A remote access to sensitive data vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	CVE-2020-0434 Not Calculated MISC
bm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 173310.	CVE-2019-0450 Not Calculated CONFIRM
bm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 reveals a stack trace on certain API requests which can allow an attacker further information about the implementation of the offering. IBM X-Force ID: 173311.	CVE-2019-0451 Not Calculated CONFIRM
bm -- maas360	IBM MaaS360 6.82 could allow a user with physical access to the device to crash the application which may enable the user to access restricted applications and device settings. IBM X-Force ID: 178505.	CVE-2020-0453 Not Calculated CONFIRM
bm -- maas360_for_ios	IBM MaaS360 3.96.62 for iOS could allow an attacker with physical access to the device to obtain sensitive information from the agent outside of the container. IBM X-Force ID: 172705.	CVE-2020-0455 Not Calculated CONFIRM
bm -- mq_and_mq_appliance	IBM MQ and MQ Appliance 8.0, 9.1 LTS, and 9.1 CD could allow an authenticated user cause a denial of service due to a memory leak. IBM X-Force ID: 175840.	CVE-2020-0467 Not Calculated CONFIRM
bm -- spectrum_protect	IBM Spectrum Protect 7.1 and 8.1 server is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker to execute arbitrary code on the system with the privileges of an administrator or user associated with the Spectrum Protect server or cause the Spectrum Protect server to crash. IBM X-Force ID: 179990.	CVE-2020-0415 Not Calculated CONFIRM

bm -- tivoli_monitoring	IBM Tivoli Monitoring 6.3.0 could allow a local attacker to execute arbitrary code on the system. By placing a specially crafted file, an attacker could exploit this vulnerability to load other DLL files located in the same directory and execute arbitrary code on the system. IBM X-Force ID: 177083.	<a href="#">CVE-2020-1311</a> yes calculated <a href="#">CONFIRM</a>
bm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0.4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 171250.	<a href="#">CVE-2020-1468</a> yes calculated <a href="#">CONFIRM</a>
bm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0.3.0 and 7.0.4.0 could allow an authenticated user to impersonate another user if the server is configured to enable Distributed Front End (DFE). IBM X-Force ID: 174955.	<a href="#">CVE-2020-1402</a> yes calculated <a href="#">CONFIRM</a>
infradead -- openconnect	OpenConnect through 8.08 mishandles negative return values from X509_check_function calls, which might assist attackers in performing man-in-the-middle attacks.	<a href="#">CVE-2020-12105</a> yes calculated <a href="#">MISC</a>
jetbrains -- golang	In JetBrains GoLand before 2019.3.2, the plugin repository was accessed via HTTP instead of HTTPS.	<a href="#">CVE-2020-11685</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- hub	In JetBrains Hub before 2020.1.12099, content spoofing in the Hub OAuth error message was possible.	<a href="#">CVE-2020-11691</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2020.1, the license server could be resolved to an untrusted host in some cases.	<a href="#">CVE-2020-11690</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- space	In JetBrains Space through 2020-04-22, the password authentication implementation was insecure.	<a href="#">CVE-2020-11796</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- space	In JetBrains Space through 2020-04-22, the session timeout period was configured improperly.	<a href="#">CVE-2020-11795</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- space	JetBrains Space through 2020-04-22 allows stored XSS in Chats.	<a href="#">CVE-2020-11416</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.4, a project administrator was able to retrieve some TeamCity server settings.	<a href="#">CVE-2020-11686</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.2, password values were shown in an unmasked format on several pages.	<a href="#">CVE-2020-11687</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.1, a user without appropriate permissions was able to import settings from the settings.kts file.	<a href="#">CVE-2020-11689</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.1, the application state is kept alive after a user ends his session.	<a href="#">CVE-2020-11688</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity 2018.2 through 2019.2.1, a project administrator was able to see scrambled password parameters used in a project. The issue was resolved in 2019.2.2.	<a href="#">CVE-2020-11938</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- youtrack	In JetBrains YouTrack before 2020.1.659, DB export was access ble to read-only administrators.	<a href="#">CVE-2020-11692</a> yes calculated <a href="#">CONFIRM</a>
		<a href="#">CVE-</a>

jetbrains -- youtrack	JetBrains YouTrack before 2020.1.659 was vulnerable to DoS that could be caused by attaching a malformed TIFF file to an issue.	<a href="#">CVE-2020-11693</a> Yes Calculated CONFIRM
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized editing of usergroups.	<a href="#">CVE-2020-11891</a> Yes Calculated MISC
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Improper input validations in the usergroup table class could lead to a broken ACL configuration.	<a href="#">CVE-2020-11890</a> Yes Calculated MISC
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized deletion of usergroups.	<a href="#">CVE-2020-11889</a> Yes Calculated MISC
jquery -- jquery	jQuery v2.2.2 allows XSS via a crafted onerror attribute of an IMG element.	<a href="#">CVE-2018-13405</a> Yes Calculated MISC
juplink -- rx4-1500_router	Juplink RX4-1500 v1.0.3 allows remote attackers to gain root access to the Linux subsystem via an unsanitized exec call (aka Command Line Injection), if the undocumented telnetd service is enabled and the attacker can authenticate as admin from the local network.	<a href="#">CVE-2020-8797</a> Yes Calculated MISC
juplink -- rx4-1500_router	httpd in Juplink RX4-1500 v1.0.3-v1.0.5 allows remote attackers to change or access router settings by connecting to the unauthenticated setup3.htm endpoint from the local network.	<a href="#">CVE-2020-8798</a> Yes Calculated MISC
lazysizes -- lazysizes	lazysizes through 5.2.0 allows execution of malicious JavaScript. The following attributes are not sanitized by the video-embed plugin: data-vimeo, data-vimeoparams, data-youtube and data-ytparams which can be abused to inject malicious JavaScript.	<a href="#">CVE-2020-7342</a> Yes Calculated MISC
libnvc -- libnvc_server	libvncclient/cursor.c in L bVNCServer through 0.9.12 has a HandleCursorShape integer overflow and heap-based buffer overflow via a large height or width value. NOTE: this may overlap CVE-2019-15690.	<a href="#">CVE-2020-7078</a> Yes Calculated MISC
libslirp -- libslirp	A use after free vulnerability in ip_reass() in ip_input.c of libslirp 4.2.0 and prior releases allows crafted packets to cause a denial of service.	<a href="#">CVE-2020-14883</a> Yes Calculated MISC
mailstore -- mailstore_outlook_add-in	In MailStore Outlook Add-in (and Email Archive Outlook Add-in) through 12.1.2, the login process does not validate the validity of the certificate presented by the server.	<a href="#">CVE-2020-11806</a> Yes Calculated CONFIRM
mediawiki -- mediawiki	The CentralAuth extension through REL1_34 for MediaWiki allows remote attackers to obtain sensitive hidden account information via an api.php?action=query&meta=globaluserinfo&guiuser= request. In other words, the information can be retrieved via the action API even though access would be denied when simply visiting wiki/Special:CentralAuth in a web browser.	<a href="#">CVE-2020-14051</a> Yes Calculated MISC
minio -- minio	MinIO versions before RELEASE.2020-04-23T00-58-49Z have an authentication bypass issue in the MinIO admin API. Given an admin access key, it is possible to perform admin API operations i.e. creating new service accounts for existing access keys - without knowing the admin secret key. This has been fixed and released in version RELEASE.2020-04-23T00-58-49Z.	<a href="#">CVE-2020-10012</a> Yes Calculated MISC CONFIRM
mozilla -- firefox	Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6826</a> Yes Calculated MISC
mozilla -- firefox	A malicious extension could have called <code>browser.identity.launchWebAuthFlow</code>, controlling the redirect_uri, and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6823</a> Yes Calculated MISC
	Initially, a user opens a Private Browsing Window and generates a	



mozilla -- firefox	password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new password - the generated passwords would have been identical, rather than independent. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6824</a> Calculated MISC
mozilla -- firefox_esr	When following a link that opened an intent://-schemed URL, causing a custom tab to be opened, Firefox for Android could be tricked into displaying the incorrect URI.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	<a href="#">CVE-2020-6827</a> Calculated MISC
mozilla -- firefox_esr	A malicious Android application could craft an Intent that would have been processed by Firefox for Android and potentially result in a file overwrite in the user's profile directory. One exploitation vector for this would be to supply a user.js file providing arbitrary malicious preference values. Control of arbitrary preferences can lead to sufficient compromise such that it is generally equivalent to arbitrary code execution.  *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	<a href="#">CVE-2020-6828</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	When reading from areas partially or fully outside the source resource with WebGL's <code>copyTexSubImage</code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-6829</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code>GMPDecodeData</code>. It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-6830</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	<a href="#">CVE-2020-6831</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-6835</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	<a href="#">CVE-2020-6839</a> Calculated MISC
msi -- true_color	Unquoted search path vulnerability in MSI True Color before 3.0.52.0 allows privilege escalation to SYSTEM.	<a href="#">CVE-2020-6842</a> Calculated MISC
nanometrics -- centaur_and_titansma_devices	Nanometrics Centaur through 4.3.23 and TitanSMA through 4.2.20 mishandle access control for the syslog log.	<a href="#">CVE-2020-6843</a> Calculated MISC
netatmo -- smart_indoor_camera	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in firmware versions prior to x.xx of Netatmo Smart Indoor Camera allows an attacker to execute commands on the device. This issue affects: Netatmo Smart Indoor Camera version and prior versions.	<a href="#">CVE-2019-17101</a> Yes MISC
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	<a href="#">CVE-2018-21138</a> Calculated CONFIRM

netgear -- gs810emx_devices	NETGEAR GS810EMX devices before 1.0.0.5 are affected by disclosure of sensitive information.	CVE-2020-1433 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2020-21166 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1., JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	CVE-2020-21230 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R6900P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8500 before 1.0.2.106, R8300 before 1.0.2.106, and WNDR3400v3 before 1.0.1.16.	CVE-2020-18704 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.0.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2020-18720 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D1500 before 1.0.0.25, D500 before 1.0.0.25, D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, EX6100v2 before 1.0.1.60, EX6150v2 before 1.0.1.60, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.16, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.18, R6020 before 1.0.0.26, R6050 before 1.0.1.16, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6220 before 1.1.0.60, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3700v5 before 1.1.0.48, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.46, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	CVE-2020-18703 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.0.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2020-18725 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.0.17, WAC510 before 5.0.0.17, WAC720 before 5.0.0.17, WAC730 before 5.0.0.17, WAC740 before 5.0.0.17, and WND930 before 5.0.0.17.	CVE-2020-21133 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects EX3700 before 1.0.0.66, EX3800 before 1.0.0.66, EX6100 before 1.0.2.20, EX6120 before 1.0.0.34, EX6150 before 1.0.0.36, EX6200	CVE-2020-18715 Yes Calculated

	before 1.0.3.84, and EX7000 before 1.0.0.60.	<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6050/JR6150 before 1.0.1.7, PR2000 before 1.0.0.17, R6220 before 1.1.0.50, WNDR3700v5 before 1.1.0.48, JNR1010v2 before 1.1.0.40, JWNR2010v5 before 1.1.0.40, WNR1000v4 before 1.1.0.40, WNR2020 before 1.1.0.40, WNR2050 before 1.1.0.40, WNR614 before 1.1.0.40, WNR618 before 1.1.0.40, and D7000 before 1.0.1.50.	<a href="#">CVE-2020-18791</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6400 before 1.0.0.60, D7000 before 1.0.1.50, D8500 before 1.0.3.29, EX6200 before 1.0.3.84, EX7000 before 1.0.0.60, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R9000 before 1.0.2.52, WNDR3400v3 before 1.0.1.16, WNR3500Lv2 before 1.2.0.46, and WNDR3700v5 before 1.1.0.48.	<a href="#">CVE-2020-18790</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-18713</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400 before 1.0.1.24, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	<a href="#">CVE-2020-18797</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.0.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18722</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.0.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18718</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.0.24, R6020 before 1.1.0.26, R6080 before 1.1.0.26, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18719</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.60, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.66.	<a href="#">CVE-2020-21111</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1.78, JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	<a href="#">CVE-2020-21231</a> yes calculated <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow	<a href="#">CVE-</a>

netgear -- multiple_devices	by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18716</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18724</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18723</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18728</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R7500v2 before 1.0.3.20, R7800 before 1.0.2.38, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<a href="#">CVE-2020-18729</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	<a href="#">CVE-2020-18749</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18721</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	<a href="#">CVE-2020-18746</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	<a href="#">CVE-2020-18743</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX6200v2 before 1.0.1.44, R6100 before 1.0.1.12, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, R7800 before 1.0.2.28, R9000 before 1.0.2.30, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-18748</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, EX6100v2 before 1.0.1.50, EX6150v2 before 1.0.1.50, EX6200v2 before 1.0.1.44, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.2.30, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<a href="#">CVE-2020-18728</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R6400v2 before 1.0.2.34, R6700 before 1.0.1.30, R6900 before 1.0.1.30, R6900P before 1.0.0.62, R7000 before 1.0.9.12, R7000P before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<a href="#">CVE-2020-18727</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-18711</a> yes calculated <a href="#">CONFIRM</a>



netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.00.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050, before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	<a href="#">CVE-2017-18787</a> 2017-18787 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.00.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	<a href="#">CVE-2017-18786</a> 2017-18786 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2017-18717</a> 2017-18717 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	<a href="#">CVE-2017-18790</a> 2017-18790 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2017-18712</a> 2017-18712 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.20, R7500 before 1.0.0.118, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	<a href="#">CVE-2017-18706</a> 2017-18706 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects EX6100 before 1.0.2.16_1.1.130, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.50, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, and WN3000RPv3 before 1.0.2.44.	<a href="#">CVE-2017-18768</a> 2017-18768 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700 before 1.0.1.48, R7500 before 1.0.0.124, R7800 before 1.0.2.58, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, and WNR2000v5-R2000 before 1.0.0.68.	<a href="#">CVE-2018-21135</a> 2018-21135 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	<a href="#">CVE-2017-18705</a> 2017-18705 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.66, D8500 before 1.0.3.35, DGN2200Bv4 before 1.0.0.94, DGN2200v4 before 1.0.0.94, R6250 before 1.0.4.14, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.30, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7900 before 1.0.2.4, R8000 before 1.0.4.2, WN2500RPv2 before 1.0.1.50, WNDR3400v3 before 1.0.1.14, and WNDR4000 before 1.0.2.10.	<a href="#">CVE-2017-18756</a> 2017-18756 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.16, R7500 before 1.0.0.116, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR4300v2 before 1.0.0.48, WNDR4300v1 before 1.0.2.90, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2017-18757</a> 2017-18757 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R6700 before 1.0.1.20, R6900 before 1.0.1.20, WNR3500Lv2 before 1.2.0.44, and WNR2000v2 before 1.2.0.8.	<a href="#">CVE-2017-18765</a> 2017-18765 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	<a href="#">CVE-2018-16165</a> 2018-16165 yes calculated CONFIRM
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DGN2200Bv4 before 1.0.0.102,	

netgear -- multiple_devices	DGN2200v4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6300v2 before 1.0.4.22, R6900P before 1.3.0.18, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, WN2500RPv2 before 1.0.1.52, and WNDR3400v3 before 1.0.1.18.	<a href="#">CVE-2020-2118</a> yes <a href="#">21163</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6400 before 1.0.0.78, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.8, R6300v2 before 1.0.4.6, R6400 before 1.0.1.12, R6700 before 1.0.1.16, R7000 before 1.0.7.10, R7100LG before 1.0.0.42, R7300DST before 1.0.0.44, R7900 before 1.0.1.12, R8000 before 1.0.3.36, R8300 before 1.0.2.74, R8500 before 1.0.2.74, WNDR3400v3 before 1.0.1.14, and WNR3500Lv2 before 1.2.0.48.	<a href="#">CVE-2020-2118</a> yes <a href="#">21162</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6100 before 1.0.1.20, R7800 before 1.0.2.40, and R9000 before 1.0.2.52.	<a href="#">CVE-2020-2117</a> yes <a href="#">18698</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.94.	<a href="#">CVE-2020-2117</a> yes <a href="#">18752</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-2117</a> yes <a href="#">18727</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-2117</a> yes <a href="#">18728</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6700 before 1.0.1.48, R7900 before 1.0.2.16, R6900 before 1.0.1.48, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R7000 before 1.0.9.34, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R7900P before 1.4.1.24, R8500 before 1.0.2.122, R8300 before 1.0.2.122, WN2500RPv2 before 1.0.1.54, EX3700 before 1.0.0.72, EX3800 before 1.0.0.72, EX6000 before 1.0.0.32, EX6100 before 1.0.2.24, EX6120 before 1.0.0.42, EX6130 before 1.0.0.24, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, D7000v2 before 1.0.0.51, D6220 before 1.0.0.46, D6400 before 1.0.0.82, and D8500 before 1.0.3.42.	<a href="#">CVE-2020-2118</a> yes <a href="#">21134</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-2117</a> yes <a href="#">18751</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	<a href="#">CVE-2020-2118</a> yes <a href="#">21145</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.46, and R9000 before 1.0.3.16.	<a href="#">CVE-2020-2118</a> yes <a href="#">21161</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-2117</a> yes <a href="#">18729</a> calculated <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	CVE-2018-21151 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.61, D6000 before 1.0.0.61, D6100 before 1.0.0.55, D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	CVE-2017-18740 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.0.1.20, R7000 before 1.0.7.10, R7000P before 1.0.0.58, R6900P before 1.0.0.58, R7100LG before 1.0.0.32, R7900 before 1.0.1.14, R8000 before 1.0.3.22, and R8500 before 1.0.2.94.	CVE-2017-18741 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, and WNR2000v5 before 1.0.0.58.	CVE-2017-18731 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DM200 before 1.0.0.52, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.16, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2018-21144 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6250 before 1.0.4.12, R6300v2 before 1.0.4.8, R6700 before 1.0.1.16, R6900 before 1.0.1.16, R7300DST before 1.0.0.54, R7900 before 1.0.1.12, R8000 before 1.0.3.32, and R8500 before 1.0.2.74.	CVE-2017-18742 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2018-21142 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.58, D6200 before 1.1.00.30, D6220 before 1.0.0.46, D6400 before 1.0.0.82, D7000 before 1.0.1.68, D7000v2 before 1.0.0.51, D7800 before 1.0.1.42, D8500 before 1.0.3.42, DC112A before 1.0.0.40, DGN2200Bv4 before 1.0.0.102, DGN2200v4 before 1.0.0.102, JNR1010v2 before 1.1.0.54, JR6150 before 1.0.1.18, JWNR2010v5 before 1.1.0.54, PR2000 before 1.0.0.24, R6020 before 1.0.0.34, R6050 before 1.0.1.18, R6080 before 1.0.0.34, R6100 before 1.0.1.22, R6120 before 1.0.0.42, R6220 before 1.1.0.68, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R6700 before 1.0.1.48, R6700v2 before 1.2.0.24, R6800 before 1.2.0.24, R6900 before 1.0.1.48, R6900P before 1.3.1.44, R6900v2 before 1.2.0.24, R7000 before 1.0.9.34, R7000P before 1.3.1.44, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R7500 before 1.0.0.124, R7500v2 before 1.0.3.38, R7900 before 1.0.2.16, R7900P before 1.4.1.24, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R8300 before 1.0.2.122, R8500 before 1.0.2.122, WN3000RP before 1.0.0.68, WN3000RPv2 before 1.0.0.68, WNDR3400v3 before 1.0.1.18, WNDR3700v4 before 1.0.2.102, WNDR3700v5 before 1.1.0.54, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, WNR1000v4 before 1.1.0.54, WNR2020 before 1.1.0.54, WNR2050 before 1.1.0.54, and WNR3500Lv2 before 1.2.0.54.	CVE-2018-21139 2020-yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2017-18730 2020-yes calculated CONFIRM
netgear -- r6220_and_wndr3700_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6220 before 1.1.0.64 and WNDR3700v5 before 1.1.0.54.	CVE-2018-21164 2020-yes calculated CONFIRM
		CVE-

netgear -- r6220_devices	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	2020- 2017- yes CVE- 2017- 18702 calculated CONFIRM
netgear -- r6700_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	2020- 2017- yes CVE- 2017- 18701 calculated CONFIRM
netgear -- r7800_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020- 2017- yes CVE- 2017- 18697 calculated CONFIRM
netgear -- r7800_devices_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020- 2017- yes CVE- 2017- 18699 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020- 2017- yes CVE- 2017- 18707 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by CSRF. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020- 2017- yes CVE- 2017- 18708 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020- 2017- yes CVE- 2017- 18709 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020- 2017- yes CVE- 2017- 18710 calculated CONFIRM
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	2020- 2018- yes CVE- 2018- 102 calculated CONFIRM
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	2020- 2018- yes CVE- 2018- 1160 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18809 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18813 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	2020- 2017- yes CVE- 2017- 18819 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18812 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18811 calculated CONFIRM
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020- 2018- yes CVE- 2018- 1126 calculated CONFIRM
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020- 2018- yes CVE- 2018- 1128 calculated CONFIRM



netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-127</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-130</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-129</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac510_devices	NETGEAR WAC510 devices before 5.0.0.17 are affected by privilege escalation.	<a href="#">CVE-2020-124</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac510_devices	NETGEAR WAC510 devices before 5.0.0.17 are affected by authentication bypass.	<a href="#">CVE-2020-125</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wndr4500_devices	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	<a href="#">CVE-2020-1717</a> Yes Calculated <a href="#">CONFIRM</a>
ntop -- ndpi	In nDPI through 3.2 Stable, the SSH protocol dissector has multiple KEXINIT integer overflows that result in a controlled remote heap overflow in concat_hash_string in ssh.c. Due to the granular nature of the overflow primitive and the ability to control both the contents and layout of the nDPI library's heap memory through remote input, this vulnerability may be abused to achieve full Remote Code Execution against any network inspection stack that is linked against nDPI and uses it to perform network traffic analysis.	<a href="#">CVE-2020-939</a> Yes Calculated <a href="#">MISC</a>
ntop -- ndpi	In nDPI through 3.2 Stable, an out-of-bounds read in concat_hash_string in ssh.c can be exploited by a network-positioned attacker that can send malformed SSH protocol messages on a network segment monitored by nDPI's library.	<a href="#">CVE-2020-940</a> Yes Calculated <a href="#">MISC</a>
opc_foundation -- ua.net_standard	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of OPC Foundation UA .NET Standard 1.04.358.30. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of sessions. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to create a denial-of-service condition against the application. Was ZDI-CAN-10295.	<a href="#">CVE-2020-967</a> Yes Calculated <a href="#">MISC</a>
openssl -- openssl	Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).	<a href="#">CVE-2020-1967</a> Yes Calculated <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">FREEBSD</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
oppo -- coloros	In ColorOS (oppo mobile phone operating system, based on AOSP frameworks/native code position/services/surfaceflinger surfaceflinger.CPP), RGB is defined on the stack but uninitialized, so when the screenShot function to RGB value assignment, will not initialize the value is returned to the attackers, leading to values on the stack information leakage, the vulnerability can be used to bypass attackers ALSR.	<a href="#">CVE-2020-11828</a> Yes Calculated <a href="#">CONFIRM</a>
paypal-adaptive -- paypal-adaptive	paypal-adaptive through 0.4.2 manipulation of JavaScript objects resulting	<a href="#">CVE-2020-</a> Yes Calculated

	in Prototype Pollution. The PayPal function could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload.	<a href="#">CVE-2020-1443</a> 2020-04-18 Calculated MISC
phproject -- phproject	In Phproject before version 1.7.8, there's a vulnerability which allows users with access to file uploads to execute arbitrary code. This is patched in version 1.7.8.	<a href="#">CVE-2020-144011</a> 2020-04-18 Calculated CONFIRM
plex -- media_server	Improper Input Validation in Plex Media Server on Windows allows a local, unauthenticated attacker to execute arbitrary Python code with SYSTEM privileges.	<a href="#">CVE-2020-144740</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is improper access control on customers search. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-14487</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there are improper access controls on product page with combinations, attachments and specific prices. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-14493</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	"In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there is improper access controls on product attributes page. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-14488</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.5.0.0 and 1.7.6.5, there are improper access control since the the version 1.5.0.0 for legacy controllers. - admin-dev/index.php/configure/shop/customer-preferences/ - admin-dev/index.php/improve/international/translations/ - admin-dev/index.php/improve/international/geolocation/ - admin-dev/index.php/improve/international/localization - admin-dev/index.php/configure/advanced/performance - admin-dev/index.php/sell/orders/delivery-slips/ - admin-dev/index.php?controller=AdminStatuses The problem is fixed in 1.7.6.5	<a href="#">CVE-2020-14479</a> 2020-04-18 Calculated CONFIRM
python-markdown2 -- python-markdown2	python-markdown2 through 2.3.8 allows XSS because element names are mishandled unless a \w+ match succeeds. For example, an attack might use elementname@ or elementname- with an onclick attribute.	<a href="#">CVE-2020-14488</a> 2020-04-18 Calculated MISC
rapid7 -- metasploit_framework	Rapid7 Metasploit Framework versions before 5.0.85 suffers from an instance of CWE-78: OS Command Injection, wherein the lnotify plugin accepts untrusted user-supplied data via a remote computer's hostname or service name. An attacker can create a specially-crafted hostname or service name to be imported by Metasploit from a variety of sources and trigger a command injection on the operator's terminal. Note, only the Metasploit Framework and products that expose the plugin system is susceptible to this issue -- notably, this does not include Rapid7 Metasploit Pro. Also note, this vulnerability cannot be triggered through a normal scan operation -- the attacker would have to supply a file that is processed with the db_import command.	<a href="#">CVE-2020-144350</a> 2020-04-18 Calculated CONFIRM
re2c -- re2c	re2c 1.3 has a heap-based buffer overflow in Scanner::fill in parse/scanner.cc via a long lexeme.	<a href="#">CVE-2020-14458</a> 2020-04-18 Calculated MISC
red_hat -- openshift_container_platform	A flaw was found in openshift-ansible. OpenShift Container Platform (OCP) 3.11 is too permissive in the way it specified CORS allowed origins during installation. An attacker, able to man-in-the-middle the connection between the user's browser and the openshift console, could use this flaw to perform a phishing attack. The main threat from this vulnerability is data confidentiality.	<a href="#">CVE-2020-14471</a> 2020-04-18 Calculated CONFIRM
red_hat -- openshift_container_platform	A flaw was found in OpenShift Container Platform version 4.1 and later. Sensitive information was found to be logged by the image registry operator allowing an attacker able to gain access to those logs, to read and write to the storage backing the internal image registry. The highest threat from this vulnerability is to data integrity.	<a href="#">CVE-2020-144712</a> 2020-04-18 Calculated CONFIRM

red_hat -- undertow	A flaw was found in all undertow-2.x.x SP1 versions prior to undertow-2.0.30.SP1, all undertow-1.x.x and undertow-2.x.x versions prior to undertow-2.1.0.Final, where the Servlet container causes servletPath to normalize incorrectly by truncating the path after semicolon which may lead to an application mapping resulting in the security bypass.	<a href="#">CVE-2020-1757</a> 2020-09-15 Calculated CONFIRM
sap -- erp_and_s/4_hana	Egypt localized withholding tax reports Clearing of Liabilities and Remittance Statement and Summary in SAP ERP (versions 618, 730, EAPPLGLO 607) and S/4 HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user, allowing reading or modification of some tax reports, due to Missing Authorization Check.	<a href="#">CVE-2020-6812</a> 2020-09-15 Calculated MISC
sap -- netweaver_as_abap	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_PHTMLB, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, is vulnerable to reflected Cross-Site Scripting (XSS) via different URL parameters as it does not sufficiently encode user controlled inputs.	<a href="#">CVE-2020-6813</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers.	<a href="#">CVE-2020-7487</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability exists on EcoStruxure Machine Expert – Basic or SoMachine Basic programming software (versions in security notification). The result of this vulnerability, DLL substitution, could allow the transference of malicious code to the controller.	<a href="#">CVE-2020-7489</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers.	<a href="#">CVE-2020-7488</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-798: Use of Hardcoded Credentials vulnerability exists in Modicon Controllers (All versions of the following CPUs and Communication Module product references listed in the Security Notifications), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.	<a href="#">CVE-2020-6859</a> 2020-09-15 Calculated MISC
schneider_electric -- v_jeo_designer_and_v_jeo_designer_basic	A CWE-426: Untrusted Search Path vulnerability exists in Vijeo Designer Basic (V1.1 HotFix 15 and prior) and Vijeo Designer (V6.9 SP9 and prior), which could cause arbitrary code execution on the system running V jeo Basic when a malicious DLL library is loaded by the Product.	<a href="#">CVE-2020-7490</a> 2020-09-15 Calculated MISC
simplesamlphp -- simplesamlphp	SimpleSAMLphp versions before 1.18.6 contain an information disclosure vulnerability. The module controller in 'SimpleSAMLModule' that processes requests for pages hosted by modules, has code to identify paths ending with '.php' and process those as PHP code. If no other suitable way of handling the given path exists it presents the file to the browser. The check to identify paths ending with '.php' does not account for uppercase letters. If someone requests a path ending with e.g. '.PHP' and the server is serving the code from a case-insensitive file system, such as on Windows, the processing of the PHP code does not occur, and the source code is instead presented to the browser. An attacker may use this issue to gain access to the source code in third-party modules that is meant to be private, or even sensitive. However, the attack surface is considered small, as the attack will only work when SimpleSAMLphp serves such content from a file system that is not case-sensitive, such as on Windows. This issue is fixed in version 1.18.6.	<a href="#">CVE-2020-6801</a> 2020-09-15 Calculated CONFIRM
sonatype -- nexus_repository_manager	An issue was discovered in Sonatype Nexus Repository Manager in versions 3.21.1 and 3.22.0. It is possible for a user with appropriate privileges to create, modify, and execute scripting tasks without use of the UI or API. NOTE: in 3.22.0, scripting is disabled by default (making this not exploitable).	<a href="#">CVE-2020-1753</a> 2020-09-15 Calculated CONFIRM
squid -- squid	An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials).	<a href="#">CVE-2020-11945</a> 2020-09-15 Calculated CONFIRM
	In Saml2 Authentication Services for ASP.NET versions before 1.0.2, and	<a href="#">MISC</a> 2020-09-15 Calculated CONFIRM

sustainsys -- saml2	between 2.0.0 and 2.6.0, there is a vulnerability in how tokens are validated in some cases. Saml2 tokens are usually used as bearer tokens - a caller that presents a token is assumed to be the subject of the token. There is also support in the Saml2 protocol for issuing tokens that is tied to a subject through other means, e.g. holder-of-key where possession of a private key must be proved. The Sustainsys.Saml2 library incorrectly treats all incoming tokens as bearer tokens, even though they have another subject confirmation method specified. This could be used by an attacker that could get access to Saml2 tokens with another subject confirmation method than bearer. The attacker could then use such a token to create a log in session. This vulnerability is patched in versions 1.0.2 and 2.7.0.	<a href="#">CVE-2020-30018</a> <a href="#">MISC</a> Notated
sysaid -- sysaid_on-premise	SysAid On-Premise 20.1.11, by default, allows the AJP protocol port, which is vulnerable to a GhostCat attack. Additionally, it allows unauthenticated access to upload files, which can be used to execute commands on the system by chaining it with a GhostCat attack.	<a href="#">CVE-2020-30019</a> <a href="#">MISC</a> Notated
tata_sonata -- smart_sf_rush_devices	An issue was discovered on Tata Sonata Smart SF Rush 1.12 devices. It has been identified that the smart band has no pairing (mode 0 Bluetooth LE security level) The data being transmitted over the air is not encrypted. Adding to this, the data being sent to the smart band doesn't have any authentication or signature verification. Thus, any attacker can control a parameter of the device.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
teeworlds -- teeworlds	Teeworlds before 0.7.4 has an integer overflow when computing a tilemap size.	<a href="#">CVE-2020-30019</a> <a href="#">MISC</a> Notated
teeworlds -- teeworlds	CServer::SendMsg in engine/server/server.cpp in Teeworlds 0.7.x before 0.7.5 allows remote attackers to shut down the server.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
tortoise-orm -- tortoise-orm	In Tortoise ORM before versions 0.15.23 and 0.16.6, various forms of SQL injection have been found for MySQL and when filtering or doing mass-updates on char/text fields. SQLite & PostgreSQL are only affected when filtering with contains, starts_with, or ends_with filters (and their case-insensitive counterparts).	<a href="#">CVE-2020-30019</a> <a href="#">MISC</a> Notated
toshiba -- multiple_devices	SHARP AQUOS series (AQUOS SH-M02 build number 01.00.05 and earlier, AQUOS SH-RM02 build number 01.00.04 and earlier, AQUOS mini SH-M03 build number 01.00.04 and earlier, AQUOS Keitai SH-N01 build number 01.00.01 and earlier, AQUOS L2 (UQ mobile/J.COM) build number 01.00.05 and earlier, AQUOS sense lite SH-M05 build number 03.00.04 and earlier, AQUOS sense (UQ mobile) build number 03.00.03 and earlier, AQUOS compact SH-M06 build number 02.00.02 and earlier, AQUOS sense plus SH-M07 build number 02.00.02 and earlier, AQUOS sense2 SH-M08 build number 02.00.05 and earlier, and AQUOS sense2 (UQ mobile) build number 02.00.06 and earlier) allow an attacker to obtain the sensitive information of the device via malicious applications installed on the device.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
toshiba -- multiple_devices	An unquoted search path vulnerability exists in HDD Password tool (for Windows) version 1.20.6620 and earlier which is stored in CANVIO PREMIUM 3TB(HD-MB30TY, HD-MA30TY, HD-MB30TS, HD-MA30TS), CANVIO PREMIUM 2TB(HD-MB20TY, HD-MA20TY, HD-MB20TS, HD-MA20TS), CANVIO PREMIUM 1TB(HD-MB10TY, HD-MA10TY, HD-MB10TS, HD-MA10TS), CANVIO SLIM 1TB(HD-SB10TK, HD-SB10TS), and CANVIO SLIM 500GB(HD-SB50GK, HD-SA50GK, HD-SB50GS, HD-SA50GS), and which was downloaded before 2020 May 10. Since it registers Windows services with unquoted file paths, when a registered path contains spaces, and a malicious executable is placed on a certain path, it may be executed with the privilege of the Windows service.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
tss-lib -- tss-lib	The keygen protocol implementation in Binance tss-lib before 1.2.0 allows attackers to generate crafted h1 and h2 parameters in order to compromise a signing round or obtain sensitive information from other parties.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
veeam -- one_agent	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HandshakeResult method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated



	in the context of the service account. Was ZDI-CAN-10401.	
veeam -- one_agent	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the PerformHandshake method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-10400.	<a href="#">CVE-2020-0914</a> Yes Calculated MISC
vesta -- vesta_control_panel	A remote command execution in Vesta Control Panel through 0.9.8-26 allows any authenticated user to execute arbitrary commands on the system via cron jobs.	<a href="#">CVE-2020-0786</a> Yes Calculated MISC
vesta -- vesta_control_panel	An elevation of privilege in Vesta Control Panel through 0.9.8-26 allows an attacker to gain root system access from the admin account via v-change-user-password (aka the user password change script).	<a href="#">CVE-2020-0787</a> Yes Calculated MISC
wordpress -- wordpress	The responsive-add-ons plugin before 2.2.7 for WordPress has incorrect access control for wp-admin/admin-ajax.php?action= requests.	<a href="#">CVE-2020-12073</a> Yes Calculated MISC
wordpress -- wordpress	The mappress-google-maps-for-wordpress plugin before 2.53.9 for WordPress does not correctly implement AJAX functions with nonces (or capability checks), leading to remote code execution.	<a href="#">CVE-2020-09077</a> Yes Calculated MISC
wordpress -- wordpress	The Catch Breadcrumb plugin before 1.5.4 for WordPress allows Reflected XSS via the s parameter (a search query). Also affected are 16 themes (if the plugin is enabled) by the same author: Alchemist and Alchemist PRO, Izabel and Izabel PRO, Chique and Chique PRO, Clean Enterprise and Clean Enterprise PRO, Bold Photography PRO, Intuitive PRO, Devotepress PRO, Clean Blocks PRO, Foodoholic PRO, Catch Mag PRO, Catch Wedding PRO, and Higher Education PRO.	<a href="#">CVE-2020-09054</a> Yes Calculated MISC
wordpress -- wordpress	The Advanced Woo Search plugin version through 1.99 for Wordpress suffers from a sensitive information disclosure vulnerability in every ajax search request via the sql field to includes/class-aws-search.php.	<a href="#">CVE-2020-12070</a> Yes Calculated MISC
wordpress -- wordpress	The users-customers-import-export-for-wp-woocommerce plugin before 1.3.9 for WordPress allows subscribers to import administrative accounts via CSV.	<a href="#">CVE-2020-12074</a> Yes Calculated MISC
wordpress -- wordpress	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks capability checks for AJAX actions.	<a href="#">CVE-2020-12075</a> Yes Calculated MISC
wordpress -- wordpress	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks CSRF nonce checks for AJAX actions. One consequence of this is stored XSS.	<a href="#">CVE-2020-12076</a> Yes Calculated MISC
wordpress -- worpdress	An issue was discovered in Elementor 2.7.4. Arbitrary file upload is possible in the Elementor Import Templates function, allowing an attacker to execute code via a crafted ZIP archive.	<a href="#">CVE-2020-09055</a> Yes Calculated MISC
zoho -- manageengine_opmanager	Zoho ManageEngine OpManager before 125120 allows an unauthenticated user to retrieve an API key via a servlet call.	<a href="#">CVE-2020-11946</a> Yes Calculated MISC
zulip -- zulip_server	Zulip Server before 2.1.3 allows XSS via the modal_link feature in the Markdown functionality.	<a href="#">CVE-2020-09445</a> Yes Calculated CONFIRM
zulip -- zulip_server	Zulip Server before 2.1.3 allows reverse tabnabbing via the Markdown functionality.	<a href="#">CVE-2020-09444</a> Yes Calculated CONFIRM
		<a href="#">CVE-</a>

zulip -- zulip_server	Zulip Server before 2.1.3 allows XSS via a Markdown link, with resultant account takeover.	<a href="#">2020-04-09</a> <a href="#">14935</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
-----------------------	--	--

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:** US-CERT  
**To:** [edigiovanna@sunnyvale.ca.gov](mailto:edigiovanna@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of April 20, 2020  
**Date:** Monday, April 27, 2020 10:18:02 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of April 20, 2020](#)

04/27/2020 06:27 AM EDT

Original release date: April 27, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ios_and_macos_and_mojave_and_tvos	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. An attacker in a privileged network position may be able to intercept network traffic.	2020-04-17	<a href="#">7.5</a>	<a href="#">CVE-2019-6203</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A type confusion vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code read/write on the system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7081</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A use-after-free vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to code execution on a system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7082</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A heap overflow vulnerability in the Autodesk FBX-SDK versions 2019.2 and earlier may lead to arbitrary code execution on a system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7085</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A buffer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code execution on a system running it.	2020-04-17	<a href="#">9.3</a>	<a href="#">CVE-2020-7080</a> <a href="#">MISC</a>
evenroute -- iqrouter	IQrouter through 3.3.1, when unconfigured, has multiple remote code execution vulnerabilities in the web-panel because of Bash Shell Metacharacter Injection.	2020-04-21	<a href="#">7.5</a>	<a href="#">CVE-2020-11963</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, there is a root user without a password, which allows attackers to gain full remote access via SSH.	2020-04-21	<a href="#">7.5</a>	<a href="#">CVE-2020-11965</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, the Lua function reset_password in the web-panel allows remote attackers to change the root password arbitrarily.	2020-04-21	<a href="#">7.5</a>	<a href="#">CVE-2020-11966</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, remote attackers can control the device (restart network, reboot, upgrade, reset) because of Incorrect Access Control.	2020-04-21	<a href="#">9</a>	<a href="#">CVE-2020-11967</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In onOpActiveChanged and related methods of AppOpsControllerImpl.java, there is a possible way to display an app overlaying other apps			

google -- android	without the notification icon that it's overlaying. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144092031	2020-04-17	9.3	<a href="#">CVE-2020-0080</a> MISC
google -- android	In finalize of AssetManager.java, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144028297	2020-04-17	7.2	<a href="#">CVE-2020-0081</a> MISC
google -- android	In ExternalVibration of ExternalVibration.java, there is a possible activation of an arbitrary intent due to unsafe deserialization. This could lead to local escalation of privilege to system_server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140417434	2020-04-17	7.2	<a href="#">CVE-2020-0082</a> MISC
google -- android	In rw_t2t_extract_default_locks_info of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310721	2020-04-17	10	<a href="#">CVE-2020-0071</a> MISC
google -- android	In rw_t2t_update_lock_attributes of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-148159613	2020-04-17	10	<a href="#">CVE-2020-0070</a> MISC
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310271	2020-04-17	10	<a href="#">CVE-2020-0072</a> MISC
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147309942	2020-04-17	10	<a href="#">CVE-2020-0073</a> MISC
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService mishandles OTA Provisioning on V40 and G7 devices. The LG ID is LVE-SMP-190006 (July 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20777</a> CONFIRM
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. A stack-based buffer overflow in the logging tool could allow an attacker to gain privileges. The LG ID is LVE-SMP-200005 (April 2020).	2020-04-17	7.5	<a href="#">CVE-2020-11873</a> CONFIRM
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. Unprivileged applications can execute shell commands via the connectivity service. The LG ID is LVE-SMP-190008 (August 2019).	2020-04-17	7.2	<a href="#">CVE-2019-20773</a> CONFIRM
	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1			



lg -- multiple_mobile_devices	software. Certain security settings, related to whether packages are verified and accepted only from known sources, are mishandled. The LG ID is LVE-SMP-190002 (April 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20780</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. LG Advanced Flash (LAF) has a buffer overflow. The LG ID is LVE-SMP-190001 (March 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20782</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Backup subsystem does not properly restrict operations or validate their input. The LG ID is LVE-SMP-190004 (June 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20778</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Account subsystem allows authorization bypass. The LG ID is LVE-SMP-190007 (August 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20772</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10.0 (MTK chipsets) software. The MTK kernel does not properly implement exception handling, allowing an attacker to gain privileges. The LG ID is LVE-SMP-200001 (February 2020).	2020-04-17	7.2	<a href="#">CVE-2020-11875</a> <a href="#">CONFIRM</a>
mitel_networks -- mivoice_connect	A remote code execution vulnerability in UCB component of Mitel MiVoice Connect before 19.1 SP1 could allow an unauthenticated remote attacker to execute arbitrary scripts due to insufficient validation of URL parameters. A successful exploit could allow an attacker to gain access to sensitive information.	2020-04-17	7.5	<a href="#">CVE-2020-10211</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by a hardcoded password. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-23	7.5	<a href="#">CVE-2018-21137</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020-04-23	7.5	<a href="#">CVE-2018-21132</a> <a href="#">CONFIRM</a>
pion -- dtls	handleIncomingPacket in conn.go in Pion DTLS before 1.5.2 lacks a check for application data with epoch 0, which allows remote attackers to inject arbitrary unencrypted data after handshake completion.	2020-04-19	7.5	<a href="#">CVE-2019-20786</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
webkitgtk -- webkitgtk_and_wpe_webkit	A use-after-free issue exists in WebKitGTK before 2.28.1 and WPE WebKit before 2.28.1 via crafted web content that allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash).	2020-04-17	7.5	<a href="#">CVE-2020-11793</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	In the media-library-assistant plugin before 2.82 for WordPress, Remote Code Execution can occur via the tax_query, meta_query, or date_query parameter in mla_gallery via an admin.	2020-04-20	7.5	<a href="#">CVE-2020-11928</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- dynamo_bim	An improper signature validation vulnerability in Autodesk Dynamo BIM versions 2.5.1 and 2.5.0 may lead to code execution through maliciously crafted DLL files.	2020-04-17	4.4	<a href="#">CVE-2020-7079</a> <a href="#">MISC</a>

autodesk -- fbx_software_development	A NULL pointer dereference vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	2020-04-17	4.3	<a href="#">CVE-2020-7084</a> MISC
autodesk -- fbx_software_development	An integer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	2020-04-17	4.3	<a href="#">CVE-2020-7083</a> MISC
bitrock -- installbuilder_autoupdate_tool	InstallBuilder AutoUpdate tool and regular installers enabling <checkForUpdates> built with versions earlier than 19.11 are vulnerable to Billion laughs attack (denial-of-service).	2020-04-20	5	<a href="#">CVE-2020-3946</a> CONFIRM
byobu_apport -- byobu_apport	Byobu Apport hook may disclose sensitive information since it automatically uploads the local user's .screenrc which may contain private hostnames, usernames and passwords. This issue affects: byobu	2020-04-17	5	<a href="#">CVE-2019-7306</a> MISC MISC
evenroute -- iqrouter	In IQrouter through 3.3.1, the Lua function diag_set_password in the web-panel allows remote attackers to change the root password arbitrarily.	2020-04-21	5	<a href="#">CVE-2020-11964</a> MISC MISC
evenroute -- iqrouter	In the web-panel in IQrouter through 3.3.1, remote attackers can read system logs because of Incorrect Access Control.	2020-04-21	5	<a href="#">CVE-2020-11968</a> MISC MISC
ftpdmin -- ftpdmin	A buffer overflow vulnerability in FTPDMIN 0.96 allows attackers to crash the server via a crafted packet.	2020-04-17	5	<a href="#">CVE-2020-10813</a> MISC MISC
google -- android	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-9 Android-10 Android ID: A-144506242	2020-04-17	4.6	<a href="#">CVE-2020-0079</a> MISC
google -- android	In releaseSecureStops of DrmPlugin.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-9 Android-10 Android ID: A-144766455	2020-04-17	4.6	<a href="#">CVE-2020-0078</a> MISC
google -- android	In get_auth_result of the FPC IRIS TrustZone app, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-146056878	2020-04-17	4.6	<a href="#">CVE-2020-0076</a> MISC
google -- android	There is a possible disclosure of RAM using a shared crypto key due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android ID: A-140879284	2020-04-17	4.9	<a href="#">CVE-2019-2056</a> MISC
huawei -- taurus_al00b_smartphones	Huawei smartphones Taurus-AL00B with versions earlier than 10.0.0.205(C00E201R7P2) have an improper authentication vulnerability. The software insufficiently validate the user's identity when a user wants to do certain operation. An attacker can trick user into installing a malicious application to exploit this vulnerability. Successful exploit may cause some information disclosure.	2020-04-20	4.3	<a href="#">CVE-2020-9070</a> CONFIRM CONFIRM
bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 170880.	2020-04-17	4.3	<a href="#">CVE-2019-4644</a> XF CONFIRM

bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 could allow an authenticated user perform actions they are not authorized to by modifying request parameters. IBM X-Force ID: 163490.	2020-04-17	5.5	<a href="#">CVE-2019-4446</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
bm -- tririga_application_platform	IBM TRIRIGA Application Platform 3.5.3 and 3.6.1 discloses sensitive information in error messages that could aid an attacker formulate future attacks. IBM X-Force ID: 175993.	2020-04-17	5	<a href="#">CVE-2020-4277</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
lg -- g3_devices	An issue was discovered in LG PC Suite for LG G3 and earlier (aka LG PC Suite v5.3.27 and earlier). DLL Hijacking can occur via a Trojan horse DLL in the current working directory. The LG ID is LVE-MOT-190001 (November 2019).	2020-04-17	4.4	<a href="#">CVE-2019-20769</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9.0 software. The HAL service has a buffer overflow that leads to arbitrary code execution. The LG ID is LVE-SMP-190013 (September 2019).	2020-04-17	4.6	<a href="#">CVE-2019-20770</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0 and 8.1 software for the DTAG carrier. RILD in the radio layer uses an uninitialized variable. The LG ID is LVE-SMP-180013 (January 2019).	2020-04-17	4.6	<a href="#">CVE-2019-20785</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService allows unconfirmed configuration changes via a modified OMACP message. The LG ID is LVE-SMP-190006 (August 2019).	2020-04-17	5	<a href="#">CVE-2019-20771</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (North America CDMA) software. The LTE protocol implementation allows a bypass of AKA (Authentication and Key Agreement). The LG ID is LVE-SMP-180014 (February 2019).	2020-04-17	6.4	<a href="#">CVE-2019-20783</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9, and 10 software. Attackers can bypass Factory Reset Protection (FRP). The LG ID is LVE-SMP-200004 (March 2020).	2020-04-17	5	<a href="#">CVE-2020-11874</a> <a href="#">CONFIRM</a>
libming -- libming	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (2 bytes) in the function decompileIF() in decompile.c.	2020-04-19	6.4	<a href="#">CVE-2020-11895</a> <a href="#">MISC</a>
libming -- libming	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (8 bytes) in the function decompileIF() in decompile.c.	2020-04-19	6.4	<a href="#">CVE-2020-11894</a> <a href="#">MISC</a>
netgear -- d6100_devices	NETGEAR D6100 devices before 1.0.0.50_0.0.50 are affected by command injection.	2020-04-21	4.6	<a href="#">CVE-2017-18792</a> <a href="#">CONFIRM</a>
netgear -- d6220_and_d6100_devices	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.28 and D6100 before 1.0.0.50_0.0.50.	2020-04-21	4.6	<a href="#">CVE-2017-18795</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWN2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-23	5.8	<a href="#">CVE-2017-18734</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and	2020-04-21	4.6	<a href="#">CVE-2017-18805</a> <a href="#">CONFIRM</a>

	WNDAP360 before 3.7.4.0.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R7800 before 1.0.2.36, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	2020-04-22	5.2	<a href="#">CVE-2017-18770</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.01.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	2020-04-20	4.6	<a href="#">CVE-2017-18850</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-21	5.2	<a href="#">CVE-2018-21147</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	4.6	<a href="#">CVE-2017-18779</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JR6150 before 1.0.1.12, JNR1010v2 before 1.1.0.44, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	6.8	<a href="#">CVE-2017-18782</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6220 before V1.1.0.50, R7800 before V1.0.2.36, WNDR3400v3 before 1.0.1.14, and WNDR3700v5 before V1.1.0.48.	2020-04-23	5.8	<a href="#">CVE-2017-18739</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	4.3	<a href="#">CVE-2017-18783</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNDR2010v5 before 1.1.0.44, JR6150 before 1.0.1.12, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before	2020-04-	6.8	<a href="#">CVE-2017-18781</a>



	1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	22		<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6300v2 before 1.0.4.8_10.0.77, R6400 before 1.0.1.24, R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, R8500 before 1.0.2.100, and D6100 before 1.0.0.50_0.0.50.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18794</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D8500 through 1.0.3.28, R6400 through 1.0.1.22, R6400v2 through 1.0.2.18, R8300 through 1.0.2.94, R8500 through 1.0.2.94, and R6100 through 1.0.1.12.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18851</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6400 before 1.0.1.24, R6700 before 1.0.1.26, R6900 before 1.0.1.28, R7000 before 1.0.9.10, R7000P before 1.0.1.16, R6900P before 1.0.1.16, and R7800 before 1.0.2.36.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18796</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2017-18835</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6100 before V1.0.0.55, D7800 before V1.0.1.24, EX6150v2 before 1.0.0.48, R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before V1.0.3.16, R7800 before V1.0.2.36, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.48.	2020-04-22	<a href="#">4.6</a>	<a href="#">CVE-2017-18773</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2017-18834</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6100 before V1.0.0.55, D7000 before V1.0.1.50, D7800 before V1.0.1.24, JNR1010v2 before 1.1.0.40, JWNDR2010v5 before 1.1.0.40, R6100 before 1.0.1.12, R6220 before 1.1.0.50, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.40, WNR2000v5 before 1.0.0.42, WNR2020 before 1.1.0.40, and WNR2050 before 1.1.0.40.	2020-04-22	<a href="#">4.6</a>	<a href="#">CVE-2017-18776</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2017-18833</a> <a href="#">CONFIRM</a>

	before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before 1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96, DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6150v2 before 1.0.1.54, EX6100v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.18, R6900P before 1.3.0.8, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R8000 before 1.0.4.4_1.1.42, R7900P before 1.1.5.14, R8000P before 1.1.5.14, R8300 before 1.0.2.110, R8500 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.14, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	2020-04-22	4.6	<a href="#">CVE-2017-18788</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	4.3	<a href="#">CVE-2017-18784</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.50, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.48, and D7000 before 1.0.1.50.	2020-04-21	4.6	<a href="#">CVE-2017-18801</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.6	<a href="#">CVE-2017-18838</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before 1.0.3.16, R7800 before 1.0.2.32, EX6200v2 before 1.0.1.50, and D7800 before 1.0.1.22.	2020-04-21	4.6	<a href="#">CVE-2017-18802</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15,			

netgear -- multiple_devices	M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18830</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.46, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.46, and D7000 before 1.0.1.50.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18841</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects R6400 before 1.0.1.14, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	2020-04-23	<a href="#">4.3</a>	<a href="#">CVE-2017-18745</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18837</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.0.36, AC1450 before 1.0.0.36, R7300 before 1.0.0.54, and R8500 before 1.0.2.94.	2020-04-20	<a href="#">6.8</a>	<a href="#">CVE-2017-18848</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18829</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R7300 before 1.0.0.54, R8500 before 1.0.2.94, DGN2200v1 before 1.0.0.55, and D2200D/D2200DW-1FRNAS before 1.0.0.32.	2020-04-20	<a href="#">6.8</a>	<a href="#">CVE-2017-18842</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18826</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18822</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and WNDAP360 before 3.7.4.0.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18806</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow. This affects R6250 before 1.0.4.12, R6400v2 before 1.0.2.32, R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	2020-04-20	4.6	<a href="#">CVE-2017-18846</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF and authentication bypass. This affects R7300DST before 1.0.0.54, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and WNDR3400v3 before 1.0.1.14.	2020-04-20	6.8	<a href="#">CVE-2017-18852</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	2020-04-20	4.6	<a href="#">CVE-2017-18849</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6100 before 1.0.1.12, R7500 before 1.0.0.108, WNDR3700v4 before 1.0.2.86, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.42.	2020-04-22	6.8	<a href="#">CVE-2017-18775</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R7100LG before 1.0.0.32, R7300DST before 1.0.0.52, R8300 before 1.0.2.94, and R8500 before 1.0.2.100.	2020-04-23	5.8	<a href="#">CVE-2017-18733</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	2020-04-23	5.8	<a href="#">CVE-2017-18744</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6100 before 1.0.1.14, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, R7500 before 1.0.0.110, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	5.8	<a href="#">CVE-2017-18764</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, and WNR2000v5 before 1.0.0.58.	2020-04-22	5.2	<a href="#">CVE-2017-18754</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated	2020-04-		<a href="#">CVE-2018-</a>



	attacker. This affects WC7500 before 6.5.3.9, WC7520 before 6.5.3.9, WC7600v1 before 6.5.3.9, and WC7600v2 before 6.5.3.9.	22	<a href="#">5.8</a>	<a href="#">21123 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21121 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-22	<a href="#">6</a>	<a href="#">CVE-2018-21120 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.58, D7800 before 1.0.1.42, R6100 before 1.0.1.28, R7500 before 1.0.0.130, R7500v2 before 1.0.3.36, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, and WNDR4500v3 before 1.0.0.56.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21113 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, R8500 before 1.0.2.74, and WNR2000v2 before 1.2.0.8.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2017-18772 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D3600 before 1.0.0.68, D6000 before 1.0.0.68, D6100 before 1.0.0.57, R6100 before 1.0.1.16, R6900P before 1.2.0.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2017-18762 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18750 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6400 before 1.0.1.14, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300 before 1.0.0.56, R7800 before 1.0.2.36, R7900 before 1.0.2.10, R8000 before 1.0.3.24, R8300 before 1.0.2.74, and R8500 before 1.0.2.74.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18767 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX6150v2 before 1.0.1.54, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R6900P before 1.2.0.22, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R6100 before 1.0.1.16, WNDR4300v2 before 1.0.0.48,	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18738 CONFIRM</a>

	WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21150 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, and R9000 before 1.0.4.12.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21112 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, EX6150v2 before 1.0.1.70, EX6100v2 before 1.0.1.70, EX6200v2 before 1.0.1.64, EX7300 before 1.0.2.136, EX6400 before 1.0.2.136, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.4.12, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21114 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18737 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-21	<a href="#">5.2</a>	<a href="#">CVE-2018-21148 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-21	<a href="#">5.2</a>	<a href="#">CVE-2018-21146 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6200v2 before 1.0.3.14, R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.1.1.20, R7000 before 1.0.7.10, R7000P/R6900P before 1.0.0.56, R7100LG before 1.0.0.30, R7900 before 1.0.1.14, R8000 before 1.0.3.22, R8500 before 1.0.2.74, and D8500 before 1.0.3.28.	2020-04-21	<a href="#">5</a>	<a href="#">CVE-2017-18799 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18732 CONFIRM</a>
	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.4.8, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000P before 1.0.0.86, R6900P			

netgear -- multiple_devices	before 1.0.0.56, R7300 before 1.0.0.54, R8300 before 1.0.2.106, R8500 before 1.0.2.106, DGN2200v4 before 1.0.0.86, DGND2200Bv4 before 1.0.0.86, R6050 before 1.0.0.86, JR6150 before 1.0.1.10, R6220 before 1.1.0.50, and WNDR3700v5 before V1.1.0.48.	2020-04-22	<a href="#">6.8</a>	<a href="#">CVE-2017-18755</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18758</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, and R6900v2 before 1.2.0.4.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18735</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, and WNDR3700v5 before 1.1.0.48.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18736</a> <a href="#">CONFIRM</a>
netgear -- r6700_and_r6800_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700v2 before 1.1.0.42 and R6800 before 1.1.0.42.	2020-04-21	<a href="#">4.3</a>	<a href="#">CVE-2017-18800</a> <a href="#">CONFIRM</a>
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by command injection. This affects R7800 before 1.0.2.16 and R9000 before 1.0.2.4.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18804</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21101</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.36 are affected by command injection.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18793</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21110</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21108</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21109</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21107</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21103</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21106</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21105</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	<a href="#">5.2</a>	<a href="#">CVE-2018-21104</a> <a href="#">CONFIRM</a>
netgear -- r8000_devices	NETGEAR R8000 devices before 1.0.4.2 are affected by a stack-based buffer overflow by an authenticated user.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18761</a> <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R8300 before 1.0.2.104 and R8500 before 1.0.2.104.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18759</a> <a href="#">CONFIRM</a>

netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18808</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WAC505 before 5.0.5.4 and WAC510 before 5.0.5.4.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21119</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by unauthenticated firmware downgrade. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020-04-23	<a href="#">6.4</a>	<a href="#">CVE-2018-21131</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by authentication bypass.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21118</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers via the traceroute handler.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21117</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21116</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21115</a> <a href="#">CONFIRM</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the sessionLocation parameter for the login page is vulnerable to cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5730</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the UI Framework Error Page reflects arbitrary, user-supplied input back to the browser, which can result in XSS. Any page that is able to trigger a UI Framework Error is susceptible to this issue.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5729</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the export functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows the export of potentially sensitive information.	2020-04-17	<a href="#">5.8</a>	<a href="#">CVE-2020-5733</a> <a href="#">MISC</a>
openmrs -- openmrs	OpenMRS 2.9 and prior copies "Referrer" header values into an html element named "redirectUrl" within many webpages (such as login.htm). There is insufficient validation for this parameter, which allows for the possibility of cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5728</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the app parameter for the ActiveVisit's page is vulnerable to cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5731</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the import functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows unauthenticated users to use a feature typically restricted to administrators.	2020-04-17	<a href="#">5.8</a>	<a href="#">CVE-2020-5732</a> <a href="#">MISC</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is an open redirection when using back parameter. The impacts can be many, and vary from the theft of information and credentials to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">5.8</a>	<a href="#">CVE-2020-5270</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.6.0.0 and 1.7.6.5, there is a reflected XSS with 'date_from' and 'date_to' parameters in the dashboard page. This problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5271</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.4.0 and 1.7.6.5, there is a reflected XSS when uploading a wrong file. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5286</a> <a href="#">MISC</a>



				<a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.1.0 and 1.7.6.5, there is a reflected XSS on AdminCarts page with `cartBox` parameter The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5276</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is a reflected XSS with `back` parameter. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5285</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.5.4.0 and 1.7.6.5, there is a reflected XSS on Exception page The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5278</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is a reflected XSS on Search page with `alias` and `search` parameters. The problem is patched in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5272</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminFeatures page by using the `id_feature` parameter. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5269</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminAttributesGroups page. The problem is patched in 1.7.6.5.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5265</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop before version 1.7.6.5, there is a reflected XSS while running the security compromised page. It allows anyone to execute arbitrary action. The problem is patched in the 1.7.6.5.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5264</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
svg2png -- svg2png	svg2png 4.1.1 allows XSS with resultant SSRF via JavaScript inside an SVG document.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-11887</a> <a href="#">MISC</a>
wordpress -- wordpress	The GTranslate plugin before 2.8.52 for WordPress has Reflected XSS via a crafted link. This requires use of the hreflang tags feature within a sub-domain or sub-directory paid option.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-11930</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In f2fs_xattr_generic_list of xattr.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation.Product: Android. Versions: Android kernel. Android ID: A-120551147.	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0067</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	In crus_afe_get_param of msm-cirrus-playback.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: Android. Versions: Android kernel. Android ID: A-139354541	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0068</a> <a href="#">CONFIRM</a>
google -- android	In authorize_enroll of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146055840	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0077</a> <a href="#">MISC</a>
	In set_shared_key of the FPC IRIS TrustZone			

google -- android	app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel/Android ID: A-146057864	2020-04-17	2.1	<a href="#">CVE-2020-0075</a> <a href="#">MISC</a>
huawei -- honor_v20_smartphones	Huawei smartphones Honor V20 with versions earlier than 10.0.0.179(C636E3R4P3), versions earlier than 10.0.0.180(C185E3R3P3), versions earlier than 10.0.0.180(C432E10R3P4) have an information disclosure vulnerability. The device does not sufficiently validate the identity of smart wearable device in certain specific scenario, the attacker need to gain certain information in the victim's smartphone to launch the attack, successful exploit could cause information disclosure.	2020-04-20	2.9	<a href="#">CVE-2020-1803</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 173308.	2020-04-17	3.5	<a href="#">CVE-2019-4749</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (MTK chipsets) software. Interaction of GPS with 911 emergency calls is mishandled. The LG ID is LVE-SMP-180012 (January 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20784</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A TrustZone trusted application can crash via crafted input. The LG ID is LVE-SMP-190003 (May 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20779</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. A TZ trusted application can crash via crafted input. The LG ID is LVE-SMP-190005 (July 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20776</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9.0 (Qualcomm SDM450, SDM845, SM6150, and SM8150 chipsets) software. Weak encryption leads to local information disclosure. The LG ID is LVE-SMP-190010 (August 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20775</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A system service allows local retrieval of the user's password. The LG ID is LVE-SMP-190009 (August 2019).	2020-04-17	2.1	<a href="#">CVE-2019-20774</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-21	3.3	<a href="#">CVE-2018-21140</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-23	2.1	<a href="#">CVE-2018-21136</a> <a href="#">CONFIRM</a>
netgear -- dst6501_and_wnr2000_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects DST6501 before 1.1.0.6 and WNR2000v2 before 1.2.0.8.	2020-04-22	3.3	<a href="#">CVE-2017-18766</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by directory traversal. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before	2020-04-20	2.1	<a href="#">CVE-2017-18824</a> <a href="#">CONFIRM</a>

	12.0.2.15.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18828</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by administrative password disclosure. This affects D6220 before V1.0.0.28, D6400 before V1.0.0.60, D8500 before V1.0.3.29, DGN2200v4 before 1.0.0.82, DGN2200Bv4 before 1.0.0.82, R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	2020-04-22	2.1	<a href="#">CVE-2017-18777</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	2.1	<a href="#">CVE-2017-18840</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18831</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	2020-04-20	2.1	<a href="#">CVE-2017-18843</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400v2 before 1.0.2.32, R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	2020-04-20	2.1	<a href="#">CVE-2017-18847</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18827</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.42, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	2020-04-22	3.3	<a href="#">CVE-2017-18763</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-21	3.5	<a href="#">CVE-2017-18821</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18832</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	2.1	<a href="#">CVE-2017-18823</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	2020-04-23	3.3	<a href="#">CVE-2017-18747</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18825</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	2.1	<a href="#">CVE-2017-18836</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	2020-04-20	2.1	<a href="#">CVE-2017-18844</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18839</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by XSS. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before			



netgear -- multiple_devices	1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96, DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6100v2 before 1.0.1.54, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, R6700v2 before 1.2.0.12, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.18, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R7900P before 1.1.5.14, R8000 before 1.0.4.4, R8000P before 1.1.5.14, R8500 before 1.0.2.110, R8300 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.8, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.42, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	2020-04-22	3.5	<a href="#">CVE-2017-18785</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	2.1	<a href="#">CVE-2017-18780</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D7000 before 1.0.1.52, D7000v2 before 1.0.0.38, D7800 before 1.0.1.24, D8500 before 1.0.3.29, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.14, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300v1 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	2.1	<a href="#">CVE-2017-18778</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6250 before V1.0.4.8, R6400 before V1.0.1.22, R6400v2 before V1.0.2.32, R7100LG before V1.0.0.32, R7300 before V1.0.0.52, R8300 before V1.0.2.94, R8500 before V1.0.2.100, D6220	2020-04-22	2.1	<a href="#">CVE-2017-18789</a> <a href="#">CONFIRM</a>

	before V1.0.0.28, D6400 before V1.0.0.60, and D8500 before V1.0.3.29.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-21	<a href="#">2.7</a>	<a href="#">CVE-2018-21141 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, D7000 before 1.0.1.50, and D1500 before 1.0.0.25.	2020-04-21	<a href="#">2.1</a>	<a href="#">CVE-2017-18798 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects GS110EMX before 1.0.0.9, GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	2020-04-22	<a href="#">3.3</a>	<a href="#">CVE-2018-21122 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX6200v2 before 1.0.1.50, EX7000 before 1.0.0.56, JR6150 before 1.0.1.18, R6050 before 1.0.1.10J, R6100 before 1.0.1.16, R6150 before 1.0.1.10, R6220 before 1.1.0.50, R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.26, R6700v2 before 1.2.0.4, R6800 before 1.0.1.10, R6900 before 1.0.1.26, R6900P before 1.0.0.58, R6900v2 before 1.2.0.4, R7000 before 1.0.9.6, R7000P before 1.0.0.58, R7100LG before 1.0.0.32, R7300 before 1.0.0.54, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.40, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR4300v1 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR3500Lv2 before 1.2.0.44.	2020-04-22	<a href="#">2.1</a>	<a href="#">CVE-2017-18769 CONFIRM</a>
netgear -- r6700_and_r6800_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38 and R6800 before 1.1.0.38.	2020-04-20	<a href="#">2.1</a>	<a href="#">CVE-2017-18845 CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.30 are affected by incorrect configuration of security settings.	2020-04-21	<a href="#">2.1</a>	<a href="#">CVE-2017-18803 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18807 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18820 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18816 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18815 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18814 CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18810 CONFIRM</a>

tenable -- tenable.sc	Stored XSS in Tenable.Sc before 5.14.0 could allow an authenticated remote attacker to craft a request to execute arbitrary script code in a user's browser session. Updated input validation techniques have been implemented to correct this issue.	2020-04-17	3.5	<a href="#">CVE-2020-5737</a> <a href="#">MISC</a>
-----------------------	---	------------	-----	---

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Source CVSS Published Score Info
abb -- system_800xa_base	Weak Registry permissions in ABB System 800xA Base allow low privileged users to read and modify registry settings related to control system functionality, allowing an authenticated attacker to cause system functions to stop or malfunction.	<a href="#">CVE-2020-5474</a> yes calculated <a href="#">MISC</a>
abb -- system_800xa_information_manager	The installations for ABB System 800xA Information Manager versions 5.1, 6.0 to 6.0.3.2 and 6.1 wrongly contain an auxiliary component. An attacker is able to use this for an XSS-like attack to an authenticated local user, which might lead to execution of arbitrary code.	<a href="#">CVE-2020-5477</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	The Configuration pages in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway for user profiles and services transfer the password in plaintext (although hidden when displayed).	<a href="#">CVE-2019-19107</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	The web server in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows access to different endpoints of the application without authenticating by accessing a specific uniform resource locator (URL) , violating the access-control (ACL) rules. This issue allows obtaining sensitive information that may aid in further attacks and privilege escalation.	<a href="#">CVE-2019-19104</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	Improper implementation of Access Control in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows an unauthorized user to access data marked as restricted, such as viewing or editing user profiles and application settings.	<a href="#">CVE-2019-19106</a> yes calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon_gateway	The backup function in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway saves the current settings and configuration of the application, including credentials of existing user accounts and other configuration's credentials in plaintext.	<a href="#">CVE-2019-19105</a> yes calculated <a href="#">MISC</a>
admidio -- admidio	SQL Injection was discovered in Admidio before version 3.3.13. The main cookie parameter is concatenated into a SQL query without any input validation/sanitization, thus an attacker without logging in, can send a GET request with arbitrary SQL queries appended to the cookie parameter and execute SQL queries. The vulnerability impacts the confidentiality of the system. This has been patched in version 3.3.13.	<a href="#">CVE-2020-11004</a> yes calculated <a href="#">MISC</a> <a href="#">CONFIRM</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	<a href="#">CVE-2020-12131</a> yes calculated <a href="#">MISC</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	<a href="#">CVE-2020-12130</a> yes calculated <a href="#">MISC</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	<a href="#">CVE-2020-12129</a> yes calculated <a href="#">MISC</a>
anchor-cms -- anchor-cms	Anchor 0.12.7 allows admins to cause XSS via crafted post content.	<a href="#">CVE-2020-12071</a> yes calculated <a href="#">MISC</a>
atlassian -- confluence_server	The attachment-uploading feature in Atlassian Confluence Server from version 6.14.0 through version 6.14.3, and version 6.15.0 before version 6.15.5 allows remote attackers to achieve stored cross-site- scripting (SXSS) via a malicious attachment with a modified `mimeType`	<a href="#">CVE-2019-21102</a> yes calculated <a href="#">MISC</a>

	parameter.	
b&r_automation -- automation_runtime	An authentication weakness in the SNMP service in B&R Automation Runtime versions 2.96, 3.00, 3.01, 3.06 to 3.10, 4.00 to 4.63, 4.72 and above allows unauthenticated users to modify the configuration of B&R products via SNMP.	<a href="#">CVE-2019-10818</a> Calculated CONFIRM
beaker -- beaker	Beaker before 0.8.9 allows a sandbox escape, enabling system access and code execution. This occurs because Electron context isolation is not used, and therefore an attacker can conduct a prototype-pollution attack against the Electron internal messaging API.	<a href="#">CVE-2020-14079</a> Calculated MISC
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.5 allows remote attackers to obtain sensitive files via Local File Inclusion.	<a href="#">CVE-2020-12112</a> Calculated MISC
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.4 allows XSS via closed captions because dangerouslySetInnerHTML in React is used.	<a href="#">CVE-2020-14113</a> Calculated MISC
bitcoin-abe -- bitcoin-abe	Abe (aka bitcoin-abe) through 0.7.2, and 0.8pre, allows XSS in __call__ in abe.py because the PATH_INFO environment variable is mishandled during a PageNotFound exception.	<a href="#">CVE-2020-14944</a> Calculated MISC
bitdefender -- antivirus_free	A vulnerability in the improper handling of junctions in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects: Bitdefender Antivirus Free versions prior to 1.0.17.	<a href="#">CVE-2020-1099</a> Calculated MISC
bson -- bson	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.	<a href="#">CVE-2020-12135</a> Calculated MISC
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shifts_btrfs_ioctl_fd_replace() calls fdget(oldfd), then without further checks passes the resulting file* into shifts_real_fdget(), which casts file->private_data, a void* that points to a filesystem-dependent type, to a "struct shifts_file_info *". As the private_data is not required to be a pointer, an attacker can use this to cause a denial of service or possibly execute arbitrary code.	<a href="#">CVE-2019-15792</a> Calculated MISC
canonical -- ubuntu	Appport creates a world writable lock file with root ownership in the world writable /var/lock/appport directory. If the appport/ directory does not exist (this is not uncommon as /var/lock is a tmpfs), it will create the directory, otherwise it will simply continue execution using the existing directory. This allows for a symlink attack if an attacker were to create a symlink at /var/lock/appport, changing appport's lock file location. This file could then be used to escalate privileges, for example. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	<a href="#">CVE-2020-8531</a> Calculated CONFIRM
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shifts_btrfs_ioctl_fd_replace() installs an fd referencing a file from the lower filesystem without taking an additional reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a refcount underflow.	<a href="#">CVE-2019-15791</a> Calculated MISC
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into init_user_ns, whereas they should have been translated into the s_user_ns for the lower filesystem. This resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts s_user_ns. A local attacker could use this to possibly bypass discretionary access control permissions.	<a href="#">CVE-2019-15793</a> Calculated MISC
	Overlayfs in the Linux kernel and shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both	<a href="#">CVE-2019-</a>



canonical -- ubuntu	replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points. On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patches change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount underflow.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
canonical -- ubuntu	Time-of-check Time-of-use Race Condition vulnerability on crash report ownership change in Apport allows for a possible privilege escalation opportunity. If fs.protected_symlinks is disabled, this can be exploited between the os.open and os.chown calls when the Apport cron script clears out crash files of size 0. A symlink with the same name as the deleted file can then be created upon which chown will be called, changing the file owner to root. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
ceph -- ceph	An issue was discovered in Ceph through 13.2.9. A POST request with an invalid tagging XML can crash the RGW process by triggering a NULL pointer exception.	<a href="#">CVE-2020-12059</a> MISC MISC MISC MISC MISC
ceph -- ceph	A path traversal flaw was found in the Ceph dashboard implemented in upstream versions v14.2.5, v14.2.6, v15.0.0 of Ceph storage and has been fixed in versions 14.2.7 and 15.1.0. An unauthenticated attacker could use this flaw to cause information disclosure on the host machine running the Ceph dashboard.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
ceph -- object_gateway	A flaw was found in the Ceph Object Gateway, where it supports request sent by an anonymous user in Amazon S3. This flaw could lead to potential XSS attacks due to the lack of proper neutralization of untrusted input.	<a href="#">CVE-2020-15704</a> MISC MISC MISC MISC MISC
contiki-ng -- contiki-ng_and_contiki	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. A buffer overflow is present due to an integer underflow during 6LoWPAN fragment processing in the face of truncated fragments in os/net/ipv6/sicslowpan.c. This results in accesses of unmapped memory, crashing the application. An attacker can cause a denial-of-service via a crafted 6LoWPAN frame.	<a href="#">CVE-2019-9183</a> CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
contiki-ng -- contiki-ng_and_contiki	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. An out of bounds write is present in the data section during 6LoWPAN fragment re-assembly in the face of forged fragment offsets in os/net/ipv6/sicslowpan.c.	<a href="#">CVE-2019-9183</a> CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
d-link -- dir-615_devices	The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism and conduct brute-force attacks.	<a href="#">CVE-2019-17525</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A cfm UDP service listening on port 65002 allows remote, unauthenticated exfiltration of administrative credentials.	<a href="#">CVE-2020-9275</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The device can be reset to its default configuration by accessing an unauthenticated URL.	<a href="#">CVE-2020-9278</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A hard-coded account allows management-interface login with high privileges. The logged-in user can perform critical tasks and take full control of the device.	<a href="#">CVE-2020-9279</a> MISC MISC MISC MISC MISC
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. Authentication can be bypassed when accessing cgi modules. This allows one to perform administrative tasks (e.g., modify the admin password) with no authentication.	<a href="#">CVE-2020-9277</a> MISC MISC MISC MISC MISC

		<a href="#">MISC</a>
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The function do_cgi(), which processes cgi requests supplied to the device's web servers, is vulnerable to a remotely exploitable stack-based buffer overflow. Unauthenticated exploitation is possible by combining this vulnerability with CVE-2020-9277.	<a href="#">CVE-2020-9276</a> Calculated <a href="#">MISC</a> <a href="#">MISC</a>
dong_joo_cho -- file_transfer_ifamily	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the .etc/ path.	<a href="#">CVE-2020-12128</a> Calculated <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit.	<a href="#">CVE-2020-5869</a> Calculated <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer.	<a href="#">CVE-2020-5870</a> Calculated <a href="#">MISC</a>
f5 -- big-iq	In BIG-IQ 6.0.0-7.0.0, a remote access vulnerability has been discovered that may allow a remote user to execute shell commands on affected systems using HTTP requests to the BIG-IQ user interface.	<a href="#">CVE-2020-5868</a> Calculated <a href="#">MISC</a>
f5 -- nginx_controller	In versions of NGINX Controller prior to 3.2.0, communication between NGINX Controller and NGINX Plus instances skip TLS verification by default.	<a href="#">CVE-2020-5864</a> Calculated <a href="#">CONFIRM</a>
f5 -- nginx_controller	In versions prior to 3.3.0, the NGINX Controller Agent installer script 'install.sh' uses HTTP instead of HTTPS to check and install packages	<a href="#">CVE-2020-5867</a> Calculated <a href="#">CONFIRM</a>
f5 -- nginx_controller	In versions of NGINX Controller prior to 3.3.0, the helper.sh script, which is used optionally in NGINX Controller to change settings, uses sensitive items as command-line arguments.	<a href="#">CVE-2020-5866</a> Calculated <a href="#">CONFIRM</a>
f5 -- nginx_controller	In versions prior to 3.3.0, the NGINX Controller is configured to communicate with its Postgres database server over unencrypted channels, making the communicated data vulnerable to interception via man-in-the-middle (MITM) attacks.	<a href="#">CVE-2020-5865</a> Calculated <a href="#">CONFIRM</a>
fifthplay -- s.a.m.i	Fifthplay S.A.M.I before 2019.3_HP2 allows unauthenticated stored XSS via a POST request.	<a href="#">CVE-2020-13132</a> Calculated <a href="#">MISC</a> <a href="#">MISC</a>
flexera -- flexnet_publisher	A Denial of Service vulnerability related to stack exhaustion has been identified in FlexNet Publisher lmadmin.exe 11.16.2. Because the message reading function calls itself recursively given a certain condition in the received message, an unauthenticated remote attacker can repeatedly send messages of that type to cause a stack exhaustion condition.	<a href="#">CVE-2019-8961</a> Calculated <a href="#">CONFIRM</a>
flexera -- flexnet_publisher	A Denial of Service vulnerability related to command handling has been identified in FlexNet Publisher lmadmin.exe version 11.16.2. The message reading function used in lmadmin.exe can, given a certain message, call itself again and then wait for a further message. With a particular flag set in the original message, but no second message received, the function eventually return an unexpected value which leads to an exception being thrown. The end result can be process termination.	<a href="#">CVE-2019-8960</a> Calculated <a href="#">CONFIRM</a>
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of vertices in U3D objects. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10568.	<a href="#">CVE-2020-14905</a> Calculated <a href="#">MISC</a> <a href="#">MISC</a>
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction	

foxit -- phantompdf	is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the AddWatermark command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9942.	<a href="#">CVE-2020-04909</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the GetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9944.	<a href="#">CVE-2020-04911</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the OCRAndExportToExcel command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9946.	<a href="#">CVE-2020-04913</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10461.	<a href="#">CVE-2020-04901</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10463.	<a href="#">CVE-2020-04903</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10193.	<a href="#">CVE-2020-04897</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10190.	<a href="#">CVE-2020-04894</a> 11/16/2020 Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the SetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9945.	<a href="#">CVE-2020-04912</a> 11/16/2020 Notated MISC
	This vulnerability allows remote attackers to execute arbitrary code on	

foxit -- phantompdf	affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the DuplicatePages command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9828.	<a href="#">CVE-2020-04889</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the ConvertToPDF command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9829.	<a href="#">CVE-2020-04890</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Save command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9831.	<a href="#">CVE-2020-04891</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10189.	<a href="#">CVE-2020-04893</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Export command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9865.	<a href="#">CVE-2020-04908</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10191.	<a href="#">CVE-2020-04895</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10192.	<a href="#">CVE-2020-04896</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10195.	<a href="#">CVE-2020-04898</a> Notated MISC
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a	<a href="#">CVE-2020-</a>



foxit -- phantompdf	malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10462.	<a href="#">CVE-2020-04902</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10464.	<a href="#">CVE-2020-04904</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the RotatePage command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9943.	<a href="#">CVE-2020-04910</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the CombineFiles command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9830.	<a href="#">CVE-2020-04892</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10132.	<a href="#">CVE-2020-04899</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the resetForm method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10614.	<a href="#">CVE-2020-04906</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10142.	<a href="#">CVE-2020-04900</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of widgets in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10650.	<a href="#">CVE-2020-04907</a> <a href="#">MISC</a> <a href="#">MISC</a> dated
	Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. This bug is similar to CVE-2020-5260(GHSA-qm7j-c969-7j4q). The fix for that bug still left the door open for an exploit where <code>_some_credential</code> is leaked (but the attacker cannot control which one). Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that are considered illegal as of the recently	<a href="#">CVE-</a>

git -- git	published Git versions can cause Git to send a "blank" pattern to helpers, missing hostname and protocol fields. Many helpers will interpret this as matching <code>_any_</code> URL, and will return some unspecified stored password, leaking the password to an attacker's server. The vulnerability can be triggered by feeding a malicious URL to <code>'git clone'</code> . However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The root of the problem is in Git itself, which should not be feeding blank input to helpers. However, the ability to exploit the vulnerability in practice depends on which helpers are in use. Credential helpers which are known to trigger the vulnerability: - Git's "store" helper - Git's "cache" helper - the "osxkeychain" helper that ships in Git's "contrib" directory Credential helpers which are known to be safe even with vulnerable versions of Git: - Git Credential Manager for Windows Any helper not in this list should be assumed to trigger the vulnerability.	<a href="#">2020-11008</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">2020-11008</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">GENTOO</a>
gitlab -- gitlab	An issue was discovered in GitLab 10.7.0 and later through 12.9.2. A Workhorse bypass could lead to job artifact uploads and file disclosure (Exposure of Sensitive Information) via request smuggling.	<a href="#">CVE-2020-14506</a> <a href="#">2020-14506</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and_enterprise_editions	An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 12.7.9, 12.8.x before 12.8.9, and 12.9.x before 12.9.3. A Workhorse bypass could lead to NuGet package and file disclosure (Exposure of Sensitive Information) via request smuggling.	<a href="#">CVE-2020-14505</a> <a href="#">2020-14505</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and_enterprise_editions	An issue was discovered in GitLab CE and EE 8.15 through 12.9.2. Members of a group could still have access after the group is deleted.	<a href="#">CVE-2020-145649</a> <a href="#">2020-145649</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
gnome -- evolution	An issue was discovered in GNOME Evolution before 3.35.91. By using the proprietary (non-RFC6068) "mailto?attach=..." parameter, a website (or other source of mailto links) can make Evolution attach local files or directories to a composed email message without showing a warning to the user, as demonstrated by an attach=. value.	<a href="#">CVE-2020-145879</a> <a href="#">2020-145879</a> <a href="#">MISC</a> <a href="#">Calculated</a>
gnu -- gnu_mailman	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code.	<a href="#">CVE-2020-146887</a> <a href="#">2020-146887</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- google_earth_pro	A vulnerability in the windows installer of Google Earth Pro versions prior to 7.3.3 allows an attacker using DLL h jacking to insert malicious local files to execute unauthenticated remote code on the targeted system.	<a href="#">CVE-2020-14895</a> <a href="#">2020-14895</a> <a href="#">MISC</a> <a href="#">Calculated</a>
grafana_labs -- grafana	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	<a href="#">CVE-2020-172245</a> <a href="#">2020-172245</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">MISC</a>
hcl -- appscan_enterprise	"HCL AppScan Enterprise uses hard-coded credentials which can be exploited by attackers to get unauthorized access to application's encrypted files."	<a href="#">CVE-2019-14327</a> <a href="#">2019-14327</a> <a href="#">MISC</a> <a href="#">Calculated</a>
hcl -- connections	"HCL Connections is vulnerable to possible information leakage and could disclose sensitive information via stack trace to a local user."	<a href="#">CVE-2020-14085</a> <a href="#">2020-14085</a> <a href="#">MISC</a> <a href="#">Calculated</a> <a href="#">CONFIRM</a>
helm -- helm	There is an information disclosure vulnerability in Helm from version 3.1.0 and before version 3.2.0. 'lookup' is a Helm template function introduced in Helm v3. It is able to lookup resources in the cluster to check for the existence of specific resources and get details about them. This can be used as part of the process to render templates. The documented behavior of 'helm template' states that it does not attach to a remote cluster. However, a the recently added 'lookup' template function circumvents this restriction and connects to the cluster even during 'helm template' and 'helm install update delete rollback --dry-run'. The user is	<a href="#">CVE-2020-14013</a> <a href="#">2020-14013</a> <a href="#">MISC</a>

	not notified of this behavior. Running `helm template` should not make calls to a cluster. This is different from `install`, which is presumed to have access to a cluster in order to load resources into Kubernetes. Helm 2 is unaffected by this vulnerability. A malicious chart author could inject a `lookup` into a chart that, when rendered through `helm template`, performs unannounced lookups against the cluster a user's `KUBECONFIG` file points to. This information can then be disclosed via the output of `helm template`. This issue has been fixed in Helm 3.2.0	MISC 2020-04-15 Not Calculated CONFIRM
hp -- j/h-series_nonstop_systems	This document describes a security vulnerability in Blade Maintenance Entity, Integrated Maintenance Entity and Maintenance Entity products. All J/H-series NonStop systems have a security vulnerability associated with an open UDP port 17185 on the Maintenance LAN which could result in information disclosure, denial-of-service attacks or local memory corruption against the affected system and a complete control of the system may also be possible. This vulnerability exists only if one gains access to the Maintenance LAN to which Blade Maintenance Entity, Integrated Maintenance Entity or Maintenance Entity product is connected. **Workaround:** Block the UDP port 17185(In the Maintenance LAN Network Switch/Firewall). Fix: Install following SPRs, which are already available: * T1805A01^AAI (Integrated Maintenance Entity) * T4805A01^AAZ (Blade Maintenance Entity). These SPRs are also usable with the following RVUs: * J06.19.00 ? J06.23.01. No fix planned for the following RVUs: J06.04.00 ? J06.18.01. No fix planned for H-Series NonStop systems. No fix planned for the product T2805 (Maintenance Entity).	CVE- 2020-04-31 Not Calculated MISC
hp -- onboard_administrator	A potential security vulnerability has been identified in HPE Onboard Administrator. The vulnerability could be remotely exploited to allow Reflected Cross Site Scripting. HPE has made the following software updates and mitigation information to resolve the vulnerability in HPE Onboard Administrator. * OA 4.95 (Linux and Windows).	CVE- 2020-04-32 Not Calculated MISC
hp -- uiot	A unauthorized remote access vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	CVE- 2020-04-33 Not Calculated MISC
hp -- uiot	A remote access to sensitive data vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	CVE- 2020-04-34 Not Calculated MISC
bm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 173310.	CVE- 2019-04-50 Not Calculated CONFIRM
bm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 reveals a stack trace on certain API requests which can allow an attacker further information about the implementation of the offering. IBM X-Force ID: 173311.	CVE- 2019-04-51 Not Calculated CONFIRM
bm -- maas360	IBM MaaS360 6.82 could allow a user with physical access to the device to crash the application which may enable the user to access restricted applications and device settings. IBM X-Force ID: 178505.	CVE- 2020-04-53 Not Calculated CONFIRM
bm -- maas360_for_ios	IBM MaaS360 3.96.62 for iOS could allow an attacker with physical access to the device to obtain sensitive information from the agent outside of the container. IBM X-Force ID: 172705.	CVE- 2020-04-55 Not Calculated CONFIRM
bm -- mq_and_mq_appliance	IBM MQ and MQ Appliance 8.0, 9.1 LTS, and 9.1 CD could allow an authenticated user cause a denial of service due to a memory leak. IBM X-Force ID: 175840.	CVE- 2020-04-57 Not Calculated CONFIRM
bm -- spectrum_protect	IBM Spectrum Protect 7.1 and 8.1 server is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker to execute arbitrary code on the system with the privileges of an administrator or user associated with the Spectrum Protect server or cause the Spectrum Protect server to crash. IBM X-Force ID: 179990.	CVE- 2020-04-15 Not Calculated CONFIRM

bm -- tivoli_monitoring	IBM Tivoli Monitoring 6.3.0 could allow a local attacker to execute arbitrary code on the system. By placing a specially crafted file, an attacker could exploit this vulnerability to load other DLL files located in the same directory and execute arbitrary code on the system. IBM X-Force ID: 177083.	<a href="#">CVE-2020-1311</a> yes calculated <a href="#">CONFIRM</a>
bm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0.4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 171250.	<a href="#">CVE-2020-1468</a> yes calculated <a href="#">CONFIRM</a>
bm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0.3.0 and 7.0.4.0 could allow an authenticated user to impersonate another user if the server is configured to enable Distributed Front End (DFE). IBM X-Force ID: 174955.	<a href="#">CVE-2020-14302</a> yes calculated <a href="#">CONFIRM</a>
infradead -- openconnect	OpenConnect through 8.08 mishandles negative return values from X509_check_function calls, which might assist attackers in performing man-in-the-middle attacks.	<a href="#">CVE-2020-12105</a> yes calculated <a href="#">MISC</a>
jetbrains -- golang	In JetBrains GoLand before 2019.3.2, the plugin repository was accessed via HTTP instead of HTTPS.	<a href="#">CVE-2020-11685</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- hub	In JetBrains Hub before 2020.1.12099, content spoofing in the Hub OAuth error message was possible.	<a href="#">CVE-2020-11691</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2020.1, the license server could be resolved to an untrusted host in some cases.	<a href="#">CVE-2020-11690</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- space	In JetBrains Space through 2020-04-22, the password authentication implementation was insecure.	<a href="#">CVE-2020-11796</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- space	In JetBrains Space through 2020-04-22, the session timeout period was configured improperly.	<a href="#">CVE-2020-11795</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- space	JetBrains Space through 2020-04-22 allows stored XSS in Chats.	<a href="#">CVE-2020-11416</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.4, a project administrator was able to retrieve some TeamCity server settings.	<a href="#">CVE-2020-11686</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.2, password values were shown in an unmasked format on several pages.	<a href="#">CVE-2020-11687</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.1, a user without appropriate permissions was able to import settings from the settings.kts file.	<a href="#">CVE-2020-11689</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.1, the application state is kept alive after a user ends his session.	<a href="#">CVE-2020-11688</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- teamcity	In JetBrains TeamCity 2018.2 through 2019.2.1, a project administrator was able to see scrambled password parameters used in a project. The issue was resolved in 2019.2.2.	<a href="#">CVE-2020-11938</a> yes calculated <a href="#">CONFIRM</a>
jetbrains -- youtrack	In JetBrains YouTrack before 2020.1.659, DB export was access ble to read-only administrators.	<a href="#">CVE-2020-11692</a> yes calculated <a href="#">CONFIRM</a>
		<a href="#">CVE-</a>



jetbrains -- youtrack	JetBrains YouTrack before 2020.1.659 was vulnerable to DoS that could be caused by attaching a malformed TIFF file to an issue.	<a href="#">CVE-2020-11693</a> Yes Calculated CONFIRM
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized editing of usergroups.	<a href="#">CVE-2020-11891</a> Yes Calculated MISC
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Improper input validations in the usergroup table class could lead to a broken ACL configuration.	<a href="#">CVE-2020-11890</a> Yes Calculated MISC
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized deletion of usergroups.	<a href="#">CVE-2020-11889</a> Yes Calculated MISC
jquery -- jquery	jQuery v2.2.2 allows XSS via a crafted onerror attribute of an IMG element.	<a href="#">CVE-2018-13405</a> Yes Calculated MISC
juplink -- rx4-1500_router	Juplink RX4-1500 v1.0.3 allows remote attackers to gain root access to the Linux subsystem via an unsanitized exec call (aka Command Line Injection), if the undocumented telnetd service is enabled and the attacker can authenticate as admin from the local network.	<a href="#">CVE-2020-8797</a> Yes Calculated MISC
juplink -- rx4-1500_router	httpd in Juplink RX4-1500 v1.0.3-v1.0.5 allows remote attackers to change or access router settings by connecting to the unauthenticated setup3.htm endpoint from the local network.	<a href="#">CVE-2020-8798</a> Yes Calculated MISC
lazysizes -- lazysizes	lazysizes through 5.2.0 allows execution of malicious JavaScript. The following attributes are not sanitized by the video-embed plugin: data-vimeo, data-vimeoparams, data-youtube and data-ytparams which can be abused to inject malicious JavaScript.	<a href="#">CVE-2020-7342</a> Yes Calculated MISC
libnvc -- libnvc_server	libvncclient/cursor.c in L bVNCServer through 0.9.12 has a HandleCursorShape integer overflow and heap-based buffer overflow via a large height or width value. NOTE: this may overlap CVE-2019-15690.	<a href="#">CVE-2020-7078</a> Yes Calculated MISC
libslirp -- libslirp	A use after free vulnerability in ip_reass() in ip_input.c of libslirp 4.2.0 and prior releases allows crafted packets to cause a denial of service.	<a href="#">CVE-2020-14883</a> Yes Calculated MISC
mailstore -- mailstore_outlook_add-in	In MailStore Outlook Add-in (and Email Archive Outlook Add-in) through 12.1.2, the login process does not validate the validity of the certificate presented by the server.	<a href="#">CVE-2020-11806</a> Yes Calculated CONFIRM
mediawiki -- mediawiki	The CentralAuth extension through REL1_34 for MediaWiki allows remote attackers to obtain sensitive hidden account information via an api.php?action=query&meta=globaluserinfo&guiuser= request. In other words, the information can be retrieved via the action API even though access would be denied when simply visiting wiki/Special:CentralAuth in a web browser.	<a href="#">CVE-2020-14051</a> Yes Calculated MISC
minio -- minio	MinIO versions before RELEASE.2020-04-23T00-58-49Z have an authentication bypass issue in the MinIO admin API. Given an admin access key, it is possible to perform admin API operations i.e. creating new service accounts for existing access keys - without knowing the admin secret key. This has been fixed and released in version RELEASE.2020-04-23T00-58-49Z.	<a href="#">CVE-2020-10012</a> Yes Calculated MISC CONFIRM
mozilla -- firefox	Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6826</a> Yes Calculated MISC
mozilla -- firefox	A malicious extension could have called <code>browser.identity.launchWebAuthFlow</code>, controlling the redirect_uri, and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6823</a> Yes Calculated MISC
	Initially, a user opens a Private Browsing Window and generates a	

mozilla -- firefox	password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new password - the generated passwords would have been identical, rather than independent. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6824</a> Calculated MISC
mozilla -- firefox_esr	When following a link that opened an intent://-schemed URL, causing a custom tab to be opened, Firefox for Android could be tricked into displaying the incorrect URI.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	<a href="#">CVE-2020-6827</a> Calculated MISC
mozilla -- firefox_esr	A malicious Android application could craft an Intent that would have been processed by Firefox for Android and potentially result in a file overwrite in the user's profile directory. One exploitation vector for this would be to supply a user.js file providing arbitrary malicious preference values. Control of arbitrary preferences can lead to sufficient compromise such that it is generally equivalent to arbitrary code execution.  *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	<a href="#">CVE-2020-6828</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	When reading from areas partially or fully outside the source resource with WebGL's <code>copyTexSubImage</code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-6829</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code>GMPDecodeData</code>. It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-6830</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	<a href="#">CVE-2020-6831</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-6835</a> Calculated MISC
mozilla -- thunderbird_and_firefox_and_firefox_esr	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	<a href="#">CVE-2020-6839</a> Calculated MISC
msi -- true_color	Unquoted search path vulnerability in MSI True Color before 3.0.52.0 allows privilege escalation to SYSTEM.	<a href="#">CVE-2020-6842</a> Calculated MISC
nanometrics -- centaur_and_titansma_devices	Nanometrics Centaur through 4.3.23 and TitanSMA through 4.2.20 mishandle access control for the syslog log.	<a href="#">CVE-2020-6843</a> Calculated MISC
netatmo -- smart_indoor_camera	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in firmware versions prior to x.xx of Netatmo Smart Indoor Camera allows an attacker to execute commands on the device. This issue affects: Netatmo Smart Indoor Camera version and prior versions.	<a href="#">CVE-2020-6849</a> Calculated MISC
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	<a href="#">CVE-2020-6848</a> Calculated CONFIRM

netgear -- gs810emx_devices	NETGEAR GS810EMX devices before 1.0.0.5 are affected by disclosure of sensitive information.	CVE-2020-1433 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2020-21166 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1., JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	CVE-2020-21230 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R6900P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8500 before 1.0.2.106, R8300 before 1.0.2.106, and WNDR3400v3 before 1.0.1.16.	CVE-2020-18704 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.0.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2020-18720 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D1500 before 1.0.0.25, D500 before 1.0.0.25, D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, EX6100v2 before 1.0.1.60, EX6150v2 before 1.0.1.60, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.16, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.18, R6020 before 1.0.0.26, R6050 before 1.0.1.16, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6220 before 1.1.0.60, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3700v5 before 1.1.0.48, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.46, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	CVE-2020-18703 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.0.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2020-18725 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.0.17, WAC510 before 5.0.0.17, WAC720 before 5.0.0.17, WAC730 before 5.0.0.17, WAC740 before 5.0.0.17, and WND930 before 5.0.0.17.	CVE-2020-21133 Yes Calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects EX3700 before 1.0.0.66, EX3800 before 1.0.0.66, EX6100 before 1.0.2.20, EX6120 before 1.0.0.34, EX6150 before 1.0.0.36, EX6200	CVE-2020-18715 Yes Calculated

	before 1.0.3.84, and EX7000 before 1.0.0.60.	<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6050/JR6150 before 1.0.1.7, PR2000 before 1.0.0.17, R6220 before 1.1.0.50, WNDR3700v5 before 1.1.0.48, JNR1010v2 before 1.1.0.40, JWNR2010v5 before 1.1.0.40, WNR1000v4 before 1.1.0.40, WNR2020 before 1.1.0.40, WNR2050 before 1.1.0.40, WNR614 before 1.1.0.40, WNR618 before 1.1.0.40, and D7000 before 1.0.1.50.	<a href="#">CVE-2020-18791</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6400 before 1.0.0.60, D7000 before 1.0.1.50, D8500 before 1.0.3.29, EX6200 before 1.0.3.84, EX7000 before 1.0.0.60, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R9000 before 1.0.2.52, WNDR3400v3 before 1.0.1.16, WNR3500Lv2 before 1.2.0.46, and WNDR3700v5 before 1.1.0.48.	<a href="#">CVE-2020-18790</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-18713</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400 before 1.0.1.24, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	<a href="#">CVE-2020-18797</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18722</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18718</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.1.00.26, R6080 before 1.1.00.26, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18719</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.60, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.66.	<a href="#">CVE-2020-21111</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1.78, JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	<a href="#">CVE-2020-21231</a> yes calculated <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow	<a href="#">CVE-</a>



netgear -- multiple_devices	by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18716</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18724</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18723</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18728</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R7500v2 before 1.0.3.20, R7800 before 1.0.2.38, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<a href="#">CVE-2020-18729</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	<a href="#">CVE-2020-18749</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18721</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	<a href="#">CVE-2020-18746</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	<a href="#">CVE-2020-18743</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX6200v2 before 1.0.1.44, R6100 before 1.0.1.12, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, R7800 before 1.0.2.28, R9000 before 1.0.2.30, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-18748</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, EX6100v2 before 1.0.1.50, EX6150v2 before 1.0.1.50, EX6200v2 before 1.0.1.44, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.2.30, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<a href="#">CVE-2020-18728</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R6400v2 before 1.0.2.34, R6700 before 1.0.1.30, R6900 before 1.0.1.30, R6900P before 1.0.0.62, R7000 before 1.0.9.12, R7000P before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<a href="#">CVE-2020-18727</a> Yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-18711</a> Yes calculated <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.00.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050, before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	<a href="#">CVE-2017-18787</a> 2017-18787 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.00.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	<a href="#">CVE-2017-18786</a> 2017-18786 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2017-18717</a> 2017-18717 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	<a href="#">CVE-2017-18790</a> 2017-18790 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2017-18712</a> 2017-18712 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.20, R7500 before 1.0.0.118, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	<a href="#">CVE-2017-18706</a> 2017-18706 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects EX6100 before 1.0.2.16_1.1.130, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.50, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, and WN3000RPv3 before 1.0.2.44.	<a href="#">CVE-2017-18768</a> 2017-18768 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700 before 1.0.1.48, R7500 before 1.0.0.124, R7800 before 1.0.2.58, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, and WNR2000v5-R2000 before 1.0.0.68.	<a href="#">CVE-2018-21135</a> 2018-21135 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	<a href="#">CVE-2017-18705</a> 2017-18705 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.66, D8500 before 1.0.3.35, DGN2200Bv4 before 1.0.0.94, DGN2200v4 before 1.0.0.94, R6250 before 1.0.4.14, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.30, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7900 before 1.0.2.4, R8000 before 1.0.4.2, WN2500RPv2 before 1.0.1.50, WNDR3400v3 before 1.0.1.14, and WNDR4000 before 1.0.2.10.	<a href="#">CVE-2017-18756</a> 2017-18756 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.16, R7500 before 1.0.0.116, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR4300v2 before 1.0.0.48, WNDR4300v1 before 1.0.2.90, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2017-18757</a> 2017-18757 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R6700 before 1.0.1.20, R6900 before 1.0.1.20, WNR3500Lv2 before 1.2.0.44, and WNR2000v2 before 1.2.0.8.	<a href="#">CVE-2017-18765</a> 2017-18765 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	<a href="#">CVE-2018-16565</a> 2018-16565 yes calculated CONFIRM
	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DGN2200Bv4 before 1.0.0.102,	

netgear -- multiple_devices	DGN2200v4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6300v2 before 1.0.4.22, R6900P before 1.3.0.18, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, WN2500RPv2 before 1.0.1.52, and WNDR3400v3 before 1.0.1.18.	<a href="#">CVE-2020-2118</a> yes <a href="#">21163</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6400 before 1.0.0.78, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.8, R6300v2 before 1.0.4.6, R6400 before 1.0.1.12, R6700 before 1.0.1.16, R7000 before 1.0.7.10, R7100LG before 1.0.0.42, R7300DST before 1.0.0.44, R7900 before 1.0.1.12, R8000 before 1.0.3.36, R8300 before 1.0.2.74, R8500 before 1.0.2.74, WNDR3400v3 before 1.0.1.14, and WNR3500Lv2 before 1.2.0.48.	<a href="#">CVE-2020-2118</a> yes <a href="#">21162</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6100 before 1.0.1.20, R7800 before 1.0.2.40, and R9000 before 1.0.2.52.	<a href="#">CVE-2020-2117</a> yes <a href="#">18698</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.94.	<a href="#">CVE-2020-2117</a> yes <a href="#">18752</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-2117</a> yes <a href="#">18727</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-2117</a> yes <a href="#">18728</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6700 before 1.0.1.48, R7900 before 1.0.2.16, R6900 before 1.0.1.48, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R7000 before 1.0.9.34, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R7900P before 1.4.1.24, R8500 before 1.0.2.122, R8300 before 1.0.2.122, WN2500RPv2 before 1.0.1.54, EX3700 before 1.0.0.72, EX3800 before 1.0.0.72, EX6000 before 1.0.0.32, EX6100 before 1.0.2.24, EX6120 before 1.0.0.42, EX6130 before 1.0.0.24, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, D7000v2 before 1.0.0.51, D6220 before 1.0.0.46, D6400 before 1.0.0.82, and D8500 before 1.0.3.42.	<a href="#">CVE-2020-2118</a> yes <a href="#">21134</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-2117</a> yes <a href="#">18751</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	<a href="#">CVE-2020-2118</a> yes <a href="#">21145</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.46, and R9000 before 1.0.3.16.	<a href="#">CVE-2020-2118</a> yes <a href="#">21161</a> calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-2117</a> yes <a href="#">18729</a> calculated <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	CVE-2018-21151 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.61, D6000 before 1.0.0.61, D6100 before 1.0.0.55, D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	CVE-2017-18740 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.0.1.20, R7000 before 1.0.7.10, R7000P before 1.0.0.58, R6900P before 1.0.0.58, R7100LG before 1.0.0.32, R7900 before 1.0.1.14, R8000 before 1.0.3.22, and R8500 before 1.0.2.94.	CVE-2017-18741 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, and WNR2000v5 before 1.0.0.58.	CVE-2017-18731 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DM200 before 1.0.0.52, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.16, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2018-21144 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6250 before 1.0.4.12, R6300v2 before 1.0.4.8, R6700 before 1.0.1.16, R6900 before 1.0.1.16, R7300DST before 1.0.0.54, R7900 before 1.0.1.12, R8000 before 1.0.3.32, and R8500 before 1.0.2.74.	CVE-2017-18742 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2018-21142 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.58, D6200 before 1.1.00.30, D6220 before 1.0.0.46, D6400 before 1.0.0.82, D7000 before 1.0.1.68, D7000v2 before 1.0.0.51, D7800 before 1.0.1.42, D8500 before 1.0.3.42, DC112A before 1.0.0.40, DGN2200Bv4 before 1.0.0.102, DGN2200v4 before 1.0.0.102, JNR1010v2 before 1.1.0.54, JR6150 before 1.0.1.18, JWNR2010v5 before 1.1.0.54, PR2000 before 1.0.0.24, R6020 before 1.0.0.34, R6050 before 1.0.1.18, R6080 before 1.0.0.34, R6100 before 1.0.1.22, R6120 before 1.0.0.42, R6220 before 1.1.0.68, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R6700 before 1.0.1.48, R6700v2 before 1.2.0.24, R6800 before 1.2.0.24, R6900 before 1.0.1.48, R6900P before 1.3.1.44, R6900v2 before 1.2.0.24, R7000 before 1.0.9.34, R7000P before 1.3.1.44, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R7500 before 1.0.0.124, R7500v2 before 1.0.3.38, R7900 before 1.0.2.16, R7900P before 1.4.1.24, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R8300 before 1.0.2.122, R8500 before 1.0.2.122, WN3000RP before 1.0.0.68, WN3000RPv2 before 1.0.0.68, WNDR3400v3 before 1.0.1.18, WNDR3700v4 before 1.0.2.102, WNDR3700v5 before 1.1.0.54, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, WNR1000v4 before 1.1.0.54, WNR2020 before 1.1.0.54, WNR2050 before 1.1.0.54, and WNR3500Lv2 before 1.2.0.54.	CVE-2018-21139 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2017-18730 yes calculated CONFIRM
netgear -- r6220_and_wndr3700_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6220 before 1.1.0.64 and WNDR3700v5 before 1.1.0.54.	CVE-2018-21164 yes calculated CONFIRM
		CVE-



netgear -- r6220_devices	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	2020- 2017- yes CVE- 2017- 18702 calculated CONFIRM
netgear -- r6700_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	2020- 2017- yes CVE- 2017- 18701 calculated CONFIRM
netgear -- r7800_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020- 2017- yes CVE- 2017- 18697 calculated CONFIRM
netgear -- r7800_devices_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	2020- 2017- yes CVE- 2017- 18699 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020- 2017- yes CVE- 2017- 18707 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by CSRF. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020- 2017- yes CVE- 2017- 18708 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	2020- 2017- yes CVE- 2017- 18709 calculated CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	2020- 2017- yes CVE- 2017- 18710 calculated CONFIRM
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	2020- 2018- yes CVE- 2018- 102 calculated CONFIRM
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	2020- 2018- yes CVE- 2018- 21160 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18809 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18813 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	2020- 2017- yes CVE- 2017- 18819 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18812 calculated CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020- 2017- yes CVE- 2017- 18811 calculated CONFIRM
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020- 2018- yes CVE- 2018- 1126 calculated CONFIRM
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020- 2018- yes CVE- 2018- 1128 calculated CONFIRM

netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-127</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-130</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-129</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac510_devices	NETGEAR WAC510 devices before 5.0.0.17 are affected by privilege escalation.	<a href="#">CVE-2020-124</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wac510_devices	NETGEAR WAC510 devices before 5.0.0.17 are affected by authentication bypass.	<a href="#">CVE-2020-125</a> Yes Calculated <a href="#">CONFIRM</a>
netgear -- wndr4500_devices	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	<a href="#">CVE-2020-1717</a> Yes Calculated <a href="#">CONFIRM</a>
ntop -- ndpi	In nDPI through 3.2 Stable, the SSH protocol dissector has multiple KEXINIT integer overflows that result in a controlled remote heap overflow in concat_hash_string in ssh.c. Due to the granular nature of the overflow primitive and the ability to control both the contents and layout of the nDPI library's heap memory through remote input, this vulnerability may be abused to achieve full Remote Code Execution against any network inspection stack that is linked against nDPI and uses it to perform network traffic analysis.	<a href="#">CVE-2020-939</a> Yes Calculated <a href="#">MISC</a>
ntop -- ndpi	In nDPI through 3.2 Stable, an out-of-bounds read in concat_hash_string in ssh.c can be exploited by a network-positioned attacker that can send malformed SSH protocol messages on a network segment monitored by nDPI's library.	<a href="#">CVE-2020-940</a> Yes Calculated <a href="#">MISC</a>
opc_foundation -- ua.net_standard	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of OPC Foundation UA .NET Standard 1.04.358.30. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of sessions. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to create a denial-of-service condition against the application. Was ZDI-CAN-10295.	<a href="#">CVE-2020-967</a> Yes Calculated <a href="#">MISC</a>
openssl -- openssl	Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).	<a href="#">CVE-2020-1967</a> Yes Calculated <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">FREEBSD</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
oppo -- coloros	In ColorOS (oppo mobile phone operating system, based on AOSP frameworks/native code position/services/surfaceflinger surfaceflinger.CPP), RGB is defined on the stack but uninitialized, so when the screenShot function to RGB value assignment, will not initialize the value is returned to the attackers, leading to values on the stack information leakage, the vulnerability can be used to bypass attackers ALSR.	<a href="#">CVE-2020-11828</a> Yes Calculated <a href="#">CONFIRM</a>
paypal-adaptive -- paypal-adaptive	paypal-adaptive through 0.4.2 manipulation of JavaScript objects resulting	<a href="#">CVE-2020-</a> Yes Calculated

	in Prototype Pollution. The PayPal function could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload.	<a href="#">CVE-2020-1443</a> 2020-04-18 Calculated MISC
phproject -- phproject	In Phproject before version 1.7.8, there's a vulnerability which allows users with access to file uploads to execute arbitrary code. This is patched in version 1.7.8.	<a href="#">CVE-2020-144011</a> 2020-04-18 Calculated CONFIRM
plex -- media_server	Improper Input Validation in Plex Media Server on Windows allows a local, unauthenticated attacker to execute arbitrary Python code with SYSTEM privileges.	<a href="#">CVE-2020-144740</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is improper access control on customers search. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-14487</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there are improper access controls on product page with combinations, attachments and specific prices. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-14493</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	"In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there is improper access controls on product attributes page. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-14488</a> 2020-04-18 Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.5.0.0 and 1.7.6.5, there are improper access control since the the version 1.5.0.0 for legacy controllers. - admin-dev/index.php/configure/shop/customer-preferences/ - admin-dev/index.php/improve/international/translations/ - admin-dev/index.php/improve/international/geolocation/ - admin-dev/index.php/improve/international/localization - admin-dev/index.php/configure/advanced/performance - admin-dev/index.php/sell/orders/delivery-slips/ - admin-dev/index.php?controller=AdminStatuses The problem is fixed in 1.7.6.5	<a href="#">CVE-2020-14479</a> 2020-04-18 Calculated CONFIRM
python-markdown2 -- python-markdown2	python-markdown2 through 2.3.8 allows XSS because element names are mishandled unless a \w+ match succeeds. For example, an attack might use elementname@ or elementname- with an onclick attribute.	<a href="#">CVE-2020-14488</a> 2020-04-18 Calculated MISC
rapid7 -- metasploit_framework	Rapid7 Metasploit Framework versions before 5.0.85 suffers from an instance of CWE-78: OS Command Injection, wherein the lnotify plugin accepts untrusted user-supplied data via a remote computer's hostname or service name. An attacker can create a specially-crafted hostname or service name to be imported by Metasploit from a variety of sources and trigger a command injection on the operator's terminal. Note, only the Metasploit Framework and products that expose the plugin system is susceptible to this issue -- notably, this does not include Rapid7 Metasploit Pro. Also note, this vulnerability cannot be triggered through a normal scan operation -- the attacker would have to supply a file that is processed with the db_import command.	<a href="#">CVE-2020-144350</a> 2020-04-18 Calculated CONFIRM
re2c -- re2c	re2c 1.3 has a heap-based buffer overflow in Scanner::fill in parse/scanner.cc via a long lexeme.	<a href="#">CVE-2020-14458</a> 2020-04-18 Calculated MISC
red_hat -- openshift_container_platform	A flaw was found in openshift-ansible. OpenShift Container Platform (OCP) 3.11 is too permissive in the way it specified CORS allowed origins during installation. An attacker, able to man-in-the-middle the connection between the user's browser and the openshift console, could use this flaw to perform a phishing attack. The main threat from this vulnerability is data confidentiality.	<a href="#">CVE-2020-14471</a> 2020-04-18 Calculated CONFIRM
red_hat -- openshift_container_platform	A flaw was found in OpenShift Container Platform version 4.1 and later. Sensitive information was found to be logged by the image registry operator allowing an attacker able to gain access to those logs, to read and write to the storage backing the internal image registry. The highest threat from this vulnerability is to data integrity.	<a href="#">CVE-2020-144712</a> 2020-04-18 Calculated CONFIRM

red_hat -- undertow	A flaw was found in all undertow-2.x.x SP1 versions prior to undertow-2.0.30.SP1, all undertow-1.x.x and undertow-2.x.x versions prior to undertow-2.1.0.Final, where the Servlet container causes servletPath to normalize incorrectly by truncating the path after semicolon which may lead to an application mapping resulting in the security bypass.	<a href="#">CVE-2020-1757</a> 2020-09-15 Calculated CONFIRM
sap -- erp_and_s/4_hana	Egypt localized withholding tax reports Clearing of Liabilities and Remittance Statement and Summary in SAP ERP (versions 618, 730, EAPPLGLO 607) and S/4 HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user, allowing reading or modification of some tax reports, due to Missing Authorization Check.	<a href="#">CVE-2020-6812</a> 2020-09-15 Calculated MISC
sap -- netweaver_as_abap	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_PHTMLB, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, is vulnerable to reflected Cross-Site Scripting (XSS) via different URL parameters as it does not sufficiently encode user controlled inputs.	<a href="#">CVE-2020-6813</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers.	<a href="#">CVE-2020-7487</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability exists on EcoStruxure Machine Expert – Basic or SoMachine Basic programming software (versions in security notification). The result of this vulnerability, DLL substitution, could allow the transference of malicious code to the controller.	<a href="#">CVE-2020-7489</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers.	<a href="#">CVE-2020-7488</a> 2020-09-15 Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-798: Use of Hardcoded Credentials vulnerability exists in Modicon Controllers (All versions of the following CPUs and Communication Module product references listed in the Security Notifications), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.	<a href="#">CVE-2020-6859</a> 2020-09-15 Calculated MISC
schneider_electric -- v_jeo_designer_and_v_jeo_designer_basic	A CWE-426: Untrusted Search Path vulnerability exists in Vjeo Designer Basic (V1.1 HotFix 15 and prior) and Vjeo Designer (V6.9 SP9 and prior), which could cause arbitrary code execution on the system running Vjeo Basic when a malicious DLL library is loaded by the Product.	<a href="#">CVE-2020-7490</a> 2020-09-15 Calculated MISC
simplesamlphp -- simplesamlphp	SimpleSAMLphp versions before 1.18.6 contain an information disclosure vulnerability. The module controller in 'SimpleSAMLModule' that processes requests for pages hosted by modules, has code to identify paths ending with '.php' and process those as PHP code. If no other suitable way of handling the given path exists it presents the file to the browser. The check to identify paths ending with '.php' does not account for uppercase letters. If someone requests a path ending with e.g. '.PHP' and the server is serving the code from a case-insensitive file system, such as on Windows, the processing of the PHP code does not occur, and the source code is instead presented to the browser. An attacker may use this issue to gain access to the source code in third-party modules that is meant to be private, or even sensitive. However, the attack surface is considered small, as the attack will only work when SimpleSAMLphp serves such content from a file system that is not case-sensitive, such as on Windows. This issue is fixed in version 1.18.6.	<a href="#">CVE-2020-6801</a> 2020-09-15 Calculated CONFIRM
sonatype -- nexus_repository_manager	An issue was discovered in Sonatype Nexus Repository Manager in versions 3.21.1 and 3.22.0. It is possible for a user with appropriate privileges to create, modify, and execute scripting tasks without use of the UI or API. NOTE: in 3.22.0, scripting is disabled by default (making this not exploitable).	<a href="#">CVE-2020-1753</a> 2020-09-15 Calculated CONFIRM
squid -- squid	An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials).	<a href="#">CVE-2020-11945</a> 2020-09-15 Calculated CONFIRM
	In Saml2 Authentication Services for ASP.NET versions before 1.0.2, and	<a href="#">MISC</a> 2020-09-15 Calculated CONFIRM



sustainsys -- saml2	between 2.0.0 and 2.6.0, there is a vulnerability in how tokens are validated in some cases. Saml2 tokens are usually used as bearer tokens - a caller that presents a token is assumed to be the subject of the token. There is also support in the Saml2 protocol for issuing tokens that is tied to a subject through other means, e.g. holder-of-key where possession of a private key must be proved. The Sustainsys.Saml2 library incorrectly treats all incoming tokens as bearer tokens, even though they have another subject confirmation method specified. This could be used by an attacker that could get access to Saml2 tokens with another subject confirmation method than bearer. The attacker could then use such a token to create a log in session. This vulnerability is patched in versions 1.0.2 and 2.7.0.	<a href="#">CVE-2020-30018</a> <a href="#">MISC</a> Notated
sysaid -- sysaid_on-premise	SysAid On-Premise 20.1.11, by default, allows the AJP protocol port, which is vulnerable to a GhostCat attack. Additionally, it allows unauthenticated access to upload files, which can be used to execute commands on the system by chaining it with a GhostCat attack.	<a href="#">CVE-2020-30019</a> <a href="#">MISC</a> Notated
tata_sonata -- smart_sf_rush_devices	An issue was discovered on Tata Sonata Smart SF Rush 1.12 devices. It has been identified that the smart band has no pairing (mode 0 Bluetooth LE security level) The data being transmitted over the air is not encrypted. Adding to this, the data being sent to the smart band doesn't have any authentication or signature verification. Thus, any attacker can control a parameter of the device.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
teeworlds -- teeworlds	Teeworlds before 0.7.4 has an integer overflow when computing a tilemap size.	<a href="#">CVE-2020-30019</a> <a href="#">MISC</a> Notated
teeworlds -- teeworlds	CServer::SendMsg in engine/server/server.cpp in Teeworlds 0.7.x before 0.7.5 allows remote attackers to shut down the server.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
tortoise-orm -- tortoise-orm	In Tortoise ORM before versions 0.15.23 and 0.16.6, various forms of SQL injection have been found for MySQL and when filtering or doing mass-updates on char/text fields. SQLite & PostgreSQL are only affected when filtering with contains, starts_with, or ends_with filters (and their case-insensitive counterparts).	<a href="#">CVE-2020-30019</a> <a href="#">MISC</a> Notated
toshiba -- multiple_devices	SHARP AQUOS series (AQUOS SH-M02 build number 01.00.05 and earlier, AQUOS SH-RM02 build number 01.00.04 and earlier, AQUOS mini SH-M03 build number 01.00.04 and earlier, AQUOS Keitai SH-N01 build number 01.00.01 and earlier, AQUOS L2 (UQ mobile/J.COM) build number 01.00.05 and earlier, AQUOS sense lite SH-M05 build number 03.00.04 and earlier, AQUOS sense (UQ mobile) build number 03.00.03 and earlier, AQUOS compact SH-M06 build number 02.00.02 and earlier, AQUOS sense plus SH-M07 build number 02.00.02 and earlier, AQUOS sense2 SH-M08 build number 02.00.05 and earlier, and AQUOS sense2 (UQ mobile) build number 02.00.06 and earlier) allow an attacker to obtain the sensitive information of the device via malicious applications installed on the device.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
toshiba -- multiple_devices	An unquoted search path vulnerability exists in HDD Password tool (for Windows) version 1.20.6620 and earlier which is stored in CANVIO PREMIUM 3TB(HD-MB30TY, HD-MA30TY, HD-MB30TS, HD-MA30TS), CANVIO PREMIUM 2TB(HD-MB20TY, HD-MA20TY, HD-MB20TS, HD-MA20TS), CANVIO PREMIUM 1TB(HD-MB10TY, HD-MA10TY, HD-MB10TS, HD-MA10TS), CANVIO SLIM 1TB(HD-SB10TK, HD-SB10TS), and CANVIO SLIM 500GB(HD-SB50GK, HD-SA50GK, HD-SB50GS, HD-SA50GS), and which was downloaded before 2020 May 10. Since it registers Windows services with unquoted file paths, when a registered path contains spaces, and a malicious executable is placed on a certain path, it may be executed with the privilege of the Windows service.	<a href="#">CVE-2020-30020</a> <a href="#">MISC</a> Notated
tss-lib -- tss-lib	The keygen protocol implementation in Binance tss-lib before 1.2.0 allows attackers to generate crafted h1 and h2 parameters in order to compromise a signing round or obtain sensitive information from other parties.	<a href="#">CVE-2020-30018</a> <a href="#">MISC</a> Notated
veeam -- one_agent	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HandshakeResult method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code	<a href="#">CVE-2020-30015</a> <a href="#">MISC</a> Notated

	in the context of the service account. Was ZDI-CAN-10401.	
veeam -- one_agent	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the PerformHandshake method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-10400.	<a href="#">CVE-2020-0914</a> Yes Calculated MISC
vesta -- vesta_control_panel	A remote command execution in Vesta Control Panel through 0.9.8-26 allows any authenticated user to execute arbitrary commands on the system via cron jobs.	<a href="#">CVE-2020-0786</a> Yes Calculated MISC
vesta -- vesta_control_panel	An elevation of privilege in Vesta Control Panel through 0.9.8-26 allows an attacker to gain root system access from the admin account via v-change-user-password (aka the user password change script).	<a href="#">CVE-2020-0787</a> Yes Calculated MISC
wordpress -- wordpress	The responsive-add-ons plugin before 2.2.7 for WordPress has incorrect access control for wp-admin/admin-ajax.php?action= requests.	<a href="#">CVE-2020-12073</a> Yes Calculated MISC
wordpress -- wordpress	The mappress-google-maps-for-wordpress plugin before 2.53.9 for WordPress does not correctly implement AJAX functions with nonces (or capability checks), leading to remote code execution.	<a href="#">CVE-2020-09077</a> Yes Calculated MISC
wordpress -- wordpress	The Catch Breadcrumb plugin before 1.5.4 for WordPress allows Reflected XSS via the s parameter (a search query). Also affected are 16 themes (if the plugin is enabled) by the same author: Alchemist and Alchemist PRO, Izabel and Izabel PRO, Chique and Chique PRO, Clean Enterprise and Clean Enterprise PRO, Bold Photography PRO, Intuitive PRO, Devotepress PRO, Clean Blocks PRO, Foodoholic PRO, Catch Mag PRO, Catch Wedding PRO, and Higher Education PRO.	<a href="#">CVE-2020-09054</a> Yes Calculated MISC
wordpress -- wordpress	The Advanced Woo Search plugin version through 1.99 for Wordpress suffers from a sensitive information disclosure vulnerability in every ajax search request via the sql field to includes/class-aws-search.php.	<a href="#">CVE-2020-12070</a> Yes Calculated MISC
wordpress -- wordpress	The users-customers-import-export-for-wp-woocommerce plugin before 1.3.9 for WordPress allows subscribers to import administrative accounts via CSV.	<a href="#">CVE-2020-12074</a> Yes Calculated MISC
wordpress -- wordpress	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks capability checks for AJAX actions.	<a href="#">CVE-2020-12075</a> Yes Calculated MISC
wordpress -- wordpress	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks CSRF nonce checks for AJAX actions. One consequence of this is stored XSS.	<a href="#">CVE-2020-12076</a> Yes Calculated MISC
wordpress -- worpdress	An issue was discovered in Elementor 2.7.4. Arbitrary file upload is possible in the Elementor Import Templates function, allowing an attacker to execute code via a crafted ZIP archive.	<a href="#">CVE-2020-09055</a> Yes Calculated MISC
zoho -- manageengine_opmanager	Zoho ManageEngine OpManager before 125120 allows an unauthenticated user to retrieve an API key via a servlet call.	<a href="#">CVE-2020-11946</a> Yes Calculated MISC
zulip -- zulip_server	Zulip Server before 2.1.3 allows XSS via the modal_link feature in the Markdown functionality.	<a href="#">CVE-2020-09445</a> Yes Calculated CONFIRM
zulip -- zulip_server	Zulip Server before 2.1.3 allows reverse tabnabbing via the Markdown functionality.	<a href="#">CVE-2020-09444</a> Yes Calculated CONFIRM
		<a href="#">CVE-</a>

zulip -- zulip_server	Zulip Server before 2.1.3 allows XSS via a Markdown link, with resultant account takeover.	2020-04-0935 CONFIRM MISC
-----------------------	--	---------------------------------

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:** [US-CERT](#)  
**To:** [wquitate@ci.sunnyvale.ca.us](mailto:wquitate@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of April 20, 2020  
**Date:** Monday, April 27, 2020 10:13:23 AM



National Cyber Awareness System:

## [Vulnerability Summary for the Week of April 20, 2020](#)

04/27/2020 06:27 AM EDT

Original release date: April 27, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ios_and_macos_and_mojave_and_tvos	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS 10.14.4, tvOS 12.2. An attacker in a privileged network position may be able to intercept network traffic.	2020-04-17	7.5	<a href="#">CVE-2019-6203</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A type confusion vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code read/write on the system running it.	2020-04-17	9.3	<a href="#">CVE-2020-7081</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A use-after-free vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to code execution on a system running it.	2020-04-17	9.3	<a href="#">CVE-2020-7082</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A heap overflow vulnerability in the Autodesk FBX-SDK versions 2019.2 and earlier may lead to arbitrary code execution on a system running it.	2020-04-17	9.3	<a href="#">CVE-2020-7085</a> <a href="#">MISC</a>
autodesk -- fbx_software_development	A buffer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code execution on a system running it.	2020-04-17	9.3	<a href="#">CVE-2020-7080</a> <a href="#">MISC</a>
evenroute -- iqrouter	IQrouter through 3.3.1, when unconfigured, has multiple remote code execution vulnerabilities in the web-panel because of Bash Shell Metacharacter Injection.	2020-04-21	7.5	<a href="#">CVE-2020-11963</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, there is a root user without a password, which allows attackers to gain full remote access via SSH.	2020-04-21	7.5	<a href="#">CVE-2020-11965</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, the Lua function reset_password in the web-panel allows remote attackers to change the root password arbitrarily.	2020-04-21	7.5	<a href="#">CVE-2020-11966</a> <a href="#">MISC</a> <a href="#">MISC</a>
evenroute -- iqrouter	In IQrouter through 3.3.1, remote attackers can control the device (restart network, reboot, upgrade, reset) because of Incorrect Access Control.	2020-04-21	9	<a href="#">CVE-2020-11967</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- android	In onOpActiveChanged and related methods of AppOpsControllerImpl.java, there is a possible way to display an app overlaying other apps without the notification icon that it's overlaying. This could lead to local escalation of privilege with User execution privileges needed. User interaction	2020-04-17	9.3	<a href="#">CVE-2020-0080</a> <a href="#">MISC</a>



	is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144092031			
google -- android	In finalize of AssetManager.java, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144028297	2020-04-17	7.2	<a href="#">CVE-2020-0081</a> <a href="#">MISC</a>
google -- android	In ExternalVibration of ExternalVibration.java, there is a possible activation of an arbitrary intent due to unsafe deserialization. This could lead to local escalation of privilege to system_server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140417434	2020-04-17	7.2	<a href="#">CVE-2020-0082</a> <a href="#">MISC</a>
google -- android	In rw_t2t_extract_default_locks_info of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310721	2020-04-17	10	<a href="#">CVE-2020-0071</a> <a href="#">MISC</a>
google -- android	In rw_t2t_update_lock_attributes of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-148159613	2020-04-17	10	<a href="#">CVE-2020-0070</a> <a href="#">MISC</a>
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310271	2020-04-17	10	<a href="#">CVE-2020-0072</a> <a href="#">MISC</a>
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147309942	2020-04-17	10	<a href="#">CVE-2020-0073</a> <a href="#">MISC</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService mishandles OTA Provisioning on V40 and G7 devices. The LG ID is LVE-SMP-190006 (July 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20777</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. A stack-based buffer overflow in the logging tool could allow an attacker to gain privileges. The LG ID is LVE-SMP-200005 (April 2020).	2020-04-17	7.5	<a href="#">CVE-2020-11873</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. Unprivileged applications can execute shell commands via the connectivity service. The LG ID is LVE-SMP-190008 (August 2019).	2020-04-17	7.2	<a href="#">CVE-2019-20773</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. Certain security settings, related to whether packages are verified and accepted only from known sources, are mishandled. The LG ID	2020-04-17	7.5	<a href="#">CVE-2019-20780</a> <a href="#">CONFIRM</a>

	is LVE-SMP-190002 (April 2019).			
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. LG Advanced Flash (LAF) has a buffer overflow. The LG ID is LVE-SMP-190001 (March 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20782</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Backup subsystem does not properly restrict operations or validate their input. The LG ID is LVE-SMP-190004 (June 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20778</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. The Account subsystem allows authorization bypass. The LG ID is LVE-SMP-190007 (August 2019).	2020-04-17	7.5	<a href="#">CVE-2019-20772</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10.0 (MTK chipsets) software. The MTK kernel does not properly implement exception handling, allowing an attacker to gain privileges. The LG ID is LVE-SMP-200001 (February 2020).	2020-04-17	7.2	<a href="#">CVE-2020-11875</a> <a href="#">CONFIRM</a>
mitel_networks -- mivoice_connect	A remote code execution vulnerability in UCB component of Mitel MiVoice Connect before 19.1 SP1 could allow an unauthenticated remote attacker to execute arbitrary scripts due to insufficient validation of URL parameters. A successful exploit could allow an attacker to gain access to sensitive information.	2020-04-17	7.5	<a href="#">CVE-2020-10211</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by a hardcoded password. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-23	7.5	<a href="#">CVE-2018-21137</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020-04-23	7.5	<a href="#">CVE-2018-21132</a> <a href="#">CONFIRM</a>
pion -- dtls	handleIncomingPacket in conn.go in Pion DTLS before 1.5.2 lacks a check for application data with epoch 0, which allows remote attackers to inject arbitrary unencrypted data after handshake completion.	2020-04-19	7.5	<a href="#">CVE-2019-20786</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
webkitgtk -- webkitgtk_and_wpe_webkit	A use-after-free issue exists in WebKitGTK before 2.28.1 and WPE WebKit before 2.28.1 via crafted web content that allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash).	2020-04-17	7.5	<a href="#">CVE-2020-11793</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	In the media-library-assistant plugin before 2.82 for WordPress, Remote Code Execution can occur via the tax_query, meta_query, or date_query parameter in mla_gallery via an admin.	2020-04-20	7.5	<a href="#">CVE-2020-11928</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- dynamo_bim	An improper signature validation vulnerability in Autodesk Dynamo BIM versions 2.5.1 and 2.5.0 may lead to code execution through maliciously crafted DLL files.	2020-04-17	4.4	<a href="#">CVE-2020-7079</a> <a href="#">MISC</a>
autodesk -- fbx_software_development_kit	A NULL pointer dereference vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	2020-04-17	4.3	<a href="#">CVE-2020-7084</a> <a href="#">MISC</a>

autodesk -- fbx_software_development	An integer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application.	2020-04-17	4.3	<a href="#">CVE-2020-7083</a> MISC
bitrock -- installbuilder_autoupdate_tool	InstallBuilder AutoUpdate tool and regular installers enabling <checkForUpdates> built with versions earlier than 19.11 are vulnerable to Billion laughs attack (denial-of-service).	2020-04-20	5	<a href="#">CVE-2020-3946</a> CONFIRM
byobu_apport -- byobu_apport	Byobu Apport hook may disclose sensitive information since it automatically uploads the local user's .screenrc which may contain private hostnames, usernames and passwords. This issue affects: byobu	2020-04-17	5	<a href="#">CVE-2019-7306</a> MISC MISC
evenroute -- iqrouter	In IQrouter through 3.3.1, the Lua function diag_set_password in the web-panel allows remote attackers to change the root password arbitrarily.	2020-04-21	5	<a href="#">CVE-2020-11964</a> MISC MISC
evenroute -- iqrouter	In the web-panel in IQrouter through 3.3.1, remote attackers can read system logs because of Incorrect Access Control.	2020-04-21	5	<a href="#">CVE-2020-11968</a> MISC MISC
ftpdmin -- ftpdmin	A buffer overflow vulnerability in FTPDMIN 0.96 allows attackers to crash the server via a crafted packet.	2020-04-17	5	<a href="#">CVE-2020-10813</a> MISC MISC
google -- android	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-144506242	2020-04-17	4.6	<a href="#">CVE-2020-0079</a> MISC
google -- android	In releaseSecureStops of DrmPlugin.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-144766455	2020-04-17	4.6	<a href="#">CVE-2020-0078</a> MISC
google -- android	In get_auth_result of the FPC IRIS TrustZone app, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146056878	2020-04-17	4.6	<a href="#">CVE-2020-0076</a> MISC
google -- android	There is a possible disclosure of RAM using a shared crypto key due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140879284	2020-04-17	4.9	<a href="#">CVE-2019-2056</a> MISC
huawei -- taurus_al00b_smartphones	Huawei smartphones Taurus-AL00B with versions earlier than 10.0.0.205(C00E201R7P2) have an improper authentication vulnerability. The software insufficiently validate the user's identity when a user wants to do certain operation. An attacker can trick user into installing a malicious application to exploit this vulnerability. Successful exploit may cause some information disclosure.	2020-04-20	4.3	<a href="#">CVE-2020-9070</a> CONFIRM CONFIRM
bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 170880.	2020-04-17	4.3	<a href="#">CVE-2019-4644</a> XF CONFIRM
bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 could allow an authenticated user perform actions they are not authorized to by modifying request parameters.	2020-04-17	5.5	<a href="#">CVE-2019-4446</a> XF

	IBM X-Force ID: 163490.			<a href="#">CONFIRM</a>
bm -- tririga_application_platform	IBM TRIRIGA Application Platform 3.5.3 and 3.6.1 discloses sensitive information in error messages that could aid an attacker formulate future attacks. IBM X-Force ID: 175993.	2020-04-17	5	<a href="#">CVE-2020-4277</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
lg -- g3_devices	An issue was discovered in LG PC Suite for LG G3 and earlier (aka LG PC Suite v5.3.27 and earlier). DLL Hijacking can occur via a Trojan horse DLL in the current working directory. The LG ID is LVE-MOT-190001 (November 2019).	2020-04-17	4.4	<a href="#">CVE-2019-20769</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9.0 software. The HAL service has a buffer overflow that leads to arbitrary code execution. The LG ID is LVE-SMP-190013 (September 2019).	2020-04-17	4.6	<a href="#">CVE-2019-20770</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0 and 8.1 software for the DTAG carrier. RILD in the radio layer uses an uninitialized variable. The LG ID is LVE-SMP-180013 (January 2019).	2020-04-17	4.6	<a href="#">CVE-2019-20785</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. WapService allows unconfirmed configuration changes via a modified OMACP message. The LG ID is LVE-SMP-190006 (August 2019).	2020-04-17	5	<a href="#">CVE-2019-20771</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (North America CDMA) software. The LTE protocol implementation allows a bypass of AKA (Authentication and Key Agreement). The LG ID is LVE-SMP-180014 (February 2019).	2020-04-17	6.4	<a href="#">CVE-2019-20783</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9, and 10 software. Attackers can bypass Factory Reset Protection (FRP). The LG ID is LVE-SMP-200004 (March 2020).	2020-04-17	5	<a href="#">CVE-2020-11874</a> <a href="#">CONFIRM</a>
libming -- libming	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (2 bytes) in the function decompileIF() in decompile.c.	2020-04-19	6.4	<a href="#">CVE-2020-11895</a> <a href="#">MISC</a>
libming -- libming	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (8 bytes) in the function decompileIF() in decompile.c.	2020-04-19	6.4	<a href="#">CVE-2020-11894</a> <a href="#">MISC</a>
netgear -- d6100_devices	NETGEAR D6100 devices before 1.0.0.50_0.0.50 are affected by command injection.	2020-04-21	4.6	<a href="#">CVE-2017-18792</a> <a href="#">CONFIRM</a>
netgear -- d6220_and_d6100_devices	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.28 and D6100 before 1.0.0.50_0.0.50.	2020-04-21	4.6	<a href="#">CVE-2017-18795</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWN2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-23	5.8	<a href="#">CVE-2017-18734</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and WNDAP360 before 3.7.4.0.	2020-04-21	4.6	<a href="#">CVE-2017-18805</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a			<a href="#">CVE-2017-</a>



netgear -- multiple_devices	buffer overflow by an authenticated user. This affects R7800 before 1.0.2.36, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	2020-04-22	<a href="#">5.2</a>	<a href="#">18770 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.01.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18850 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-21	<a href="#">5.2</a>	<a href="#">CVE-2018-21147 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	<a href="#">4.6</a>	<a href="#">CVE-2017-18779 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JR6150 before 1.0.1.12, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	<a href="#">6.8</a>	<a href="#">CVE-2017-18782 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6220 before V1.0.0.50, R7800 before V1.0.2.36, WNDR3400v3 before 1.0.1.14, and WNDR3700v5 before V1.1.0.48.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18739 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	<a href="#">4.3</a>	<a href="#">CVE-2017-18783 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, JR6150 before 1.0.1.12, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	<a href="#">6.8</a>	<a href="#">CVE-2017-18781 CONFIRM</a>

	before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6300v2 before 1.0.4.8_10.0.77, R6400 before 1.0.1.24, R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, R8500 before 1.0.2.100, and D6100 before 1.0.0.50_0.0.50.	2020-04-21	4.6	<a href="#">CVE-2017-18794</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D8500 through 1.0.3.28, R6400 through 1.0.1.22, R6400v2 through 1.0.2.18, R8300 through 1.0.2.94, R8500 through 1.0.2.94, and R6100 through 1.0.1.12.	2020-04-20	4.6	<a href="#">CVE-2017-18851</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6400 before 1.0.1.24, R6700 before 1.0.1.26, R6900 before 1.0.1.28, R7000 before 1.0.9.10, R7000P before 1.0.1.16, R6900P before 1.0.1.16, and R7800 before 1.0.2.36.	2020-04-21	4.6	<a href="#">CVE-2017-18796</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.3	<a href="#">CVE-2017-18835</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D6100 before V1.0.0.55, D7800 before V1.0.1.24, EX6150v2 before 1.0.0.48, R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before V1.0.3.16, R7800 before V1.0.2.36, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.48.	2020-04-22	4.6	<a href="#">CVE-2017-18773</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.3	<a href="#">CVE-2017-18834</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6100 before V1.0.0.55, D7000 before V1.0.1.50, D7800 before V1.0.1.24, JNR1010v2 before 1.1.0.40, JWNDR2010v5 before 1.1.0.40, R6100 before 1.0.1.12, R6220 before 1.1.0.50, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.40, WNR2000v5 before 1.0.0.42, WNR2020 before 1.1.0.40, and WNR2050 before 1.1.0.40.	2020-04-22	4.6	<a href="#">CVE-2017-18776</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.3	<a href="#">CVE-2017-18833</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before 1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96, DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6150v2 before 1.0.1.54, EX6100v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.18, R6900P before 1.3.0.8, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R8000 before 1.0.4.4_1.1.42, R7900P before 1.1.5.14, R8000P before 1.1.5.14, R8300 before 1.0.2.110, R8500 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.14, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	2020-04-22	<a href="#">4.6</a>	<a href="#">CVE-2017-18788</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by XSS. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	<a href="#">4.3</a>	<a href="#">CVE-2017-18784</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.50, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.48, and D7000 before 1.0.1.50.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18801</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18838</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6100 before 1.0.1.14, R7500 before 1.0.0.110, R7500v2 before 1.0.3.16, R7800 before 1.0.2.32, EX6200v2 before 1.0.1.50, and D7800 before 1.0.1.22.	2020-04-21	<a href="#">4.6</a>	<a href="#">CVE-2017-18802</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15,	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18830</a> <a href="#">CONFIRM</a>

	M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects R6220 before 1.1.0.46, R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, WNDR3700v5 before 1.1.0.46, and D7000 before 1.0.1.50.	2020-04-20	4.6	<a href="#">CVE-2017-18841</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects R6400 before 1.0.1.14, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	2020-04-23	4.3	<a href="#">CVE-2017-18745</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.6	<a href="#">CVE-2017-18837</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.0.36, AC1450 before 1.0.0.36, R7300 before 1.0.0.54, and R8500 before 1.0.2.94.	2020-04-20	6.8	<a href="#">CVE-2017-18848</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.6	<a href="#">CVE-2017-18829</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R7300 before 1.0.0.54, R8500 before 1.0.2.94, DGN2200v1 before 1.0.0.55, and D2200D/D2200DW-1FRNAS before 1.0.0.32.	2020-04-20	6.8	<a href="#">CVE-2017-18842</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.6	<a href="#">CVE-2017-18826</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by vertical privilege escalation. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	4.6	<a href="#">CVE-2017-18822</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects WAC510 before 1.3.0.10, WAC120 before 2.1.4, WNDAP620 before 2.1.3, WND930 before 2.1.2, WN604 before 3.3.7, WNDAP660 before 3.7.4.0, WNDAP350 before 3.7.4.0, WNAP320 before 3.7.4.0, WNAP210v2 before 3.7.4.0, and WNDAP360 before 3.7.4.0.	2020-04-21	4.6	<a href="#">CVE-2017-18806</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow. This affects R6250 before 1.0.4.12, R6400v2 before 1.0.2.32,			<a href="#">CVE-2017-</a>



netgear -- multiple_devices	R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	2020-04-20	<a href="#">4.6</a>	<a href="#">18846 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF and authentication bypass. This affects R7300DST before 1.0.0.54, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and WNDR3400v3 before 1.0.1.14.	2020-04-20	<a href="#">6.8</a>	<a href="#">CVE-2017-18852 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6220 before 1.0.0.26, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.30, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R6900P before 1.0.0.56, R7000 before 1.0.9.4, R7000P before 1.0.0.56, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.44, R8300 before 1.0.2.100_1.0.82, and R8500 before 1.0.2.100_1.0.82.	2020-04-20	<a href="#">4.6</a>	<a href="#">CVE-2017-18849 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6100 before 1.0.1.12, R7500 before 1.0.0.108, WNDR3700v4 before 1.0.2.86, WNDR4300v1 before 1.0.2.88, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.42.	2020-04-22	<a href="#">6.8</a>	<a href="#">CVE-2017-18775 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R7100LG before 1.0.0.32, R7300DST before 1.0.0.52, R8300 before 1.0.2.94, and R8500 before 1.0.2.100.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18733 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.74.	2020-04-23	<a href="#">5.8</a>	<a href="#">CVE-2017-18744 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6100 before 1.0.1.14, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, R7500 before 1.0.0.110, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2017-18764 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, and WNR2000v5 before 1.0.0.58.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2017-18754 CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WC7500 before 6.5.3.9, WC7520 before 6.5.3.9, WC7600v1 before 6.5.3.9, and WC7600v2 before 6.5.3.9.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21123 CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	2020-04-22	5.8	<a href="#">CVE-2018-21121</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects WAC120 before 2.1.7, WAC505 before 5.0.5.4, WAC510 before 5.0.5.4, WNAP320 before 3.7.11.4, WNAP210v2 before 3.7.11.4, WNDAP350 before 3.7.11.4, WNDAP360 before 3.7.11.4, WNDAP660 before 3.7.11.4, WNDAP620 before 2.1.7, WND930 before 2.1.5, and WN604 before 3.3.10.	2020-04-22	6	<a href="#">CVE-2018-21120</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6100 before 1.0.0.58, D7800 before 1.0.1.42, R6100 before 1.0.1.28, R7500 before 1.0.0.130, R7500v2 before 1.0.3.36, R7800 before 1.0.2.52, R8900 before 1.0.4.12, R9000 before 1.0.4.12, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, and WNDR4500v3 before 1.0.0.56.	2020-04-22	5.8	<a href="#">CVE-2018-21113</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, R8500 before 1.0.2.74, and WNR2000v2 before 1.2.0.8.	2020-04-22	5.8	<a href="#">CVE-2017-18772</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D3600 before 1.0.0.68, D6000 before 1.0.0.68, D6100 before 1.0.0.57, R6100 before 1.0.1.16, R6900P before 1.2.0.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, WNDR3700v4 before 1.0.2.88, WNDR4300v1 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	2020-04-22	5.8	<a href="#">CVE-2017-18762</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-23	5.8	<a href="#">CVE-2017-18750</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, D8500 before 1.0.3.39, R6400 before 1.0.1.14, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.4, R7100LG before 1.0.0.32, R7300 before 1.0.0.56, R7800 before 1.0.2.36, R7900 before 1.0.2.10, R8000 before 1.0.3.24, R8300 before 1.0.2.74, and R8500 before 1.0.2.74.	2020-04-22	5.2	<a href="#">CVE-2017-18767</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects EX6150v2 before 1.0.1.54, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000 before 1.0.9.10, R7000P before 1.2.0.22, R6900P before 1.2.0.22, R7100LG before 1.0.0.32, R7300DST before 1.0.0.54, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R6100 before 1.0.1.16, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	2020-04-23	5.8	<a href="#">CVE-2017-18738</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a			

netgear -- multiple_devices	stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-22	5.2	<a href="#">CVE-2018-21150</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, R7500v2 before 1.0.3.38, R7800 before 1.0.2.52, R8900 before 1.0.4.12, and R9000 before 1.0.4.12.	2020-04-22	5.2	<a href="#">CVE-2018-21112</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.44, EX6150v2 before 1.0.1.70, EX6100v2 before 1.0.1.70, EX6200v2 before 1.0.1.64, EX7300 before 1.0.2.136, EX6400 before 1.0.2.136, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.4.12, WN3000RPv2 before 1.0.0.56, WN3000RPv3 before 1.0.2.52, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	2020-04-22	5.2	<a href="#">CVE-2018-21114</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-23	5.8	<a href="#">CVE-2017-18737</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-21	5.2	<a href="#">CVE-2018-21148</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before 1.0.0.54.	2020-04-21	5.2	<a href="#">CVE-2018-21146</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6200v2 before 1.0.3.14, R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.1.1.20, R7000 before 1.0.7.10, R7000P/R6900P before 1.0.0.56, R7100LG before 1.0.0.30, R7900 before 1.0.1.14, R8000 before 1.0.3.22, R8500 before 1.0.2.74, and D8500 before 1.0.3.28.	2020-04-21	5	<a href="#">CVE-2017-18799</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, PLW1000v2 before 1.0.0.14, and PLW1010v2 before 1.0.0.14.	2020-04-23	5.8	<a href="#">CVE-2017-18732</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6300v2 before 1.0.4.8, R6400v2 before 1.0.2.32, R6700 before 1.0.1.22, R6900 before 1.0.1.22, R7000P before 1.0.0.86, R6900P before 1.0.0.56, R7300 before 1.0.0.54, R8300 before 1.0.2.106, R8500 before 1.0.2.106, DGN2200v4 before 1.0.0.86, DGND2200Bv4	2020-04-22	6.8	<a href="#">CVE-2017-18755</a> <a href="#">CONFIRM</a>

	before 1.0.0.86, R6050 before 1.0.0.86, JR6150 before 1.0.1.10, R6220 before 1.1.0.50, and WNDR3700v5 before V1.1.0.48.			
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	2020-04-22	5.2	<a href="#">CVE-2017-18758</a> CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, and R6900v2 before 1.2.0.4.	2020-04-23	5.8	<a href="#">CVE-2017-18735</a> CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, and WNDR3700v5 before 1.1.0.48.	2020-04-23	5.8	<a href="#">CVE-2017-18736</a> CONFIRM
netgear -- r6700_and_r6800_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700v2 before 1.1.0.42 and R6800 before 1.1.0.42.	2020-04-21	4.3	<a href="#">CVE-2017-18800</a> CONFIRM
netgear -- r7800_and_r9000_devices	Certain NETGEAR devices are affected by command injection. This affects R7800 before 1.0.2.16 and R9000 before 1.0.2.4.	2020-04-21	4.6	<a href="#">CVE-2017-18804</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21101</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.36 are affected by command injection.	2020-04-21	4.6	<a href="#">CVE-2017-18793</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21110</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21108</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21109</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21107</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21103</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21106</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21105</a> CONFIRM
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.60 are affected by command injection by an authenticated user.	2020-04-23	5.2	<a href="#">CVE-2018-21104</a> CONFIRM
netgear -- r8000_devices	NETGEAR R8000 devices before 1.0.4.2 are affected by a stack-based buffer overflow by an authenticated user.	2020-04-22	5.2	<a href="#">CVE-2017-18761</a> CONFIRM
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R8300 before 1.0.2.104 and R8500 before 1.0.2.104.	2020-04-22	5.2	<a href="#">CVE-2017-18759</a> CONFIRM
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	2020-04-21	4.6	<a href="#">CVE-2017-18808</a> CONFIRM



netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects WAC505 before 5.0.5.4 and WAC510 before 5.0.5.4.	2020-04-22	<a href="#">5.2</a>	<a href="#">CVE-2018-21119</a> <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by unauthenticated firmware downgrade. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	2020-04-23	<a href="#">6.4</a>	<a href="#">CVE-2018-21131</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by authentication bypass.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21118</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers via the traceroute handler.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21117</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21116</a> <a href="#">CONFIRM</a>
netgear -- xr500_devices	NETGEAR XR500 devices before 2.3.2.32 are affected by remote code execution by unauthenticated attackers.	2020-04-22	<a href="#">5.8</a>	<a href="#">CVE-2018-21115</a> <a href="#">CONFIRM</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the sessionLocation parameter for the login page is vulnerable to cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5730</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the UI Framework Error Page reflects arbitrary, user-supplied input back to the browser, which can result in XSS. Any page that is able to trigger a UI Framework Error is susceptible to this issue.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5729</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the export functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows the export of potentially sensitive information.	2020-04-17	<a href="#">5.8</a>	<a href="#">CVE-2020-5733</a> <a href="#">MISC</a>
openmrs -- openmrs	OpenMRS 2.9 and prior copies "Referrer" header values into an html element named "redirectUrl" within many webpages (such as login.htm). There is insufficient validation for this parameter, which allows for the possibility of cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5728</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the app parameter for the ActiveVisit's page is vulnerable to cross-site scripting.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-5731</a> <a href="#">MISC</a>
openmrs -- openmrs	In OpenMRS 2.9 and prior, the import functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows unauthenticated users to use a feature typically restricted to administrators.	2020-04-17	<a href="#">5.8</a>	<a href="#">CVE-2020-5732</a> <a href="#">MISC</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is an open redirection when using back parameter. The impacts can be many, and vary from the theft of information and credentials to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">5.8</a>	<a href="#">CVE-2020-5270</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.6.0.0 and 1.7.6.5, there is a reflected XSS with 'date_from' and 'date_to' parameters in the dashboard page. This problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5271</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.4.0 and 1.7.6.5, there is a reflected XSS when uploading a wrong file. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5286</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.1.0 and 1.7.6.5, there is a reflected XSS on AdminCarts	2020-04-	<a href="#">4.3</a>	<a href="#">CVE-2020-5276</a>

	page with `cartBox` parameter The problem is fixed in 1.7.6.5	20		<a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is a reflected XSS with `back` parameter. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5285</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.5.4.0 and 1.7.6.5, there is a reflected XSS on Exception page The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5278</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is a reflected XSS on Search page with `alias` and `search` parameters. The problem is patched in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5272</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminFeatures page by using the `id_feature` parameter. The problem is fixed in 1.7.6.5	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5269</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminAttributesGroups page. The problem is patched in 1.7.6.5.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5265</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
prestashop -- prestashop	In PrestaShop before version 1.7.6.5, there is a reflected XSS while running the security compromised page. It allows anyone to execute arbitrary action. The problem is patched in the 1.7.6.5.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-5264</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
svg2png -- svg2png	svg2png 4.1.1 allows XSS with resultant SSRF via JavaScript inside an SVG document.	2020-04-17	<a href="#">4.3</a>	<a href="#">CVE-2020-11887</a> <a href="#">MISC</a>
wordpress -- wordpress	The GTranslate plugin before 2.8.52 for WordPress has Reflected XSS via a crafted link. This requires use of the hreflang tags feature within a sub-domain or sub-directory paid option.	2020-04-20	<a href="#">4.3</a>	<a href="#">CVE-2020-11930</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In f2fs_xattr_generic_list of xattr.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation.Product: Android. Versions: Android kernel. Android ID: A-120551147.	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0067</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	In crus_afe_get_param of msm-cirrus-playback.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: Android. Versions: Android kernel. Android ID: A-139354541	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0068</a> <a href="#">CONFIRM</a>
google -- android	In authorize_enroll of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146055840	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0077</a> <a href="#">MISC</a>
google -- android	In set_shared_key of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2020-0075</a>

	privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-146057864			<a href="#">MISC</a>
huawei -- honor_v20_smartphones	Huawei smartphones Honor V20 with versions earlier than 10.0.0.179(C636E3R4P3), versions earlier than 10.0.0.180(C185E3R3P3), versions earlier than 10.0.0.180(C432E10R3P4) have an information disclosure vulnerability. The device does not sufficiently validate the identity of smart wearable device in certain specific scenario, the attacker need to gain certain information in the victim's smartphone to launch the attack, successful exploit could cause information disclosure.	2020-04-20	<a href="#">2.9</a>	<a href="#">CVE-2020-1803</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
bm -- maximo_asset_management	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 173308.	2020-04-17	<a href="#">3.5</a>	<a href="#">CVE-2019-4749</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (MTK chipsets) software. Interaction of GPS with 911 emergency calls is mishandled. The LG ID is LVE-SMP-180012 (January 2019).	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2019-20784</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A TrustZone trusted application can crash via crafted input. The LG ID is LVE-SMP-190003 (May 2019).	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2019-20779</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 software. A TZ trusted application can crash via crafted input. The LG ID is LVE-SMP-190005 (July 2019).	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2019-20776</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 9.0 (Qualcomm SDM450, SDM845, SM6150, and SM8150 chipsets) software. Weak encryption leads to local information disclosure. The LG ID is LVE-SMP-190010 (August 2019).	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2019-20775</a> <a href="#">CONFIRM</a>
lg -- multiple_mobile_devices	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, 8.1, and 9.0 software. A system service allows local retrieval of the user's password. The LG ID is LVE-SMP-190009 (August 2019).	2020-04-17	<a href="#">2.1</a>	<a href="#">CVE-2019-20774</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-21	<a href="#">3.3</a>	<a href="#">CVE-2018-21140</a> <a href="#">CONFIRM</a>
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	2020-04-23	<a href="#">2.1</a>	<a href="#">CVE-2018-21136</a> <a href="#">CONFIRM</a>
netgear -- dst6501_and_wnr2000_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects DST6501 before 1.1.0.6 and WNR2000v2 before 1.2.0.8.	2020-04-22	<a href="#">3.3</a>	<a href="#">CVE-2017-18766</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by directory traversal. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">2.1</a>	<a href="#">CVE-2017-18824</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15,			

netgear -- multiple_devices	M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18828</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by administrative password disclosure. This affects D6220 before V1.0.0.28, D6400 before V1.0.0.60, D8500 before V1.0.3.29, DGN2200v4 before 1.0.0.82, DGN2200Bv4 before 1.0.0.82, R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	2020-04-22	2.1	<a href="#">CVE-2017-18777</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	2.1	<a href="#">CVE-2017-18840</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18831</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	2020-04-20	2.1	<a href="#">CVE-2017-18843</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400v2 before 1.0.2.32, R7000P/R6900P before 1.0.0.56, R7900 before 1.0.1.18, R8300 before 1.0.2.100_1.0.82, R8500 before 1.0.2.100_1.0.82, and D8500 before 1.0.3.29.	2020-04-20	2.1	<a href="#">CVE-2017-18847</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	3.5	<a href="#">CVE-2017-18827</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNDR2010v5 before 1.1.0.42, PR2000 before 1.0.0.18, R6050 before 1.0.1.10, R6120 before 1.0.0.30, R6220 before 1.1.0.50, R6700v2 before 1.2.0.4, R6800 before 1.2.0.4, R6900v2 before 1.2.0.4, WNDR3700v5 before 1.1.0.48, WNR1000v4 before 1.1.0.42, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	2020-04-22	3.3	<a href="#">CVE-2017-18763</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.			



netgear -- multiple_devices	before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18821</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">3.5</a>	<a href="#">CVE-2017-18832</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">2.1</a>	<a href="#">CVE-2017-18823</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	2020-04-23	<a href="#">3.3</a>	<a href="#">CVE-2017-18747</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">3.5</a>	<a href="#">CVE-2017-18825</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">2.1</a>	<a href="#">CVE-2017-18836</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, and D7000 before 1.0.1.50.	2020-04-20	<a href="#">2.1</a>	<a href="#">CVE-2017-18844</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects M4300-28G before 12.0.2.15, M4300-52G before 12.0.2.15, M4300-28G-POE+ before 12.0.2.15, M4300-52G-POE+ before 12.0.2.15, M4300-8X8F before 12.0.2.15, M4300-12X12F before 12.0.2.15, M4300-24X24F before 12.0.2.15, M4300-24X before 12.0.2.15, M4300-48X before 12.0.2.15, and M4200 before 12.0.2.15.	2020-04-20	<a href="#">3.5</a>	<a href="#">CVE-2017-18839</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by XSS. This affects D3600 before 1.0.0.67, D6000 before 1.0.0.67, D6100 before 1.0.0.56, D6200 before 1.1.00.24, D6220 before 1.0.0.32, D6400 before 1.0.0.66, D7000 before 1.0.1.52, D7000v2 before 1.0.0.44, D7800 before 1.0.1.30, D8500 before 1.0.3.35, DGN2200v4 before 1.0.0.96,			

netgear -- multiple_devices	DGN2200Bv4 before 1.0.0.96, EX2700 before 1.0.1.28, EX6100v2 before 1.0.1.54, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.52, EX6400 before 1.0.1.72, EX7300 before 1.0.1.72, EX8000 before 1.0.0.102, JNR1010v2 before 1.1.0.44, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.46, R6700 before 1.0.1.36, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, R6700v2 before 1.2.0.12, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.18, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.58, R7500 before 1.0.0.118, R7500v2 before 1.0.3.24, R7800 before 1.0.2.40, R7900 before 1.0.2.4, R7900P before 1.1.5.14, R8000 before 1.0.4.4, R8000P before 1.1.5.14, R8500 before 1.0.2.110, R8300 before 1.0.2.110, R9000 before 1.0.2.52, WN2000RPTv3 before 1.0.1.8, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.42, WNDR3400v3 before 1.0.1.16, WNDR3700v4 before 1.0.2.94, WNDR4300 before 1.0.2.96, WNDR4300v2 before 1.0.0.50, WNDR4500v3 before 1.0.0.50, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.44, WNR2050 before 1.1.0.44, and WNR3500Lv2 before 1.2.0.46.	2020-04-22	3.5	<a href="#">CVE-2017-18785</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects D6200 before 1.1.00.24, D7000 before 1.0.1.52, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6020 before 1.0.0.26, R6050 before 1.0.1.12, R6080 before 1.0.0.26, R6120 before 1.0.0.36, R6220 before 1.1.0.60, R6700v2 before 1.2.0.12, R6800 before 1.2.0.12, R6900v2 before 1.2.0.12, WNDR3700v5 before 1.1.0.50, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	2.1	<a href="#">CVE-2017-18780</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.28, D6400 before 1.0.0.60, D7000 before 1.0.1.52, D7000v2 before 1.0.0.38, D7800 before 1.0.1.24, D8500 before 1.0.3.29, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.14, JWNDR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.14, R6220 before 1.1.0.60, R6400 before 1.1.0.26, R6400v2 before 1.0.2.46, R6700v2 before 1.2.0.2, R6800 before 1.2.0.2, R6900v2 before 1.2.0.2, R7100LG before 1.0.0.32, R7300DST before 1.0.0.56, R7500 before 1.0.0.112, R7500v2 before 1.0.3.24, R7800 before 1.0.2.36, R7900P before 1.1.4.6, R8000P before 1.1.4.6, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.94, WNDR3700v5 before 1.1.0.50, WNDR4300v1 before 1.0.2.96, WNDR4300v2 before 1.0.0.52, WNDR4500v3 before 1.0.0.52, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	2020-04-22	2.1	<a href="#">CVE-2017-18778</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6250 before V1.0.4.8, R6400 before V1.0.1.22, R6400v2 before V1.0.2.32, R7100LG before V1.0.0.32, R7300 before V1.0.0.52, R8300 before V1.0.2.94, R8500 before V1.0.2.100, D6220 before V1.0.0.28, D6400 before V1.0.0.60, and D8500 before V1.0.3.29.	2020-04-22	2.1	<a href="#">CVE-2017-18789</a> <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by denial			

netgear -- multiple_devices	of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	2020-04-21	<a href="#">2.7</a>	<a href="#">CVE-2018-21141</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6700v2 before 1.1.0.38, R6800 before 1.1.0.38, D7000 before 1.0.1.50, and D1500 before 1.0.0.25.	2020-04-21	<a href="#">2.1</a>	<a href="#">CVE-2017-18798</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects GS110EMX before 1.0.0.9, GS810EMX before 1.0.0.5, XS512EM before 1.0.0.6, and XS724EM before 1.0.0.6.	2020-04-22	<a href="#">3.3</a>	<a href="#">CVE-2018-21122</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX6200v2 before 1.0.1.50, EX7000 before 1.0.0.56, JR6150 before 1.0.1.18, R6050 before 1.0.1.10J, R6100 before 1.0.1.16, R6150 before 1.0.1.10, R6220 before 1.1.0.50, R6250 before 1.0.4.12, R6300v2 before 1.0.4.12, R6400 before 1.0.1.24, R6400v2 before 1.0.2.32, R6700 before 1.0.1.26, R6700v2 before 1.2.0.4, R6800 before 1.0.1.10, R6900 before 1.0.1.26, R6900P before 1.0.0.58, R6900v2 before 1.2.0.4, R7000 before 1.0.9.6, R7000P before 1.0.0.58, R7100LG before 1.0.0.32, R7300 before 1.0.0.54, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R7900 before 1.0.1.18, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.2.40, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR4300v1 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR3500Lv2 before 1.2.0.44.	2020-04-22	<a href="#">2.1</a>	<a href="#">CVE-2017-18769</a> <a href="#">CONFIRM</a>
netgear -- r6700_and_r6800_devices	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects R6700v2 before 1.1.0.38 and R6800 before 1.1.0.38.	2020-04-20	<a href="#">2.1</a>	<a href="#">CVE-2017-18845</a> <a href="#">CONFIRM</a>
netgear -- r7800_devices	NETGEAR R7800 devices before 1.0.2.30 are affected by incorrect configuration of security settings.	2020-04-21	<a href="#">2.1</a>	<a href="#">CVE-2017-18803</a> <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18807</a> <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18820</a> <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18816</a> <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18815</a> <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18814</a> <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	2020-04-21	<a href="#">3.5</a>	<a href="#">CVE-2017-18810</a> <a href="#">CONFIRM</a>
tenable -- tenable.sc	Stored XSS in Tenable.Sc before 5.14.0 could allow an authenticated remote attacker to craft a request to execute arbitrary script code in a user's	2020-04-		<a href="#">CVE-2020-</a>

	browser session. Updated input validation techniques have been implemented to correct this issue.	17	3.5	5737 <a href="#">MISC</a>
--	---	----	-----	------------------------------

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Source CVSS Published Score Info
abb -- system_800xa_base	Weak Registry permissions in ABB System 800xA Base allow low privileged users to read and modify registry settings related to control system functionality, allowing an authenticated attacker to cause system functions to stop or malfunction.	<a href="#">CVE-2020-2474</a> Yes Calculated <a href="#">MISC</a>
abb -- system_800xa_information_manager	The installations for ABB System 800xA Information Manager versions 5.1, 6.0 to 6.0.3.2 and 6.1 wrongly contain an auxiliary component. An attacker is able to use this for an XSS-like attack to an authenticated local user, which might lead to execution of arbitrary code.	<a href="#">CVE-2020-2477</a> Yes Calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon-gateway	The Configuration pages in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway for user profiles and services transfer the password in plaintext (although hidden when displayed).	<a href="#">CVE-2020-19107</a> Yes Calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon-gateway	The web server in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows access to different endpoints of the application without authenticating by accessing a specific uniform resource locator (URL) , violating the access-control (ACL) rules. This issue allows obtaining sensitive information that may aid in further attacks and privilege escalation.	<a href="#">CVE-2020-19104</a> Yes Calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon-gateway	Improper implementation of Access Control in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway allows an unauthorized user to access data marked as restricted, such as viewing or editing user profiles and application settings.	<a href="#">CVE-2020-19106</a> Yes Calculated <a href="#">MISC</a>
abb -- tg/s_telephone_gateway_and_6186/11_telefon-gateway	The backup function in ABB Telephone Gateway TG/S 3.2 and Busch-Jaeger 6186/11 Telefon-Gateway saves the current settings and configuration of the application, including credentials of existing user accounts and other configuration's credentials in plaintext.	<a href="#">CVE-2020-19105</a> Yes Calculated <a href="#">MISC</a>
admidio -- admidio	SQL Injection was discovered in Admidio before version 3.3.13. The main cookie parameter is concatenated into a SQL query without any input validation/sanitization, thus an attacker without logging in, can send a GET request with arbitrary SQL queries appended to the cookie parameter and execute SQL queries. The vulnerability impacts the confidentiality of the system. This has been patched in version 3.3.13.	<a href="#">CVE-2020-11004</a> Yes Calculated <a href="#">MISC</a> <a href="#">CONFIRM</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo).	<a href="#">CVE-2020-12131</a> Yes Calculated <a href="#">MISC</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function.	<a href="#">CVE-2020-12130</a> Yes Calculated <a href="#">MISC</a>
airdesk_pro -- airdesk_pro_app_for_ios	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder function.	<a href="#">CVE-2020-12129</a> Yes Calculated <a href="#">MISC</a>
anchor-cms -- anchor-cms	Anchor 0.12.7 allows admins to cause XSS via crafted post content.	<a href="#">CVE-2020-12071</a> Yes Calculated <a href="#">MISC</a>
atlassian -- confluence_server	The attachment-uploading feature in Atlassian Confluence Server from version 6.14.0 through version 6.14.3, and version 6.15.0 before version 6.15.5 allows remote attackers to achieve stored cross-site-scripting (SXSS) via a malicious attachment with a modified `mimeType` parameter.	<a href="#">CVE-2020-11102</a> Yes Calculated <a href="#">MISC</a>
	An authentication weakness in the SNMP service in B&R Automation	<a href="#">CVE-2020-</a>



b&r_automation -- automation_runtime	Runtime versions 2.96, 3.00, 3.01, 3.06 to 3.10, 4.00 to 4.63, 4.72 and above allows unauthenticated users to modify the configuration of B&R products via SNMP.	<a href="#">CVE-2019-19108</a> Calculated CONFIRM
beaker -- beaker	Beaker before 0.8.9 allows a sandbox escape, enabling system access and code execution. This occurs because Electron context isolation is not used, and therefore an attacker can conduct a prototype-pollution attack against the Electron internal messaging API.	<a href="#">CVE-2020-14079</a> Calculated MISC
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.5 allows remote attackers to obtain sensitive files via Local File Inclusion.	<a href="#">CVE-2020-12112</a> Calculated MISC
bigbluebutton -- bigbluebutton	BigBlueButton before 2.2.4 allows XSS via closed captions because dangerouslySetInnerHTML in React is used.	<a href="#">CVE-2020-14113</a> Calculated MISC
bitcoin-abe -- bitcoin-abe	Abe (aka bitcoin-abe) through 0.7.2, and 0.8pre, allows XSS in __call__ in abe.py because the PATH_INFO environment variable is mishandled during a PageNotFound exception.	<a href="#">CVE-2020-11944</a> Calculated MISC
bitdefender -- antivirus_free	A vulnerability in the improper handling of junctions in Bitdefender Antivirus Free can allow an unprivileged user to substitute a quarantined file, and restore it to a privileged location. This issue affects: Bitdefender Antivirus Free versions prior to 1.0.17.	<a href="#">CVE-2020-3099</a> Calculated MISC
bson -- bson	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.	<a href="#">CVE-2020-12135</a> Calculated MISC
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shifts_btrfs_ioctl_fd_replace() calls fdget(oldfd), then without further checks passes the resulting file* into shifts_real_fdget(), which casts file->private_data, a void* that points to a filesystem-dependent type, to a "struct shifts_file_info *". As the private_data is not required to be a pointer, an attacker can use this to cause a denial of service or possibly execute arbitrary code.	<a href="#">CVE-2019-15792</a> Calculated MISC
canonical -- ubuntu	Apport creates a world writable lock file with root ownership in the world writable /var/lock/apport directory. If the apport/ directory does not exist (this is not uncommon as /var/lock is a tmpfs), it will create the directory, otherwise it will simply continue execution using the existing directory. This allows for a symlink attack if an attacker were to create a symlink at /var/lock/apport, changing apport's lock file location. This file could then be used to escalate privileges, for example. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	<a href="#">CVE-2020-8831</a> Calculated CONFIRM
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, shifts_btrfs_ioctl_fd_replace() installs an fd referencing a file from the lower filesystem without taking an additional reference to that file. After the btrfs ioctl completes this fd is closed, which then puts a reference to that file, leading to a refcount underflow.	<a href="#">CVE-2019-15791</a> Calculated MISC
canonical -- ubuntu	In shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, several locations which shift ids translate user/group ids before performing operations in the lower filesystem were translating them into init_user_ns, whereas they should have been translated into the s_user_ns for the lower filesystem. This resulted in using ids other than the intended ones in the lower fs, which likely did not map into the shifts s_user_ns. A local attacker could use this to possibly bypass discretionary access control permissions.	<a href="#">CVE-2019-15793</a> Calculated MISC
canonical -- ubuntu	Overlayfs in the Linux kernel and shifts, a non-upstream patch to the Linux kernel included in the Ubuntu 5.0 and 5.3 kernel series, both replace vma->vm_file in their mmap handlers. On error the original value is not restored, and the reference is put for the file to which vm_file points.	<a href="#">CVE-2019-15794</a> Calculated MISC

	On upstream kernels this is not an issue, as no callers dereference vm_file following after call_mmap() returns an error. However, the aufs patches change mmap_region() to replace the fput() using a local variable with vma_fput(), which will fput() vm_file, leading to a refcount underflow.	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Time-of-check Time-of-use Race Condition vulnerability on crash report ownership change in Apport allows for a possible privilege escalation opportunity. If fs.protected_symlinks is disabled, this can be exploited between the os.open and os.chown calls when the Apport cron script clears out crash files of size 0. A symlink with the same name as the deleted file can then be created upon which chown will be called, changing the file owner to root. Fixed in versions 2.20.1-0ubuntu2.23, 2.20.9-0ubuntu7.14, 2.20.11-0ubuntu8.8 and 2.20.11-0ubuntu22.	<a href="#">CVE-2020-8833</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ceph -- ceph	An issue was discovered in Ceph through 13.2.9. A POST request with an invalid tagging XML can crash the RGW process by triggering a NULL pointer exception.	<a href="#">CVE-2020-12059</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ceph -- ceph	A path traversal flaw was found in the Ceph dashboard implemented in upstream versions v14.2.5, v14.2.6, v15.0.0 of Ceph storage and has been fixed in versions 14.2.7 and 15.1.0. An unauthenticated attacker could use this flaw to cause information disclosure on the host machine running the Ceph dashboard.	<a href="#">CVE-2020-1699</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ceph -- object_gateway	A flaw was found in the Ceph Object Gateway, where it supports request sent by an anonymous user in Amazon S3. This flaw could lead to potential XSS attacks due to the lack of proper neutralization of untrusted input.	<a href="#">CVE-2020-1760</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
contiki-ng -- contiki-ng_and_contiki	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. A buffer overflow is present due to an integer underflow during 6LoWPAN fragment processing in the face of truncated fragments in os/net/ipv6/sicslowpan.c. This results in accesses of unmapped memory, crashing the application. An attacker can cause a denial-of-service via a crafted 6LoWPAN frame.	<a href="#">CVE-2019-1783</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
contiki-ng -- contiki-ng_and_contiki	An issue was discovered in Contiki-NG through 4.3 and Contiki through 3.0. An out of bounds write is present in the data section during 6LoWPAN fragment re-assembly in the face of forged fragment offsets in os/net/ipv6/sicslowpan.c.	<a href="#">CVE-2019-1859</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
d-link -- dir-615_devices	The login page on D-Link DIR-615 T1 20.10 devices allows remote attackers to bypass the CAPTCHA protection mechanism and conduct brute-force attacks.	<a href="#">CVE-2020-17525</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A cfm UDP service listening on port 65002 allows remote, unauthenticated exfiltration of administrative credentials.	<a href="#">CVE-2020-9275</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The device can be reset to its default configuration by accessing an unauthenticated URL.	<a href="#">CVE-2020-9278</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A hard-coded account allows management-interface login with high privileges. The logged-in user can perform critical tasks and take full control of the device.	<a href="#">CVE-2020-9279</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dsl-2640b_b2_devices	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. Authentication can be bypassed when accessing cgi modules. This allows one to perform administrative tasks (e.g., modify the admin password) with no authentication.	<a href="#">CVE-2020-9277</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices.	<a href="#">CVE-</a>

d-link -- dsl-2640b_b2_devices	The function do_cgi(), which processes cgi requests supplied to the device's web servers, is vulnerable to a remotely exploitable stack-based buffer overflow. Unauthenticated exploitation is possible by combining this vulnerability with CVE-2020-9277.	<a href="#">CVE-2020-9276</a> Yes Calculated MISC
dong_joo_cho -- file_transfer_ifamily	DONG JOO CHO File Transfer iFamily 2.1 allows directory traversal related to the ./etc/ path.	<a href="#">CVE-2020-12128</a> Yes Calculated MISC
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit.	<a href="#">CVE-2020-5869</a> Yes Calculated MISC
f5 -- big-iq	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer.	<a href="#">CVE-2020-5870</a> Yes Calculated MISC
f5 -- big-iq	In BIG-IQ 6.0.0-7.0.0, a remote access vulnerability has been discovered that may allow a remote user to execute shell commands on affected systems using HTTP requests to the BIG-IQ user interface.	<a href="#">CVE-2020-5868</a> Yes Calculated MISC
f5 -- nginx_controller	In versions of NGINX Controller prior to 3.2.0, communication between NGINX Controller and NGINX Plus instances skip TLS verification by default.	<a href="#">CVE-2020-5864</a> Yes Calculated CONFIRM
f5 -- nginx_controller	In versions prior to 3.3.0, the NGINX Controller Agent installer script 'install.sh' uses HTTP instead of HTTPS to check and install packages	<a href="#">CVE-2020-5867</a> Yes Calculated CONFIRM
f5 -- nginx_controller	In versions of NGINX Controller prior to 3.3.0, the helper.sh script, which is used optionally in NGINX Controller to change settings, uses sensitive items as command-line arguments.	<a href="#">CVE-2020-5866</a> Yes Calculated CONFIRM
f5 -- nginx_controller	In versions prior to 3.3.0, the NGINX Controller is configured to communicate with its Postgres database server over unencrypted channels, making the communicated data vulnerable to interception via man-in-the-middle (MiTM) attacks.	<a href="#">CVE-2020-5865</a> Yes Calculated CONFIRM
fifthplay -- s.a.m.i	Fifthplay S.A.M.I before 2019.3_HP2 allows unauthenticated stored XSS via a POST request.	<a href="#">CVE-2020-14132</a> Yes Calculated MISC
flexera -- flexnet_publisher	A Denial of Service vulnerability related to stack exhaustion has been identified in FlexNet Publisher lmadm.exe 11.16.2. Because the message reading function calls itself recursively given a certain condition in the received message, an unauthenticated remote attacker can repeatedly send messages of that type to cause a stack exhaustion condition.	<a href="#">CVE-2020-8961</a> Yes Calculated CONFIRM
flexera -- flexnet_publisher	A Denial of Service vulnerability related to command handling has been identified in FlexNet Publisher lmadm.exe version 11.16.2. The message reading function used in lmadm.exe can, given a certain message, call itself again and then wait for a further message. With a particular flag set in the original message, but no second message received, the function eventually return an unexpected value which leads to an exception being thrown. The end result can be process termination.	<a href="#">CVE-2020-8960</a> Yes Calculated CONFIRM
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of vertices in U3D objects. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10568.	<a href="#">CVE-2020-04905</a> Yes Calculated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the AddWatermark command of the communication API. The	<a href="#">CVE-2020-04909</a> Yes Calculated MISC

	issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9942.	<a href="#">CVE-2020-14890</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the GetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9944.	<a href="#">CVE-2020-14891</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the OCRAndExportToExcel command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9946.	<a href="#">CVE-2020-14893</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10461.	<a href="#">CVE-2020-14890</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10463.	<a href="#">CVE-2020-14893</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10193.	<a href="#">CVE-2020-14897</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10190.	<a href="#">CVE-2020-14894</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the SetFieldValue command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9945.	<a href="#">CVE-2020-14892</a> <a href="#">MISC</a> Unrated
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the	<a href="#">CVE-2020-</a>



	handling of the DuplicatePages command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9828.	<a href="#">CVE-2020-04889</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the ConvertToPDF command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9829.	<a href="#">CVE-2020-04890</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Save command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9831.	<a href="#">CVE-2020-04891</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10189.	<a href="#">CVE-2020-04893</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Export command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9865.	<a href="#">CVE-2020-04898</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10191.	<a href="#">CVE-2020-04895</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10192.	<a href="#">CVE-2020-04896</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10195.	<a href="#">CVE-2020-04898</a> <a href="#">11150</a> dated <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the	<a href="#">CVE-2020-04902</a> <a href="#">11150</a> dated <a href="#">MISC</a>

	end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10462.	
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10464.	<a href="#">CVE-2020-04904</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the RotatePage command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9943.	<a href="#">CVE-2020-04910</a> Notated MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the CombineFiles command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9830.	<a href="#">CVE-2020-04892</a> Notated MISC
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10132.	<a href="#">CVE-2020-04899</a> Notated MISC
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the resetForm method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10614.	<a href="#">CVE-2020-04906</a> Notated MISC
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10142.	<a href="#">CVE-2020-04900</a> Notated MISC
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of widgets in XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10650.	<a href="#">CVE-2020-04907</a> Notated MISC
	Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. This bug is similar to CVE-2020-5260(GHSA-qm7j-c969-7j4q). The fix for that bug still left the door open for an exploit where <code>_some_</code> credential is leaked (but the attacker cannot control which one). Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that are considered illegal as of the recently published Git versions can cause Git to send a "blank" pattern to helpers, missing hostname and protocol fields. Many helpers will interpret this as matching <code>_any_</code> URL, and will return some unspecified stored password,	<a href="#">CVE-2020-11008</a> MISC

git -- git	leaking the password to an attacker's server. The vulnerability can be triggered by feeding a malicious URL to `git clone`. However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The root of the problem is in Git itself, which should not be feeding blank input to helpers. However, the ability to exploit the vulnerability in practice depends on which helpers are in use. Credential helpers which are known to trigger the vulnerability: - Git's "store" helper - Git's "cache" helper - the "osxkeychain" helper that ships in Git's "contrib" directory Credential helpers which are known to be safe even with vulnerable versions of Git: - Git Credential Manager for Windows Any helper not in this list should be assumed to trigger the vulnerability.	<a href="#">CONFIRM</a> <a href="#">CVE-2020-1511</a> <a href="#">MISC</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a> <a href="#">GENTOO</a>
gitlab -- gitlab	An issue was discovered in GitLab 10.7.0 and later through 12.9.2. A Workhorse bypass could lead to job artifact uploads and file disclosure (Exposure of Sensitive Information) via request smuggling.	<a href="#">CVE-2020-1506</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 12.7.9, 12.8.x before 12.8.9, and 12.9.x before 12.9.3. A Workhorse bypass could lead to NuGet package and file disclosure (Exposure of Sensitive Information) via request smuggling.	<a href="#">CVE-2020-1505</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and_enterprise_edition	An issue was discovered in GitLab CE and EE 8.15 through 12.9.2. Members of a group could still have access after the group is deleted.	<a href="#">CVE-2020-1549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gnome -- evolution	An issue was discovered in GNOME Evolution before 3.35.91. By using the proprietary (non-RFC6068) "mailto?attach=..." parameter, a website (or other source of mailto links) can make Evolution attach local files or directories to a composed email message without showing a warning to the user, as demonstrated by an attach=. value.	<a href="#">CVE-2020-15879</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- gnu_mailman	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code.	<a href="#">CVE-2020-16037</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- google_earth_pro	A vulnerability in the windows installer of Google Earth Pro versions prior to 7.3.3 allows an attacker using DLL h jacking to insert malicious local files to execute unauthenticated remote code on the targeted system.	<a href="#">CVE-2020-15895</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana_labs -- grafana	Grafana before 6.7.3 allows table-panel XSS via column.title or cellLinkTooltip.	<a href="#">CVE-2020-16245</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
hcl -- appscan_enterprise	"HCL AppScan Enterprise uses hard-coded credentials which can be exploited by attackers to get unauthorized access to application's encrypted files."	<a href="#">CVE-2020-16327</a> <a href="#">MISC</a> <a href="#">MISC</a>
hcl -- connections	"HCL Connections is vulnerable to possible information leakage and could disclose sensitive information via stack trace to a local user."	<a href="#">CVE-2020-16085</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
helm -- helm	There is an information disclosure vulnerability in Helm from version 3.1.0 and before version 3.2.0. 'lookup' is a Helm template function introduced in Helm v3. It is able to lookup resources in the cluster to check for the existence of specific resources and get details about them. This can be used as part of the process to render templates. The documented behavior of 'helm template' states that it does not attach to a remote cluster. However, a the recently added 'lookup' template function circumvents this restriction and connects to the cluster even during 'helm template' and 'helm install update delete rol back --dry-run'. The user is not notified of this behavior. Running 'helm template' should not make calls to a cluster. This is different from 'install', which is presumed to have access to a cluster in order to load resources into Kubernetes. Helm 2 is	<a href="#">CVE-2020-16013</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	unaffected by this vulnerability. A malicious chart author could inject a 'lookup' into a chart that, when rendered through 'helm template', performs unannounced lookups against the cluster a user's 'KUBECONFIG' file points to. This information can then be disclosed via the output of 'helm template'. This issue has been fixed in Helm 3.2.0	
hp -- j/h-series_nonstop_systems	This document describes a security vulnerability in Blade Maintenance Entity, Integrated Maintenance Entity and Maintenance Entity products. All J/H-series NonStop systems have a security vulnerability associated with an open UDP port 17185 on the Maintenance LAN which could result in information disclosure, denial-of-service attacks or local memory corruption against the affected system and a complete control of the system may also be possible. This vulnerability exists only if one gains access to the Maintenance LAN to which Blade Maintenance Entity, Integrated Maintenance Entity or Maintenance Entity product is connected. **Workaround:** Block the UDP port 17185(In the Maintenance LAN Network Switch/Firewall). Fix: Install following SPRs, which are already available: * T1805A01^AAI (Integrated Maintenance Entity) * T4805A01^AAZ (Blade Maintenance Entity). These SPRs are also usable with the following RVUs: * J06.19.00 ? J06.23.01. No fix planned for the following RVUs: J06.04.00 ? J06.18.01. No fix planned for H-Series NonStop systems. No fix planned for the product T2805 (Maintenance Entity).	<a href="#">CVE-2020-0431</a> 2020-04-31 Calculated MISC
hp -- onboard_administrator	A potential security vulnerability has been identified in HPE Onboard Administrator. The vulnerability could be remotely exploited to allow Reflected Cross Site Scripting. HPE has made the following software updates and mitigation information to resolve the vulnerability in HPE Onboard Administrator. * OA 4.95 (Linux and Windows).	<a href="#">CVE-2020-0432</a> 2020-04-32 Calculated MISC
hp -- uiot	A unauthorized remote access vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	<a href="#">CVE-2020-0433</a> 2020-04-33 Calculated MISC
hp -- uiot	A remote access to sensitive data vulnerability was discovered in HPE IOT + GCP version(s): 1.4.0, 1.4.1, 1.4.2, 1.2.4.2.	<a href="#">CVE-2020-0434</a> 2020-04-34 Calculated MISC
bm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 173310.	<a href="#">CVE-2019-0450</a> 2019-04-50 Calculated CONFIRM
bm -- cloud_app_management	IBM Cloud App Management 2019.3.0 and 2019.4.0 reveals a stack trace on certain API requests which can allow an attacker further information about the implementation of the offering. IBM X-Force ID: 173311.	<a href="#">CVE-2019-0451</a> 2019-04-51 Calculated CONFIRM
bm -- maas360	IBM MaaS360 6.82 could allow a user with physical access to the device to crash the application which may enable the user to access restricted applications and device settings. IBM X-Force ID: 178505.	<a href="#">CVE-2020-0453</a> 2020-04-53 Calculated CONFIRM
bm -- maas360_for_ios	IBM MaaS360 3.96.62 for iOS could allow an attacker with physical access to the device to obtain sensitive information from the agent outside of the container. IBM X-Force ID: 172705.	<a href="#">CVE-2019-0435</a> 2019-04-35 Calculated CONFIRM
bm -- mq_and_mq_appliance	IBM MQ and MQ Appliance 8.0, 9.1 LTS, and 9.1 CD could allow an authenticated user cause a denial of service due to a memory leak. IBM X-Force ID: 175840.	<a href="#">CVE-2020-0467</a> 2020-04-67 Calculated CONFIRM
bm -- spectrum_protect	IBM Spectrum Protect 7.1 and 8.1 server is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker to execute arbitrary code on the system with the privileges of an administrator or user associated with the Spectrum Protect server or cause the Spectrum Protect server to crash. IBM X-Force ID: 179990.	<a href="#">CVE-2020-0415</a> 2020-04-15 Calculated CONFIRM
bm -- tivoli_monitoring	IBM Tivoli Monitoring 6.3.0 could allow a local attacker to execute arbitrary code on the system. By placing a specially crafted file, an attacker could exploit this vulnerability to load other DLL files located in	<a href="#">CVE-2020-0411</a> 2020-04-11 Calculated CONFIRM



	the same directory and execute arbitrary code on the system. IBM X-Force ID: 177083.	<a href="#">CVE-2020-11687</a> 2020-11-10 Yes Calculated CONFIRM
bm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0.4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 171250.	<a href="#">CVE-2020-11688</a> 2020-11-10 Yes Calculated CONFIRM
bm -- urbancode_deploy	IBM UrbanCode Deploy (UCD) 7.0.3.0 and 7.0.4.0 could allow an authenticated user to impersonate another user if the server is configured to enable Distributed Front End (DFE). IBM X-Force ID: 174955.	<a href="#">CVE-2020-11689</a> 2020-11-10 Yes Calculated CONFIRM
infradead -- openconnect	OpenConnect through 8.08 mishandles negative return values from X509_check_function calls, which might assist attackers in performing man-in-the-middle attacks.	<a href="#">CVE-2020-11690</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- goland	In JetBrains GoLand before 2019.3.2, the plugin repository was accessed via HTTP instead of HTTPS.	<a href="#">CVE-2020-11691</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- hub	In JetBrains Hub before 2020.1.12099, content spoofing in the Hub OAuth error message was possible.	<a href="#">CVE-2020-11692</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA before 2020.1, the license server could be resolved to an untrusted host in some cases.	<a href="#">CVE-2020-11693</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- space	In JetBrains Space through 2020-04-22, the password authentication implementation was insecure.	<a href="#">CVE-2020-11694</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- space	In JetBrains Space through 2020-04-22, the session timeout period was configured improperly.	<a href="#">CVE-2020-11695</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- space	JetBrains Space through 2020-04-22 allows stored XSS in Chats.	<a href="#">CVE-2020-11696</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.4, a project administrator was able to retrieve some TeamCity server settings.	<a href="#">CVE-2020-11697</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.2, password values were shown in an unmasked format on several pages.	<a href="#">CVE-2020-11698</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.1, a user without appropriate permissions was able to import settings from the settings.kts file.	<a href="#">CVE-2020-11699</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.2.1, the application state is kept alive after a user ends his session.	<a href="#">CVE-2020-11700</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity 2018.2 through 2019.2.1, a project administrator was able to see scrambled password parameters used in a project. The issue was resolved in 2019.2.2.	<a href="#">CVE-2020-11701</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- youtrack	In JetBrains YouTrack before 2020.1.659, DB export was access ble to read-only administrators.	<a href="#">CVE-2020-11702</a> 2020-11-10 Yes Calculated CONFIRM
jetbrains -- youtrack	JetBrains YouTrack before 2020.1.659 was vulnerable to DoS that could be caused by attaching a malformed TIFF file to an issue.	<a href="#">CVE-2020-11703</a> 2020-11-10 Yes Calculated CONFIRM

joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized editing of usergroups.	<a href="#">CVE-2020-11891</a> 2020-11-18 MISC
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Improper input validations in the usergroup table class could lead to a broken ACL configuration.	<a href="#">CVE-2020-11890</a> 2020-11-18 MISC
joomla! -- joomla!	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized deletion of usergroups.	<a href="#">CVE-2020-11889</a> 2020-11-18 MISC
jquery -- jquery	jQuery v2.2.2 allows XSS via a crafted onerror attribute of an IMG element.	<a href="#">CVE-2018-18405</a> 2018-12-19 MISC
juplink -- rx4-1500_router	Juplink RX4-1500 v1.0.3 allows remote attackers to gain root access to the Linux subsystem via an unsanitized exec call (aka Command Line Injection), if the undocumented telnetd service is enabled and the attacker can authenticate as admin from the local network.	<a href="#">CVE-2020-7797</a> 2020-11-18 MISC
juplink -- rx4-1500_router	httpd in Juplink RX4-1500 v1.0.3-v1.0.5 allows remote attackers to change or access router settings by connecting to the unauthenticated setup3.htm endpoint from the local network.	<a href="#">CVE-2020-7798</a> 2020-11-18 MISC
lazysizes -- lazysizes	lazysizes through 5.2.0 allows execution of malicious JavaScript. The following attributes are not sanitized by the video-embed plugin: data-vimeo, data-vimeoparams, data-youtube and data-ytparams which can be abused to inject malicious JavaScript.	<a href="#">CVE-2020-7642</a> 2020-11-18 MISC
libnvc -- libnvc_server	libvncclient/cursor.c in L bVNCServer through 0.9.12 has a HandleCursorShape integer overflow and heap-based buffer overflow via a large height or width value. NOTE: this may overlap CVE-2019-15690.	<a href="#">CVE-2020-7788</a> 2020-11-18 MISC
libslirp -- libslirp	A use after free vulnerability in ip_reass() in ip_input.c of libslirp 4.2.0 and prior releases allows crafted packets to cause a denial of service.	<a href="#">CVE-2020-7683</a> 2020-11-18 MISC
mailstore -- mailstore_outlook_add-in	In MailStore Outlook Add-in (and Email Archive Outlook Add-in) through 12.1.2, the login process does not validate the validity of the certificate presented by the server.	<a href="#">CVE-2020-11806</a> 2020-11-18 CONFIRM
mediawiki -- mediawiki	The CentralAuth extension through REL1_34 for MediaWiki allows remote attackers to obtain sensitive hidden account information via an api.php?action=query&meta=globaluserinfo&guiuser= request. In other words, the information can be retrieved via the action API even though access would be denied when simply visiting wiki/Special:CentralAuth in a web browser.	<a href="#">CVE-2020-16051</a> 2020-11-18 MISC
minio -- minio	MinIO versions before RELEASE.2020-04-23T00-58-49Z have an authentication bypass issue in the MinIO admin API. Given an admin access key, it is possible to perform admin API operations i.e. creating new service accounts for existing access keys - without knowing the admin secret key. This has been fixed and released in version RELEASE.2020-04-23T00-58-49Z.	<a href="#">CVE-2020-7712</a> 2020-11-18 MISC
mozilla -- firefox	Mozilla developers Tyson Smith, Bob Clary, and Alexandru Michis reported memory safety bugs present in Firefox 74. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6826</a> 2020-11-18 MISC
mozilla -- firefox	A malicious extension could have called <code>browser.identity.launchWebAuthFlow</code> , controlling the redirect_uri, and through the Promise returned, obtain the Auth code and gain access to the user's account at the service provider. This vulnerability affects Firefox < 75.	<a href="#">CVE-2020-6823</a> 2020-11-18 MISC
mozilla -- firefox	Initially, a user opens a Private Browsing Window and generates a password for a site, then closes the Private Browsing Window but leaves Firefox open. Subsequently, if the user had opened a new Private Browsing Window, revisited the same site, and generated a new	<a href="#">CVE-2020-6824</a> 2020-11-18 MISC

	password - the generated passwords would have been identical, rather than independent. This vulnerability affects Firefox < 75.	<a href="#">MISC</a>
mozilla -- firefox_esr	When following a link that opened an intent://-schemed URL, causing a custom tab to be opened, Firefox for Android could be tricked into displaying the incorrect URI.   *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	<a href="#">CVE-2020-0827</a> <a href="#">MISC</a> Calculated
mozilla -- firefox_esr	A malicious Android application could craft an Intent that would have been processed by Firefox for Android and potentially result in a file overwrite in the user's profile directory. One exploitation vector for this would be to supply a user.js file providing arbitrary malicious preference values. Control of arbitrary preferences can lead to sufficient compromise such that it is generally equivalent to arbitrary code execution.  *Note: This issue only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.7.	<a href="#">CVE-2020-0828</a> <a href="#">MISC</a> Calculated
mozilla -- thunderbird_and_firefox_and_firefox_esr	When reading from areas partially or fully outside the source resource with WebGL's <code>copyTexSubImage</code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-0829</a> <a href="#">MISC</a> Calculated
mozilla -- thunderbird_and_firefox_and_firefox_esr	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code>GMPDecodeData</code>. It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-0829</a> <a href="#">MISC</a> Calculated
mozilla -- thunderbird_and_firefox_and_firefox_esr	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	<a href="#">CVE-2020-0829</a> <a href="#">MISC</a> Calculated
mozilla -- thunderbird_and_firefox_and_firefox_esr	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.	<a href="#">CVE-2020-0829</a> <a href="#">MISC</a> Calculated
mozilla -- thunderbird_and_firefox_and_firefox_esr	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.	<a href="#">CVE-2020-0819</a> <a href="#">MISC</a> Calculated
msi -- true_color	Unquoted search path vulnerability in MSI True Color before 3.0.52.0 allows privilege escalation to SYSTEM.	<a href="#">CVE-2020-0842</a> <a href="#">MISC</a> Calculated
nanometrics -- centaur_and_titansma_devices	Nanometrics Centaur through 4.3.23 and TitanSMA through 4.2.20 mishandle access control for the syslog log.	<a href="#">CVE-2020-0842</a> <a href="#">MISC</a> Calculated
netatmo -- smart_indoor_camera	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in firmware versions prior to x.xx of Netatmo Smart Indoor Camera allows an attacker to execute commands on the device. This issue affects: Netatmo Smart Indoor Camera version and prior versions.	<a href="#">CVE-2019-10101</a> <a href="#">MISC</a> Calculated
netgear -- d3600_and_d6000_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.76 and D6000 before 1.0.0.76.	<a href="#">CVE-2018-21138</a> <a href="#">CONFIRM</a>
netgear -- gs810emx_devices	NETGEAR GS810EMX devices before 1.0.0.5 are affected by disclosure of sensitive information.	<a href="#">CVE-2018-14313</a> <a href="#">CONFIRM</a>

netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2017-21166 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1., JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	CVE-2017-21230 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.60, D8500 before 1.0.3.29, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R6900P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8500 before 1.0.2.106, R8300 before 1.0.2.106, and WNDR3400v3 before 1.0.1.16.	CVE-2017-18704 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2017-18720 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects D1500 before 1.0.0.25, D500 before 1.0.0.25, D6100 before 1.0.0.55, D7000 before 1.0.1.50, D7800 before 1.0.1.28, EX6100v2 before 1.0.1.60, EX6150v2 before 1.0.1.60, JNR1010v2 before 1.1.0.46, JR6150 before 1.0.1.16, JWNR2010v5 before 1.1.0.46, PR2000 before 1.0.0.18, R6020 before 1.0.0.26, R6050 before 1.0.1.16, R6080 before 1.0.0.26, R6100 before 1.0.1.20, R6220 before 1.1.0.60, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WN3000RPv3 before 1.0.2.50, WN3100RPv2 before 1.0.0.40, WNDR3700v5 before 1.1.0.48, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.46, WNR2000v5 before 1.0.0.62, WNR2020 before 1.1.0.46, and WNR2050 before 1.1.0.46.	CVE-2017-18703 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2017-18725 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects WAC505 before 5.0.0.17, WAC510 before 5.0.0.17, WAC720 before 5.0.0.17, WAC730 before 5.0.0.17, WAC740 before 5.0.0.17, and WND930 before 5.0.0.17.	CVE-2017-21133 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by reflected XSS. This affects EX3700 before 1.0.0.66, EX3800 before 1.0.0.66, EX6100 before 1.0.2.20, EX6120 before 1.0.0.34, EX6150 before 1.0.0.36, EX6200 before 1.0.3.84, and EX7000 before 1.0.0.60.	CVE-2017-18715 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects R6050/JR6150 before 1.0.1.7, PR2000 before 1.0.0.17, R6220 before 1.1.0.50, WNDR3700v5 before 1.1.0.48, JNR1010v2 before 1.1.0.40,	CVE-2017- yes



	JWNR2010v5 before 1.1.0.40, WNR1000v4 before 1.1.0.40, WNR2020 before 1.1.0.40, WNR2050 before 1.1.0.40, WNR614 before 1.1.0.40, WNR618 before 1.1.0.40, and D7000 before 1.0.1.50.	<a href="#">CVE-2020-18791</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by stored XSS. This affects D6400 before 1.0.0.60, D7000 before 1.0.1.50, D8500 before 1.0.3.29, EX6200 before 1.0.3.84, EX7000 before 1.0.0.60, R6250 before 1.0.4.16, R6300v2 before 1.0.4.18, R6400 before 1.01.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7300DST before 1.0.0.56, R7900 before 1.0.1.26, R8000 before 1.0.4.4, R8300 before 1.0.2.106, R8500 before 1.0.2.106, R9000 before 1.0.2.52, WNDR3400v3 before 1.0.1.16, WNR3500Lv2 before 1.2.0.46, and WNDR3700v5 before 1.1.0.48.	<a href="#">CVE-2020-18717</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2020-18713</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects R6400 before 1.0.1.24, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	<a href="#">CVE-2020-18797</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18722</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18718</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.1.00.26, R6080 before 1.1.00.26; R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18719</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.75, D6000 before 1.0.0.75, D6100 before 1.0.0.60, R7800 before 1.0.2.52, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300 before 1.0.2.104, WNDR4300v2 before 1.0.0.58, WNDR4500v3 before 1.0.0.58, and WNR2000v5 before 1.0.0.66.	<a href="#">CVE-2020-18111</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.57, D6220 before 1.0.0.40, D6400 before 1.0.0.74, D7000 before 1.0.1.60, D7800 before 1.0.1.34, D8500 before 1.0.3.39, DGN2200v4 before 1.0.0.94, DGN2200Bv4 before 1.0.0.94, EX2700 before 1.0.1.42, EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6100 before 1.0.2.18, EX6120 before 1.0.0.32, EX6130 before 1.0.0.22, EX6150 before 1.0.0.34_1.0.70, EX6200 before 1.0.3.82_1.1.117, EX6400 before 1.0.1.78, EX7000 before 1.0.0.56, EX7300 before 1.0.1.78, JNR1010v2 before 1.1.0.42, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.42, PR2000 before 1.0.0.22, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R6250 before 1.0.4.14, R6300v2 before 1.0.4.12, R6400v2 before 1.0.2.34, R6700 before 1.0.1.26, R6900 before 1.0.1.26, R6900P before 1.2.0.22, R7000 before 1.0.9.6, R7000P before 1.2.0.22, R7100LG before 1.0.0.40, R7300DST before 1.0.0.54, R7500 before 1.0.0.110, R7500v2 before 1.0.3.26, R7800 before 1.0.2.44, R7900 before 1.0.1.26, R8000 before 1.0.3.48, R8300 before 1.0.2.104, R8500 before 1.0.2.104, R9000 before 1.0.3.10, WN2000RPTv3 before 1.0.1.26, WN2500RPv2 before 1.0.1.46, WN3000RPv3 before 1.0.2.66, WN3100RPv2 before 1.0.0.56, WNDR3400v3 before 1.0.1.14, WNDR3700v4 before 1.0.2.96, WNDR3700v5 before 1.1.0.54, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.42, WNR2000v5 before 1.0.0.64, WNR2020 before 1.1.0.42, and WNR2050 before 1.1.0.42.	<a href="#">CVE-2020-21231</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18716</a> yes calculated <a href="#">CONFIRM</a>
	Certain NETGEAR devices are affected by a stack-based buffer overflow	<a href="#">CVE-</a>

netgear -- multiple_devices	by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<del>CVE-2020-1017-08724</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<del>CVE-2020-1017-08723</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<del>CVE-2020-1017-08726</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R7500v2 before 1.0.3.20, R7800 before 1.0.2.38, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<del>CVE-2020-1018-21229</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.10, JWNR2010v5 before 1.1.0.44, R6050 before 1.0.1.10, R6100 before 1.0.1.16, R6220 before 1.1.0.50, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR3700v4 before 1.0.2.88, WNDR3700v5 before 1.1.0.48, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, WNR1000v4 before 1.1.0.44, WNR2000v5 before 1.0.0.58, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	<del>CVE-2020-1017-08749</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<del>CVE-2020-1017-08721</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6000 before 1.0.0.24, EX6130 before 1.0.0.16, EX6400 before 1.0.1.60, EX7000 before 1.0.0.50, EX7300 before 1.0.1.60, and WN2500RPv2 before 1.0.1.46.	<del>CVE-2020-1017-08746</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by authentication bypass. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.20, R6700 before 1.0.1.20, R6900 before 1.0.1.20, R7000 before 1.0.7.10, R7100LG before V1.0.0.32, R7300DST before 1.0.0.52, R7900 before 1.0.1.16, R8000 before 1.0.3.36, R8300 before 1.0.2.94, R8500 before 1.0.2.94, WNDR3400v3 before 1.0.1.12, and WNR3500Lv2 before 1.2.0.40.	<del>CVE-2020-1017-08743</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects EX6200v2 before 1.0.1.44, R6100 before 1.0.1.12, R7500 before 1.0.0.108, R7500v2 before 1.0.3.10, R7800 before 1.0.2.28, R9000 before 1.0.2.30, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<del>CVE-2020-1017-08748</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, EX6100v2 before 1.0.1.50, EX6150v2 before 1.0.1.50, EX6200v2 before 1.0.1.44, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, R6100 before 1.0.1.16, R7500 before 1.0.0.110, R7800 before 1.0.2.32, R9000 before 1.0.2.30, WN3000RPv3 before 1.0.2.50, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<del>CVE-2020-1018-21228</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects D7800 before 1.0.1.34, R6400v2 before 1.0.2.34, R6700 before 1.0.1.30, R6900 before 1.0.1.30, R6900P before 1.0.0.62, R7000 before 1.0.9.12, R7000P before 1.0.0.62, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.50, and WNDR4500v3 before 1.0.0.50.	<del>CVE-2020-1018-21227</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6400 before 1.0.1.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.34, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<del>CVE-2020-1017-08711</del> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.00.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050, before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before	<del>CVE-2020-1017-08787</del> yes calculated <a href="#">CONFIRM</a>

	1.1.0.44, and WNR2050 before 1.1.0.44.	
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection. This affects D6200 before 1.1.0.24, JNR1010v2 before 1.1.0.44, JR6150 before 1.0.1.12, JWNR2010v5 before 1.1.0.44, PR2000 before 1.0.0.20, R6050 before 1.0.1.12, WNR1000v4 before 1.1.0.44, WNR2020 before 1.1.0.44, and WNR2050 before 1.1.0.44.	CVE-2020-18786 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.0.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	CVE-2020-18717 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R6700 before 1.0.1.26, R7000 before 1.0.9.10, R7100LG before 1.0.0.32, R7900 before 1.0.1.18, R8000 before 1.0.3.54, and R8500 before 1.0.2.100.	CVE-2020-18790 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	CVE-2020-18712 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.20, R7500 before 1.0.0.118, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	CVE-2020-18706 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects EX6100 before 1.0.2.16, 1.1.130, EX6100v2 before 1.0.1.70, EX6150v2 before 1.0.1.54, EX6200v2 before 1.0.1.50, EX6400 before 1.0.1.60, EX7300 before 1.0.1.60, and WN3000RPv3 before 1.0.2.44.	CVE-2020-18768 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6700 before 1.0.1.48, R7500 before 1.0.0.124, R7800 before 1.0.2.58, R8900 before 1.0.4.2, R9000 before 1.0.4.2, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, and WNR2000v5-R2000 before 1.0.0.68.	CVE-2020-21135 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.20, R7500 before 1.0.0.118, R7500v2 before 1.0.3.20, R7800 before 1.0.2.40, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.62.	CVE-2020-18705 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6220 before 1.0.0.32, D6400 before 1.0.0.66, D8500 before 1.0.3.35, DGN2200Bv4 before 1.0.0.94, DGN2200v4 before 1.0.0.94, R6250 before 1.0.4.14, R6300v2 before 1.0.4.18, R6400 before 1.0.1.32, R6400v2 before 1.0.2.44, R6700 before 1.0.1.36, R6900 before 1.0.1.30, R6900P before 1.3.0.8, R7000 before 1.0.9.14, R7000P before 1.3.0.8, R7100LG before 1.0.0.34, R7900 before 1.0.2.4, R8000 before 1.0.4.2, WN2500RPv2 before 1.0.1.50, WNDR3400v3 before 1.0.1.14, and WNDR4000 before 1.0.2.10.	CVE-2020-18756 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.30, R6100 before 1.0.1.16, R7500 before 1.0.0.116, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR4300v2 before 1.0.0.48, WNDR4300v1 before 1.0.2.90, and WNDR4500v3 before 1.0.0.48.	CVE-2020-18757 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6300v2 before 1.0.4.8, R6400 before 1.0.1.22, R6400v2 before 1.0.2.32, R6700 before 1.0.1.20, R6900 before 1.0.1.20, WNR3500Lv2 before 1.2.0.44, and WNR2000v2 before 1.2.0.8.	CVE-2020-18765 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	CVE-2020-21165 yes calculated CONFIRM
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DGN2200Bv4 before 1.0.0.102, DGN2200v4 before 1.0.0.102, EX3700 before 1.0.0.70, EX3800 before 1.0.0.70, EX6000 before 1.0.0.30, EX6100 before 1.0.2.22, EX6120 before 1.0.0.40, EX6130 before 1.0.0.22, EX6150 before 1.0.0.38, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6300v2 before	CVE-2020-21163 yes

	1.0.4.22, R6900P before 1.3.0.18, R7000P before 1.3.0.18, R7300DST before 1.0.0.62, R7900P before 1.3.0.10, R8000 before 1.0.4.12, R8000P before 1.3.0.10, WN2500RPv2 before 1.0.1.52, and WNDR3400v3 before 1.0.1.18.	<a href="#">CVE-2007-2117</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D6400 before 1.0.0.78, EX6200 before 1.0.3.86, EX7000 before 1.0.0.64, R6250 before 1.0.4.8, R6300v2 before 1.0.4.6, R6400 before 1.0.1.12, R6700 before 1.0.1.16, R7000 before 1.0.4.12, R7100LG before 1.0.0.42, R7300DST before 1.0.0.44, R7900 before 1.0.1.12, R8000 before 1.0.3.36, R8300 before 1.0.2.74, R8500 before 1.0.2.74, WNDR3400v3 before 1.0.1.14, and WNR3500Lv2 before 1.2.0.48.	<a href="#">CVE-2007-2118</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R6100 before 1.0.1.20, R7800 before 1.0.2.40, and R9000 before 1.0.2.52.	<a href="#">CVE-2007-2117</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by an attacker's ability to read arbitrary files. This affects EX3700 before 1.0.0.64, EX3800 before 1.0.0.64, EX6120 before 1.0.0.32, EX6130 before 1.0.0.16, R6300v2 before 1.0.4.12, R6700 before 1.0.1.26, R6900 before 1.0.1.22, R7000 before 1.0.9.6, R7300DST before 1.0.0.52, R7900 before 1.0.1.12, R8000 before 1.0.3.24, and R8500 before 1.0.2.94.	<a href="#">CVE-2007-2117</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2007-2117</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2007-2117</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects R6700 before 1.0.1.48, R7900 before 1.0.2.16, R6900 before 1.0.1.48, R7000P before 1.3.1.44, R6900P before 1.3.1.44, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R7000 before 1.0.9.34, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R7900P before 1.4.1.24, R8500 before 1.0.2.122, R8300 before 1.0.2.122, WN2500RPv2 before 1.0.1.54, EX3700 before 1.0.0.72, EX3800 before 1.0.0.72, EX6000 before 1.0.0.32, EX6100 before 1.0.2.24, EX6120 before 1.0.0.42, EX6130 before 1.0.0.24, EX6150v1 before 1.0.0.42, EX6200 before 1.0.3.88, EX7000 before 1.0.0.66, D7000v2 before 1.0.0.51, D6220 before 1.0.0.46, D6400 before 1.0.0.82, and D8500 before 1.0.3.42.	<a href="#">CVE-2007-2118</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.52, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, and WNDR4500v3 before 1.0.0.48.	<a href="#">CVE-2007-2117</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, DM200 before 1.0.0.50, R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	<a href="#">CVE-2007-2118</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D7800 before 1.0.1.34, R7800 before 1.0.2.46, and R9000 before 1.0.3.16.	<a href="#">CVE-2007-2118</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.00.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2007-2117</a> yes calculated <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects D7800 before 1.0.1.34, R7500v2 before 1.0.3.26, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR4300v2 before 1.0.0.54, and WNDR4500v3 before	<a href="#">CVE-2007-2118</a> yes calculated <a href="#">CONFIRM</a>



	1.0.0.54.	<a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D3600 before 1.0.0.61, D6000 before 1.0.0.61, D6100 before 1.0.0.55, D7800 before 1.0.1.28, R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, R9000 before 1.0.2.40, WNDR3700v4 before 1.0.2.88, WNDR4300 before 1.0.2.90, WNDR4300v2 before 1.0.0.48, WNDR4500v3 before 1.0.0.48, and WNR2000v5 before 1.0.0.58.	<a href="#">CVE-2020-18740</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6250 before 1.0.4.8, R6300v2 before 1.0.4.8, R6700 before 1.0.1.20, R7000 before 1.0.7.10, R7000P before 1.0.0.58, R6900P before 1.0.0.58, R7100LG before 1.0.0.32, R7900 before 1.0.1.14, R8000 before 1.0.3.22, and R8500 before 1.0.2.94.	<a href="#">CVE-2020-18741</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R6100 before 1.0.1.16, R7500 before 1.0.0.112, R7500v2 before 1.0.3.20, R7800 before 1.0.2.36, and WNR2000v5 before 1.0.0.58.	<a href="#">CVE-2020-18731</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects DM200 before 1.0.0.52, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.16, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	<a href="#">CVE-2020-21144</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by CSRF. This affects JR6150 before 1.0.1.10, R6050 before 1.0.1.10, R6250 before 1.0.4.12, R6300v2 before 1.0.4.8, R6700 before 1.0.1.16, R6900 before 1.0.1.16, R7300DST before 1.0.0.54, R7900 before 1.0.1.12, R8000 before 1.0.3.32, and R8500 before 1.0.2.74.	<a href="#">CVE-2020-18742</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by denial of service. This affects R6100 before 1.0.1.22, R7500 before 1.0.0.122, R7800 before 1.0.2.42, R8900 before 1.0.3.10, R9000 before 1.0.3.10, WNDR3700v4 before 1.0.2.96, WNDR4300 before 1.0.2.98, WNDR4300v2 before 1.0.0.54, WNDR4500v3 before 1.0.0.54, and WNR2000v5 before 1.0.0.64.	<a href="#">CVE-2020-21142</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects D1500 before 1.0.0.27, D500 before 1.0.0.27, D6100 before 1.0.0.58, D6200 before 1.1.0.30, D6220 before 1.0.0.46, D6400 before 1.0.0.82, D7000 before 1.0.1.68, D7000v2 before 1.0.0.51, D7800 before 1.0.1.42, D8500 before 1.0.3.42, DC112A before 1.0.0.40, DGN2200Bv4 before 1.0.0.102, DGN2200v4 before 1.0.0.102, JNR1010v2 before 1.1.0.54, JR6150 before 1.0.1.18, JWNR2010v5 before 1.1.0.54, PR2000 before 1.0.0.24, R6020 before 1.0.0.34, R6050 before 1.0.1.18, R6080 before 1.0.0.34, R6100 before 1.0.1.22, R6120 before 1.0.0.42, R6220 before 1.1.0.68, R6250 before 1.0.4.30, R6300v2 before 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.60, R6700 before 1.0.1.48, R6700v2 before 1.2.0.24, R6800 before 1.2.0.24, R6900 before 1.0.1.48, R6900P before 1.3.1.44, R6900v2 before 1.2.0.24, R7000 before 1.0.9.34, R7000P before 1.3.1.44, R7100LG before 1.0.0.48, R7300 before 1.0.0.68, R7500 before 1.0.0.124, R7500v2 before 1.0.3.38, R7900 before 1.0.2.16, R7900P before 1.4.1.24, R8000 before 1.0.4.18, R8000P before 1.4.1.24, R8300 before 1.0.2.122, R8500 before 1.0.2.122, WN3000RP before 1.0.0.68, WN3000RPv2 before 1.0.0.68, WNDR3400v3 before 1.0.1.18, WNDR3700v4 before 1.0.2.102, WNDR3700v5 before 1.1.0.54, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.56, WNR1000v4 before 1.1.0.54, WNR2020 before 1.1.0.54, WNR2050 before 1.1.0.54, and WNR3500Lv2 before 1.2.0.54.	<a href="#">CVE-2020-21139</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an unauthenticated attacker. This affects D6200 before 1.1.0.24, R6020 before 1.0.0.30, R6080 before 1.0.0.30, R6120 before 1.0.0.36, R6700v2 before 1.1.0.42, R6800 before 1.1.0.42, and R6900v2 before 1.1.0.42.	<a href="#">CVE-2020-18730</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- r6220_and_wndr3700_devices	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6220 before 1.1.0.64 and WNDR3700v5 before 1.1.0.54.	<a href="#">CVE-2020-21164</a> Not yet calculated. <a href="#">CONFIRM</a>
netgear -- r6220_devices	NETGEAR R6220 devices before 1.1.0.60 are affected by incorrect configuration of security settings.	<a href="#">CVE-2020-18702</a> Not yet calculated. <a href="#">CONFIRM</a>

netgear -- r6700_devices	Certain NETGEAR devices are affected by reflected XSS. This affects R6700 before 1.0.1.36 and R6900 before 1.0.1.34.	<a href="#">CVE-2020-18701</a> yes calculated <a href="#">CONFIRM</a>
netgear -- r7800_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	<a href="#">CVE-2020-18697</a> yes calculated <a href="#">CONFIRM</a>
netgear -- r7800_devices_and_r9000_devices	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects R7800 before 1.0.2.40 and R9000 before 1.0.2.52.	<a href="#">CVE-2020-18699</a> yes calculated <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by a buffer overflow by an authenticated user. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	<a href="#">CVE-2020-18707</a> yes calculated <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by CSRF. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	<a href="#">CVE-2020-18708</a> yes calculated <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects R8300 before 1.0.2.94 and R8500 before 1.0.2.94.	<a href="#">CVE-2020-18709</a> yes calculated <a href="#">CONFIRM</a>
netgear -- r8300_and_r8500_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects R8300 before 1.0.2.106 and R8500 before 1.0.2.106.	<a href="#">CVE-2020-18710</a> yes calculated <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	<a href="#">CVE-2020-18102</a> yes calculated <a href="#">CONFIRM</a>
netgear -- readynas_devices	NETGEAR ReadyNAS devices before 6.9.3 are affected by CSRF.	<a href="#">CVE-2020-18160</a> yes calculated <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	<a href="#">CVE-2020-18809</a> yes calculated <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	<a href="#">CVE-2020-18813</a> yes calculated <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices, running ReadyNAS OS versions prior to 6.8.0 are affected by incorrect configuration of security settings.	<a href="#">CVE-2020-18819</a> yes calculated <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	<a href="#">CVE-2020-18812</a> yes calculated <a href="#">CONFIRM</a>
netgear -- readynas_os	NETGEAR ReadyNAS OS 6 devices running ReadyNAS OS versions prior to 6.8.0 are affected by stored XSS.	<a href="#">CVE-2020-18811</a> yes calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-18126</a> yes calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by authentication bypass. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-18128</a> yes calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-18127</a> yes calculated <a href="#">CONFIRM</a>

netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-2018-0330</a> yes calculated <a href="#">CONFIRM</a>
netgear -- wac505_and_wac510_devices	Certain NETGEAR devices are affected by disclosure of sensitive information. This affects WAC505 before 5.0.0.17 and WAC510 before 5.0.0.17.	<a href="#">CVE-2020-2018-129</a> yes calculated <a href="#">CONFIRM</a>
netgear -- wac510_devices	NETGEAR WAC510 devices before 5.0.0.17 are affected by privilege escalation.	<a href="#">CVE-2020-2018-2124</a> yes calculated <a href="#">CONFIRM</a>
netgear -- wac510_devices	NETGEAR WAC510 devices before 5.0.0.17 are affected by authentication bypass.	<a href="#">CVE-2020-2018-2125</a> yes calculated <a href="#">CONFIRM</a>
netgear -- wndr4500_devices	NETGEAR WNDR4500v3 devices before 1.0.0.48 are affected by denial of service.	<a href="#">CVE-2020-2017-0714</a> yes calculated <a href="#">CONFIRM</a>
ntop -- ndpi	In nDPI through 3.2 Stable, the SSH protocol dissector has multiple KEXINIT integer overflows that result in a controlled remote heap overflow in concat_hash_string in ssh.c. Due to the granular nature of the overflow primitive and the ability to control both the contents and layout of the nDPI library's heap memory through remote input, this vulnerability may be abused to achieve full Remote Code Execution against any network inspection stack that is linked against nDPI and uses it to perform network traffic analysis.	<a href="#">CVE-2020-0939</a> yes dated <a href="#">MISC</a>
ntop -- ndpi	In nDPI through 3.2 Stable, an out-of-bounds read in concat_hash_string in ssh.c can be exploited by a network-positioned attacker that can send malformed SSH protocol messages on a network segment monitored by nDPI's library.	<a href="#">CVE-2020-0940</a> yes dated <a href="#">MISC</a>
opc_foundation -- ua.net_standard	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of OPC Foundation UA .NET Standard 1.04.358.30. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of sessions. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to create a denial-of-service condition against the application. Was ZDI-CAN-10295.	<a href="#">CVE-2020-0867</a> yes dated <a href="#">MISC</a>
openssl -- openssl	Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).	<a href="#">CVE-2020-1967</a> yes <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">FREEBSD</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
oppo -- coloros	In ColorOS (oppo mobile phone operating system, based on AOSP frameworks/native code position/services/surfaceflinger surfaceflinger.CPP), RGB is defined on the stack but uninitialized, so when the screenShot function to RGB value assignment, will not initialize the value is returned to the attackers, leading to values on the stack information leakage, the vulnerability can be used to bypass attackers ALSR.	<a href="#">CVE-2020-0828</a> yes calculated <a href="#">CONFIRM</a>
paypal-adaptive -- paypal-adpative	paypal-adaptive through 0.4.2 manipulation of JavaScript objects resulting in Prototype Pollution. The PayPal function could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload.	<a href="#">CVE-2020-0843</a> yes dated <a href="#">MISC</a>
		<a href="#">CVE-</a>

phproject -- phproject	In Phproject before version 1.7.8, there's a vulnerability which allows users with access to file uploads to execute arbitrary code. This is patched in version 1.7.8.	<a href="#">CVE-2020-14011</a> Verified Calculated CONFIRM
plex -- media_server	Improper Input Validation in Plex Media Server on Windows allows a local, unauthenticated attacker to execute arbitrary Python code with SYSTEM privileges.	<a href="#">CVE-2020-5740</a> Verified Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is improper access control on customers search. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-5487</a> Verified Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there are improper access controls on product page with combinations, attachments and specific prices. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-5493</a> Verified Calculated CONFIRM
prestashop -- prestashop	"In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there is improper access controls on product attributes page. The problem is fixed in 1.7.6.5.	<a href="#">CVE-2020-5488</a> Verified Calculated CONFIRM
prestashop -- prestashop	In PrestaShop between versions 1.5.0.0 and 1.7.6.5, there are improper access control since the the version 1.5.0.0 for legacy controllers. - admin-dev/index.php/configure/shop/customer-preferences/ - admin-dev/index.php/improve/international/translations/ - admin-dev/index.php/improve/international/geolocation/ - admin-dev/index.php/improve/international/localization - admin-dev/index.php/configure/advanced/performance - admin-dev/index.php/sell/orders/delivery-slips/ - admin-dev/index.php?controller=AdminStatuses The problem is fixed in 1.7.6.5	<a href="#">CVE-2020-5479</a> Verified Calculated CONFIRM
python-markdown2 -- python-markdown2	python-markdown2 through 2.3.8 allows XSS because element names are mishandled unless a \w+ match succeeds. For example, an attack might use elementname@ or elementname- with an onclick attribute.	<a href="#">CVE-2020-11888</a> Verified Calculated MISC
rapid7 -- metasploit_framework	Rapid7 Metasploit Framework versions before 5.0.85 suffers from an instance of CWE-78: OS Command Injection, wherein the Inotify plugin accepts untrusted user-supplied data via a remote computer's hostname or service name. An attacker can create a specially-crafted hostname or service name to be imported by Metasploit from a variety of sources and trigger a command injection on the operator's terminal. Note, only the Metasploit Framework and products that expose the plugin system is susceptible to this issue -- notably, this does not include Rapid7 Metasploit Pro. Also note, this vulnerability cannot be triggered through a normal scan operation -- the attacker would have to supply a file that is processed with the db_import command.	<a href="#">CVE-2020-7350</a> Verified Calculated CONFIRM
re2c -- re2c	re2c 1.3 has a heap-based buffer overflow in Scanner::fill in parse/scanner.cc via a long lexeme.	<a href="#">CVE-2020-10458</a> Verified Calculated MISC MISC MISC
red_hat -- openshift_container_platform	A flaw was found in openshift-ansible. OpenShift Container Platform (OCP) 3.11 is too permissive in the way it specified CORS allowed origins during installation. An attacker, able to man-in-the-middle the connection between the user's browser and the openshift console, could use this flaw to perform a phishing attack. The main threat from this vulnerability is data confidentiality.	<a href="#">CVE-2020-10741</a> Verified Calculated CONFIRM
red_hat -- openshift_container_platform	A flaw was found in OpenShift Container Platform version 4.1 and later. Sensitive information was found to be logged by the image registry operator allowing an attacker able to gain access to those logs, to read and write to the storage backing the internal image registry. The highest threat from this vulnerability is to data integrity.	<a href="#">CVE-2020-10712</a> Verified Calculated CONFIRM
red_hat -- undertow	A flaw was found in all undertow-2.x.x SP1 versions prior to undertow-2.0.30.SP1, all undertow-1.x.x and undertow-2.x.x versions prior to undertow-2.1.0.Final, where the Servlet container causes servletPath to normalize incorrectly by truncating the path after semicolon which may	<a href="#">CVE-2020-1757</a> Verified Calculated CONFIRM



	lead to an application mapping resulting in the security bypass.	
sap -- erp_and_s/4_hana	Egypt localized withholding tax reports Clearing of Liabilities and Remittance Statement and Summary in SAP ERP (versions 618, 730, EAPPLGLO 607) and S/4 HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user, allowing reading or modification of some tax reports, due to Missing Authorization Check.	<a href="#">CVE-2020-0412</a> Calculated MISC
sap -- netweaver_as_abap	SAP NetWeaver AS ABAP Business Server Pages Test Application SBSPEXT_PHTMLB, versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, is vulnerable to reflected Cross-Site Scripting (XSS) via different URL parameters as it does not sufficiently encode user controlled inputs.	<a href="#">CVE-2020-0413</a> Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers.	<a href="#">CVE-2020-0487</a> Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') vulnerability exists on EcoStruxure Machine Expert – Basic or SoMachine Basic programming software (versions in security notification). The result of this vulnerability, DLL substitution, could allow the transference of malicious code to the controller.	<a href="#">CVE-2020-0489</a> Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers.	<a href="#">CVE-2020-0488</a> Calculated MISC
schneider_electric -- multiple_modicon_controllers	A CWE-798: Use of Hardcoded Credentials vulnerability exists in Modicon Controllers (All versions of the following CPUs and Communication Module product references listed in the Security Notifications), which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.	<a href="#">CVE-2020-0459</a> Calculated MISC
schneider_electric -- v_jeo_designer_and_v_jeo_designer_basic	A CWE-426: Untrusted Search Path vulnerability exists in Vjeo Designer Basic (V1.1 HotFix 15 and prior) and Vjeo Designer (V6.9 SP9 and prior), which could cause arbitrary code execution on the system running Vjeo Basic when a malicious DLL library is loaded by the Product.	<a href="#">CVE-2020-0490</a> Calculated MISC
simplesamlphp -- simplesamlphp	SimpleSAMLphp versions before 1.18.6 contain an information disclosure vulnerability. The module controller in 'SimpleSAMLModule' that processes requests for pages hosted by modules, has code to identify paths ending with '.php' and process those as PHP code. If no other suitable way of handling the given path exists it presents the file to the browser. The check to identify paths ending with '.php' does not account for uppercase letters. If someone requests a path ending with e.g. '.PHP' and the server is serving the code from a case-insensitive file system, such as on Windows, the processing of the PHP code does not occur, and the source code is instead presented to the browser. An attacker may use this issue to gain access to the source code in third-party modules that is meant to be private, or even sensitive. However, the attack surface is considered small, as the attack will only work when SimpleSAMLphp serves such content from a file system that is not case-sensitive, such as on Windows. This issue is fixed in version 1.18.6.	<a href="#">CVE-2020-0401</a> Calculated CONFIRM
sonatype -- nexus_repository_manager	An issue was discovered in Sonatype Nexus Repository Manager in versions 3.21.1 and 3.22.0. It is possible for a user with appropriate privileges to create, modify, and execute scripting tasks without use of the UI or API. NOTE: in 3.22.0, scripting is disabled by default (making this not exploitable).	<a href="#">CVE-2020-01753</a> Calculated CONFIRM
squid -- squid	An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials).	<a href="#">CVE-2020-11945</a> MISC CONFIRM Calculated CONFIRM MISC
	In Saml2 Authentication Services for ASP.NET versions before 1.0.2, and between 2.0.0 and 2.6.0, there is a vulnerability in how tokens are validated in some cases. Saml2 tokens are usually used as bearer tokens - a caller that presents a token is assumed to be the subject of the token. There is also support in the Saml2 protocol for issuing tokens that is tied	<a href="#">CVE-2020-</a>

sustainsys -- saml2	to a subject through other means, e.g. holder-of-key where possession of a private key must be proved. The Sustainsys.Saml2 library incorrectly treats all incoming tokens as bearer tokens, even though they have another subject confirmation method specified. This could be used by an attacker that could get access to SAML2 tokens with another subject confirmation method than bearer. The attacker could then use such a token to create a log in session. This vulnerability is patched in versions 1.0.2 and 2.7.0.	<a href="#">CVE-2020-10568</a> <a href="#">MISC</a> <a href="#">MISC</a> dated <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysaid -- sysaid_on-premise	SysAid On-Premise 20.1.11, by default, allows the AJP protocol port, which is vulnerable to a GhostCat attack. Additionally, it allows unauthenticated access to upload files, which can be used to execute commands on the system by chaining it with a GhostCat attack.	<a href="#">CVE-2020-10569</a> <a href="#">MISC</a> <a href="#">MISC</a> calculated
tata_sonata -- smart_sf_rush_devices	An issue was discovered on Tata Sonata Smart SF Rush 1.12 devices. It has been identified that the smart band has no pairing (mode 0 Bluetooth LE security level) The data being transmitted over the air is not encrypted. Adding to this, the data being sent to the smart band doesn't have any authentication or signature verification. Thus, any attacker can control a parameter of the device.	<a href="#">CVE-2020-10539</a> <a href="#">MISC</a> dated <a href="#">MISC</a>
teeworlds -- teeworlds	Teeworlds before 0.7.4 has an integer overflow when computing a tilemap size.	<a href="#">CVE-2020-10787</a> <a href="#">MISC</a> calculated
teeworlds -- teeworlds	CServer::SendMsg in engine/server/server.cpp in Teeworlds 0.7.x before 0.7.5 allows remote attackers to shut down the server.	<a href="#">CVE-2020-10066</a> <a href="#">MISC</a> dated <a href="#">MISC</a>
tortoise-orm -- tortoise-orm	In Tortoise ORM before versions 0.15.23 and 0.16.6, various forms of SQL injection have been found for MySQL and when filtering or doing mass-updates on char/text fields. SQLite & PostgreSQL are only affected when filtering with contains, starts_with, or ends_with filters (and their case-insensitive counterparts).	<a href="#">CVE-2020-10010</a> <a href="#">MISC</a> dated <a href="#">CONFIRM</a>
toshiba -- multiple_devices	SHARP AQUOS series (AQUOS SH-M02 build number 01.00.05 and earlier, AQUOS SH-RM02 build number 01.00.04 and earlier, AQUOS mini SH-M03 build number 01.00.04 and earlier, AQUOS Keitai SH-N01 build number 01.00.01 and earlier, AQUOS L2 (UQ mobile/J:COM) build number 01.00.05 and earlier, AQUOS sense lite SH-M05 build number 03.00.04 and earlier, AQUOS sense (UQ mobile) build number 03.00.03 and earlier, AQUOS compact SH-M06 build number 02.00.02 and earlier, AQUOS sense plus SH-M07 build number 02.00.02 and earlier, AQUOS sense2 SH-M08 build number 02.00.05 and earlier, and AQUOS sense2 (UQ mobile) build number 02.00.06 and earlier) allow an attacker to obtain the sensitive information of the device via malicious applications installed on the device.	<a href="#">CVE-2020-5471</a> <a href="#">MISC</a> dated <a href="#">MISC</a>
toshiba -- multiple_devices	An unquoted search path vulnerability exists in HDD Password tool (for Windows) version 1.20.6620 and earlier which is stored in CANVIO PREMIUM 3TB(HD-MB30TY, HD-MA30TY, HD-MB30TS, HD-MA30TS), CANVIO PREMIUM 2TB(HD-MB20TY, HD-MA20TY, HD-MB20TS, HD-MA20TS), CANVIO PREMIUM 1TB(HD-MB10TY, HD-MA10TY, HD-MB10TS, HD-MA10TS), CANVIO SLIM 1TB(HD-SB10TK, HD-SB10TS), and CANVIO SLIM 500GB(HD-SB50GK, HD-SA50GK, HD-SB50GS, HD-SA50GS), and which was downloaded before 2020 May 10. Since it registers Windows services with unquoted file paths, when a registered path contains spaces, and a malicious executable is placed on a certain path, it may be executed with the privilege of the Windows service.	<a href="#">CVE-2020-5469</a> <a href="#">MISC</a> dated <a href="#">MISC</a>
tss-lib -- tss-lib	The keygen protocol implementation in Binance tss-lib before 1.2.0 allows attackers to generate crafted h1 and h2 parameters in order to compromise a signing round or obtain sensitive information from other parties.	<a href="#">CVE-2020-10118</a> <a href="#">MISC</a> dated <a href="#">MISC</a>
veeam -- one_agent	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the HandshakeResult method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-10401.	<a href="#">CVE-2020-10915</a> <a href="#">MISC</a> dated <a href="#">MISC</a>
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of VEEAM One Agent 9.5.4.4587. Authentication is not required to exploit this vulnerability. The specific flaw exists within the	<a href="#">CVE-2020-</a>

veeam -- one_agent	PerformHandshake method. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of the service account. Was ZDI-CAN-10400.	<a href="#">CVE-2020-14914</a> 2020- yes calculated <a href="#">MISC</a>
vesta -- vesta_control_panel	A remote command execution in Vesta Control Panel through 0.9.8-26 allows any authenticated user to execute arbitrary commands on the system via cron jobs.	<a href="#">CVE-2020-10786</a> 2020- yes calculated <a href="#">MISC</a>
vesta -- vesta_control_panel	An elevation of privilege in Vesta Control Panel through 0.9.8-26 allows an attacker to gain root system access from the admin account via v-change-user-password (aka the user password change script).	<a href="#">CVE-2020-10787</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- wordpress	The responsive-add-ons plugin before 2.2.7 for WordPress has incorrect access control for wp-admin/admin-ajax.php?action= requests.	<a href="#">CVE-2020-10773</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- wordpress	The mappress-google-maps-for-wordpress plugin before 2.53.9 for WordPress does not correctly implement AJAX functions with nonces (or capability checks), leading to remote code execution.	<a href="#">CVE-2020-14077</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- wordpress	The Catch Breadcrumb plugin before 1.5.4 for WordPress allows Reflected XSS via the s parameter (a search query). Also affected are 16 themes (if the plugin is enabled) by the same author: Alchemist and Alchemist PRO, Izabel and Izabel PRO, Chique and Chique PRO, Clean Enterprise and Clean Enterprise PRO, Bold Photography PRO, Intuitive PRO, Devotepress PRO, Clean Blocks PRO, Foodoholic PRO, Catch Mag PRO, Catch Wedding PRO, and Higher Education PRO.	<a href="#">CVE-2020-14054</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- wordpress	The Advanced Woo Search plugin version through 1.99 for Wordpress suffers from a sensitive information disclosure vulnerability in every ajax search request via the sql field to includes/class-aws-search.php.	<a href="#">CVE-2020-12070</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- wordpress	The users-customers-import-export-for-wp-woocommerce plugin before 1.3.9 for WordPress allows subscribers to import administrative accounts via CSV.	<a href="#">CVE-2020-10774</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- wordpress	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks capability checks for AJAX actions.	<a href="#">CVE-2020-12075</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- wordpress	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks CSRF nonce checks for AJAX actions. One consequence of this is stored XSS.	<a href="#">CVE-2020-12076</a> 2020- yes calculated <a href="#">MISC</a>
wordpress -- worpdress	An issue was discovered in Elementor 2.7.4. Arbitrary file upload is possible in the Elementor Import Templates function, allowing an attacker to execute code via a crafted ZIP archive.	<a href="#">CVE-2020-14055</a> 2020- yes calculated <a href="#">MISC</a>
zoho -- manageengine_opmanager	Zoho ManageEngine OpManager before 125120 allows an unauthenticated user to retrieve an API key via a servlet call.	<a href="#">CVE-2020-11946</a> 2020- yes calculated <a href="#">MISC</a>
zulip -- zulip_server	Zulip Server before 2.1.3 allows XSS via the modal_link feature in the Markdown functionality.	<a href="#">CVE-2020-9445</a> 2020- yes calculated <a href="#">CONFIRM</a>
zulip -- zulip_server	Zulip Server before 2.1.3 allows reverse tabnabbing via the Markdown functionality.	<a href="#">CVE-2020-9444</a> 2020- yes calculated <a href="#">CONFIRM</a>
zulip -- zulip_server	Zulip Server before 2.1.3 allows XSS via a Markdown link, with resultant account takeover.	<a href="#">CVE-2020-94935</a> 2020- yes calculated <a href="#">CONFIRM</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870





From: [Homeland Security News Wire](#)  
To: [info@hcn.sunnyvale.ca.us](mailto:info@hcn.sunnyvale.ca.us)  
Subject: COVID-19 Weekly Roundup  
Date: Sunday, April 26, 2020 2:29:58 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



## COVID-19 WEEKLY ROUNDUP

BIOMETRICS BORDER/IMMIG. BUSINESS CYBERSECURITY DETECTION DISASTERS GOVERNMENT INFRASTRUCTURE  
PUBLIC HEALTH PUBLIC SAFETY REGIONAL SCI-TECH SURVEILLANCE TERRORISM TRANSPORTATION WATER

Sunday 26 April 2020 vol. 14 no. 27

### The Brief

## Economic Reopening Begins, as Two Promising Drugs Suffer Setbacks

Five things, among many others, caught our eye this week: On Saturday, the number of worldwide coronavirus deaths passed 205,000, with the U.S. death toll reaching 55,094; European governments outlined their plans for reopening their economy, and several have started on the process of going back to normal, or, rather, the new normal; the FDA issued a stern warning that hydroxychloroquine, alone or in combination with azithromycin – touted by President Trump as “game changers” – should not be used to treat COVID-19 outside of a hospital or formal clinical trial; a similar disappointment befell the antiviral medicine remdesivir from Gilead Sciences, which failed to speed the improvement of patients with COVID-19 or prevent them from dying; the Justice Department got a court order to stop a Florida church from selling on its website an industrial bleach which the church marketed as a miracle treatment for the virus – the DOJ move came a few days before last Thursday’s White House briefing, in which Trump mused about whether household disinfectant injections or ingestion could be effective in treating the coronavirus.

[Read more](#)

### COVID-19: Update

## Trump Adds Confusion on COVID-19 Treatments as U.S. Deaths Top 50,000

Direct sunlight, injected disinfectants, heat. Those were some of the remedies for coronavirus infection President Donald Trump mentioned during yesterday’s White House task force briefing. Today the manufacturers of Lysol and Dettol cleaners, as well as the Environmental Protection Agency (EPA) and the CDC, issued statements and warnings contradicting Trump’s remarks. They warned consumers against ingesting any disinfectants, and urged them to follow the warning labels on disinfectants containers. The FDA on Friday has issued a strong statement urging doctors and patients not to use hydroxychloroquine and azithromycin to treat COVID-19 patients outside of controlled medical trials. The warning came after the largest retrospective test of the two compounds has proven ineffective in treating the disease relative to a placebo, while having serious side effects, including death, in some cases. The U.S. has so far recorded 884,004 cases and 50,360 deaths.

[Read more](#)

### COVID-19: Origins

## The New Coronavirus Was Not Man-Made, Study Shows

New research finds that SARS-CoV-2, the new coronavirus that causes COVID-19, is the result of the natural process of evolution rather than a product of laboratory engineering. Ana Sandoiu writes in *Medical News Today* that in the new study, which appears in the journal *Nature Medicine*, Kristian Andersen, Ph.D., an associate professor of immunology and microbiology at the Scripps Research Institute in La Jolla, CA, and

colleagues set out to see what they could deduce about the origin of the new coronavirus from analyzing the genomic data available. As the authors mention in their paper, since the start of the COVID-19 outbreak, researchers have been trying to grapple with the origins of the virus that caused it. The scientists found that the receptor-binding domain of the spike protein had evolved to target ACE2 so effectively that it could only have been the result of natural selection and not of genetic engineering. Furthermore, the molecular structure of the backbone of SARS-CoV-2 supported this finding. If scientists had engineered the new coronavirus purposely as a pathogen, explain the researchers, the starting point would likely have been the backbone of another virus in the coronavirus family.

[Read more](#)

#### Tracing

### France, Europe Mull Controversial Coronavirus Tracing Apps

France's parliament votes next week on plans to use a controversial tracing app to help fight the coronavirus, as the country eases its lockdown next month. Lisa Bryant writes in *VOA News* that French Digital Affairs Minister Cedric O says the downloadable app would notify smartphone users when they cross people with COVID-19, helping authorities track and reduce the spread of the pandemic. In a video on the ruling party's Facebook page, O said the so-called "Stop COVID" app will fully respect people's liberties, and will be completely voluntary and anonymous. It also will be temporary — lasting only as long as the pandemic, he added. The government wants to launch the app on May 11, the date it has set to begin easing a two-month lockdown in the country. It initially announced a parliamentary debate on the technology, but that's been changed to a vote, after major pushback from lawmakers.

[Read more](#)

#### Testing

### Israel Launches New “Contactless” Roadside COVID-19 Testing Booths Which Have Zero Contact between Nurse and Patient

Israel has launched a network of new 'contactless' roadside covid-19 testing booths which have zero contact between nurse and patient. The *Daily Mail* reports that the country has offered to share the design, which is relatively cheap and easy to produce, with other countries as part of the fight against the coronavirus pandemic. The booths, produced by healthcare companies together with civilian and military partners, provide an entirely sealed, sterile environment for the medic, and can be quickly disinfected between patients. Tests are carried out using two rubber gloves which are attached to the outer wall with airtight seals. Results are processed in a matter of hours and reported directly via the patient's electronic health record.

[Read more](#)

#### Antibodies

### Abbott Launches COVID-19 Antibody Test

Abbott has launched its third test for coronavirus (COVID-19) and will start shipping it in the U.S. The test is a serology test – also called an antibody test – which could be a critical next step in battling this virus. Abbott says its test helps to detect the **IgG antibody to SARS-CoV-2**. An antibody is a protein that the body produces in the late stages of infection and may remain for up to months and possibly years after a person has recovered. Detecting these IgG antibodies will help determine if a person was previously infected with the virus that causes COVID-19. The new antibody test is to be used on Abbott's ARCHITECT i1000SR and i2000SR laboratory instruments, which can run up to 100-200 tests an hour.

[Read more](#)

### Antibody Tests for Coronavirus Can Miss the Mark

Dozens of blood tests are rapidly coming on the market to identify

people who have been exposed to the coronavirus by checking for antibodies against it. The Food and Drug Administration doesn't set standards for these kinds of tests, but even those that meet the government's informal standard may produce many false answers and provide false assurances. The imperfect results could be a big disappointment to people who are looking toward these tests to help them return to something resembling a normal life. First of all, it's not clear whether someone who has antibodies to the coronavirus in their blood is actually immune. Your body produces these antibodies within about a week of infection. Another problem is that test results are wrong much more frequently than you might expect. While tests may truthfully say they are more than 90% accurate, in practical use they can often perform far below that level.

[Read more](#)

#### Vaccines

### Britain Starts Testing Vaccine for Coronavirus on Humans

Britain has performed the first human trial of a coronavirus vaccine in Europe. Zlatica Hoke writes in *VOA News* that two volunteers were injected Thursday in the city of Oxford, where a university team developed the vaccine in less than three months. Hundreds of other volunteers will be injected with the trial vaccine, and the same number will get a vaccine for meningitis so the results can be compared. Volunteers will not know which vaccine they are getting. The trial offers new hope just as an antiviral drug – remdesivir -- proved ineffective against coronavirus on patients in China.

[Read more](#)

### Coronavirus: Could the Pandemic Be Controlled Using Existing Vaccines Like MMR or BCG?

The race is on to develop a vaccine that can protect us from the COVID-19 pandemic. An impressive **115 vaccine candidates** are currently being investigated, but it is still many months before a vaccine might be approved. Sarah L Caddy writes in *The Conversation* that we already have hundreds of licensed vaccines for over 25 different viruses and bacteria that infect humans. We can protect ourselves against infections ranging from cholera to rabies. The common aim of all vaccines is to induce an immune response that prevents future disease. Is it possible that one of these existing vaccines could also induce protection against SARS-CoV-2, the virus causing COVID-19? Repurposing drugs is a popular strategy for treating COVID-19, as exemplified by the **many trials** using the Ebola drug remdesivir, or the antimalarial drug hydroxychloroquine. If an already-approved vaccine could reduce the severity of COVID-19, this would be really good news. The BCG vaccine has received recent attention for being a widely used vaccine that **may help control COVID-19**. A handful of studies identified an interesting association between the severity of COVID-19 in a country and how many of the population were vaccinated with BCG. The BCG vaccine apparently reduces the damage caused by COVID-19.

[Read more](#)

#### Hydroxychloroquine / azithromycin

### Study Calls into Question Use of Malaria Drug for COVID-19

By Chris Dall

A retrospective study of patients with COVID-19 found no evidence that the anti-malaria drug hydroxychloroquine, either with or without the antibiotic azithromycin, reduced mortality or the need for mechanical ventilation. Researchers also found that hydroxychloroquine alone was associated with increased mortality. Early excitement about the combination was based on a small French study, and President Donald Trump soon began touting the combination as a potential "game changer," but the findings from the study, which is the largest to date to report on outcomes from treating COVID-19 patients with the anti-malaria drug and uses a database that has been used for many different

studies, suggest that the hydroxychloroquine/azithromycin combination may not be as promising for treating COVID-19 as some have hoped.

[Read more](#)

## **FDA Warns about Hydroxychloroquine Dangers, Cites Serious Effects**

The Food and Drug Administration (FDA) warned Friday that people should not take chloroquine and hydroxychloroquine to treat COVID-19 outside of a hospital or formal clinical trial, citing reports of “serious heart rhythm problems.” Madeline Farber writes for [Fox News](#) that many of those adverse effects occurred in patients with the virus who were treated with the anti-malaria drugs, often in combination with azithromycin, also known as Z-Pak. President Trump has described such drugs as a potential “game-changer,” although results from clinical trials are not yet in to show whether they are effective. “We will continue to investigate risks associated with the use of hydroxychloroquine and chloroquine for COVID-19 and communicate publicly when we have more information,” the FDA wrote. The adverse events reported include abnormal heart rhythms such as QT interval prolongation, dangerously rapid heart rate called ventricular tachycardia and ventricular fibrillation, and in some cases, death, the agency said. The FDA did not say how many deaths have been reported. Patients who also have other health issues such as heart and kidney disease are likely to be at increased risk of these heart problems when receiving these medicines. The malaria drugs are not approved for use in COVID-19 patients, but the FDA is allowing hydroxychloroquine and chloroquine products donated to the Strategic National Stockpile to be distributed and used in limited circumstances, such as for certain hospitalized patients with COVID-19, the agency noted.

[Read more](#)

**Face masks**

## **NIST Tool Could Help Hospitals Repurpose Rooms for Disinfecting N95 Masks**

In response to the COVID-19 pandemic, hospitals across the United States are disinfecting N95 masks by placing them in repurposed rooms or shipping containers injected with a disinfectant known as vaporized hydrogen peroxide, or VHP. A [new tool](#) from the [National Institute of Standards and Technology](#) (NIST) can help hospitals and medical professionals determine which rooms should be used to disinfect N95 masks. The tool estimates the amount of VHP masks would receive and suggests that larger rooms containing fewer objects, with less-reactive surfaces and slower ventilation, maintain VHP concentration the best.

[Read more](#)

**Make it at home**

## **As the Coronavirus Interrupts Global Supply Chains, People Have an Alternative – Make It at Home**

As COVID-19 [wreaks havoc on global supply chains](#), a [trend of moving manufacturing closer to customers](#) could go so far as to put miniature manufacturing plants in people’s living rooms. Most products in Americans’ homes are labeled “Made in China,” but even those bearing the words “Made in USA” frequently have [parts from China](#) that are now often delayed. The coronavirus pandemic closed so many factories in China that [NASA could observe the resultant drop in pollution from space](#), and some products are becoming harder to find. Joshua M. Pearce writes in [The Conversation](#) that at the same time, there are open-source, freely available digital designs for making millions of items with 3D printers, and their numbers are [growing exponentially](#), as is an interest in open hardware design [in academia](#). Some designs are already being shared for [open-source medical hardware to help during the pandemic](#), like [face shields](#), [masks](#) and [ventilators](#). The free digital product designs go far beyond pandemic hardware. The cost of 3D printers has dropped low enough to be accessible to most Americans. People can download,



customize and print a remarkable range of products at home, and they often end up [costing less than it takes to purchase them](#).

[Read more](#)

#### Hospitalization

### Factors Associated with Hospitalization and Critical Illness among 4,103 Patients with COVID-19 Disease in New York City

Little is known about factors associated with hospitalization and critical illness in COVID-19 positive patients. Christopher M. Petrilli et al. write in [medRxiv](#) that they conducted a cross-sectional analysis of all patients with laboratory-confirmed COVID-19 treated at a single academic health system in New York City between 1 March 2020 and 2 April 2020, with follow up through 7 April 2020. Primary outcomes were hospitalization and critical illness (intensive care, mechanical ventilation, hospice and/or death). The researchers' conclusions: Age and comorbidities are powerful predictors of hospitalization; however, admission oxygen impairment and markers of inflammation are most strongly associated with critical illness.

[Read more](#)

#### Nursing homes

### What the Pandemic Teaches Us about Nursing Home Care

Nested in communities across the US, nursing homes serve as a societal safety net. Nursing homes provide essential care to individuals unable to live in the community. Roughly [1.3 million](#) residents live in nursing homes receiving assistance with daily activities of living such as meals, dressing, and socialization. Additionally, more than [3 million](#) older adults are discharged annually to nursing homes following a hospital stay to receive rehabilitative services like physical therapy and skilled nursing care. The [University of Pennsylvania](#) says that more than 2,000 nursing homes in the US have reported Covid-19 cases within their facilities, often accompanied by [heart-wrenching rates of death](#). Combatting the avalanche of death posed by the novel coronavirus in nursing homes requires concerted effort to align several conflicting priorities that have afflicted nursing homes for years. Covid-19 puts into full view the regulatory structures and payment models that jeopardize care for long term care residents and those receiving post-acute care.

[Read more](#)

#### Real U.K. toll

### The Real U.K. Coronavirus Death Toll Is Much Higher Than First Feared

Every day the number of COVID-19 deaths reported from hospitals across the U.K. make headlines. But every time they are underestimates of the true death toll, just a snapshot of what is happening in wards across the country. Dominic Gilbert writes in [The Telegraph](#) that for a better estimate of the scale of the pandemic in the UK, the total number of deaths, including those not linked to coronavirus, hold some clues. Thousands of excess deaths are now being reported across the country, leading to the highest weekly death toll since records began. And amid a meagre testing regime which has not yet passed 20,000 people a day, the number of deaths linked to Covid-19 is likely to be vastly understated.

[Read more](#)

#### U.K.

### Coronavirus: The U.K. Could Be over the Peak

While most British people [support the lockdown](#), they will still be keen to know when the epidemic has reached its peak. Well, they don't need to wait any longer – the answer is in. Data suggests that the UK is most likely [over the peak](#). Christian Yates writes in [The Conversation](#) that [data released by NHS England](#), in which deaths are aggregated by the date of death rather than the date of reporting, shows a clear decline in recent days. “While the figures are subject to constant revision, the numbers are starting to give us a coherent picture of the shape of the epidemic,” he writes. “Knowing that we have passed the peak is important because it shows that we can, with great effort and sacrifice, bring this disease under control.” He notes that

the numbers are not always clear, for several reasons: there are large numbers of different sources for the figures in the U.K. – the different branches of the [NHS](#), [government websites](#) and the [Office for National Statistics](#) – all of whose figures differ slightly. A more obfuscating factor is the lag between people dying and their deaths being reported. In rare instances, this can be as long as a month, although the vast majority of deaths make their way into the government’s daily totals within a week. And even when these daily numbers are reported by date of death (as in the NHS numbers in the top figure), there are reasons to doubt that they are a true reflection of the number of deaths. “Still, being over the peak is indisputably positive news,” he notes. “Although not cause for celebration, reaching the plateau is perhaps cause for a somber degree of relief.”

[Read more](#)

#### **South Korea**

### **How South Korea Flattened the Coronavirus Curve with Technology**

As countries around the world consider how best to reopen their countries, it’s worth considering how South Korea has been able to “[flatten the curve](#)” and even hold parliamentary elections without resorting to lockdowns. Michael Ahn writes in [The Conversation](#) that after seeing an initial spike in COVID-19 infections in February, South Korea implemented several measures to bring the disease’s [spread under control](#), a progression he has followed as a [researcher on public policy](#). South Korea was able to lower the number of new infections from [851 on March 3 to 22 infections as of 17 April](#) and the mortality rate from COVID-19 hovers [around 2 percent](#).

Several measures contribute to [Korea’s success](#), but two measures were critical in the country’s ability to flatten the curve: extensive testing for the disease and a national system for promptly and effectively tracking people infected with COVID-19.

[Read more](#)

#### **France**

### **Two Months of COVID-19 Lockdown Will Cost France 120 Billion euros, Report Says**

France’s nearly two-month-long coronavirus lockdown is expected to cost the country some 120 billion euros in lost revenue while “forced savings” are estimated to reach 55 billion euros, the state-funded French Economic Observatory said on Monday. “During the lockdown, the Gross Domestic Product (GDP) was cut by 32 percent, corresponding to five points of GDP for the whole of 2020,” [the state-funded French Economic Observatory \(OFCE\) wrote](#). The observatory went on to say that “almost 60 percent of the drop in national income was absorbed by public administrations” and 35 percent by businesses. France’s economic recovery depends on how much the French spend once lockdown is lifted, it said. [France24 notes](#), however, that although the French are expected to have shored up 55 billion euros in so-called forced savings during the planned 17 March to 11 May lockdown period – meaning they will have spent less than they earned – they are not expected to spend these savings “completely or rapidly” once lockdown is lifted given the continuing uncertainties over Covid-19.

[Read more](#)

#### **Models**

### **The Problem of Modeling**

The lessons starting to emerge from the coronavirus crisis are predominantly not epidemiological but highly general aspects of public policy, Paul Collier writes: the over-reliance on expert modelling and the mismanagement of public services. “The current epidemic is a classic application of what economists call ‘radical uncertainty’: in a world that has inevitably become too complex to be adequately captured in models, a world of both ‘known unknowns’ and ‘unknown unknowns,’ the most sensible response to the question ‘what should we do?’ is ‘I don’t know,’” he argues.

[Read more](#)

## After Repeated Failures, It's Time to Permanently Dump Epidemic Models

Since the AIDS epidemic, people have been pumping out such models with often incredible figures. For AIDS, the Public Health Service announced (without documenting) **there would be 450,000 cases by the end of 1993**, with 100,000 in that year alone. The media faithfully parroted it. **There were 17,325** by the end of that year, with about 5,000 in 1993. SARS (2002-2003) was supposed to kill **perhaps “millions,”** based on analyses. **It killed 744** before disappearing. CDC predicted 1.4 million would die from Ebola, but the final death toll was 8,000. Michael Fumento writes in *Issues & Insights* that Oxford University Neil Ferguson predicted 200 million bird flu deaths, and 50,000 BSE death – but the actual number of deaths were 440 and 200, respectively. In the current crisis, Ferguson is the author of the **most alarming model**, and the one most influential in the implementation of the draconian quarantines worldwide, projecting a maximum of 2.2 million American deaths and 550,000 United Kingdom deaths unless there were severe restrictions for 18 months or until a vaccine was developed. “Assuming it’s possible to model an epidemic at all,” Fumento writes, “any that the mainstream press relays will have been designed to promote panic.”

[Read more](#)

### The Hong Kong option

## Study Examines How Hong Kong Managed First Wave of COVID-19 Without Resorting to Complete Lockdown

Hong Kong appears to have averted a major COVID-19 outbreak up to March 31, 2020, by adopting far less drastic control measures than most other countries, with a combination of border entry restrictions, quarantine and isolation of cases and contacts, together with some degree of social distancing, according to a new observational study published in *The Lancet Public Health* journal. The study suggests testing and contact tracing and population behavioral changes -- measures which have far less disruptive social and economic impact than total lockdown -- can meaningfully control COVID-19. The public health measures implemented to suppress local transmission in Hong Kong are probably feasible in many locations worldwide, and could be rolled out in other countries with sufficient resources, researchers say. However, the researchers caution that because a variety of measures were used simultaneously, it is not possible to disentangle the individual effects of each one.

[Read more](#)

### Crisis leadership

## The Secret to Germany's COVID-19 Success: Angela Merkel Is a Scientist

The spread of the coronavirus has been accompanied by an exponential growth of misinformation disseminated on social media. Saskia Miller writes that as misinformation proliferates and lines between fact and fiction are routinely and nonchalantly crossed, world leaders must, now more than ever, illuminate a thoughtful path forward, one reliant on science and evidence-based reasoning. Indeed, many have. “One leader goes further still. Trusted by her people to navigate this outbreak’s murky waters, without inciting or succumbing to a pandemic of the mind, one politician is less a commander in chief and more a scientist in chief: Angela Merkel.”

[Read more](#)

### Brazil

## Brazil: Jair Bolsonaro's Strategy of Chaos Hinders Coronavirus Response

By João Nunes, Deisy Ventura, and Gabriela Spanghero Lotta

Brazil faces a tremendous uphill struggle in its response to COVID-19, the disease associated with the new coronavirus. Already eroded by years of budget cuts, the country's public health system, the Sistema Único de Saúde (SUS), has been further undermined by the president, Jair

Bolsonaro. Last week he participated in a demonstration during which opposition to lockdown measures was combined with calls for a military intervention to shut down Brazil's congress and supreme court. Since coming to power in January 2019, Bolsonaro has led an attack on science and professional expertise – cutting research funds, substituting managers of research institutes with inexperienced political appointees, and publicly intimidating scientists. COVID-19 is a new phase of this ongoing war.

[Read more](#)

#### Perspective

### Autocrats See Opportunity in Disaster

The world is distracted and the public need saving. It is a strongman's dream. All the world's attention is on COVID-19. The *Economist* writes that rulers everywhere have realized that now is the perfect time to do outrageous things, safe in the knowledge that the rest of the world will barely notice. Many are taking advantage of the pandemic to grab more power for themselves. No fewer than 84 have enacted emergency laws vesting extra powers in the executive. "In some cases, these powers are necessary to fight the pandemic and will be relinquished when it is over. But in many cases they are not, and won't be. The places most at risk are those where democracy's roots are shallow and institutional checks are weak." The *Economist* continues: "Take Hungary, where the prime minister, Viktor Orban, has been eroding checks and balances for a decade. Under a new coronavirus law, he can now rule by decree. He has become, in effect, a dictator."

[Read more](#)

#### Authoritarians

### Gulf States Use Coronavirus Threat to Tighten Authoritarian Controls and Surveillance

Governments across the Middle East have moved to upgrade their surveillance capabilities under the banner of combatting COVID-19, the disease linked to the new coronavirus. Matthew Hedges writes in *The Conversation* that overtly **repressive policies** have been commonplace across the Middle East for years, notably in Egypt, Iraq and Syria, where violent measures have been taken to control populations. As a result of technological advances, an increase in political engagement and changes of leadership, the states of the Gulf Cooperation Council (GCC) – Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the United Arab Emirates (UAE) – have also **upgraded their form of authoritarianism** in recent years. This has seen policies of partial economic liberalization and market-based reforms used to obscure an increase in repression and surveillance, for example by containing the work of civil society groups. Following the pattern in which authoritarian states tend to exploit common threats, some of the GCC states are now manipulating the current pandemic to enhance their social power and control.

[Read more](#)

#### Recovery

### EU Approves \$580 Billion to Mitigate COVID-19 Consequences

The European Union approved a \$580 billion aid package to help mitigate the consequences of coronavirus pandemic lockdowns in member countries. *VOA News* reports that European Council President Charles Michel said Thursday the package was expected to be operational by 1 June. Michel said it would help pay lost wages, keep companies afloat and fund health care systems. At Thursday's virtual summit, the EU leaders also agreed on a recovery fund, without giving a specific figure, intended to rebuild the 27-nation bloc's economies. However, officials said \$1.1 trillion to \$1.6 trillion would be needed. European Commission President Ursula von der Leyen said the impact of the economic crisis following the coronavirus outbreak is unprecedented in modern times.

[Read more](#)

### Government tells U.K. Businesses: Time to Get



## Back to Work

Businesses are being discreetly advised by ministers on how to get people back to work in the coming days and weeks amid growing concerns over the **economic impact of the lockdown**. Harry Yorke, Gordon Rayner, and Hayley Dixon write in *The Telegraph* that the government believes there is plenty of room within the existing restrictions for more people to be working, and is now actively encouraging firms to reopen. British Steel, house builder Persimmon and McDonalds are among the latest in a **growing number of firms announcing that they are reopening** despite the lockdown. It came as the chief medical officer said there was now “scope for maneuver” to ease some restrictions in the near future because the transmission rate of the virus is now within a manageable range. Scientific advisers have told ministers that Britain should be in a position to start lifting the lockdown by mid-May, with a team of experts compiling a detailed report on the issue for **Boris Johnson when he returns to work next week**. Ministers are already making plans for **garden centers**, car dealerships and other retailers where social distancing can be maintained, to reopen during the first phase of a gradual exit from lockdown. New data shows that increasing numbers of people are venturing out to shops, parks and workplaces as the nation grows tired of staying at home.

[Read more](#)

### Argument

## Ministers Can’t Keep Hiding Behind the Science

It’s dishonest and cowardly to keep pretending that how and when the lockdown is lifted isn’t a political judgment call. Matthew Parris writes that the political leaders of the country – the U.K. in his case, but any country – must have the courage to share with the public the *political* – political, not medical – choices they must make, and take ownership “of the trade-offs that only politics can settle: trade-offs between deaths caused by one disease and deaths caused by others less immediately in the public eye; between the longevity of the elderly and the education of the young; between mortality in April 2020 and debt that will scar a whole generation; between loss of life and loss of livelihood.” Whichever side you come down on in this trade-off, Parris write. somebody’s got to say there’s a trade-off, and it isn’t ‘the’ science. “It is for the ministers who will make the judgment to be upfront with the public about the human cost. They can ‘follow’ the science, cite the science, be guided by the science, but in the end the science will lead them to a point where paths diverge.”

[Read more](#)

### Exit strategy

## It’s Time to Admit Our COVID-19 “Exit Strategy” Might Just Look Like a More Flexible Version of Lockdown

As the COVID-19 curve starts to flatten in Australia and New Zealand, people are rightly wondering how we will roll back current lockdown policies. Australia’s federal health minister **Greg Hunt says** Australia is looking to South Korea, Japan and Singapore to inform our exit strategy. New Zealand is relaxing some **measures** from next week. Toby Phillips writes in *The Conversation* that a long-term solution – a vaccine – is many months, probably years, away. In the meantime, we must rely on social distancing policies to contain the epidemic – and begin to accept the idea that an “exit strategy” may really look more like a more flexible version of lockdown.

[Read more](#)

## Fumbling for the Exit Strategy

Suddenly everyone has a plan. Ideas for exiting the COVID-19 lockdown are spreading faster than the virus ever did. Spain has let builders return to work, Italy has opened stationers and bookshops, Denmark is allowing children back into nurseries and primary schools. South Africa’s opposition is calling for a relaxed “smart lockdown”. In America

President Donald Trump has been sparring with state governors over who should decide what reopens when. The *Economist* writes that every country is different, but already two things are clear. First, governments need to explain to their people that the world is not about to return to normal. Without a vaccine or a therapy, life will be constrained and economies will remain depressed. Second, testing and contact-tracing are vital to keeping the virus at bay. Countries that failed to invest enough in them when the disease first emerged in China risk repeating the mistake.

[Read more](#)

## One Simple Number Can Solve Boris's Grimly Complex Lockdown Dilemma

When Boris Johnson returns to work, he will have to grapple with a difficult decision. The British economy is on the brink, and must be revived, but the PM cannot risk the dreaded second coronavirus peak. Leaders of countries must make tough decisions in difficult situations, and Allister Heath writes that Boris's decision ranks below the Cuban missile crisis matrix, of course, but above Tony Blair's Iraq War calculations or Margaret Thatcher's Falklands choices. "The Prime Minister faces a series of horrible moral and practical dilemmas best understood through elementary mathematics. The key concept is the Ro (pronounced R-nought): If the Ro is under 1, every victim infects fewer than one other person each, so the virus remains contained; if it is above 1, they each pass the virus to more than one other, contaminating swathes of the population quickly."

[Read more](#)

## How to Build and Deploy Testing Systems at Unprecedented Scale

Without a vaccine or therapeutic drugs, neither of which is guaranteed, countries thus face a future of bouncing in and out of lockdown every few months, with infection rates ebbing and flowing in response. "The result will be mounting death tolls, depressed economies and confidence-sapping uncertainty. This can, however, be partly ameliorated by extensive testing for the virus. Testing enables the government to keep tabs on the disease, reveals which social-distancing measures work, and, if those testing positive remain at home, instills confidence in the public that it is safe to go out," the *Economist* argues.

[Read more](#)

**COVID-19: Also noted this week**

## Hidden Outbreaks | Fighting Future Pandemics | Coronavirus in Africa, and more

- Trump Just Mused About Whether Disinfectant Injections Could Treat the Coronavirus. Really.
- Trump Claims Controversial Comment about Injecting Disinfectants Was "Sarcastic"
- Sunlight and Humidity Kill Coronavirus the Fastest: U.S. Scientists
- How Common is COVID-19? What 2 Controversial Antibody Studies Can and Can't Tell Us.
- "Absolutely Insane": Anti-Vaxxers Promote Coronavirus Conspiracies
- Coronavirus in Africa: How deadly could COVID-19 become?
- New York Antibody Study Estimates 13.9% of Residents Have Had the Coronavirus, Gov. Cuomo Says
- Israeli Startup's Breath Test Device to Sniff Out COVID-19 Set to Start Trials
- EU Push for Coronavirus Contact Tracing Suffers Setback
- Bill Gates on How to Fight Future Pandemics
- Two Errors Our Minds Make When Trying to Grasp the Pandemic
- 'Reopen' Protestors Are A Minority Whom Public-Health Experts Say Threaten the Majority
- Israel Shows Us the Future of Protest
- Coronavirus Medical Expenses Could Cost the U.S. up to \$654

BILLION as the Healthcare System Strains to Provide Ventilators, Hospital Beds and Care for Patients with Years of Complications from the Virus to Come, Study Suggests

- Hidden Outbreaks Spread Through U.S. Cities Far Earlier Than Americans Knew, Estimates Say
- Why a Second Coronavirus Wave Is on the Horizon, and What that Means for the U.K.'s Exit Strategy
- How Abortion, Guns and Church Closings Made Coronavirus a Culture War
- Officials Knew Coronavirus Could Spread at the Houston Rodeo and Proceeded with the Event Anyway
- *Washington Post*: U.S. Officials at WHO Relayed Real-Time Coronavirus Information to Trump Administration
- How Coronavirus Infected Some, but Not All, in a Restaurant
- The Months of Magical Thinking: As the Coronavirus Swept over China, Some Experts Were in Denial
- The U.S. Army Is Racing to Build Makeshift Coronavirus Hospitals
- When Will a Second Wave of the Coronavirus Hit, and What Will It Look Like?
- Can the World Find a Good COVID-19 Vaccine Quickly Enough?
- A New Statistic Reveals Why America's Coronavirus Numbers Are Flat
- CDC Labs Were Contaminated, Delaying Coronavirus Testing, Officials Say
- Without More Tests, America Can't Reopen
- U.S. Hospitals Are Going to Crazy Lengths to Get Masks
- Scant Testing in US Migration System Risks Spreading Virus
- Europe Coronavirus Death Toll Tops 100,000
- PM's Lockdown Dilemma — Risk Killing the Economy or Thousands of People?
- Life after Lockdown: Coronavirus: Plane Fares to Soar after Lockdown Is Lifted as Airlines Lose Middle Seats
- France Plans a Different Path Back to Normality
- Business Group in Idaho Offers Coronavirus Antibody Tests

[Read more](#)

---

BIOMETRICS | BORDER/IMMIG. | BUSINESS | CYBERSECURITY | DETECTION | DISASTERS | GOVERNMENT | INFRASTRUCTURE  
PUBLIC HEALTH | PUBLIC SAFETY | REGIONAL | SCI-TECH | SURVEILLANCE | TERRORISM | TRANSPORTATION | WATER

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



Advertising & Marketing [advertise@newswirepubs.com](mailto:advertise@newswirepubs.com)

Editorial [editor@newswirepubs.com](mailto:editor@newswirepubs.com)

General [info@newswirepubs.com](mailto:info@newswirepubs.com)

2010-2011 © News Wire Publications, LLC News Wire Publications, LLC

220 Old Country Road | Suite 200 | Mineola | New York | 11501

[Permissions and Policies](#)

Homeland Security News Wire, 220 Old Country Road, Suite 200, Mineola, NY 11501

SafeUnsubscribe™ [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)

Forward email | Update Profile | About our service provider

Sent by [hsnewswire@newswirepubs.com](mailto:hsnewswire@newswirepubs.com)

**From:** [CLA Public Section](#)  
**To:** [Melissa Tronquet](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, April 17, 2020 3:08:36 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive](#) (961,536 articles)



[North America](#) | [Global](#)

**USA**

[North America](#)

[Employee Benefits & Pensions](#)



### **Beware the Snake in the Grass: COBRA Election Notice Considerations During The COVID-19 Pandemic**

**Faegre Drinker Biddle & Reath LLP**

With most of the nation on lockdown due to the COVID-19 pandemic, many employers are in the unfortunate position of having to lay off workers or...

### **Payroll Tax Relief Provisions of COVID-19 Legislation**

**Morrison & Foerster LLP**

In response to the coronavirus pandemic, Congress has passed legislation to encourage continued payment of wages and benefits by providing relief to...

### **Tax Effects on Paycheck Protection Program Borrowers**

**Bryan Cave Leighton Paisner LLP**

With regard to the interplay of various tax provisions of the CARES Act and the Paycheck Protection Program (PPP), we note the following: If a...

### **A Deeper Dive into the Paycheck Protection Program under the CARES Act**

**Sullivan & Worcester LLP**

Sullivan recently issued a client alert that explores the law and lore of the



Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act")...

---

### **Key Retirement Plan Components of the Coronavirus Aid, Relief, and Economic Security Act**

**Nutter McClennen & Fish LLP**

The Coronavirus Aid, Relief, and Economic Security Act (the "Act") provides retirement plan relief and makes financial assistance available to...

---

### **Is fiduciary breach litigation limited to retirement plans?** [Video](#)

**Hall Benefits Law**

Is fiduciary breach litigation limited to retirement plans?...

---

### **Employee benefit changes under the CARES Act: What employers need to know**

**Thompson Coburn LLP**

The Coronavirus Aid, Relief and Economic Security (CARES) Act was signed into law by the President on March 27, 2020 to provide much-needed relief...

---

### **COVID-19: Health and Welfare Benefits and Relief Included in the CARES Act**

**McDermott Will & Emery**

For health and welfare plan sponsors, the CARES Act relief includes, among other things, increased access to COVID-19 diagnostic testing and...

---

### **Retirement Plan Relief and Temporary Student Loan Benefits in the CARES Act**

**McDermott Will & Emery**

For retirement plan sponsors, the CARES Act relief includes relaxed plan distribution and loan rules designed to provide participants with greater...

---

### **The CARES Act - Summary of Tax Provisions**

**Michael Best & Friedrich LLP**

On March 27, 2020, President Trump signed into law the "Coronavirus Aid, Relief, and Economic Security Act," commonly referred to as the "CARES Act."...

---

### **CARES Act Impact on Employee Benefits and Compensation**

**Kelley Drye & Warren LLP**

On March 27, 2020, the President signed into law the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act"), the third phase of...

---

### **COVID 19: Emerging Investment Risks for Pension Schemes**

**Squire Patton Boggs**

Daily policy initiatives by governments across the world who are desperate to avoid the worst ravages of an economic recession are fuelling a lot of...

---

### **ESOP Companies Should Address Cash Flow Before It's Too Late**

**Fox Rothschild LLP**

Employee Stock Ownership Plans are a unique form of retirement plan designed to invest primarily in employer securities. Under most privately held...

---

## **PPP Covers Health and Retirement Plan Contributions**

### **Graydon Head & Ritchey LLP**

Most small businesses are aware of the loans backed by the Small Business Administration (“SBA”) to help maintain cash flow and retain workers...

---

## **SBA Releases Additional Guidance via Updates to Frequently Asked Questions on Paycheck Protection Program Loans**

### **Haynes and Boone LLP**

On April 8, 2020, the Small Business Administration (“SBA”) provided additional guidance on the Paycheck Protection Program (“PPP”) through an update...

---

## **Summary of CARES Act Provisions Affecting Employer-Sponsored Retirement Plans**

### **Fox Rothschild LLP**

The Coronavirus Aid, Relief and Economic Security Act or CARES Act, signed into law on March 27, 2020, includes many employment and employee benefit...

---

## **COVID-19 Guide to Emergency Cost Reduction: Compensation and Benefits**

### **Holland & Knight LLP**

As the COVID-19 crisis continues, many employers are facing the difficult challenge of determining how to achieve significant cost...

---

## **Issuing EINs an Issue for International Entities**

### **Cadwalader Wickersham & Taft LLP**

As part of the routine “know-your-customer” onboarding process, lenders are required to obtain the employer identification number (“EIN”) and other...

---

## **Retirement Benefit Expenses Covered under the CARES Act’s Paycheck Protection Program**

### **Haynes and Boone LLP**

The Paycheck Protection Program (the “PPP”) under the CARES Act aims to assist small businesses affected by COVID-19 by covering certain operating...

---

## **COVID-19: CARES Act Changes to Retirement Accounts, Health Plans and other Employee Benefits**

### **Bass, Berry & Sims PLC**

On March 27, the House voted overwhelmingly to approve H.R. 748—the Coronavirus Aid, Relief, and Economic Security Act (CARES Act)—a \$2.2 trillion...

---

## **CARES Act Expands COVID-19 Testing and Other Health and Welfare Benefits**

### **Covington & Burling LLP**

On March 27, 2020, President Trump signed the largest economic stimulus bill in U.S. history: the Coronavirus Aid, Relief, and Economic Security Act...

---

## **CARES Act: Implications for Businesses**

### **Thompson Hine LLP**

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), a roughly \$2 trillion coronavirus response bill signed into law yesterday, is...

---

### **Federal and Selected State Tax Updates in Response to Coronavirus (COVID-19)**

[Massachusetts](#)

[New York](#)

[Virginia](#)

[District of Columbia](#)

#### **Goulston & Storrs PC**

The following is a brief summary of recent tax related regulatory and legislative developments related to the COVID-19 pandemic, as of April 3, 2020...

---

### **Client Alert: CARES Act Retirement Plans - What Employers Need to Know**

#### **Bowditch & Dewey LLP**

The CARES Act (Coronavirus Aid, Relief, and Economic Security Act), effective as of March 27, 2020, has several provisions aimed at making it easier...

---

### **The CARES Act and Short-Time Compensation Programs**

#### **Covington & Burling LLP**

As reported in our Client Alert, the new Coronavirus Aid, Relief, and Economic Security (CARES) Act includes provisions to increase the use of...

---

### **Podcast: Key Decisions for Defined Contribution Plan Sponsors Under the CARES Act**

[Audio](#)

#### **Ropes & Gray LLP**

In this Ropes & Gray podcast, benefits partners Loretta Richard and Josh Lichtenstein discuss the Coronavirus Aid, Relief and Economic Security Act...

---

### **IRS Clarifies ACA 'Pay or Play' Rules to Individual Health Reimbursement Arrangements (IHRAs)**

#### **Hall Benefits Law**

New proposed regulations from the IRS are designed to clarify the nondiscrimination rules pertaining to Individual Coverage Health Reimbursement...

---

### **Preparing Qualified Plans for COVID-19-Related Needs**

#### **Sidley Austin LLP**

As a result of the economic uncertainty and business disruptions related to the COVID-19 pandemic, plan sponsors may be reviewing their qualified...

---

### **IRS Provides Guidance For HSAs and Retirement Plans**

#### **Krieg DeVault**

The IRS provided special relief from the April 15, 2020, Federal income tax return filing and payment deadline in response to the ongoing COVID-19...

---

### **Impact of SBA Affiliation Rules on Eligibility for Paycheck Protection Loans and EIDLs under the CARES Act**

#### **Berger Singerman LLP**

Impact of SBA Affiliation Rules on Eligibility for Paycheck Protection Loans and EIDLs under the CARES Act April 6, 2020 In response to the COVID-19...



---

## **Why Controlled Group Status Matters to Both Health and Welfare Benefits and Retirement Plans**

### **Hall Benefits Law**

A controlled group is a group of businesses that have common control by ownership. The most common form of this arrangement is a parent company that...

---

## **CARES Act Social Security Tax Deferral and Employee Retention Credits**

### **McDermott Will & Emery**

The broad-based employer and employee relief provided under the Coronavirus Aid, Relief, and Economic Security (CARES) Act includes two forms of...

---

## **PBGC Announces COVID-19 Extensions for Premium Payments and Other Filing Deadlines**

### **Proskauer Rose LLP**

On April 10, 2020, the Pension Benefit Guaranty Corporation (the "PBGC") announced that deadlines for upcoming premium payments and certain other...

---

## **Congress Shows It CARES by Waiving 2020 Required Minimum Distributions, Saving Retirees from Locking in Losses**

### **Sidley Austin LLP**

As noted in a recent Update, the Setting Every Community Up for Retirement Enhancement Act of 2019 and related legislation (the SECURE Act), signed...

---

## **State and Local Tax Responses to COVID-19: Relief from Withholding Requirements for Telecommuting Employees**

### **Baker McKenzie**

With many employees now telecommuting due to the COVID-19 outbreak, employers could face additional state income tax withholding requirements if...

---

## **COVID-19 Layoffs Can Cause Partial Retirement Plan Termination**

### **Frost Brown Todd LLC**

The COVID-19 pandemic has caused nationwide "shelter-at-home" proclamations from state and local governments resulting in nonessential businesses...

---

## **Benefit Related Provisions of the CARES Act and Other Federal Relief**

### **Sullivan & Worcester LLP**

This alert, from the Employment & Benefits practice group, focuses on the various retirement, welfare and fringe benefit related changes that have...

---

## **Departments Issue Guidance Under FFCRA and CARES Act Affecting Health Plans**

### **Winston & Strawn LLP**

The Departments of Labor (DOL), Health and Human Services (HHS), and Treasury (collectively, the Departments) recently issued FAQ guidance (the FAQs)...

---



## **Calculating Plan Loan Limits under the CARES Act: Application of the One-Year Lookback**

**Faegre Drinker Biddle & Reath LLP**

The Coronavirus Aid, Relief, and Economic Security (CARES) Act temporarily increases the plan loan limit for loans to qualified individuals (as...

---

## **COVID-19-Related Tax Credits; Deferral of Payment of Employer Social Security Tax**

**Jackson Lewis PC**

The Families First Coronavirus Relief Act (FFCRA) and the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) make two separate, but...

---

## **CARES Act Provides Important Relief for Retail & Hospitality Companies**

**Morgan Lewis**

This edition of Morgan Lewis Retail Did You Know? Examines how the Coronavirus Aid, Relief, and Economic Security (CARES) Act impacts...

---

## **COVID-19 Pandemic: Tax Relief Affecting Nonprofits**

**McGuireWoods LLP**

Nonprofits, like individuals and for-profit businesses, are facing significant hardships due to the COVID-19 pandemic. Recent legislation and...

---

## **COVID-19: COVID-19 Considerations: Employer Sponsored Retirement Plans**

**K&L Gates**

In the wake of the COVID-19 pandemic and the resulting economic uncertainty, many employers and employees alike are searching for ways to be...

---

## **Summary of the Impact of the CARES Act on Retirement Plans**

**Taft Stettinius & Hollister LLP**

In an effort to help individuals weather the economic downturn created by the COVID-19 pandemic, the Coronavirus Aid, Relief and Economic Security...

---

## **The Advantages and Challenges of Supplemental Unemployment Benefit Plans**

**Ogletree Deakins**

The economic and financial consequences of the ongoing COVID-19 crisis have forced some employers to furlough and lay off workers, resulting in...

---

## **Code Section 139: Little Known Disaster Relief Benefits Now in the Spotlight**

**Faegre Drinker Biddle & Reath LLP**

As most of the nation continues under lockdown due to the COVID-19 pandemic, we have received inquiries about ways employers can provide additional...

---

## **COVID-19: COVID-19 Considerations: Compensation Topics**

**K&L Gates**

In the wake of the COVID-19 pandemic and the resulting economic uncertainty, many employers are searching for ways to be financially prepared in the...

---

## **Exploring the Contours of the Employee Retention Credit**

### **Sullivan & Worcester LLP**

In an effort to incentivize businesses to retain employees during the COVID-19 pandemic, the Coronavirus Aid, Relief, and Economic Security Act...

---

## **Cannabis Businesses and the CARES Act Employee Retention Credit**

### **Greenspoon Marder LLP**

While cannabis businesses are excluded from most economic recovery packages related to COVID-19, these companies may still qualify for the employment...

---

## **What Tax Actions Should Companies Be Taking Now?**

### **Winston & Strawn LLP**

Along with all of the other Covid-19 legal developments, there are a few tax provisions that may have been overshadowed, but that can provide...

---

## **CARES Act Provisions Affecting Employee Benefits**

### **Robinson & Cole LLP**

On March 27, 2020, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), a bipartisan deal on a \$2+...

---

## **Reductions-in-Force, Layoffs and Furloughs Can Trigger Unexpected PBGC Reporting and Pension Plan Funding Obligations**

### **Baker & Hostetler LLP**

Many employers now are taking actions to reduce workforces, primarily by laying off employees, furloughing employees, or offering retirement or...

---

## **Updates on Texas and Federal CARES Act Unemployment Insurance Benefits**

Texas

### **Cozen O'Connor**

The Texas Workforce Commission has updated its guidance regarding the availability of unemployment insurance benefits, as supplemented by the federal...

---

## **COVID-19 — Tax Planning Opportunity for Defined Benefit Participants?**

### **McDermott Will & Emery**

Much has been written about the new CARES Act distribution that allows impacted COVID-19 participants to access up to \$100,000 in their tax-qualified...

---

## **Can I Get an E-Witness? Retirement Plan Consents in the Age of Social Distancing**

### **Ogletree Deakins**

As the world faces the ongoing threat of the coronavirus pandemic, pension plan administration is often taking place from remote working locations...

---

## **IRS Extends the Form 5500 Due Dates for Some Employee Benefit Plans**

### **Jackson Lewis PC**

The Internal Revenue Service has broadened the filing and payment relief

provided under prior guidance. IRS Notice 2020-23 postpones, among other...

---

**Employee Benefit Plan Provisions Included in COVID-19 Relief From the IRS**  
**Day Pitney LLP**

In response to the COVID-19 pandemic, the IRS has released a series of notices extending certain filing, payment and other deadlines. Many of these...

---

**SUMMARY: CARES Act for Non-Profits**

**Goulston & Storrs PC**

Below is a summary of a variety of recent federal and state responses to the COVID-19 pandemic, with a focus on certain provisions of the CARES Act...

---

**Retirement Plan Issues and COVID-19: Additional Relief Issued By IRS**

**Haynes and Boone LLP**

The IRS issued Notice 2020-23 (the "Notice"), postponing various employee benefit related deadlines under the Internal Revenue Code. Under the Notice...

---

**CARES Act Provisions of Related ESOP-Owned Companies**

**Winston & Strawn LLP**

On March 27, 2020, President Trump signed into law a massive \$2 trillion stimulus bill, the Coronavirus Aid, Relief, and Economic Security Act (the...

---

**COVID-19 Considerations: Midyear Reductions or Suspensions of Employer & Matching Contributions to 401(k) and Defined Contribution Plans**

**Mintz**

Beyond COVID-19's devastating impact on public health is its second order effects on the U.S. and world economy. Businesses of all sizes need to trim...

---

**District Court Rules in Favor of Fiduciaries in Recent Prudence, Loyalty Breach Claim**

New York

**Hall Benefits Law**

A recent lawsuit argued in the federal appeals court for the Southern District of New York handed a win to plan fiduciaries on a prudence and breach...

---

**Nonqualified Deferred Compensation Plan Sponsors: COVID-19 Pandemic Considerations**

**McCarter & English LLP**

This Alert discusses certain considerations for employers that sponsor nonqualified deferred compensation plans, in light of business/market...

---

**Employment Question of the Day: April 10, 2020**

**Fredrikson & Byron PA**

Many employers are trying to adjust their workforces with minimal economic impact on employees and long-term business planning. Short-time...

---

**Louisiana Eases Requirements for Unemployment Insurance in Emergency Proclamation**

Louisiana



### **Phelps Dunbar LLP**

Under an emergency proclamation signed by Louisiana Gov. John Bel Edwards on April 7, additional changes have been made to loosen eligibility...

---

### **CARES Act Provisions Affecting Employee Benefit Plans**

#### **Vedder Price PC**

On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security (CARES) Act (the "Act") was signed into law with the intention of easing the...

---

### **Health Plan Provisions and FAQs in COVID-19 Related Guidance**

#### **Ford & Harrison LLP**

On March 27, the President signed the Coronavirus Aid, Relief and Economic Security Act ("CARES Act" or "Act"), which contains a number of tax- and...

---

## **Employment & Labor**



### **UPDATED: Emergency legislation and measures around the world (COVID-19)**

#### **Lexology PRO**

A list of key recent emergency legislation and measures implemented by nations across the world in response to COVID-19.

---

### **COVID-19: Key updates for compliance teams**

#### **PRO Compliance**

Lexology Pro Compliance takes a look at some of the most informative articles published on Lexology this week for compliance teams to stay up-to-date with some of the biggest challenges brought about by the COVID-19 outbreak, including key guidance from regulators around the world and practical tips to manage business responses to the pandemic.

---

### **It only gets better with age: Supreme Court clarifies ADEA protections for federal employees**

#### **McDermott Will & Emery**

Older federal employees just got a boost from the Supreme Court's recent interpretation of the causation standard under the federal sector provision...

---

### **If Pain, Yes Gain—Part 84: New York State Paid Sick Leave Law Signed**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: New York's paid sick leave law, applicable to employers of all sizes, goes into effect on September 30, 2020, permitting employees...

---

### **Employment Question of the Day: April 6, 2020**

#### **Fredrikson & Byron PA**

In general, no, a properly-classified essential worker cannot preemptively self-quarantine and refuse to come to work due to a generic fear of the...

---

### **Congressional Health Care Priorities in the Fourth Coronavirus Legislative Package**



### **Brownstein Hyatt Farber Schreck LLP**

On Friday, March 27, the Coronavirus Aid, Relief and Economic Security (CARES) Act was signed into law. This bill, aimed at addressing the economic...

---

### **IRS Provides Guidance on Refundable and Advance Tax Credits Under CARES and FFCRA Acts**

#### **Akerman LLP**

On March 31, the IRS issued guidance on the paid leave tax credits provided by the Families First Coronavirus Response Act (the FFCRA) and the...

---

### **Amendments to Proposed Legislation Would Change Municipalization / Eminent Domain Takeovers of Electric, Gas and Water Utilities**

#### **Nossaman LLP**

We've previously reported on Senate Bill 917, which was introduced on February 3, 2020, by Senator Wiener (D-San Francisco) to establish a process...

---

### **U.S. Department of Labor Issues Temporary Rule on the Families First Coronavirus Response Act**

#### **Epstein Becker Green**

On April 1, 2020, the day that the Families First Coronavirus Response Act ("FFCRA" or "Act") became effective, the Wage and Hour Division of the U.S...

---

### **Executive Compensation Planning Ideas in an Economic Downturn**

#### **Hall Benefits Law**

Any time the economy is growing, it's important to consider and plan for the next economic slowdown. When exactly this will occur is something that...

---

### **Layoffs vs. Furloughs: What's the Difference in California?**

California

#### **Fisher Phillips**

There has been much confusion lately about the meaning of the terms "layoff" and "furlough." Neither term has any specific meaning in California...

---

### **DOL Offers Definition of Healthcare Provider under FFCRA**

#### **Bass, Berry & Sims PLC**

Since the passage of the Families First Coronavirus Response Act (FFCRA), many healthcare organizations, especially those with a structure that...

---

### **What Small Businesses Need to Know about New PPP Guidance**

#### **Bradley Arant Boult Cummings LLP**

Last week, the Small Business Administration (SBA) published its Interim Final Rule providing formal guidance on the implementation of the Paycheck...

---

### **Michigan Issues Executive Order Implementing COVID-19 Job Leave Protections**

Michigan

#### **Proskauer Rose LLP**

On April 3, 2020, Michigan Governor Gretchen Whitmer issued Executive Order 2020-36, which, effectively immediately, prohibits Michigan employers...

---

## **COVID-19 & Cybersecurity: What Companies and Employees Should Know About Remote Working**

**Faegre Drinker Biddle & Reath LLP**

The spread of COVID-19 has prompted an enormous shift by organizations to the use and implementation of remote working solutions for a wide range and...

---

## **SBA Provides Much Needed Guidance for PPP Loans**

**Lane Powell PC**

As the Small Business Association (SBA) and U.S. Treasury scramble to get the Paycheck Protection Program (PPP) going from zero to...

---

## **M&A in the COVID Era - Part III - A Dealmaker's Guide to Post-COVID-19 Purchase and Sale Agreements**

**Mintz**

As the global COVID-19 pandemic continues, M&A activity has slowed considerably, with buyers and sellers taking a "wait and see" approach to the...

---

## **Ten Common Benefits Issues Related to the COVID-19 Pandemic, Employee Furloughs and Reductions in Force**

**Littler Mendelson PC**

There are many more than 10 issues that are of concern to employers in connection with the current crisis. Nevertheless, employers are dealing with...

---

## **CARES Act Employee-Related Stimulus - FAQs on Employee Retention Credits and Payroll Tax Deferral**

**Pepper Hamilton LLP**

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) provides additional payroll-related relief to employers struggling to...

---

## **CARES Act Benefits for Tax-Exempt Organizations**

**Steptoe & Johnson LLP**

The House and Senate have passed "Phase Three" of a congressional response to the COVID-19 emergency, and the President signed it on Friday, March 27...

---

## **Arizona Directs Additional Businesses To Cease Operations**

Arizona

**Fisher Phillips**

In response to the COVID-19 coronavirus outbreak, Arizona Governor Ducey issued a "Stay Home, Stay Healthy, Stay Connected" order last week requiring...

---

## **Concluding Contracts becomes a Home Office Challenge - a Cheat Sheet**

**VISCHER AG**

The coronavirus demands high levels of flexibility and creativity from companies: As many employees work from home, established workflows are...

---

## **CARES Act Delivers Much-Needed COVID-19 Relief, Assistance to Healthcare Industry**

### **Barnes & Thornburg LLP**

In the wake of the COVID-19 pandemic, the CARES Act provides, among other things, economic assistance to healthcare providers and entities providing...

---

### **DOL Provides Further Guidance on Pandemic Unemployment Assistance**

#### **Littler Mendelson PC**

On Sunday April 5, 2020, the U.S. Department of Labor (DOL) issued Unemployment Insurance Program Letter (UIPL) 16-20 to provide further guidance on...

---

### **Interplay Between Paycheck Protection Program Loans and Payroll Tax Provisions under FFCRA and the CARES Act**

#### **Akerman LLP**

Congress enacted the Families First Coronavirus Response Act (FFCRA), which requires certain employers to provide paid leave to workers who are...

---

### **IRS Issues Guidance for CARES Act Employee Retention Credit**

#### **Mintz**

On March 31, the IRS issued guidance related to the employee retention credit enacted in the CARES Act. The employee retention credit was discussed in...

---

### **US DOL Issues Additional Guidance Regarding Paid Leave Under Families First Coronavirus Response Act**

#### **Hunton Andrews Kurth LLP**

The Families First Coronavirus Response Act (the "Act") is set to take effect on April 1, 2020. As we previously reported, the Act requires that...

---

### **UPDATED: Department of Labor Issues Guidance for Families First Coronavirus Response Act**

#### **Mintz**

The Department of Labor ("DOL") has updated the guidance it previously issued regarding the Families First Coronavirus Response Act, which goes into...

---

### **Working from Home During the Pandemic? Turn Alexa and Siri Off!**

#### **Robinson & Cole LLP**

The transition from work-from-the-office to work-from-home has been rapid during the pandemic. All of a sudden, millions of workers are working from...

---

### **U.S. Congress Gives Employers an Incentive to Retain Employees in CARES Act**

#### **Bryan Cave Leighton Paisner LLP**

Section 2301 of the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") , enacted on March 27, 2020, introduces an employee...

---

### **CARES ACT HIGHLIGHTS: Paycheck Protection Program and FFCRA Amendments**

#### **Kelley Drye & Warren LLP**

On March 27, 2020, the President signed the Coronavirus Aid, Relief, and



Economic Security Act ("CARES Act") into law. The CARES Act's purpose is...

---

### **FCRA Disclosure May Include "Concise" Explanation of Consumer Report**

**Shawe Rosenthal LLP**

The U.S. Court of Appeals for the Ninth Circuit found that required disclosure to applicants and employees before obtaining a consumer report under...

---

### **Employment Question of the Day: April 7, 2020**

**Fredrikson & Byron PA**

In limited circumstances, an employee may be entitled to receive Emergency Paid Sick Leave (EPSL) and Emergency Family Medical Leave Act (E-FMLA)...

---

### **Department of Labor Guidance on Families First Coronavirus Response Act: Employer Takeaways Part Two**

**Lewis Rice LLC**

The discussion that follows is a continuation of our analysis of key interpretive guidance from the Department of Labor ("DOL") on the Families First...

---

### **When and to Whom Does an Employer Have a Duty to Report a COVID-19 Case?**

**Venable LLP**

As the number of COVID-19 cases in the United States continues to grow, an increasing number of employers are faced with the question: If someone in...

---

### **DOL Issues New Regulations Clarifying Emergency Paid Sick Leave Act and Emergency Family and Medical Leave Expansion Act**

**Graydon Head & Ritchey LLP**

Yesterday, the Department of Labor posted temporary regulations addressing how workers and employers will benefit from the protections and relief...

---

### **New York Enacts Statewide Sick Leave Law**

**Littler Mendelson PC**

On April 3, 2020, New York State Governor Andrew Cuomo signed a comprehensive budget bill that, among other things, amends the New York Labor Law<sup>1</sup> to...

---

### **Revised Families First Coronavirus Response Act Becomes Law — Five Things Healthcare Providers Need to Know**

**McGuireWoods LLP**

On March 16, 2020, the U.S. House of Representatives unanimously passed corrections to the Families First Coronavirus Response Act (H.R. 6201), which...

---

### **Michigan Governor's Executive Order Sets Further Restrictions, Prohibits Discrimination**

**Michigan**

**Barnes & Thornburg LLP**

In Michigan, an April 3 Executive Order, Executive Order 2020-36, which took effect immediately, established further restrictions on individuals who...

---



## **New Paid Sick Leave Requirements Impact Government Contractors**

### **Covington & Burling LLP**

Recent legislation significantly expanded many workers' entitlement to paid sick leave and paid family leave. These new benefits take effect on April...

---

## **DOL's Regulations for FFCRA, Part II: Calculating Amounts and Pay for Leave, Intermittent Leave, and How it Works with PTO**

### **Bradley Arant Boult Cummings LLP**

In Part I of this post we covered some of the logistics you need to get started with the FFCRA paid leave provisions. Today we will continue our...

---

## **Updated DOL Guidance - What Employers Need To Know On The First Day Of The FFCRA**

### **Kelley Drye & Warren LLP**

The Families First Coronavirus Response Act ("FFCRA") is effective today, April 1. In honor of this undoubtedly daunting occasion for employers with...

---

## **Pennsylvania Secretary of Health Issues Order Mandating that Building Owners Clean High-Touch Areas in Accordance with CDC Guidance**

[Pennsylvania](#)

### **Littler Mendelson PC**

In its latest response to the COVID-19 pandemic, Pennsylvania has ordered mandatory cleaning protocols for large buildings throughout the...

---

## **Summary of CARES Act for Employers**

### **Mintz**

Congress has now passed the Coronavirus Aid, Relief and Economic Security Act or CARES Act - Federal government's Phase III response to the health and...

---

## **San Francisco Bay Area Shelter-In-Place Orders Extended Until "At Least" May 1, 2020**

[California](#)

### **Baker McKenzie**

At noon today, San Francisco, Alameda, San Mateo, Santa Clara, Santa Cruz, Marin, and Contra Costa counties extended their Shelter-In-Place Orders...

---

## **Eleventh Circuit Resets Title VII Retaliation Claim Standard**

### **Eversheds Sutherland (US) LLP**

Undaunted by COVID-19, the Eleventh Circuit pressed forward with its work in *Monaghan v. Worldpay US, Inc.*, 2020 WL 1608155 (11th Cir. Apr. 2, 2020)...

---

## **The CARES Act: A Summary Overview of Federal Tax Changes Affecting Businesses**

### **Mintz**

In response to the COVID-19 crisis, the United States, like many states and foreign governments, has reacted by easing tax burdens on businesses and...

---

## **DOL Released 100+ Pages of Detailed Temporary Regulations**

### **Kelley Drye & Warren LLP**

The U.S. Department of Labor has just issued over one hundred pages of detailed temporary regulations, effective from April 1, 2020 to December 31...

---

### **COVID-19 - Emergency Forgivable Loans for Small U.S. Businesses**

#### **Osler Hoskin & Harcourt LLP**

On April 5, 2020, we published an Update describing the newly established Paycheck Protection Program (PPP) under the...

---

### **CORONAVIRUS CRISIS Employment and Benefits Cost-Savings Option**

#### **Sullivan & Worcester LLP**

Cost Saving Option Ease of Implementation; Duration Key Legal Issues Cost Savings Employee Impact Reduction in employee hours/salary Easy to moderate...

---

### **COVID-19 U.S.: Summary of key business tax relief provisions under the CARES Act**

#### **Hogan Lovells**

The CARES (Coronavirus Aid, Relief, and Economic Security) Act (Public Law No. 116-136) was Signed into law on March 27, 2020 in an effort to provide...

---

### **Investigating Complaints Containing Second-Hand Information in the COVID-19 Era**

#### **Jackson Lewis PC**

As the country faces a wave of COVID-19 closure orders, individuals are being encouraged to report violations. Hypothetically, these reports could...

---

### **Healthcare Employers Spared Burden of FFCRA By Last Minute DOL Guidance**

#### **Holland & Hart LLP**

The Families First Coronavirus Response Act created a bizarre contradiction for healthcare employers. While hospitals, clinics and other patient care...

---

### **U.S. Supreme Court Rules Federal Workers Can Sue Over 'Any' Age Bias**

#### **Gordon Rees Scully Mansukhani**

On April 6, 2020, the United States Supreme Court issued its opinion in Babb v. Wilkie, holding that federal employees have a claim of age...

---

### **SBA Paycheck Protection Program with Eligibility Questionnaire**

#### **Nelson Mullins Riley & Scarborough LLP**

On Friday, April 3, 2020, eligible lenders began accepting applications for loans under the \$349 billion Paycheck Protection Program, the cornerstone...

---

### **DOL Says FFCRA Paid Leave is Not Available During Worksite Closures and Furloughs**

#### **Baker McKenzie**

As a further update to our post here, on Thursday, the DOL issued an additional 22 FAQs on FFCRA, addressing required certifications for leave...

---



**Some good news for employers: Supreme Court reverses Court of Appeal's decision that Morrisons was vicariously liable for unlawful disclosure of personal data by rogue employee**

**Ropes & Gray LLP**

WM Morrisons Supermarkets plc v Various Claimants [2020] UKSC 12 (1 April 2020). Morrisons has won its appeal from the Court of Appeal's decision...

---

**What DOL's New Rule Means for FFCRA's Small Business Exemption**

**Kelley Drye & Warren LLP**

On April 1, 2020, the Department of Labor ("DOL") posted a temporary rule issuing regulations for implementing the Families First Coronavirus...

---

**COVID-19: Managing the Security Risks of a Remote Workforce**

**K2 Intelligence/Financial Integrity Network**

As COVID-19 remains prevalent, working remotely has become the new normal. This means that many organizations will have people working from home for...

---

**An Actual Arbitration Agreement Is Required for Enforcement**

**Shawe Rosenthal LLP**

An employer could not enforce an arbitration agreement, purportedly requiring its employees to arbitrate any work-related disputes, where it could...

---

**New York State Passes Guaranteed Sick Leave for Working New Yorkers Beyond COVID-19**

[New York](#)

**Sheppard Mullin Richter & Hampton LLP**

On April 3, 2020, Governor Cuomo passed Assembly Bill A9506B, which will grant most New Yorkers paid sick leave annually, building on temporary...

---

**Bonus! DOL Opinion Letters Clarify Regular Rate Calculation for Workplace Perks**

**Barnes & Thornburg LLP**

U.S. Department of Labor (DOL) Wage and Hour Division administrator recently issued three opinion letters, each concerning whether certain employee...

---

**COVID-19: Cyber Readiness for Remote Access Workers**

**Berger Singerman LLP**

With employees abiding work-at-home directives and IT departments adding resources, buying equipment, and generally transitioning to full-scale...

---

**Connecticut Governor Limits COVID-19 Liability for Providers and Facilities, Restricts Surprise Billing for COVID-19 Treatment, and Expands the Health Care Workforce in Recent Executive Orders.**

[Connecticut](#)

**Robinson & Cole LLP**

Governor Lamont issued two new Executive Orders designed to expand the health care workforce, immunize providers from COVID-19-related liability, and...

---

**CCM COVID-19 Alert - President Signs CARES Act Into Law**

### **Clingen Callow & McLean LLC**

On Friday, March 27, 2020, the U.S. House of Representatives passed the "Coronavirus Aid, Relief and Economic Security Act" (the "Act"), which the...

---

### **Supreme Court Clarifies Standard Federal Workers Must Meet in Age Discrimination Lawsuits**

#### **Ford & Harrison LLP**

On April 6, 2020, the U.S. Supreme Court held that federal-sector plaintiffs in age discrimination cases brought under the Age...

---

### **DOL's new FFCRA regulations and Q&As on COVID-19 paid leave clarify documentation and other requirements**

#### **Hogan Lovells**

On April 1, 2020, the Department of Labor ("DOL" or the "Department") issued regulations implementing the Families First Coronavirus Response Act...

---

### **Employers and Hiring Managers Beware: The Sixth Circuit Reminds Us That Preselection Decisions May Cast Doubt On Hiring Process and Selection Criteria**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The Sixth Circuit Court of Appeals recently reversed summary judgment in favor of an employer on failure to promote claims, finding...

---

### **DOL's Regulations for the FFCRA, Part I: Who's Covered, Posting, Documentation, Shelter-in Place Order, and Other Fun Items**

#### **Bradley Arant Boult Cummings LLP**

At the end of last week, the Department of Labor issued 125 pages of FFCRA guidance, including actual temporary regulations and 20 new Q&As (so we...

---

### **New York Enacts Statewide Paid Sick Leave Law as Part of FY 2021 Budget** New

York

#### **Proskauer Rose LLP**

On April 3, 2020, New York Governor Andrew Cuomo signed into law the fiscal year 2021 New York State budget, which, notably for employers, includes a...

---

### **Is the company's unpaid internship legal?**

#### **Raymond Law Group LLC**

There is a long tradition of internships or on-the-job training in just about any business. The situation is usually win-win — Young inexperienced...

---

### **New York Enacts Statewide Permanent Paid Sick Leave Law** New York

#### **Ford & Harrison LLP**

On April 3, 2020, New York State Governor Andrew M. Cuomo signed into law the 2021 fiscal year budget that includes an unpaid and paid sick leave...

---

### **Reminder: NY Employers Must Provide Specific Unemployment Benefits Notice to Separated and Furloughed Employees** New York

#### **Fox Rothschild LLP**



The Families First Coronavirus Response Act includes a provision that provides emergency funding to the states to assist with the processing and...

---

**COVID-19 Washington Update: April 1, 2020** Washington

**Kelley Drye & Warren LLP**

Today's federal response to the COVID-19 pandemic included announcements from various federal agencies, as well as continued...

---

**COVID-19: FDA and USDA Guidance on Worker Safety and Sanitation in Food Production Facilities**

**Bryan Cave Leighton Paisner LLP**

As the COVID-19 pandemic has continued to escalate, both the Food and Drug Administration ("FDA") and the U.S. Department of Agriculture ("USDA")...

---

**COVID-19 Employment Law Update: Employer Rights and Responsibilities Following Additional Guidance from the EEOC on the ADA, ADEA and Title VII**  
**Greenbaum, Rowe, Smith & Davis LLP**

Because COVID-19 is now considered a direct threat, employers are afforded greater latitude in the invasiveness of their medical inquiries and...

---

**Employment Question of the Day: April 2, 2020**

**Fredrikson & Byron PA**

COVID-19 is impacting businesses across the country, and employers are being forced to reduce employee costs. Each day, more and more employers are...

---

**Time Is Money: A Quick Wage-Hour Tip on ... Joint Employer Status Under the Fair Labor Standards Act**

**Epstein Becker Green**

With the March 16, 2020 effective date of the new rule interpreting joint employer status under the Fair Labor Standards Act ("FLSA") almost upon us...

---

**Five things you should know about the DOL's new Coronavirus paid leave rules**  
**Thompson Coburn LLP**

The U.S. Department of Labor has issued its interim rule implementing the paid leave rules mandated by the Families First Coronavirus Response Act...

---

**COVID-19 Washington Update: March 30, 2020** Washington

**Kelley Drye & Warren LLP**

Today (and over the weekend) federal response to the COVID-19 pandemic included announcements from the White House and various federal agencies, as...

---

**New York Passes Paid Sick Leave Through Budget** New York

**Goldberg Segalla LLP**

The budgetary process in New York has long included legislation affecting employers doing business in New York. Many will recall that New York Paid...

---

## **Maryland's Stay at Home Order and Maryland Businesses**

Maryland

### **Venable LLP**

As of 8:00 p.m. On March 30, 2020, Governor Hogan's state-wide stay at home order was put in place, further impacting the employees, operations, and...

---

## **Working From Home Has Its Challenges...**

### **Holland & Hart LLP**

My daycare and commuting circumstances have changed and I would like to make changes to my cafeteria plan elections. Am I permitted to revoke or...

---

## **NLRB Delays Effective Date of 'Election Protection' Final Rule**

### **Ogletree Deakins**

On March 31, 2020, the National Labor Relations Board (NLRB) announced that it had finalized a series of amendments to its blocking-charge policy...

---

## **Employment Question of the Day: April 3, 2020**

### **Fredrikson & Byron PA**

As you likely know now, the Families First Coronavirus Response Act (FFCRA) applies to all private employers with fewer than 500 employees. Therefore...

---

## **Coronavirus Job Retention Scheme**

### **Travers Smith LLP**

The Coronavirus Job Retention Scheme (Scheme) is a government-funded scheme that provides a contribution towards wage costs for employers who stand...

---

## **Staffing Alternatives for Community Residential Settings: Leasing Employees from Day Training and Habilitation Programs During the COVID-19 Outbreak**

### **Fredrikson & Byron PA**

The staffing shortage faced by Minnesota's Community Residential Settings (CRS) has been exacerbated by the COVID-19 outbreak, making it even more...

---

## **New York State Enacts New Non-COVID Sick Leave Entitlements**

New York

### **Manatt Phelps & Phillips LLP**

On April 3, 2020, New York Governor Andrew Cuomo signed into law legislation creating completely new, non-COVID-related sick leave entitlements for...

---

## **L.A. Mayor Issues Order Requiring Large Employers To Provide COVID-19 Paid Sick Leave**

### **Manatt Phelps & Phillips LLP**

On March 27, 2020, the City of Los Angeles passed the COVID-19 Supplemental Paid Sick Leave ordinance (SPSLO), which was signed into law by Mayor...

---

## **No Rest for the Weary - DOL Adds to Q&A Guidance**

### **Shawe Rosenthal LLP**

The Department of Labor continues to issue guidance on the Families First Coronavirus Response Act. Following issuance on April 1, 2020 of its...



---

## **SBA Issues Continued Guidance on PPP Loans**

### **Bradley Arant Boult Cummings LLP**

On April 7, 2020, the Small Business Administration (SBA) issued additional guidance on the Paycheck Protection Program (PPP) in the form of answers...

---

## **New York Law Mandates Prevailing Wage for Private Construction** New York

### **Jackson Lewis PC**

Private construction projects in New York will become subject to new prevailing wage requirements pursuant to legislation signed by Governor Andrew...

---

## **New York State Enacts Sick Leave Law** New York

### **Epstein Becker Green**

On March 17, 2020, Governor Andrew Cuomo announced a three-way agreement with the New York State Legislature that includes, in addition to mandatory...

---

## **FFCRA leave management spreadsheet updated DOL guidance on ffcra and more**

### **Stradling Yocca Carlson & Rauth**

Stradling has prepared a spreadsheet that allows employers to track employee eligibility for Emergency Paid Sick Leave (EPSL) and Expanded Family and...

---

## **California Court of Appeal Addresses Whether There are Limits to Vacation Payout Requirement for "Unlimited" Vacation Policies** California

### **Little Mendelson PC**

On April 1, 2020, a California Court of Appeal issued a long-awaited decision relating to the use of so-called "unlimited" vacation plans. In...

---

## **Various Cities in South Florida Require Residents and Workers to Wear Face Masks** Florida

### **Smith Currie & Hancock**

The City of Miami and the City of Miami Beach issued emergency orders that require all employees and customers in grocery stores, restaurants...

---

## **Massachusetts Business Litigation Session Rejects "ABC Test" for Joint Employer Status** Massachusetts

### **Seyfarth Shaw LLP**

In an attempt to extend the reach of state wage/hour laws to reach more defendants, Plaintiffs' lawyers have sought to expand the employment...

---

## **10th Circuit Upholds Hospital's Rejection of Applicant Under ADA**

### **Holland & Hart LLP**

The rules surrounding medical examinations under the Americans with Disabilities Act (ADA) can be tricky. The U.S. 10th Circuit Court of Appeals...

---

## **City of Los Angeles Supplemental COVID-19 Paid Sick Leave Will Proceed, but As Superseded by the Mayor's Public Order** California

### **Jackson Lewis PC**

On March 27, 2020, the City of Los Angeles City Council passed an ordinance requiring that employers with 500 or more employees nationally offer 80...

---

### **Checklist For Managing Work-From-Home Employees During the Pandemic**

#### **Baker McKenzie**

The COVID-19 pandemic has forced employers to require many employees to work from home. To assist employers in updating and implementing these...

---

### **LA tries to close gap left by Families First**

#### **Constangy Brooks Smith & Prophete LLP**

On March 27, the Los Angeles City Council passed a paid sick leave ordinance to require that large employers provide additional paid sick leave for...

---

### **Executive Order No. 7V and COVID-19: Connecticut Governor Issues Safe Workplace Rules for Essential Businesses and Essential Employees**

Connecticut

#### **Gordon Rees Scully Mansukhani**

On April 7, 2020, Connecticut Governor Ned Lamont issued Executive Order No. 7V, titled "Protection of Public Health and Safety During Covid-19..."

---

### **Employer Obligations to Notify Employees of Wage Reductions**

#### **Jackson Lewis PC**

As wage reductions become a common solution to the uncertain environment resulting from the COVID-19 pandemic, U.S. employers have had to make some...

---

### **A Herculean Task: Proving a Competitor's Knowledge and Participation in an Unfair Competition Case**

Texas

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: A recent case out of the Court of Appeals in Houston, Texas highlights the challenges in proving liability against a third-party...

---

### **State and Local Leave Initiatives and Responses to the COVID-19 Pandemic**

#### **Morgan Lewis**

In addition to the federal government action to provide paid leave to workers impacted by the coronavirus (COVID-19) outbreak, numerous states and...

---

### **Disclaiming Implied Warranties in New Home Contracts**

#### **Bradley Arant Boult Cummings LLP**

In many states, the implied warranties of workmanship and habitability automatically attach to contracts between builder-vendors and new home buyers...

---

### **State Notice Requirements for Employee Pay Reductions**

#### **Pepper Hamilton LLP**

In response to the financial pressures of the COVID-19 crisis, many employers are considering pay reductions as an alternative to...



---

## **Key Employment-Related Provisions in Newly Enacted CARES Act**

### **Hunton Andrews Kurth LLP**

On March 27, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act (CARES), an unprecedented \$2 trillion economic...

---

## **Senate-Passed COVID-19 Legislation Includes Payroll Tax Provisions**

### **Covington & Burling LLP**

Late Wednesday night, the Senate passed (96-0) the Coronavirus Aid, Relief, and Economic Security ("CARES") Act, the third Coronavirus-related piece...

---

## **COVID-19 CARES Act Paycheck Protection Program Interim Final Rule Updates**

### **Day Pitney LLP**

On April 2, the U.S. Treasury released Paycheck Protection Program - Interim Final Rule, which provides formal guidance to the Paycheck Protection...

---

## **Illinois Implements Mandatory Sexual Harassment Prevention for Employers to be Completed by December 31, 2020**

[Illinois](#)

### **Baker Sterchi Cowden & Rice LLC**

Public Act 101-0221, the Workplace Transparency Act, amended the Illinois Human Rights Act ("IHRA") and now requires Illinois employers to provide...

---

## **Los Angeles, New York Impose New Construction Requirements and Restrictions Due to COVID-19**

[California](#)

[New York](#)

### **Jackson Lewis PC**

While the Occupational Safety and Health Administration (OSHA) and some states have offered guidance to prevent employee exposure to COVID-19, Los...

---

## **DOL Regulations: Employee Leave under the Families First Coronavirus Response Act**

### **Nelson Mullins Riley & Scarborough LLP**

The United States Department of Labor ("DOL") released temporary regulations ("regulations" or "guidance") interpreting the Families First Coronavirus...

---

## **Whistleblowers Watch Stimulus Money From Inside**

### **Squire Patton Boggs**

Whistleblowers watch from inside when a business receives stimulus money. Whistleblowers, with their unique access to business operations, follow the...

---

## **Are Essential Employees Required to Wear Masks/Face Coverings in the Workplace?**

### **Crowell & Moring LLP**

On Friday, April 3, 2020, the Centers for Disease Control and Prevention (CDC) issued guidance recommending that individuals wear cloth face...

---

## **Many Voices, One Community Podcast**

[Audio](#)

### **DLA Piper**

In the first episode of DLA Piper's Many Voices, One Community podcast, partner Cara Edwards and Catalyst...

---

### **Retail Industry Best Practices During the COVID-19 Pandemic** California

#### **Step toe & Johnson LLP**

As more states issue "stay-at-home" orders to reduce the spread of the coronavirus, a majority of retailers have shuttered all of their stores - for...

---

### **Contagious: US Class Actions and Anticipated Trends Based on the COVID-19 Pandemic**

#### **Baker McKenzie**

As the number of COVID-19 cases around the world continues to rise, governments are ordering people to self-quarantine at home to limit the spread of...

---

### **COVID-19 Entertainment Update: Guidance for Entertainment Companies**

#### **Skadden Arps Slate Meagher & Flom LLP**

The global coronavirus (COVID-19) crisis continues to have a devastating impact across all segments of the entertainment industry. The cancellation or...

---

### **Update #2: Waterloo, Iowa Enacts Ban the Box Restrictions** Iowa

#### **Seyfarth Shaw LLP**

On April 3, 2020, the lawsuit brought by the Iowa Association of Business and Industry (the "Association") against the City of Waterloo and the...

---

### **DC Council Adopts Expanded Sick Leave, Unemployment Amendments**

#### **Littler Mendelson PC**

On April 7, 2020, the D.C. Council unanimously passed its second emergency COVID-19 relief bill, the COVID-19 Response Supplemental Emergency...

---

### **Texas Federal Court Rules Dallas's Paid Sick Leave Ordinance Unconstitutional**

Texas

#### **Hunton Andrews Kurth LLP**

As detailed in our previous alert on this issue, on August 1, 2019, Dallas joined a host of states, cities and counties across the country when it...

---

### **#WorkforceWednesday: FFCRA Regulations, COVID-19 and Multinational Employers, Data Protection**

#### **Epstein Becker Green**

Last week, the U.S. Department of Labor issued temporary regulations providing clarification on the Families First Coronavirus Response Act (FFCRA)...

---

### **The DOL's Temporary Rule About FFCRA Paid Leave Provides More Guidance**

#### **Nutter McClennen & Fish LLP**

The U.S. Department of Labor issued a Temporary Rule on April 1 providing further guidance with respect to the paid leave available under the...

---



**Los Angeles City Passes New Ordinance Requiring Large Employers to Provide Paid Sick Leave in Addition to Pre-Existing State and Local Paid Sick Leave Mandates** California

**Goldberg Segalla LLP**

Los Angeles City passed a new paid sick leave ordinance on March 27, 2020, created to close a “loophole” under the federal Families First Coronavirus...

---

**UPDATE: Extension of Georgia Statewide Shelter-In-Place Order** Georgia

**Smith Currie & Hancock**

On April 8, 2020, Brian Kemp, Georgia Governor, issued Executive Order 04.08.20.02, which extends the Georgia Shelter In Place Order for a period of...

---

**CARES Act Augments Small Business Loan Programs: What You Need to Know to Act Now**

**Bradley Arant Boult Cummings LLP**

On Friday, March 27, 2020, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) intending to address...

---

**Labor & Employment Alert: Guidance on Ohio Unemployment Compensation**

Ohio

**Brouse McDowell**

For employers contemplating/in the midst of instituting layoffs/furloughs, the State is requesting that you provide your laid off employees with...

---

**Documentation Requirements for COVID-19-Related Leave**

**Patterson Belknap Webb & Tyler LLP**

As employees begin requesting leave under the recently-passed New York legislation providing COVID-19-related sick leave (the “New York Act”) and the...

---

**DOL Clarifies Certification for Covered Reasons to Take FFCRA Leave: Part Two in a Five-Part Series**

**Squire Patton Boggs**

In the first installment of this five-part series exploring the US Department of Labor (DOL) regulations (29 CFR Part 826) interpreting the Families...

---

**CARES Act**

**Bass, Berry & Sims PLC**

The bipartisan Coronavirus Aid, Relief, and Economic Security Act (CARES Act) became effective Friday, March 27, following overwhelming approval by...

---

**Protecting Multi-Tenant Residential Maintenance Employees from COVID-19**

**Goulston & Storrs PC**

Multi-tenant residential housing properties face numerous financial and operational challenges from the outbreak of Coronavirus disease 2019...

---

**San Francisco Expected to Require Employers with 500 or More Employees to Provide Paid Public Health Emergency Leave**

### **Littler Mendelson PC**

On April 7, 2020, the San Francisco Board of Supervisors adopted an emergency ordinance (the "PHELO") that requires private employers with 500 or...

---

### **The L.A. Story of Supplemental Paid Sick Leave**

#### **Littler Mendelson PC**

Things have been pretty chaotic and confusing for employers and employees during the COVID-19 public health emergency. Unfortunately, in an effort to...

---

### **Cal/OSHA Issues Guidance for Agricultural Employers on COVID-19 Infection Prevention**

#### **Littler Mendelson PC**

The California Division of Occupational Safety and Health, better known as Cal/OSHA, recently issued safety and health guidance for agricultural...

---

### **Aggregation Rules May Prevent Private Equity Portfolio Companies From Taking Full Advantage of the New Employee Retention Credit Under The CARES Act**

#### **Kramer Levin Naftalis & Frankel LLP**

Section 2301 of the recent Coronavirus Aid, Relief, and Economic Security (CARES) Act (the Act) provides "eligible employers" with a refundable credit...

---

### **New Jersey Executive Order No. 122 Mandates Stricter Protocols for Businesses During COVID-19 Pandemic**

New Jersey

#### **Day Pitney LLP**

In his continuing effort to mitigate community spread of COVID-19, New Jersey Governor Murphy signed Executive Order No. 122 on April 8. The Order...

---

### **New Jersey Restricts Nonessential Construction; Issues New Mandates for Retail, Manufacturing, Warehouses and Essential Construction**

New Jersey

#### **Fox Rothschild LLP**

New Jersey Gov. Phil Murphy issued Executive Order No. 122 on Wednesday, April 8, 2020, halting all nonessential construction projects and placing...

---

### **New York Passes Statewide Paid Sick Leave Law**

New York

#### **Baker & Hostetler LLP**

Just weeks after New York state implemented an Emergency COVID-19 Paid Sick Leave Law, late last week, New York state passed a statewide paid sick...

---

### **Dealing with Employee Protests and Strikes due to COVID-19 Concerns**

#### **Cozen O'Connor**

The COVID-19 outbreak has rendered many workplaces dormant, but frontline workers in the grocery, delivery, and medical fields are feeling the...

---

### **Salaried-Basis Employees in the World of Temporary COVID-19 Furloughs**

#### **Barnes & Thornburg LLP**

In light of the COVID-19 pandemic, workplaces across the country are experiencing fast-paced furloughs (temporary layoffs). In the haste to



implement...

---

### **New L.A. Order Requires Employers to Provide Face Coverings**

#### **Manatt Phelps & Phillips LLP**

On April 7, 2020, Los Angeles Mayor Eric Garcetti issued an emergency order requiring nonmedical essential workers to wear nonmedical-grade face...

---

### **NLRB General Counsel Releases Emergency Bargaining Case Summaries**

#### **Hunton Andrews Kurth LLP**

An employer's duty to bargain may change during emergency situations, and the General Counsel for the National Labor Relations Board released a...

---

### **Ninth Circuit Strikes Down California Wage Statement Class Action for Plaintiff's Failure to Show "Real World Consequences" to Establish Standing**

#### **Hunton Andrews Kurth LLP**

The Ninth Circuit recently overturned a district court's grant of class certification on a wage statement claim under California Labor Code §226...

---

### **Connecticut Imposes 'Safe Workplace' Rules for Essential Businesses**

Connecticut

#### **Jackson Lewis PC**

Connecticut Governor Ned Lamont and the Connecticut Department of Economic and Community Development (DECD) have issued new "legally binding" rules...

---

### **Key Employment-Related Provisions In Newly-Enacted CARES Act**

#### **Hunton Andrews Kurth LLP**

On March 27, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act ("CARES"), an unprecedented \$2 trillion economic...

---

### **Mastering Work from Home during COVID-19: Avoiding the Pajama Predicament and Other Pitfalls**

Audio

#### **Ogletree Deakins**

Many employers and public accommodations are seeing an increase in requests for animals as an accommodation under the Americans with Disabilities Act...

---

### **CA Exempts PPE From Sales and Use Taxes Before Agreeing to Acquire 200 Million PPE Items Monthly**

Texas

#### **Manatt Phelps & Phillips LLP**

As requirements for donning personal protective equipment (PPE) grow for essential workers, the government is working to balance PPE demand while...

---

### **Documentation Requirements for Payroll Tax Credits and Employee Eligibility Under FFCRA**

#### **Brownstein Hyatt Farber Schreck LLP**

Under the Families First Coronavirus Response Act (FFCRA), employers with fewer than 500 employees are required to provide certain paid sick and...

---

## **Knowing the Way to San Jose's Emergency Paid Sick Leave Ordinance**

### **Littler Mendelson PC**

On April 7, 2020, the San Jose, California City Council adopted two essentially identical ordinances that require covered employers to provide...

---

## **To Disclose or Not to Disclose: Why Businesses Should Not Stay Silent Amid COVID-19**

### **Dickinson Wright**

As of publication, the coronavirus disease 2019 (COVID-19 or the "coronavirus") has evolved into a global pandemic, affecting more than 180 countries...

---

## **COVID-19 and California Workers' Compensation Claims: Compensability and Risk Avoidance Considerations**

California

### **Goldberg Segalla LLP**

Throughout California, officials have responded to the threat of the novel coronavirus and COVID-19 by closing down schools, banning large gatherings...

---

## **UberBLACK Drivers May Be Employees, Not Independent Contractors**

### **Shawe Rosenthal LLP**

In another case of interest regarding the gig economy, the U.S. Court of Appeals for the Third Circuit reversed a federal district court ruling that...

---

## **Coronavirus Relief Bill Update**

### **Masuda Funai Eifert & Mitchell Ltd**

Under the mandate of the Families First Coronavirus Response Act ("Act"), the U.S. Department of Labor ("DOL") announced that the effective date is...

---

## **Department of Labor's New Regulations and Guidance on the Family First Coronavirus Relief Act ("FFCRA")**

### **Buchalter**

On April 6, 2020, the Department of Labor ("DOL") promulgated a temporary rule ("Rule") interpreting and giving further guidance on the Families...

---

## **SEC Awards \$2 Million to Whistleblower**

### **Cadwalader Wickersham & Taft LLP**

The SEC awarded \$2 million to a whistleblower for providing information that led to a successful enforcement action. According to the SEC, the...

---

## **California Revises Guidance on Conditional Suspension of WARN Act Notice Requirements**

California

### **Manatt Phelps & Phillips LLP**

California employers faced with difficult layoff decisions were provided additional guidance by the Department of Industrial Relations (DIR)...

---

## **Federal Judge Scales Back Nationwide Class Claims in Case of Escaping Gerbils**

California

### **Hunton Andrews Kurth LLP**



In a favorable decision for retailers, a California federal court judge scaled back a proposed class action seeking to bring nationwide class claims...

---

**NDAs may be bad politics, but they are good business**

**Raymond Law Group LLC**

Michael Bloomberg is no longer in the presidential race, yet many still remember how he was taken to task by Elizabeth Warren. The two were part of a...

---

**Client Alert: McMaster Extends Unemployment Benefits to Furloughed Workers**

**Shumaker Loop & Kendrick**

South Carolina Governor Henry McMaster signed Executive Order No. 2020-22, extending unemployment benefits to workers furloughed with pay during the...

---

**Center for Disease Control Issues Interim Guidance for Implementing Safety Practices for Employees Exposed to Person with Suspected or Confirmed COVID-19**

**Clingen Callow & McLean LLC**

On April 8, 2020, the US Center for Disease Control issued interim guidance, found here ("Interim Guidance"), for critical infrastructure workers...

---

**Massachusetts Extends Non-Essential Business Closures Until May 4 and Updates List of Essential Services**

[Massachusetts](#)

**Greenberg Traurig LLP**

On March 31, 2020, Massachusetts Governor Charlie Baker announced several updates related to the COVID-19 outbreak, including extending the...

---

**UK's landmark group claim for compensation under data protection laws - Morrison's found not vicariously liable for actions of rogue employee**

**Ropes & Gray LLP**

A landmark group claim for compensation under data protection laws in the UK between employees and employer has failed. The UK's Supreme Court has...

---

**US Department of Labor Publishes Regulations Clarifying Various Aspects of the Families First Coronavirus Response Act (US)**

**Squire Patton Boggs**

Some questions answered, many still remain On April 1, 2020, the U.S. Department of Labor (DOL) released new regulations (29 CFR Part 826), attempting...

---

**DOL Issues Families First Coronavirus Response Act Regulations**

**Pepper Hamilton LLP**

On April 1, the U.S. Department of Labor (DOL) posted a temporary rule issuing regulations pursuant to the Emergency Paid Sick Leave Act...

---

**Highlights of the cumulative DOL guidance and regulations include the following:**

**Venable LLP**

The Wage and Hour Division of the U.S. Department of Labor (DOL) has issued guidance that provides answers to commonly asked questions that have...

---

**Coronavirus: Employee furloughs, reductions-in-force and similar temporary cost-saving measures in the US - Part 1**

**DLA Piper**

The rapidly evolving coronavirus disease 2019 (COVID-19) pandemic is affecting employers in numerous ways, including critical challenges to...

---

**CISA Updates Guidance on Essential Critical Infrastructure Workers; More States Issue Stay-at-Home Orders**

**Bradley Arant Boult Cummings LLP**

Over the weekend, the Cybersecurity & Infrastructure Security Agency (CISA) issued updated guidance expounding on its classification of workers who...

---

**Additional OSHA Guidance on COVID-19**

**Robinson & Cole LLP**

OSHA previously issued guidance on preparing workplaces for COVID-19, which we covered on the blog a few weeks ago. The agency has been busy issuing...

---

**Thailand: State of Emergency and Imposed Measures to Contain COVID-19 and Implications for Employers**

**Baker McKenzie**

As we continue to face and operate in an environment of considerable uncertainty due to the COVID-19 pandemic, organizations around the world have...

---

**Public Charity Spin-Off**

**Morrison & Foerster LLP**

As corporations explore how best to address the current crisis—both health and economic—posed by COVID-19, many are looking to utilize their existing...

---

**DOL Provides Further Guidance on FFCRA's Emergency Paid Sick Leave and Emergency Family Medical Leave and Publishes Required Poster**

**Goldberg Segalla LLP**

On March 19, 2020, Goldberg Segalla's Employment and Labor team issued an alert summarizing the basic requirements of the Families First Coronavirus...

---

**New York Enacts Mandatory Sick Leave Law**

New York

**Kelley Drye & Warren LLP**

Amidst the COVID-19 melee, the New York Legislature passed its Budget for Fiscal Year 2021, which included a mandatory paid sick leave bill, signed...

---

**Emerging Technologies Washington Update - Coronavirus Response**

**McGuireWoods Consulting LLC**

The Paycheck Protection Program (PPP), the \$349 billion CARES Act loan program for small businesses and eligible individuals, launched last Friday to...

---



## **Massachusetts Court Provides Guidance on Joint Employer Liability and the Scope of the Outside Salesperson Exemption**

Massachusetts

### **Littler Mendelson PC**

In *Jinks v. Credico (USA) LLC* (March 31, 2020), Judge Kenneth Salinger in the Business Litigation Session of the Massachusetts Superior Court...

---

## **NJ Governor Orders Non-Essential Brick-and-Mortar Retail Closure, Remote Work Implementation**

New Jersey

### **Morgan Lewis**

New Jersey Governor Phil Murphy on March 21 signed Executive Orders 107 and 108, which took effect at 9:00 pm the same day. Executive Order 107...

---

## **Michigan Extends “Stay Home, Stay Safe” Order with Additional Restrictions on Retail Businesses**

### **Littler Mendelson PC**

NOTE: Because the COVID-19 situation is dynamic, with new governmental measures each day, employers should consult with counsel for the latest...

---

## **CORONAVIRUS RELIEF BILL: The CARES Act - Provisions Affecting U.S. Employers and Employees, Part II**

### **Bryan Cave Leighton Paisner LLP**

The Coronavirus Aid, Relief, and Economic Security Act (“CARES Act” or “Act”), enacted on March 27, 2020, has been the subject of government agency...

---

## **Mayor Garcetti Signs Emergency Orders Increasing Worker Protections and Mandating Supplemental Paid Sick Leave**

### **Payne & Fears LLP**

An Employer with more than 500 employees within the City of Los Angeles or more than 2,000 employees withi...

---

## **New Guidance Tightens COVID-19 Restrictions on Massachusetts Employers, and the Massachusetts Attorney General Revises Guidance on Furloughs**

Massachusetts

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 7, 2020, the Massachusetts Executive Office of Housing and Economic Development (“EOHED”) issued its updated COVID-19...

---

## **Mississippi Governor Issues State-Wide Shelter-In-Place Order**

Mississippi

### **Fisher Phillips**

Mississippi Governor Tate Reeves recently issued Executive Order No. 1466 requiring all residents of the state to remain in their homes until April...

---

## **Labor & Employment Alert: Update On the Federal Government’s \$600 Unemployment Increase**

### **Brouse McDowell**

Based on information published by the Department of Labor (DOL) last Saturday, here is an update on what is happening with the Federal...

---

### **“Protecting IP Assets”**

#### **Quarles & Brady LLP**

With so many people working from home, many of the safeguards and systems that companies rely on to protect their information become less effective...

---

### **OSHA to Most Employers: Limited Exemption from Recording Requirement for Employees' COVID 19 Cases**

#### **Jenner & Block LLP**

By Gabrielle Sigel, Co-Chair, Environmental and Workplace Health and Safety Law Practice On April 10, 2020, US OSHA partially retracted its initial...

---

### **Insights: SBA Seeks to Quell Concerns over Lender Liability in the Paycheck Protection Program**

#### **Boies Schiller Flexner LLP**

On March 27, 2020, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act. The CARES Act created the \$349 billion...

---

### **Employment Question of the Day: April 8, 2020**

#### **Fredrikson & Byron PA**

The COVID-19 outbreak has wreaked havoc on American businesses, as millions of employees have lost their jobs and many businesses have been forced to...

---

### **LA Mayor Issues Emergency Order Providing Paid Sick Leave to Certain Employees Affected by COVID-19**

#### **Paul Hastings LLP**

Los Angeles Mayor Eric Garcetti declined to sign the City Council's March 27, 2020 Supplemental Sick Leave Ordinance, opining that it imposed...

---

### **IRS provides guidance permitting employers to immediately receive covid-19-related tax credits**

#### **Shearman & Sterling LLP**

The Families First Coronavirus Response Act (the “Families First Act”) and the Coronavirus Aid, Relief, and Economic Security Act (“CARES Act”)...

---

### **PPP Affiliation Not What it Used to Be**

#### **Lane Powell PC**

What a difference a week can make! COVID-19 is requiring constant adaptation and flexibility on a scale not seen in our lifetimes on all sorts of...

---

### **The Families First Coronavirus Response Act: What You Need to Know - Updated on March 19, 2020**

#### **McDermott Will & Emery**

The Families First Coronavirus Response Act (H.R. 6201) was signed into law on March 18, 2020. This summary reflects these changes. Would...

---

### **New York Enacts Statewide Permanent Paid Sick Leave Law**

[New York](#)



## **Ius Laboris**

New York State Governor Andrew M. Cuomo has signed into law a permanent program for unpaid and paid sick leave for all New York employees. This...

---

## **FFCRA Leave Regulations Issued by DOL on April 1 Revise and Expand FAQs**

### **Quarles & Brady LLP**

On April 1, the Department of Labor (DOL) released temporary regulations that effectuate the Emergency Paid Sick Leave Act (EPSLA) and Emergency...

---

## **Michigan Extends Its Stay-at-Home Order Through April 30, 2020**

Michigan

### **Ogletree Deakins**

On April 9, 2020, Michigan Governor Gretchen Whitmer issued an updated "Stay Home, Stay Safe" Executive Order (EO) 2020-42, which extends the state's...

---

## **"Paycheck Protection Program" Loans: SBA Guidance Continues to Trickle Out, Provides Potential Opportunity for Applicants with Foreign Operations**

### **Quarles & Brady LLP**

Small businesses and their lenders received additional guidance from the U.S. Small Business Administration ("SBA") on the new Paycheck Protection...

---

## **District of Columbia Expands D.C.'s FMLA and Unemployment Insurance Provisions**

District of Columbia

### **Quarles & Brady LLP**

The District of Columbia City Council enacted emergency COVID-19 legislation on March 17, 2020, the COVID-19 Response Emergency Amendment Act (the...

---

## **Massachusetts CARES: The Commonwealth Implements the CARES Act's Unemployment Benefits**

Massachusetts

### **Little Mendelson PC**

On Thursday, April 9, 2020, Massachusetts Governor Charlie Baker's administration announced the partial implementation of unemployment benefits in...

---

## **CARES Act: Mid-Sized Business Lending Program**

### **White & Case LLP**

Under Title IV of the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act"), Congress has authorized US\$500 billion of funding for...

---

## **New York Employers' Leave Obligations for COVID-19 Absences Under Federal, State and Local Law**

New York

### **Fox Rothschild LLP**

If you are a New York employer and trying to make sense of how new and old paid leave laws apply to your employees affected by COVID-19, you are not...

---

## **CDC Issues Guidance on Potential COVID-19 Exposure in Critical Infrastructure**

### **Quarles & Brady LLP**

Last night, the Centers for Disease Control and Prevention ("CDC") set forth

safety guidelines [cdc.gov] for critical infrastructure employers to...

---

**New York Court of Appeals Delivers News to Employers in Postmates Case: Couriers are Employees, Not Independent Contractors** [New York](#)

**Patterson Belknap Webb & Tyler LLP**

The New York State Court of Appeals recently issued a decision in a closely-watched case that helps to clarify the landscape regarding independent...

---

**New York State Enacts Paid Sick Leave Law** [New York](#)

**Ogletree Deakins**

On April 3, 2020, the State of New York enacted a long-expected statewide paid sick leave law that will impact all private employers in New York. The...

---

**New York Enacts Mandatory Sick Leave Law** [New York](#)

**Kelley Drye & Warren LLP**

Amidst the COVID-19 melee, the New York Legislature passed its Budget for Fiscal Year 2021, which included a mandatory paid sick leave bill, signed...

---

**CARES Act: Calculating Employee Headcount Under SBA "Affiliation Rules"**

**Frankfurt Kurnit Klein & Selz PC**

The recently passed Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act") expands the availability of certain loans administered by the...

---

**"Employees Cannot Mandate an Accommodation"**

**Shawe Rosenthal LLP**

As the U.S. Court of Appeals for the Sixth Circuit found, an employee must engage in the reasonable accommodation process and must provide medical...

---

**South Carolina Governor Authorizes Use of COVID-19 Support Payments by Employers to Employees** [South Carolina](#)

**Jackson Lewis PC**

South Carolina Governor Henry McMaster has issued Executive Order No. 2020-22, which allows employers to make voluntary "COVID-19 Support Payments"...

---

**Update on Most Recent US DOL Guidance on Unemployment Provisions of CARES Act (US)**

**Squire Patton Boggs**

The US Department of Labor (DOL) has issued a number of publications offering guidance to the states for implementing certain federal unemployment...

---

**New Judicial Guidance Addresses No-Accrual Vacation Policies Under California Law** [California](#)

**Paul Hastings LLP**

Employers increasingly offer a fringe benefit that many employees find attractive: unlimited, but unaccrued, paid vacation or time off ("PTO"). Under...

---



## **CARES Act Offers Liquidity to Eligible Businesses and Mid-Sized Companies (500 - 10,000 employees)**

### **Dykema Gossett PLLC**

Insight on Eligibility and Requirements for Obtaining Financial Assistance For Mid-Sized Companies and Eligible Businesses (other than Air Carriers...

---

## **Michigan Governor Issues Executive Order Creating Protected Class of COVID-19 Positive Employees** Michigan

### **Dykema Gossett PLLC**

In an apparent attempt to further reduce the spread of COVID-19 in Michigan, on Friday, April 3, Michigan Governor Gretchen Whitmer issued Executive...

---

## **New York Adopts Statewide Sick and Safe Leave Law** New York

### **McGuireWoods LLP**

On April 3, the State of New York amended the New York Labor Law to provide sick and safe leave for all New York employees, joining the numerous...

---

## **COVID-19 and Emergency Leave Plans, Retirement Saving, and Insider Trading** **Bryan Cave Leighton Paisner LLP**

The devastating impact of the Coronavirus (COVID-19) needs no introduction. BCLP has consolidated all of its client alerts regarding Coronavirus...

---

## **Sealing Criminal Records - The Basics** Illinois

### **Amal Law Group**

The majority of criminal convictions in Illinois, regardless of class, are sealable, including Class X felonies. (20 ILCS 2630/5.2). This means that...

---

## **CDC Updates Guidance for Critical Infrastructure Workers Exposed to COVID-19** **Littler Mendelson PC**

In yet another significant move, on April 8, 2020, the U.S. Centers for Disease Control and Prevention (CDC) published additional guidance for...

---

## **Today in Washington - April 10, 2020: COVID-19 Updates** Washington

### **Hall Render Killian Heath & Lyman PC**

HHS announced delivery of the initial \$30 billion in relief funding to providers that is part of the \$100 billion relief fund provided for in the...

---

## **CARES Act Employee Retention Tax Credit Guide for Employers**

### **Brownstein Hyatt Farber Schreck LLP**

The Coronavirus Aid, Relief, and Economic Security (CARES) Act provides access to a tax credit for employers whose businesses have been impacted by...

---

## **The Coronavirus Aid, Relief, and Economic Security Act: Significant Provisions for Employers**

### **Hogan Lovells**

On March 27, 2020, the President signed into law a massive two trillion dollar stimulus bill addressing a wide range of challenges to our economy...

---

**State and Local Tax Responses to COVID-19: States Grapple with CARES Act Conformity; Additional States Extend Tax Filing and Payment Deadlines; State Tax Tribunals Postpone Hearings** [Massachusetts](#) [New Jersey](#)

**Baker McKenzie**

States and local jurisdictions continue to grapple with novel tax issues in response to the COVID-19 outbreak. On Friday, March 27, 2020, President...

---

**Labor & Employment Alert: \$1.6 Billion to Ohio Employers Approved to Overcome COVID-19** [Ohio](#)

**Brouse McDowell**

The Ohio Bureau of Workers' Compensation (Ohio BWC) Board of Directors today approved distribution of \$1.6 billion to Ohio employers to help them...

---

**Considerations when reducing executive salaries**

**Shearman & Sterling LLP**

In the wake of the market disruption caused by the COVID-19 outbreak, a number of employers have announced temporary salary reductions as a means of...

---

**COVID-19 Shelter-in-Place Orders May Be Threatening Trade Secrets: What to Know**

**Paul Hastings LLP**

The COVID-19 pandemic has fundamentally changed working life. To date, in the United States, approximately 85% of states have enacted shelter-in-place...

---

**Alternatives to Laying Off Employees: Benefits Available for Ohio Employees with Reduced Hours** [Ohio](#)

**Vorys Sater Seymour and Pease LLP**

As employers grapple with the economic effects of COVID-19, reductions in hours and furloughs present difficult-but-effective cost reduction...

---

**DOT Issues COVID-19 Enforcement Discretion for Cylinder Requalification Requirements**

**Keller and Heckman LLP**

On April 6, 2020, the U.S. Department of Transportation (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) issued a Notice of...

---

**DOL's new FFCRA Regulations and Q&As on COVID-19 paid leave clarify documentation and other requirements**

**Hogan Lovells**

On April 1, 2020, the Department of Labor ("DOL" or the "Department") issued regulations implementing the Families First Coronavirus Response Act...

---

**Seattle Bans Employers from Requiring Medical Verification for Paid Sick Leave for 60 Days** [Washington](#)

**Jackson Lewis PC**

Under Seattle's Paid Sick and Safe Time (PSST) law, an employer normally may



require verification (including a doctor's note) for the use of PSST...

---

### **National Guard members are protected under USERRA - What employers need to know about employees in the National Guard**

#### **Reed Smith LLP**

On April 1, 2020, U.S. Defense Secretary Mark Esper said that states have the option of using the National Guard to enforce stay-at-home orders amid...

---

### **State and Local Tax Responses to COVID-19: States Grapple with CARES Act Conformity; Additional States Extend Tax Filing and Payment Deadlines; State Tax Tribunals Postpone Hearings**

Massachusetts

New Jersey

#### **Baker McKenzie**

States and local jurisdictions continue to grapple with novel tax issues in response to the COVID-19 outbreak. On Friday, 27 March 2020, President...

---

### **Georgia's Shelter-in-Place Order imposes new restrictions in an effort to slow the spread of COVID-19**

Georgia

#### **Reed Smith LLP**

As COVID-19 continues to spread rapidly, with the number of confirmed cases in the U.S. well above 200,000, Georgia has now joined the growing number...

---

### **Interacting with State and Local Law Enforcement During the COVID-19 Crisis**

#### **Michael Best & Friedrich LLP**

With each passing day of the pandemic, state, county, and municipal authorities are entering unprecedented orders restricting the legal rights of...

---

### **California Assembly (Again) Considers Bill Requiring Employers to Accommodate Medical Cannabis Use**

California

#### **Seyfarth Shaw LLP**

Marijuana (cannabis) remains a Schedule I drug under the federal Controlled Substances Act. And, more than a decade ago, the California Supreme Court...

---

### **COVID-19 Weekly Round-up (06 April-12 April 2020)**

#### **Lexology PRO**

The COVID-19 pandemic is entering its peak phase across much of Europe and North America, with shelter-in-place orders issued in many US states and...

---

### **San Francisco and San Jose Seek to Implement Supplemental Paid Sick Leave Requirements for Larger Employers**

California

#### **Jackson Lewis PC**

Two California cities, San Francisco and San Jose adopted emergency ordinances to expand paid sick leave and emergency Family Medical Leave Act...

---

### **City of Los Angeles Orders Certain Employers to Protect Workers or Risk Imprisonment**

#### **Sheppard Mullin Richter & Hampton LLP**

On April 7, 2020, Mayor Eric Garcetti doubled down his efforts to curtail the

spread of the novel coronavirus in the workplace by issuing the Worker...

## **The New York Shared Work Program - An Alternative to Employee Layoffs** New

York

### **Wilson Elser**

New York employers continue to grapple with the sudden and long-term effects of the coronavirus pandemic and attendant stay-at-home and travel...

## **Title VII and COVID-19: Mitigating Community Spread of Workplace Discrimination**

### **Michael Best & Friedrich LLP**

The widespread proliferation of the 2019 novel Coronavirus across the United States is presenting a host of unprecedented challenges. National...

## **FAQs for Companies with Employees or Interests in Singapore**

### **Fisher Phillips**

Singapore, like many other countries, is amending its laws and regulations in light of the world-wide coronavirus pandemic. Here are answers to some...

## **FAQs: Section 139**

### **Baker & Hostetler LLP**

Various strategies including the creation of a "disaster relief fund," are being designed to qualify under Internal Revenue Code Section 139...

## **Los Angeles Joins the Trend, as States and Localities Adopt Face Covering Requirements**

### **Littler Mendelson PC**

NOTE: Because the COVID-19 situation is dynamic, with new governmental measures each day, employers should consult with counsel for the latest...

## **Paid Leave Under the Families First Coronavirus Response Act** Video

### **McGuireWoods LLP**

Join McGuireWoods labor and employment group as a follow-up to our March 24 webinar on the paid employee leave requirements of the federal Families...

## **NIOSH Posts Posters on 3D Printing with Filaments, Metal Powders**

### **Bergeson & Campbell PC**

The National Institute for Occupational Safety and Health (NIOSH) has posted two posters from the NIOSH Nanotechnology Research Center (NTRC) on 3D...

## **Revised Bay Area Health Orders Clarify, Extend, and Strengthen Prior Shelter-in-Place Orders**

### **Baker McKenzie**

With special thanks to Teresa Michaud and Sara Pitt for contributing. Revised Health Orders were handed down yesterday across the Bay Area (Alameda...

## **Updated: Are My Employees Exempt from Travel Restrictions as Critical Sector**



## **Employees Under the Minnesota Stay-At-Home Order?**

### **Fredrikson & Byron PA**

Minnesota's Governor issued a stay-at-home Order on March 25, 2020, and then extended this order on April 8, 2020. How do I know if my employees are...

---

## **Connecticut Issues Mandatory Safe Workplace Rules for Essential Businesses and Nonprofits Still in Operation Amid COVID-19 Pandemic**

Connecticut

### **Littler Mendelson PC**

On April 7, 2020, the governor of Connecticut issued Executive Order No. 7V ("EO 7V") which, among other things, requires every workplace in the...

---

## **New York State Enacts Paid Sick Leave Program and Extends PAUSE Restrictions (US)**

New York

### **Squire Patton Boggs**

In light of the ongoing pandemic crisis, on April 6, 2020, Governor Andrew Cuomo announced that he is extending the "PAUSE" restrictions in New York...

---

## **Newly Updated Workplace FAQs For Healthcare Providers And 8-Point COVID-19 Action Plan**

### **Fisher Phillips**

The healthcare industry is truly on the front lines of the nation's and the world's response to COVID-19. As a result, healthcare providers, their...

---

## **COVID 19: City Of Los Angeles Imposes New Paid Sick Leave Obligations on Employers With 500+ U.S. Employees**

California

### **Hunton Andrews Kurth LLP**

In the face of unprecedented challenges due to COVID-19, employers have been forced to balance the need to mitigate current health risks against the...

---

## **How to manage data protection requirements in times of COVID-19.**

### **Freshfields Bruckhaus Deringer**

The COVID-19 outbreak affects aspects - among many others - that are governed by data protection laws. Employers might have to take measures to...

---

## **Expansion of Eligibility and Additional Guidance on the Paycheck Protection Program (Title I of the CARES Act)**

### **Sheppard Mullin Richter & Hampton LLP**

On April 7, 2020, the U.S. Department of Treasury (Treasury) released a 4/7/2020 Frequently Asked Questions sheet (FAQ) with respect to the...

---

## **"Protecting Sensitive Company Information When Working Remotely"**

### **Quarles & Brady LLP**

With so many people working from home, many of the safeguards and systems that companies rely on to protect their information become less effective...

---

## **UK and US leave and pay provisions during coronavirus**

### **Ius Laboris**

Yes, employees will be entitled to the employer's usual sick leave and pay provisions, including statutory sick pay. The government has announced...

---

### **US: Comparing the Presidential Candidates' Labor Policies: Part One**

**Baker McKenzie**

In Part One of this two-part article, we examine the key labor policy proposals advanced by the leading Democratic contenders of the 2020 race - Sen...

---

### **A Toolkit for Directors & Officers of US Companies Amid COVID-19**

Delaware

**Goulston & Storrs PC**

The current COVID-19 crisis has rapidly re-shaped everyday life around the world, and our understanding of the impact this disruption to daily...

---

### **PA Mandates Unemployment Benefits Notice to Employees**

Pennsylvania

**Fox Rothschild LLP**

A new Pennsylvania law (Act 9 of 2020) requires Pennsylvania employers to provide notice to employees about unemployment compensation benefits at the...

---

### **Challenges in Returning Employees Back to Work After COVID-19**

Audio

**Littler Mendelson PC**

The novel coronavirus (COVID-19) has created significant workplace challenges across the United States. Many employers have had to restructure their...

---

### **How to Close Restaurant and Retail Businesses During Coronavirus and Plan for a Successful Reopen**

**Bowditch & Dewey LLP**

As the novel coronavirus impacts economies across the world small business owners are facing unprecedented challenges and making extremely difficult...

---

### **Staffing Company Liable for Low Level Employee's FLSA Violations**

**Shawe Rosenthal LLP**

In a warning to employers about their responsibility for the actions of low level employees under the FLSA, the U.S. Court of Appeals for the Ninth...

---

### **DOL Finalizes FFCRA Regulations**

**Holland & Hart LLP**

After days of uncertainty and looming deadlines created by the Families First Coronavirus Response Act (FFCRA), the DOL has finally issued some...

---

### **Cost-cutting considerations in the time of COVID-19 (Part 3 - employment issues outside the US)**

**DLA Piper**

As coronavirus disease 2019 (COVID-19) continues to impact the global economy in unprecedented ways, companies worldwide are facing difficult...

---

### **LA Mayor Issues Emergency Order Increasing Large Employers' Paid Sick Leave Obligations During COVID-19**



### **McGuireWoods LLP**

As McGuireWoods previously reported, in response to the Families First Coronavirus Response Act's (FFCRA) exclusion of private employers with 500 or...

---

### **Employer FAQs On Paycheck Protection Loans**

#### **Fisher Phillips**

The Coronavirus Aid, Relief and Economic Security (CARES) Act provides much-needed economic relief to businesses impacted by the COVID-19 crisis...

---

### **Unemployment Insurance Benefits under the CARES Act**

#### **Covington & Burling LLP**

In response to the growing unemployment numbers due to business slowdowns across the country, the Coronavirus Aid, Relief, and Economic Security...

---

### **New CDC Guidance for Employers When Employees Are Potentially Exposed to COVID-19**

#### **Crowell & Moring LLP**

On April 8, 2020, the Centers for Disease Control and Prevention (CDC) issued Interim Guidance for implementing safety practices for critical...

---

### **CARES Act Summary for Coops**

#### **Eversheds Sutherland (US) LLP**

On Friday, March 27, 2020, the President signed into law a massive stimulus package - the Coronavirus Aid Relief, and Economic Security (CARES) Act -...

---

### **South Carolina Allows Employers to Provide COVID-19 Support Payments to Furloughed Employees Receiving Unemployment Benefits**

South Carolina

#### **Ogletree Deakins**

On April 7, 2020, South Carolina Governor Henry McMaster issued Executive Order 2020-22. This order allows employers to provide furloughed employees...

---

### **Seyfarth Policy Matters Newsletter - April 3, 2020**

#### **Seyfarth Shaw LLP**

Department of Labor Issues Regulations on the Families First Coronavirus Response Act (FFCRA). On April 1, the Department of Labor issued final...

---

### **Psychiatric Workers' Compensation Disability Claims in a Pandemic Environment**

Michigan

#### **Foster Swift Collins & Smith PC**

There are scores of workers on the front lines fighting the consequences of the COVID-19 pandemic - doctors, nurses, EMTs, paramedics, police...

---

### **Employment Question of the Day: April 9, 2020**

#### **Fredrikson & Byron PA**

In Minnesota, an employee with COVID-19 is entitled to Workers' Compensation benefits only if he or she contracted the virus due to an exposure at...

---

## About-Face on Face Masks

### Akerman LLP

On Sunday, April 12, 2020, New York became the latest jurisdiction to require employers to supply cloth or surgical masks to employees who are...

---

## Discriminatory and Nondiscriminatory Comments Can Combine to Create Hostile Work Environment

### Shawe Rosenthal LLP

A hostile work environment can be created through a combination of both explicitly discriminatory and non-discriminatory (but offensive) comments...

---

## OSHA Relieves Most Employers from Recording COVID-19 Infections as Workplace Injuries

### Clingen Callow & McLean LLC

We have fielded the following question many times. "One of our employees has tested positive for COVID-19. Must we report this as a work-place..."

---

## The \$600 Billion Main Street Loan Programs: Is Your Technology or Life Sciences Company Eligible?

### Fenwick & West LLP

The Federal Reserve and Department of Treasury published additional details regarding two new loan programs that provide up to \$600 billion for...

---

## COVID-19 Pandemic Small Business Lending Under the CARES Act's Paycheck Protection Program

### Skadden Arps Slate Meagher & Flom LLP

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which became law on March 27, 2020, authorized \$349 billion for the Small Business...

---

## OSHA Issues Guidance for Employers in Package Delivery Industry

### Littler Mendelson PC

On April 13, 2020, the U.S. Department of Labor's Occupational Safety and Health Administration (OSHA) issued guidance to employers in the package...

---

## New Jersey Law Prohibits COVID-19-Related Employment Discrimination New

Jersey

### Faegre Drinker Biddle & Reath LLP

On March 20, 2020, New Jersey Governor Phil Murphy signed a new law meant to protect employees who take COVID-19-related leave. New Jersey Assembly...

---

## COVID-19 Class Actions Weekly Round-Up - For the week of April 6, 2020

### Bennett Jones LLP

As detailed in last week's round-up, the COVID-19 pandemic has already led to a flurry of class actions in the United States and, to a lesser extent...

---

## Disclosing Employee's COVID-19 Status to Employer



### **Holland & Hart LLP**

Healthcare providers struggle to know if and when they may disclose a patient's COVID-19 status to an employer. The analysis differs somewhat...

---

### **Los Angeles, California Adopts Rules to Implement Supplemental Paid Sick Leave Order**

#### **Littler Mendelson PC**

At 9:15 p.m. On April 7, 2020, Los Angeles Mayor Eric Garcetti issued an emergency order that immediately required certain employers to provide...

---

### **NY Workers' Compensation Weekly COVID-19 Update: April 3, 2020**

New York

#### **Goldberg Segalla LLP**

The coronavirus pandemic has presented employers, Workers' Compensation insurers, and third-party administrators with unprecedented challenges—both...

---

### **Minnesota Legislative Update: An Unprecedented State of the State**

Minnesota

#### **Faegre Drinker Biddle & Reath LLP**

The COVID-19 response remains the sole focus of state government. The Walz administration issued new Executive Orders addressing health care and...

---

### **Broadcasts and Podcasts: Paycheck Protection Program**

Video

#### **Phillips Lytle LLP**

Paycheck Protection Program Brought About By Coronavirus Outbreak - Discussion With Rosa Pizzi, WBEN, April 2020...

---

### **Top Workplace Lawyers Scramble To Master Unemployment**

#### **Nelson Mullins Riley & Scarborough LLP**

Many employment attorneys pride themselves on breezing through their clients' thorniest legal quandaries, but the recent federal unemployment...

---

### **EPA Publishes Draft Risk Evaluation of Asbestos, Will Hold Virtual Peer Review Meeting**

#### **Bergeson & Campbell PC**

The U.S. Environmental Protection Agency (EPA) published the draft risk evaluation of asbestos on March 30, 2020. EPA will publish a notice of...

---

### **Protected Concerted Activity: The Next COVID-19 Challenge For Union And Non-Union Employers Alike**

#### **Fisher Phillips**

As businesses face daily new challenges in the wake of the COVID-19 pandemic, many are now confronting a new challenge: demands from their own...

---

### **Client Alert: Expanded Unemployment Benefits Through the Federal CARES Act**

#### **Bowditch & Dewey LLP**

On March 27, 2020, the President signed into law the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act"). Among other things, the...

---

## **How to Respond to Requests for Client Overadvances Under the CARES Act** **Robbins, Salomon & Patt, Ltd.**

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), a comprehensive legislation in response to the COVID-19 pandemic signed into law...

---

## **Class Action Litigation Related to COVID-19: Filed and Anticipated Cases** **Pierce Atwood LLP**

Although the COVID-19 pandemic is still unfolding, class actions related to the coronavirus have already arrived and are on the rise. Despite...

---

## **N.Y. Passes Additional Sick Leave Legislation and N.J. Amends Existing Leave, Insurance Laws**

New Jersey

New York

### **Holland & Knight LLP**

New York and New Jersey are at the forefront of legislative action to protect employees' rights within their states by granting additional sick leave...

---

## **CARES Act Assistance for Nonprofit Employers: Update on Loans to Larger Nonprofits**

### **Caplin & Drysdale, Chartered**

On March 27, the Coronavirus Aid, Relief, and Economic Security ("CARES") Act was signed into law. This Alert updates our previous Alert's discussion...

---

## **Client Alert: Massachusetts Updates Essential Services List - See What Can Continue and What Must Stop**

Massachusetts

### **Bowditch & Dewey LLP**

Yesterday, on March 31, 2020, Governor Baker issued an order extending the closure of non-essential businesses and organizations for in-person...

---

## **New York Enacts Statewide Paid Sick Leave Law**

New York

### **Vedder Price PC**

On April 3, 2020, New York State Governor Andrew Cuomo signed into law a statewide Paid Sick Leave Law (the "Law" or "PSLL"). The PSLL is in addition...

---

## **L.A. Moves to Shut Down Non-Essential Businesses, But Construction Continues**

### **Holland & Knight LLP**

Los Angeles Mayor Eric Garcetti said that as of April 3, 2020, eight businesses had been referred for criminal prosecution for failing to comply with...

---

## **Expansive Exclusion of Health Care Providers from Paid Sick Leave and Paid FMLA Leave—From Doctor's Offices to Nursing Homes**

### **Venable LLP**

As we previously wrote here, the Families First Coronavirus Response Act (the Act), signed into law by President Trump on March 18, 2020, creates two...

---

## **IRS Offers Form 5500 Deadline Relief Taxpayers with Filing Deadlines Before**



**July 15**

### **Hall Benefits Law**

Amidst the Coronavirus pandemic and resulting business disruption, many employers have been concerned about meeting the Form 5500 filing deadline for...

---

### **Financial Daily Dose 4.13.2020 | Top Story: Oil-producing countries reach broad agreement to cut**

#### **Robins Kaplan LLP**

Saudi Arabia and Russia have reached a truce in their oil-production spat, joining together with OPEC and other oil-producing nations to “slash...”

---

### **San Francisco And San Jose Provide Emergency Paid Sick Leave To Cover FFCRA Coverage Gaps**

#### **Fisher Phillips**

San Francisco and San Jose have joined the growing list of local California jurisdictions to adopt COVID-19-specific paid sick leave measures...

---

### **Working Remotely, NLRB Continues Delivering On Certain Appointed Rounds**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: During the COVID-19 crisis, the NLRB (for the most part) has truncated its operations to those operations and functions that can...

---

### **An Alcoholic Employee May Not Come to Work Drunk**

#### **Shawe Rosenthal LLP**

As the U.S. Court of Appeals for the Fifth Circuit stated, “an employer can hold alcoholic employees to the same standards as other employees, even...”

---

### **Arbitration in the Fifth - March 2020**

Texas

#### **Haynes and Boone LLP**

In television drama, there is nothing like a cliffhanger to keep the audience coming back. As discussed below, in March the Fifth Circuit may have...

---

### **Notable Amendments Made to New York’s Wage Parity Law Will Affect Home Health Care Employers**

New York

#### **Littler Mendelson PC**

On April 3, 2020, New York Governor Andrew Cuomo signed the 2020-2021 State Budget bills, part of which amended the Home Health Care Worker Wage...

---

### **Cloth Face Coverings At Work: Are They Personal Protective Equipment, And Who Pays For Them?**

#### **Fisher Phillips**

The CDC recently recommended the use of homemade cloth face coverings in public settings, which raised many questions among in the workplace law...

---

### **CORONAVIRUS RELIEF BILL: The CARES Act - Provisions Affecting U.S. Employers and Employees, Part I**

### **Bryan Cave Leighton Paisner LLP**

The Coronavirus Aid, Relief, and Economic Security Act ("CARES Act" or "Act"), enacted on March 27, 2020, has been the subject of government agency...

---

### **Client Alert: CARES Act Temporary Rule for Paid Sick Leave and Expanded FMLA**

#### **Bowditch & Dewey LLP**

The Department of Labor has released its temporary rule implementing the Paid Sick Leave ("PSL") and expanded FMLA ("eFMLA") provisions of the...

---

### **COVID-19: What NC Employers Need to Know About Unemployment Benefits**

North Carolina

#### **Fox Rothschild LLP**

During the COVID-19 pandemic, "unemployment" has become a household name along with hand sanitizer, toilet paper and social distancing. As of April 3...

---

### **Paid Leave and Coronavirus—Part X: Families First Act Updated FAQs and OMB Reviewing Final Regulation**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The Families First Coronavirus Response Act ("FFCRA" or the "Act") goes into effect tomorrow April 1, 2020. As covered employers...

---

### **Client Alert: Labor Conditions Tied To CARES Act Loans To Employers With 500 to 10,000 Employees**

#### **Bowditch & Dewey LLP**

Title IV of the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") authorizes the Secretary of the Treasury to create a loan program for...

---

### **California Resources Available to Employers Dealing with COVID-19 Related Issues**

California

#### **Jackson Lewis PC**

As COVID-19 cases grow in California, lawsuits are already being filed against essential business employers, alleging companies did not or are not...

---

### **Second Circuit Lets Collective Action Proceed Where Class Action Fails**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The Second Circuit has held that the standard for final FLSA collective action certification is less stringent than the standard...

---

### **WFH is the New Black, Part 2: The DOL Presses Pause on the "Continuous Workday" Rule**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The U.S. DOL has suspended its "continuous workday" rule for employees working from home as a result of COVID-19. This development...

---

### **Los Angeles Supplemental Paid Sick Leave Order**

California

#### **Cozen O'Connor**



On April 7, 2020, Los Angeles Mayor Eric Garcetti issued an order titled: Supplemental Paid Sick Leave Due to COVID-19. The order suspended and...

---

**COVID-19 Webinar Series: IT, Cybersecurity, and Privacy Impacts on Remote Work Webinar Recording** [Video](#)

**Bradley Arant Boult Cummings LLP**

In the wake of COVID-19, cities, counties and states across the nation are issuing “shelter in place” orders to curb nonessential movement of...

---

**Coronavirus Guidance for employers Northern Ireland- News - Eversheds Sutherland**

**Eversheds Sutherland (US) LLP**

Increases to compensation limits for tribunal claims and other amounts payable under employment legislation in Northern Ireland. The new statutory...

---

**PH COVID-19 Client Alert Series: Expanded Guidance from the CDC and EEOC Paul Hastings LLP**

Last week, the Centers for Disease Control (“CDC”) issued new and expanded guidance concerning workplace safety for critical infrastructure workers...

---

**COVID-19: New DOL and IRS Guidance Interpreting the Families First Coronavirus Response Act**

**Wilmer Cutler Pickering Hale and Dorr LLP**

On April 1, 2020, The U.S. Department of Labor issued temporary regulations interpreting the Families First Coronavirus Response Act (FFCRA). As...

---

**Zooming In: “Zoom’s” Significant Privacy and Data Security Risks brought to Light Again (and Again)**

**K&L Gates**

It hasn’t even been 10 days since our previous Blog on Zoom, which highlighted a number of privacy and data security issues prevalent in the use of...

---

**It’s Springtime for Wage and Hour Rights: Worker-Friendly Changes to Wage & Overtime Regulations Are Blooming in Colorado** [Colorado](#)

**Cozen O'Connor**

In the midst of growing alarm over the coronavirus pandemic and an almost all-consuming focus on public health, workplace and legal developments...

---

**REVISED: COVID-19 U.S.: Navigating the Paycheck Protection Program (PPP) under the CARES Act and recent SBA guidance**

**Hogan Lovells**

On Friday, March 27, 2020, President Trump signed Into law H.R. 748, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) to address...

---

**New York Issues Executive Order Requiring Employers to Provide Essential Workers with Face Masks** [New York](#)

**Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 13, 2020, Governor Cuomo issued Executive Order (“EO”) 202.16, requiring employers to provide essential workers with face...

---

#### **CARES Act Section 3610 Guidance**

##### **Crowell & Moring LLP**

Section 3610 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) permits government agencies to modify the terms of existing...

---

#### **Client Alert: Employee Documentation for FFCRA Leave - IRS Guidance**

##### **Bowditch & Dewey LLP**

The IRS has released FAQs regarding tax credits available to employers under the Families First Coronavirus Response Act (the “FFCRA”). At questions...

---

#### **CMS Updates Blanket Waivers to Help Expand Health Care Workforce**

##### **Robinson & Cole LLP**

On April 9, 2020 the Centers for Medicare and Medicaid Services (CMS) updated blanket waivers issued previously in response to the COVID-19 public...

---

#### **UPDATED: Summary COVID-19: Paycheck Protection Program (PPP)**

##### **Goulston & Storrs PC**

The U.S. Small Business Administration (SBA) is authorized to guarantee up to \$349 billion in loans to eligible borrowers through the Paycheck...

---

#### **COVID-19: DOL Releases New Guidance Regarding the Families First Coronavirus Response Act**

##### **Wilmer Cutler Pickering Hale and Dorr LLP**

As mentioned in our previous alert, the recently enacted Families First Coronavirus Response Act (FFCRA) requires that employers with fewer than 500...

---

#### **OSHA Sheds Light on COVID-19 Recording Requirements**

##### **Littler Mendelson PC**

On April 10, 2020, in a Friday night memo, the Occupational Safety and Health Administration (OSHA) updated its guidance on whether employers are...

---

#### **The Coming Wave of Post-CARES Fraud Cases: How to Protect Yourself**

##### **Kelley Drye & Warren LLP**

Aid to Businesses Under the CARES Act The Coronavirus Aid, Relief and Economic Security (CARES) Act, H.R. 748, was signed into law by the President...

---

#### **Roadmap for Small Businesses for the Paycheck Protection Program - Keeping American Workers Paid and Employed Act**

##### **Sullivan & Worcester LLP**

I. Title I, 1102(a) of the CARES Act amends Section 7(a)(2) of the Small Business Act (the “SBA Act”), section F, to which is added a new subsection...

---



## **COVID-19 and Teleworking: State and Local Employment Tax Issues**

### **Eversheds Sutherland (US) LLP**

Given the dramatic limitations on business travel and mandatory work-from home policies caused by COVID-19 concerns, multistate employers should...

---

## **Use of Hotels and Other Real Estate Facilities for COVID-19 Response**

### **Jones Day**

In Short The Situation: The COVID-19 pandemic has caused a severe shortage of hospital and other real estate facilities needed to address the current...

---

## **Expanded Unemployment Insurance Access and Benefits: 4 Key Takeaways From the CARES Act**

### **Faegre Drinker Biddle & Reath LLP**

On March 27, 2020, the Coronavirus Aid, Relief and Economic Security Act (CARES Act) was signed into law, providing an estimated \$2 trillion stimulus...

---

## **Top 10 Compensation and Benefits Issues for Employers in Light of the COVID-19 Pandemic**

### **Goodwin Procter LLP**

As the COVID-19 pandemic continues to unfold, many employers are faced with questions about the impact of economic changes and workforce reductions...

---

## **New COVID-19 Requirement for Michigan Employers**

Michigan

### **Pepper Hamilton LLP**

Client Alert Businesses across the United States, and around the world, are dealing with the COVID-19 crisis in a variety of ways. In recent days and...

---

## **New York State Orders Employers to Provide Masks to Public-Facing Employees**

New York

### **Fox Rothschild LLP**

On April 12, 2020, New York Gov. Andrew Cuomo issued an executive order requiring all essential businesses or entities to provide employees with face...

---

## **Executive Order 2020-42: "Stay-Home, Stay Safe" Order Extended until April 30**

### **Foster Swift Collins & Smith PC**

Governor Whitmer's newest order, Executive Order 2020-42 ("EO 2020-42"), updates and replaces her previous "stay-home, stay-safe order," Executive...

---

## **Massachusetts Department of Paid Family Leave Releases New Guidance**

Massachusetts

### **Jackson Lewis PC**

The current circumstances surrounding the COVID-19 crisis have brought paid family and Medical Leave to the forefront of the national consciousness...

---

## **Mayor Garcetti Replaces and Supersedes LA City Council's Supplemental Paid Sick Leave Ordinance and Adds Additional Requirements for Essential Businesses**

### **Epstein Becker Green**

As discussed in a previous Advisory, on March 27, 2020, the Los Angeles City Council unanimously passed an ordinance that added a new Article 5-72HH...

---

### **DOL Clarifies CARES Act Unemployment Ambiguities**

#### **Hogan Lovells**

On April 4, 2020, the U.S. Department of Labor ("DOL") provided clarity on the scope of the \$600 per week supplemental benefit available under the...

---

### **Employers Mandated to Provide Emergency Paid Sick Leave and Emergency FMLA Leave Amid COVID-19**

#### **Morgan Lewis**

The Families First Coronavirus Response Act imposes a mandate on all employers with fewer than 500 employees, and on all federal and state employers...

---

### **A Spectrum of Issues in the Time of COVID-19**

#### **Hopkins & Carley**

While this post may not fit under the header of the "Privacy Hacker", I wanted to step aside from privacy and security and share some insight on...

---

### **New Jersey Expands Business Shutdowns, Imposes New Rules On Essential Businesses And Retail Customers**

New Jersey

#### **Fisher Phillips**

New Jersey Governor Phil Murphy just issued an Executive Order that expands the existing statewide partial business shutdown and regulates onsite...

---

### **Government Measures Worldwide in Response to COVID-19**

#### **Thompson Hine LLP**

Foreign Investment Review Board (FIRB): With effect from March 29, 2020, the following changes have been made to the FIRB frame...

---

### **IRS Issues Initial Tax Guidance for Advance Payment of Employee Retention Credits and Families First Credits**

#### **Ropes & Gray LLP**

On March 31, 2020, the IRS and the Treasury Department issued guidance for businesses, to implement the refundable employment tax credits for...

---

### **Additional Funding Opportunities Under the CARES Act and Certain Credit Facilities of the Federal Reserve for Mid and Large-Sized Businesses**

#### **Frost Brown Todd LLC**

While many businesses will be able to take advantage of the SBA Paycheck Protection Program loans and Economic Injury Disaster Loans, there are...

---

### **Preparing for Trade Secret and Restrictive Covenant Litigation While the Court Near You is Closed**

Delaware

#### **Seyfarth Shaw LLP**



Imagine this scenario: You are the General Counsel of a company in a particularly competitive industry. A key company employee who has access to some...

---

### **New CDC Guidance for Critical Workers Returning to Work After Potential COVID-19 Exposure**

#### **Barnes & Thornburg LLP**

The CDC has posted Interim Guidance to assist employers of critical infrastructure workers in safely returning those employees to work after...

---

### **Federal and New York State COVID-19 Sick Leave Laws Update**

#### **Phillips Lytle LLP**

Federal and New York State COVID-19 Sick Leave Laws Update The U.S. Department of Labor (DOL) has issued a model notice and guidance for the recently...

---

### **COVID-19 Executive Compensation Q&As: Focus on Incentive Plans and Nonqualified Deferred Compensation**

#### **Pepper Hamilton LLP**

This article answers questions about incentive plan considerations and nonqualified deferred compensation issues arising from the economic downturn...

---

### **Labor Department Issues Guidance on Calculating FLSA “Regular Rate”**

#### **McGuireWoods LLP**

On March 26, 2020, the U.S. Department of Labor (DOL) issued a series of opinion letters clarifying how to calculate properly an employee’s “regular...

---

### **Measures Landlords and Property Managers Can Take in Response to a Reported COVID-19 Infection**

#### **Newmeyer Dillion**

Most landlords and property managers are now familiar with steps they should be taking to reduce the spread of COVID-19. But what if a tenant or...

---

### **New York State Workers’ Compensation Board COVID-19 Initiative—Rolling Updates Since March 7, 2020**

New York

#### **Goldberg Segalla LLP**

In response to the COVID-19 pandemic mitigation initiatives in New York State, including Gov. Cuomo’s Executive Order and sequelae, the New York...

---

### **Michigan Extends Stay-at-Home Restrictions, Imposes Additional Obligations on Businesses**

Michigan

#### **Pepper Hamilton LLP**

Client Alert In response to the ongoing COVID-19 pandemic, Michigan Gov. Gretchen Whitmer issued Executive Order 2020-42 (Order), which took effect...

---

### **District of Columbia Expands Sick Leave and Unemployment Eligibility**

District of

Columbia

#### **Manatt Phelps & Phillips LLP**

On April 10, the District of Columbia enacted the COVID-19 Response Supplemental Emergency Amendment Act of 2020 (the Act). Among other things, the...

---

#### **Alert for Not-for-Profit Entities**

##### **Fried Frank Harris Shriver & Jacobson LLP**

The Coronavirus Aid, Relief, and Economic Security Act ("CARES Act"), a \$2 trillion economic relief bill signed into law on March 27, 2020, includes...

---

#### **Wait - the DOL Made Their FFCRA Guidance LESS Useful?!!**

##### **Shawe Rosenthal LLP**

I don't like it when the federal agencies don't play fair. I previously blogged about the EEOC's sneaky change in its position on whether sexual...

---

#### **OSHA Issues COVID-19 Alert Identifying Safety Tips for Package Delivery Workers**

##### **Jackson Lewis PC**

In light of the ongoing safety concerns related to COVID-19, OSHA issued an alert identifying various voluntary safety measures that employers can...

---

#### **Need to Reduce Staff? Consider Shared Work Programs to Lessen the Pain**

##### **Robinson & Cole LLP**

March 26, 2020 Need to Reduce Staff? Consider Shared Work Programs to Lessen the Pain Authored by Matthew T. Miklave The upending of the business...

---

#### **OSHA Issues COVID-19 Interim Enforcement Response Plan**

##### **Littler Mendelson PC**

Continuing its recent trend to update employers on COVID-19 safety, on April 13, 2020, the Occupational Safety and Health Administration (OSHA)...

---

#### **FTC and DOJ Issue Joint Antitrust Statement Regarding COVID-19 and Competition in Labor Markets**

##### **McDermott Will & Emery**

The COVID-19 pandemic has placed additional stressors on labor markets, particularly for healthcare workers and essential employees. While...

---

#### **COVID-19: Update - New Jersey and New York Executive Orders' Impact on Construction Projects**

[New Jersey](#)

[New York](#)

##### **K&L Gates**

Governor Murphy issued the Statewide "Stay at Home" Order, Executive Order No. 107 (E.O. 107), on March 21, 2020, which closed all non-essential...

---

#### **South Carolina continues to expand availability of unemployment benefits**

##### **Constangy Brooks Smith & Prophete LLP**

Like many other states, South Carolina has taken steps to ensure unemployment benefits are available to workers affected by COVID-19. The Department...

---



## 7 Takeaways from Labor Dept.'s COVID-19 Paid Leave Rule, Law360

### Morgan Lewis

The U.S. Department of Labor has moved quickly to implement New emergency paid sick leave laws, but the...

---

## Measuring Worker Temperatures Could Lead To Wage And Hour Claims

California

Pennsylvania

### Fisher Phillips

Employers could face potential wage and hour claims under federal and state law if they do not compensate employees for time spent having their body...

---

## COVID-19 Workplace Health & Safety Updates

### Graydon Head & Ritchey LLP

A new week brings some important updates for employers related to their workplace health and safety obligations in the context of the current...

---

## New York State Orders Essential Businesses to Provide Masks to Public-Facing Employees

New York

### Fox Rothschild LLP

On April 12, 2020, Gov. Andrew Cuomo issued an executive order requiring all essential businesses or entities to provide employees with face...

---

## Hold on to Your Hat! The IRS Gives Us Some Good News

### Breazeale Sachse & Wilson LLP

The IRS has just issued a new set of FAQs that essentially give us an outline of what some of the FFRCA-related forms should look like. This outline...

---

## Evolving Interpretations of the FFCRA and CARES Act

### Vinson & Elkins LLP

Normally, when a new federal law affecting employers and employees is enacted, employment lawyers and their clients have plenty of time to get up to...

---

## New Virginia Law Will Prohibit LGBT Discrimination And Expand Workplace Lawsuits

Virginia

### Fisher Phillips

Virginia Governor Ralph Northam (D) just signed into law this weekend sweeping legislation that not only protects the rights of LGBT Virginians in...

---

## Class Certification Granted In Staffing Company Workplace Bias Suit

### Seyfarth Shaw LLP

Seyfarth Synopsis: For nearly a decade, the aftershocks of the U.S. Supreme Court's decision in Wal-Mart Stores, Inc. v. Dukes have curtailed the...

---

## New COVID-19-Related Obligations for Los Angeles Employers

California

### Ius Laboris

The City of Los Angeles has implemented three Executive Orders that directly impact employers. The orders address paid sick leave due to COVID-19...

---

**New Jersey Amends State Mini-WARN Act: Mass Layoffs Due to COVID-19 Do Not Trigger NJ WARN; Other NJ WARN Act Amendments Delayed** New Jersey

**Ogletree Deakins**

We previously reported on amendments to the New Jersey mini-WARN Act (known officially as the Millville Dallas Airmotive Plant Job Loss Notification...

---

**Looking Ahead: A Comprehensive Guide to COVID-19 Employment Decisions Through Downsizing, Furloughs, and Return to Work**

**Payne & Fears LLP**

After weeks of adjustment to the sudden spread of COVID-19, including dramatic business slowdowns, government shutdown orders, and financial rescue...

---

**Episode 6: Dawn Raids**

**Winston & Strawn LLP**

What are dawn raids and how can companies and the law firms representing them prepare? In this Episode of Winston & Strawn's Competition Corner...

---

**How to Determine Eligibility Under SBA Affiliation Rules for the CARES Act Paycheck Protection Program**

**Faegre Drinker Biddle & Reath LLP**

Under the CARES Act, approximately \$350 billion in forgivable loans for small businesses is available through the Paycheck Protection Program (PPP)...

---

**The Board Reinstates Dana Corp. Challenges to Voluntary Recognition**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: In a continuation of its push to protect employee free choice, the NLRB issued a final rule on April 1 that returns to the Board's...

---

**COVID 19: Washington State COVID Resource Guide** Washington

**K&L Gates**

Unemployment benefits will provide temporary partial income to individuals who lose their job through ...

---

**Evaluating New Jersey's New WARN Amendments & Urging The State to Suspend the Effective Date** New Jersey

**Seyfarth Shaw LLP**

Seyfarth Synopsis: In January, New Jersey amended its Millville Dallas Airmotive Plant Job Loss Notification Act ("NJ WARN"), in an attempt to push...

---

**New guidance from CDC provides model for OSHA compliance**

**Constangy Brooks Smith & Prophete LLP**

The Centers for Disease Control and Prevention, and The Cybersecurity and Infrastructure Security Agency, have just issued a new Interim Guidance...

---

**The Coronavirus, Corporate Governance and Shareholder Value**

**Fried Frank Harris Shriver & Jacobson LLP**



The Coronavirus is testing companies in ways unimaginable just a couple of months ago. The challenges for CEOs and corporate boards transcend...

---

### **Employer Concerns - COVID-19**

#### **Schulte Roth & Zabel LLP**

As COVID-19 spreads across the globe, employers must act quickly while continuing to comply with applicable employment laws and the evolving guidance...

---

### **Paid Leave and Coronavirus—Part XI: Department of Labor Issues Families First Coronavirus Response Act (“FFCRA”) Final Regulations**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: As reported through our “Paid Leave and Coronavirus” series, the Families First Coronavirus Response Act (“FFCRA” or the “Act”)...

---

### **Updated COVID-19 FAQs for employers with U.S. employees**

#### **Reed Smith LLP**

The worldwide COVID-19 pandemic has had, and will continue to have, a substantial impact on the U.S. workplace...

---

### **Every Business That Received a Payroll Protection Program Loan (PPP Loan) CARES About Forgiveness**

#### **Lane Powell PC**

Expansion of the payroll protection program (PPP) loans has emerged as a key form of relief provided by the CARES Act, but amid the euphoria and...

---

### **Employment Question of the Day: April 13, 2020**

#### **Fredrikson & Byron PA**

Yes. There are two conditions attached to a loan granted to a mid-sized business that require the business to give up certain rights under federal...

---

### **NJ Delays Expansion of WARN Act in Light of Coronavirus Crisis**

New Jersey

#### **Fox Rothschild LLP**

On April 14, 2020, New Jersey Gov. Phil Murphy signed into law a new set of amendments to the NJ WARN Act - the state’s version of the federal Worker...

---

### **It is Now Easier For Federal Workers to Prove Age Bias**

#### **Kelley Drye & Warren LLP**

Last week, the US Supreme Court made it easier for a federal worker to establish a claim for age bias. This decision does not impact private employers...

---

### **OSHA Issues Guidance Limiting Recordkeeping Requirements of COVID-19 Cases for Certain Employers**

#### **Proskauer Rose LLP**

On April 10, 2020, the Department of Labor’s Occupational Safety and Health Administration (“OSHA”) issued guidance clarifying certain employers’...

---

## **Cloth Face Masks Required for Rhode Island Employees Through May 18, 2020**

Rhode Island

### **Pierce Atwood LLP**

On April 14, 2020, Governor Raimondo issued the Twenty-First Supplemental Emergency Declaration — Requiring Cloth Face Masks At Work. The Order is...

---

## **OSHA Publishes Interim Enforcement Response Plan for COVID-19 Inspections**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 13, 2020, OSHA released an Interim Enforcement Response Plan for Coronavirus Disease 2019 (COVID-19) which is intended to...

---

## **CARES Act Payroll Tax Credits, Unemployment Benefits Enhancements, and Lending Programs Impact Compensation, Furlough, and Layoff Strategies**

### **Vedder Price PC**

The Coronavirus Aid, Relief, and Economic Security Act, commonly known as the CARES Act (the "Act"), enacted March 27, 2020, contains several...

---

## **FAQs on COVID-19 Group Health Plan Coverage Implementation**

### **Faegre Drinker Biddle & Reath LLP**

The Department of Labor (DOL), the Department of Health and Human Services (HHS), and the Department of the Treasury (collectively, "the...

---

## **UAE Issues New Ministerial Resolutions on Employment Stability and Remote Working in Response to COVID-19**

### **Hunton Andrews Kurth LLP**

As we are undergoing a period of concern for both employers and employees in the UAE given the lack of certainty regarding how long the...

---

## **The EEOC Provides Further Guidance on Managing Disability and Accommodation Issues in the Age of COVID-19 (Part I)**

### **Vorys Sater Seymour and Pease LLP**

While the COVID-19 pandemic has caused employers to cease or reduce operations, their legal obligations generally continue. The EEOC made clear in a...

---

## **Los Angeles Mayor Issues Order Requiring Use of Nonmedical Grade Face Coverings**

California

### **Barnes & Thornburg LLP**

Los Angeles Mayor Eric Garcetti has issued an emergency order requiring many nonmedical workers who provide essential services to wear...

---

## **Joint DOJ & FTC Antitrust Guidance Warns Employers About Colluding and Sharing Competitive Data During the COVID-19 Crisis**

### **Littler Mendelson PC**

Last month federal agencies adjusted antitrust guidelines to facilitate collaboration between competing companies where the information-sharing and...

---



## **COVID-19: Temporary Work-From-Home Models and PCI DSS Compliance**

**Hunton Andrews Kurth LLP**

As of early April, hundreds of millions of workers around the world are affected by “stay-at-home” or “station-in-place” orders issued by governments...

---

## **Working Wise - Volume 8**

**K&L Gates**

The coronavirus pandemic (“COVID-19”) is top of mind for all employers, regardless of location, size, and industry. The federal...

---

## **Federal Reserve Releases Details of Main Street Lending Program**

**Pepper Hamilton LLP**

On April 9, the Federal Reserve released term sheets for its widely anticipated Main Street Lending Program to ensure credit flows to small and...

---

## **Payroll Protection Program SBA Loans**

**Masuda Funai Eifert & Mitchell Ltd**

Executive Summary Small businesses with no more than 500 employees may take advantage of an expanded eligibility of Small Business Administration...

---

## **FAQs: Loan Programs for Larger Businesses Under Title IV of the CARES Act**

**Latham & Watkins LLP**

US Congress set to make more than \$500 billion available to eligible larger businesses.

---

## **How To Avoid Wrongful Death And Injury Claims For Workplace COVID-19 Exposure**

**Fisher Phillips**

Employers are starting to be served with wrongful death and personal injury lawsuits alleging an employee’s exposure to COVID-19 at work should lead...

---

## **Why might businesses want to mediate employment disputes?**

Connecticut

**Raymond Law Group LLC**

Employment disputes are something that any employer in Connecticut will want to avoid. Nevertheless, no matter how careful business owners are to...

---

## **Main Street Lending: How Public Companies Should Prepare to Borrow Under These CARES Act Programs**

**McGuireWoods LLP**

On April 9, 2020, the Treasury Department and the Federal Reserve each issued a press release (Treasury release and Federal Reserve release)...

---

## **How to Respond to Union Information Requests Regarding COVID-19**

**Barnes & Thornburg LLP**

In the wake of the COVID-19 pandemic, many unionized employers are facing a steady stream of information requests from unions representing their...

---

## **Navigating California's Local Paid Sick Leave Ordinances in Light of COVID-19**

California

### **Duane Morris LLP**

In California, several cities have taken measures to mandate private employers that are not covered under the FFCRA to provide paid sick leave for...

---

## **OSHA Publishes Enforcement Guidance on Recording Cases of COVID-19**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 10, 2020, OSHA released new Interim Guidance to Compliance Safety and Health Officers (CSHOs) for enforcing the...

---

## **US COVID-19: Employee Temperature Screening: What Employers Need To Consider When Deciding Whether To Implement a Screening Process**

### **Bryan Cave Leighton Paisner LLP**

In light of concerns about the spread of the novel coronavirus in the workplace, employers are confronting important questions pertaining to the...

---

## **Virginia Enacts Comprehensive Whistleblower Protection**

Virginia

### **Jackson Lewis PC**

Virginia Governor Ralph Northam has signed a comprehensive whistleblower protection law, the first of its kind for Virginia. The Whistleblower Law...

---

## **TOP TIP: Mid-Atlantic Employers Your Governor(s) Just Issued a Shut-Down (or Other) Order. What Does This Mean**

### **Shawe Rosenthal LLP**

In light of the COVID-19 pandemic, governors in Delaware, the District of Columbia, Maryland, New Jersey, New York, Pennsylvania and Virginia have...

---

## **New Jersey Passes Bill to Amend NJ WARN, Create Mass Layoff Exception, Delay Severance, Notice Obligations**

New Jersey

### **Jackson Lewis PC**

The New Jersey Legislature has passed a bill to amend the Millville-Dallas Airmotive Plant Job Loss Notification Act (New Jersey WARN Law) to create...

---

## **New CDC Face Mask Guidance Raises Liability Issues**

### **Seyfarth Shaw LLP**

The Centers for Disease Control and Prevention (CDC) and Federal Occupational Safety and Health Administration (OSHA) have issued guidance documents...

---

## **First COVID-19 wrongful death suit filed in the US - What are the wider implications?**

### **CMS Cameron McKenna Nabarro Olswang LLP**

It has recently been reported that the first wrongful death lawsuit has been filed in the United States related to the COVID-19 outbreak. The case...

---

## **Lessons from Amazon's Termination of a Warehouse Worker who Protested about Unsafe Conditions**



### **Katz Marshall & Banks LLP**

Amazon's recent stunning and outrageous decision to fire an employee who protested unsafe conditions at a Staten Island warehouse highlights many...

---

### **Solving the Pay Puzzle: Wage and Hour Issues During the Coronavirus Pandemic**

#### **Breazeale Sachse & Wilson LLP**

The novel coronavirus continues to cause frustration for employers whose workforces are being impacted by the rapid spread of the virus, leading to a...

---

### **COVID-19: Department of Labor Publishes Temporary Rules for the Implementation of the FFCRA**

#### **K&L Gates**

The Families First Coronavirus Response Act ("FFCRA" or "Act") was passed by the Senate and signed into law by President Trump on March 18, 2020. The...

---

### **California Recommends Face Coverings, While San Diego County Requires Them For Certain Workers And Issues New Posting Requirements**

California

#### **Hunton Andrews Kurth LLP**

The California Public Health Department issued Guidance recommending that all Californians wear cloth face coverings when in public for essential...

---

### **IRS Updates Guidance on CARES Act Payroll Tax Deferrals**

#### **McGuireWoods LLP**

The CARES Act permits employers to defer the deposit and payment of the employer's portion of Social Security taxes that otherwise would be due...

---

### **New York Enacts Mandatory Sick Leave Law**

#### **Kelley Drye & Warren LLP**

Amidst the COVID-19 melee, the New York Legislature passed its Budget for Fiscal Year 2021, which included a mandatory paid sick leave bill, signed by...

---

### **Key California Employment Law Cases: March 2020**

California

#### **Payne & Fears LLP**

Neither the Fair Labor Standards Act nor federal common law provide an employer with a right to seek contribution or indemnification from another...

---

### **Masks and Face Coverings: What Employers Need to Know**

#### **Littler Mendelson PC**

NOTE: Because the COVID-19 situation and response are dynamic, with new governmental measures each day, employers should consult with counsel for the...

---

### **Department of Labor Additional Guidance on the Families First Coronavirus Response Act**

#### **Breazeale Sachse & Wilson LLP**

The Department of Labor ("DOL") has updated its guidance regarding the Families First Coronavirus Response Act, providing more answers, but also...

---

## **Coronavirus Relief Bill Update**

### **Masuda Funai Eifert & Mitchell Ltd**

Under the mandate of the Families First Coronavirus Response Act (H.R. 6201), the U.S. Treasury Department, the Internal Revenue Service (“IRS”), and...

---

## **OSHA Provides Recordkeeping Guidance To Employers For COVID-19 Cases**

### **Fisher Phillips**

The Department of Labor’s Occupational Safety and Health Administration just issued guidance for enforcing OSHA’s recordkeeping requirements for...

---

## **City of Los Angeles Enacts Modified Supplemental Paid Sick Leave Ordinance and New “Worker Protection Order”**

### **Goldberg Segalla LLP**

On April 1, 2020, we issued an alert advising that the Los Angeles City Council proposed a Supplemental Paid Sick Leave ordinance that would apply to...

---

## **Unionized Covid-19 Loan Recipients Face Troubling Non-Abrogation Commitment**

### **Fisher Phillips**

In an increasingly desperate business climate, thousands of businesses are expected to apply for emergency loans created by the Coronavirus Aid...

---

## **Workers’ Comp Defense Blog Provides Michigan Case and Legislative Updates**

### **Foster Swift Collins & Smith PC**

Lansing, Mich. - Foster Swift Workers’ Compensation defense attorneys Brian Goodenough (practice leader), Alicia Birach, Michael Cassar, Tyler Olney...

---

## **Coronavirus Aid, Relief, And Economic Security (CARES) Act payroll tax relief provisions - a quick look for nonprofits and microenterprises**

### **DLA Piper**

The Employee Retention Tax Credit is a tax credit against the employer portion of certain FICA taxes which reduces or eliminates cash outlays for...

---

## **The Families First Coronavirus Response Act: Employment Considerations for Non-Profit Organizations**

### **Dechert LLP**

This alert addresses some of the most common concerns and questions that non-profit organizations confront in understanding how to comply with the...

---

## **FTC and DOJ on Alert for Anticompetitive Employer Agreements Regarding COVID-19 Frontline Workers**

### **Winston & Strawn LLP**

On April 13, 2020, the Department of Justice’s (DOJ) Antitrust Division and the Federal Trade Commission’s (FTC) Bureau of Competition jointly...

---

## **Main Street Lending Program Offers Additional Relief to Small and Mid-Size**



## **Businesses Under the CARES Act**

### **Akerman LLP**

On April 9, 2020, the Federal Reserve established a Main Street Lending Program (Main Street) under the Coronavirus Economic Stabilization Act of...

---

## **EEOC stops issuing right-to-sue letters in response to COVID-19, delaying litigation deadlines**

### **Reed Smith LLP**

In an effort to delay litigation deadlines, the Equal Employment Opportunity Commission (EEOC) has stopped issuing Right-to-Sue Letters amid the...

---

## **CARES ACT - Employment, Compensation, Payroll Tax and Paid Leave Provisions**

### **Mayer Brown**

In the third and final of a series, our employment and benefits teams take an in depth look at the provisions of the Coronavirus Aid, Relief, and...

---

## **Best Practices and Insights in the Age of COVID-19 for Owners/Developers of Multi-Family Housing Complexes**

### **Michael Best & Friedrich LLP**

It is clear COVID-19's economic impact has permeated through a variety of industries, and owners and developers of multi-family housing, such as...

---

## **Spotlight: taxation of executives in USA**

### **Cleary Gottlieb Steen & Hamilton LLP**

A general introduction to the tax regime applicable to executives in USA, including key tax planning considerations.

---

## **COVID-19 Washington Update: April 3, 2020**

### **Kelley Drye & Warren LLP**

While continuing to solicit broad feedback on future response packages, Speaker Pelosi today indicated a "phase four" bill would likely focus on...

---

## **High Court Clarifies Federal Worker Standard for Liability in ADEA Claims**

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

On April 6, 2020, the United States Supreme Court issued its 8-1 decision in Babb v. Wilkie, which resolves a circuit split over the causation...

---

## **CARES ACT - Changes for Retirement Plans**

### **Mayer Brown**

In the second of a series, our benefits team takes an in depth look at the provisions of the Coronavirus Aid, Relief, and Economic Security Act (the...

---

## **IRS Issues Guidance on COVID-19-Related Tax Credits Available to Employers Under the FFCRA**

### **Proskauer Rose LLP**

On April 1, 2020, the Internal Revenue Service ("IRS") posted on its website a

series of frequently asked questions (“FAQs”) that explain the...

---

### **Tips for Reducing Workers' Compensation Claims for Remote Workers**

**Ice Miller LLP**

In today's changing world, many more employees are now working from home. It can be difficult to monitor or control the safety precautions in the...

---

### **Los Angeles's COVID-19 Sick Leave Ordinance**

**Baker & Hostetler LLP**

Los Angeles has enacted a COVID-19 Sick Leave Ordinance, requiring that employers provide employees with sick leave for COVID-19-related reasons...

---

### **Hopeful Family-Friendly Movies Should Make Us Think About a Post-COVID Workplace**

**Ford & Harrison LLP**

In the midst of today's climate, it somehow seems trivial to write about “entertainment” and how it pertains to the world of HR and employers. After...

---

### **DOL Regulations Clarify Paid Leave Requirements Under the Families First Coronavirus Response Act**

**McCarter & English LLP**

The U.S. Department of Labor (DOL) has now issued temporary regulations providing guidance on the Families First Coronavirus Response Act (FFCRA)...

---

### **Los Angeles Issues New Sick Leave Rules**

**Proskauer Rose LLP**

On March 27, 2020, the Los Angeles City Council approved a new ordinance that would have required Los Angeles employers to provide up to 80 hours of...

---

### **Supreme Court: Federal Employees Can Sue Over Any Age Discrimination in Employment Decision**

**Jackson Lewis PC**

The U.S. Supreme Court has ruled that federal government employees can sue for age discrimination under the Age Discrimination in Employment Act of...

---

### **US COVID-19: DOL (Yet Again) Publishes Revised Guidance on the Families First Coronavirus Response Act**

**Bryan Cave Leighton Paisner LLP**

This weekend, the Department of Labor (“DOL”) released yet another set of updated and revised Questions and Answers (“Q&A”) regarding the Families...

---

### **CARES Act Expected to be Signed Soon; Employers May Defer Some Payroll Tax Deposits Due on Monday**

**Covington & Burling LLP**

Earlier this afternoon, the House passed by voice vote the Coronavirus Aid, Relief, and Economic Security (“CARES”) Act, the third...

---



## **FAQs on Paycheck Protection Program loans: The SBA's interpretation of the CARES Act**

**Greensfelder, Hemker & Gale, P.C.**

The U.S. Department of the Treasury released a set of frequently asked questions late on April 6, 2020, to clarify several issues with Paycheck...

---

## **DOL Posts Temporary Rule Issuing Regulations Under the Coronavirus Response Act**

**Phelps Dunbar LLP**

The Department of Labor (DOL) published a temporary rule issuing regulations to implement the Families First Coronavirus Response Act (FFCRA), which...

---

## **Counties Increase Restrictions Under Stay-At-Home Order, and That Is Just Fine With Governor Newsom**

**Manatt Phelps & Phillips LLP**

General Overview As California Governor Gavin Newsom reported preliminary, encouraging signs that his "stay at home" order is slowing the spread of...

---

## **Continued Uncertainty About Employee Leave Under the Families First Coronavirus Response Act**

**Crowell & Moring LLP**

The Families First Coronavirus Response Act (FFCRA) was enacted on March 18, 2020 and creates two new types of leave for employees of (primarily)...

---

## **New COVID-19-Related Obligations for Los Angeles Employers**

**Ford & Harrison LLP**

On April 7, 2020, the City of Los Angeles implemented three executive orders that directly impact employers: (1) the Supplemental...

---

## **Department of Labor "posting" requirement for paid leave - may require distributing notice electronically**

**Clingen Callow & McLean LLC**

The Families First Coronavirus Response Act (or, FFCRA) was the first legislation designed to provide employees with enhanced benefits caused by the...

---

## **California Court of Appeal Addresses Unlimited Vacation Policies for the First Time in McPherson v. EF Intercultural Foundation, Inc.**

[California](#)

**Sheppard Mullin Richter & Hampton LLP**

On April 1, 2020, the California Court of Appeal issued the first published decision addressing unlimited vacation policies under California law...

---

## **OFCCP Streamlines FAAP Approval Process During COVID-19 Pandemic**

**Jackson Lewis PC**

Consistent with its efforts to encourage federal contractors to consider functional affirmative action plans (FAAPs) as an alternative to...

---

## **Due to COVID-19, EEOC Suspends Issuing Case Closure Documents**

### **Fox Rothschild LLP**

The U.S. Equal Employment Opportunity Commission (EEOC) announced on April 7 that, due to the COVID-19 pandemic, it has temporarily suspended issuing...

---

### **Duty to Report Employees Who Test Positive for COVID-19**

#### **Cozen O'Connor**

Among the many issues facing employers who have employees that have tested positive for the coronavirus, one that has not received a lot of attention...

---

### **Mitigating Employment Litigation Claims in the Complex Landscape of COVID-19**

#### **Baker McKenzie**

Predictions about the spread of COVID-19 through significant parts of the population and its effects on American life are staggering. The Centers for...

---

### **Corporation and Charitable Foundation Grants During the COVID-19 Pandemic**

#### **Baker McKenzie**

This alert discusses various strategies for corporations and corporate foundations to assist in the fight against the COVID-19 pandemic through grants...

---

### **Employees with Possible Exposure to COVID-19: New CDC Guidance**

#### **Brooks Pierce McLendon Humphrey & Leonard LLP**

This question is becoming more common for essential businesses that continue to operate during quarantines. On April 8, the CDC issued a new Interim...

---

### **Faith-Based Organization Eligibility for SBA Loans Under CARES Act**

#### **Brooks Pierce McLendon Humphrey & Leonard LLP**

The Coronavirus Aid, Relief, and Economic Security Act (CARES) enacted on March 27, 2020 contained several provisions related to the provision of...

---

### **Childcare Relief for Essential Critical Infrastructure Employees**

#### **Jackson Lewis PC**

Many employees and employers, in recent weeks, have been adjusting to the new normal of working from home due to California's Shelter-in-Place order...

---

### **Do Employers Count Employees of Foreign Affiliates When Determining Eligibility Under the Paycheck Protection Program?**

#### **Jackson Lewis PC**

Applicants in the Small Business Administration's (SBA) Business Loan Programs (which include the Paycheck Protection Program (PPP)) are generally...

---

### **New Guidance and Required Posters Issued by the DOL for Paid Sick and FMLA Leave under the Families First Coronavirus Response Act (FFCRA)**

#### **Baker McKenzie**

The Department of Labor just published its first round of guidance on the FFCRA, including two fact sheets and a FAQ explaining key provisions of the...

---



## **Los Angeles Issues Two New Public Orders On COVID-19**

### **Proskauer Rose LLP**

On Tuesday, Los Angeles Mayor Eric Garcetti issued two new public orders in response to COVID-19's continued growth and effect on essential businesses...

---

## **Loan Forgiveness Applies to February 15, 2020 - April 26, 2020 Lay-Off/Rehires**

### **Smith Currie & Hancock**

Would a contractor lose loan forgiveness if the contractor finds it necessary to temporarily lay off employees now, then rehire them after receiving...

---

## **FFCRA Small Business Exemption Creates Opportunity and Confusion for Employers**

### **Ice Miller LLP**

On April 1, 2020—the same day the requirements of the Families First Coronavirus Response Act ("FFCRA" or "Act") went into effect—the U.S. Department...

---

## **Using COVID-19 disaster relief funds to assist employees**

### **Greensfelder, Hemker & Gale, P.C.**

The COVID-19 pandemic has caused significant burdens for employers and employees alike. While some businesses struggle to survive, others are...

---

## **Update: NLRB Delays Implementation of Final Election Rule Changes to July 31, 2020**

### **Proskauer Rose LLP**

As we reported here, on April 1, 2020, the NLRB published its final rule making three amendments to its rules and regulations governing union...

---

## **DOL Issues Guidance Regarding CARES Act Unemployment Provisions**

### **Troutman Sanders LLP**

Authors Richard Gerakitis, Partner, Troutman Sanders Emily E. Schifter, Associate, Troutman Sanders Susan K. Lessack, Partner, Pepper Hamilton Tracey...

---

## **IRS publishes detailed guidance on tax credits for employers who give paid sick leave and emergency FMLA what documentation may employers ask for?**

### **Clingen Callow & McLean LLC**

The Families First Coronavirus Response Act (the "FFCRA"), signed by President Trump on March 18, 2020, provides small and midsize employers...

---

## **Did You Notice? - Requirements to Provide Notice of Paid Leave Under FFCRA**

### **Step toe & Johnson LLP**

On March 18, 2020, the Families First Coronavirus Response Act (FFCRA) was enacted to require covered employers - generally those with fewer than 500...

---

## **FFCRA Documentation and Record Keeping: What Employers Need to Know**

### **Ice Miller LLP**

The close of March and open of April 2020 brought in both Q2 of 2020 and some updated guidance from the U.S. Department of Labor (DOL) and the U.S...

---

### **Weighing the Options: FFCRA and CARES Act Present Alternatives for Small Businesses Facing Hard Choices**

#### **Ogletree Deakins**

Untangling the web of options presented to small employers under the Families First Coronavirus Response Act (FFCRA) and Coronavirus Aid, Relief, and...

---

### **Suit Filed Against Governor Baker to Re-open Recreational Marijuana Businesses**

#### **Burns & Levinson LLP**

On Tuesday, April 7, 2020, five recreational (adult-use) marijuana companies and one individual, a veteran of the U.S. armed forces, filed suit...

---

### **The Families First Coronavirus Response Act Regulations: Part One in a Five-part Series**

#### **Squire Patton Boggs**

On April 1, 2020 (no, not an April Fool's Day joke!), the US Department of Labor (DOL) issued its final regulations interpreting the Families First...

---

### **IRS Releases Guidance on Coronavirus-Related Payroll Tax Credits**

#### **Covington & Burling LLP**

On March 31, the IRS released multiple pieces of guidance regarding provisions of the Families First Coronavirus Response Act ("FFCRA") and the...

---

### **Paid Sick Leave Under the FFCRA: What Does It Mean To Be Unable To Work Due To A Quarantine or Isolation Order?**

#### **Constangy Brooks Smith & Prophete LLP**

The Families First Coronavirus Response Act requires employers with fewer than 500 employees to provide paid sick leave and expanded family and...

---

### **California Supreme Court: Employees who settle their own wage and hour claims still have standing to pursue PAGA**

California

#### **Reed Smith LLP**

The California Supreme Court ruled on March 12, 2020 that an individual plaintiff's settlement of their claims against an employer for purported wage...

---

### **Safeguarding Participant Contributions to Your 401(k) Plan**

#### **Fox Rothschild LLP**

In light of the economic disruption created by the COVID-19 pandemic, employers are exploring all available avenues to cut costs. Many are wondering...

---

### **OSHA issues temporary enforcement guidance on respiratory protection**

#### **Constangy Brooks Smith & Prophete LLP**

On March 14, the Occupational Safety and Health Administration issued initial Guidance explaining that due to the shortage of N95 filtering facepiece...



---

## **NLRB ALJ Reinforces Protection for Concerted Activity in Camp Counselor's Termination**

**Jackson Lewis PC**

On March 25, 2020, a National Labor Relations Board Administrative Law Judge ("ALJ") emphasized the broad reach of Section 7 of the National Labor...

---

## **Recent Changes to Unemployment: What Employers Need to Know**

**Wilmer Cutler Pickering Hale and Dorr LLP**

On March 27, 2020, President Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), an economic stimulus package...

---

## **CARES Act retirement and health plan relief: Practical implications for employers**

**DLA Piper**

The Coronavirus Aid, Relief and Economic Security Act (the CARES Act) contains several provisions affecting retirement plans and health and welfare...

---

## **The Coronavirus Aid, Relief, and Economic Security Act: Assistance Available to Passenger Airlines and Airports**

**Mintz**

On March 27, 2020, President Trump signed into law the "Coronavirus Aid, Relief, and Economic Security Act" (the "CARES Act"), a \$2+ trillion stimulus...

---

## **In the Nick of Time: Department of Labor Issues Regulations Interpreting the Families First Coronavirus Response Act**

**Dykema Gossett PLLC**

On April 1, the DOL provided employers with further clarity on the FFCRA by publishing temporary regulations. These regulations will be effective...

---

## **CDC Guidance on Worker Exposure to COVID-19 in Critical Infrastructure Businesses**

**Fox Rothschild LLP**

In their efforts to slow the spread of the novel coronavirus, COVID-19, many states have issued executive orders mandating that non-essential...

---

## **IRS Announces Penalty Relief for Employers Who Fail to Deposit Employment Taxes in Anticipation of COVID-19-Related Tax Credits**

**Day Pitney LLP**

Notice 2020-22 (Notice) provides penalty relief for employers who fail to deposit employment taxes in anticipation of the allowance of the new tax...

---

## **PPP Loan Eligibility: Do You Count Foreign Employees or Just U.S. Employees?**

**Miller Canfield PLC**

The U.S. Small Business Administration ("SBA") has issued new guidance on the new Paycheck Protection Program ("PPP"), which currently makes loans...

---

## **CARES Act 2020: Federal Reserve Measures in Response to COVID-19**

### **Baker McKenzie**

This alert discusses the federal loan components of the recent coronavirus stimulus package signed into law on Friday March 27, the Coronavirus Aid...

---

### **SEC issues \$2 million whistleblower award**

#### **Buckley LLP**

On April 3, the SEC announced an approximately \$2 million award to a whistleblower in an enforcement action. According to the SEC's press release...

---

### **Considerations for Limiting Liability for Manufacturers and Importers of Masks and PPE During the COVID-19 Crisis**

#### **Troutman Sanders LLP**

Introduction The demand for personal protective equipment (PPE) across the globe has created a shortage in hospitals and medical facilities for those...

---

### **EEOC Reminds Employers: Antidiscrimination Laws Continue to Apply During the COVID-19 Pandemic (US)**

#### **Squire Patton Boggs**

The United States currently is experiencing an unprecedented public health emergency due to the COVID-19 virus. The economic fallout of this crisis...

---

### **CARES Act: Unemployment Relief**

#### **Patterson Belknap Webb & Tyler LLP**

On March 27, 2020, the President signed into law the Coronavirus Aid, Relief, and Economic Security Act (the "CARES Act" or the "Act"), a \$2 trillion...

---

### **Cal/OSHA Issues COVID-19 Guidance for Agricultural Employers**

California

#### **Ogletree Deakins**

On April 7, 2020, the California Department of Industrial Relations' Division of Occupational Safety and Health (Cal/OSHA) issued COVID-19 Safety and...

---

### **Critical Infrastructure: Do's and Don'ts**

#### **Nelson Mullins Riley & Scarborough LLP**

Employers engaged in critical infrastructure face significant challenges in maintaining business operations while ensuring the health of their...

---

### **The Families First Coronavirus Response Act of 2020**

#### **Squire Patton Boggs**

On March 18, 2020, the US Senate passed, by a margin of 90 to eight, the Families First Coronavirus Response Act of 2020 (Act), aimed at providing...

---

### **Vicarious Liability for Employee's Data Breach: Key Takeaways from the U.K. Supreme Court's Judgment**

#### **Akin Gump Strauss Hauer & Feld LLP**

On April 1, 2020, the U.K. Supreme Court handed down its judgment in the case of WM Morrison Supermarkets plc v Various Claimants [2020] UKSC 12, the...

---



## **The Employee Retention Tax Credit: Aggregation Aggravation**

### **Baker & Hostetler LLP**

Employers navigating the incentives included in the Coronavirus Aid, Relief, and Economic Security (CARES) Act (P.L. 116-136) must undertake the...

---

## **Coronavirus: Congressional leaders and the Trump Administration reach agreement on massive COVID-19 relief and economic stimulus package**

### **DLA Piper**

Senate Republican and Democratic leaders and the Trump Administration announced on Wednesday, March 25, 2020, that they have reached a deal on the...

---

## **Financial Lifelines, Waivers and Other Support for Hospitals and Healthcare Systems Responding to the Coronavirus Pandemic**

### **Squire Patton Boggs**

In just the past week, the federal government has issued a flurry of legislative and regulatory aid packages, programs and rule changes for...

---

## **COVID-19 and Practical Guidance for Medical and Dental Offices**

### **Day Pitney LLP**

Day Pitney is pleased to offer this practical guide for medical and dental offices seeking useful information related to the impact the novel...

---

## **San Francisco Enacts Emergency Ordinance: Public Health Emergency Leave**

### **Duane Morris LLP**

The PHELO addresses the FFCRA's coverage gap by establishing minimum requirements for private employers with more than 500 employees...

---

## **DOL Issues Newly Updated Guidance on Critical Issues for Employers Regarding the Families First Coronavirus Response Act**

### **Morrison & Foerster LLP**

On March 28, 2020, the United States Department of Labor ("DOL") published additional guidance on nearly two dozen more "critical issues" that the...

---

## **Los Angeles Requires Face Coverings to Protect Workers**

### **Fox Rothschild LLP**

On April 7, 2020, Los Angeles Mayor Eric Garcetti issued a Worker Protection Order ("Order") (revised on April 9, 2020) ordering further protections...

---

## **May The Fourth Be With You: Minnesota Stay-At-Home Order Extended to May 4**

### **Jackson Lewis PC**

On April 8, 2020, Minnesota State Governor Tim Walz issued Emergency Executive Order 20-33 Extending Stay at Home Order and Temporary Closure of Bars...

---

## **Beltway Buzz, April 10, 2020**

### **Ogletree Deakins**

On April 9, 2020, the U.S. Senate failed to approve a measure that would have added \$251 billion in funding for the Small...

---

### **A Timely Reminder: Employee Complaints About Working Conditions Are Protected**

#### **Dykema Gossett PLLC**

As employee complaints about safety and the availability of personal protection equipment ("PPE") mount, employers should remember that the law...

---

### **Updated workplace cleaning guidelines from the CDC and a new OSHA poster!**

#### **Shawe Rosenthal LLP**

The Centers for Disease Control recently updated its guidelines for cleaning and disinfecting, including those that apply to employers. These...

---

### **Covid-19 and the NLRB: Effective Date of New "Election Protection" Rule Postponed**

#### **Vorys Sater Seymour and Pease LLP**

Labor professionals waiting for the new rule on certain employee free choice issues to go into effect will have to wait a little longer. The NLRB...

---

### **Returning to Work: Can Employers Still Require Doctors' Notes from Employees Who Test Positive for COVID-19?**

#### **Ice Miller LLP**

Students of Greek mythology will recall the story of Scylla and Charybdis, two monsters in Homer's Odyssey that patrolled the uncharted waters of the...

---

### **DOL Guidance Clarifies Nuances on How FFCRA Leave May Be Used: Part Three in a Five-Part Series**

#### **Squire Patton Boggs**

In the first installment of this five-part series exploring the US Department of Labor (DOL) regulations (29 CFR Part 826) interpreting the Families...

---

### **How to Pay for FFCRA Leave Part Four in a Five-Part Series**

#### **Squire Patton Boggs**

In the first installment of this five-part series exploring the US Department of Labor (DOL) regulations (29 CFR Part 826) interpreting the Families...

---

### **Recent COVID-19-Related Executive Orders Impact Connecticut Employers**

#### **Ford & Harrison LLP**

Over the past few days, Connecticut Governor Ned Lamont has issued Executive Orders 7V, 7W and 7X, the latest in a series of...

---

### **Employer COVID-19 Responses May Trigger Additional State and Local Wage Payment, Notice and Other Obligations**

#### **Faegre Drinker Biddle & Reath LLP**

In the midst of the COVID-19 pandemic, state and local "stay at home" orders and the resulting financial and business impact, many employers have...



---

**In the Nick of Time: Department of Labor Issues Temporary Regulations Interpreting the Families First Coronavirus Response Act**

**Dykema Gossett PLLC**

On April 1, the DOL provided employers with further clarity on the FFCRA by publishing temporary regulations. These regulations will be effective...

---

**Federal Reserve and Treasury announce new Main Street Lending Program**

**Eversheds Sutherland (US) LLP**

On April 9, 2020, the Federal Reserve and Treasury announced a package of new financial assistance programs to provide up to \$2.3 trillion in loans to...

---

**Providing Tax-Advantaged Employee Assistance in the Wake of COVID-19**

**Michael Best & Friedrich LLP**

In the face of substantial economic strain on a workforce that has been furloughed, laid off or otherwise removed from a normally reliable stream of...

---

**Top Five Labor Law Developments for March 2020**

**Jackson Lewis PC**

Employers affected by the COVID-19 pandemic may receive some financial relief from the Coronavirus Aid, Relief, and Economic Security (CARES) Act...

---

**IRS Issues Guidance on Required Documentation Necessary to Obtain Tax Credits on Paid Sick Leave and Emergency FMLA Leave Requests**

**Vorys Sater Seymour and Pease LLP**

The Families First Coronavirus Response Act (FFCRA) requires that most private employers with 500 or fewer employees and most public sector...

---

**EEOC Updates COVID-19 Guidance**

**Spencer Fane LLP**

On April 9, the Equal Employment Opportunity Commission ("EEOC") updated its guidance for employers entitled "What You Should Know About COVID-19 and...

---

**Ironing out the Details: The Department of Labor Updates and Adds to Its FFCRA Guidance Faqs**

**Dykema Gossett PLLC**

As employers try to comply with the new Families First Coronavirus Response Act's (FFCRA) paid sick leave and expanded family and medical leave...

---

**SBA and Treasury Announce Mobilization for Paycheck Protection Act in the US**

**Baker McKenzie**

On March 31, SBA Administrator Jovita Carranza and Treasury Secretary Steven T. Mnuchin announced that the SBA and Treasury Department have initiated...

---

**What Employers Need To Know About The Unemployment Provisions Of The CARES Act**

**Fisher Phillips**

The U.S. Department of Labor recently issued a series of guidances to assist employers and employees in understanding the unemployment provisions of...

---

**USDOL Issues Opinion Letter on Inclusion of Longevity Bonus in the Regular Rate**

**Fox Rothschild LLP**

The USDOL has been quite busy lately in issuing regulations and other guidance relating to the provisions in the Families First Coronavirus Response...

---

**The City of Los Angeles Mandates Supplemental Paid Sick Leave Effective Immediately**

**Sheppard Mullin Richter & Hampton LLP**

California and Los Angeles currently require covered employers to provide eligible employees with paid sick leave benefits. Effective immediately...

---

**OSHA Extends Suspension of N95 Annual Fit Testing to All Industries**

**Ogletree Deakins**

On April 8, 2020, the Occupational Safety and Health Administration (OSHA) issued an enforcement memorandum titled Expanded Temporary Enforcement...

---

**EEOC addresses ongoing questions about COVID-19, the ADA and other EEO laws**

**Greensfelder, Hemker & Gale, P.C.**

On April 9, 2020, the Equal Employment Opportunity Commission (EEOC) issued its updated Technical Assistance Questions and Answers titled "What You...

---

**Avoiding Negligence Per Se Claims For Non-Compliance With Social Distancing Orders In The US**

**Bryan Cave Leighton Paisner LLP**

The measures implemented by state and local governments in response to the spread of COVID-19 vary widely, from suggested guidelines to mandatory...

---

**COVID-19: Key Questions Franchisors Are Asking**

**DLA Piper**

As the coronavirus disease 2019 (COVID-19) crisis has escalated, each of us is being inundated with communications about it...

---

**Federal Contractors May Be Eligible for Reimbursement of Paid Leave Under CARES Act**

**Fox Rothschild LLP**

As federal agencies close facilities due to the COVID-19 outbreak and related quarantine orders, the contractors working on federal projects have...

---

**CARES Act: Changes to Unemployment Compensation Present Opportunities to Businesses and Employees**

**Stinson LLP**

During these unprecedented times when businesses are deciding how to adjust



work schedules and/or close facilities in light of supply and demand...

---

**OSHA Issues New Guidance Given N95 Mask Shortage During COVID-19 Pandemic**

**Fisher Phillips**

The Occupational Safety and Health Administration (OSHA) just issued interim Enforcement Guidance regarding respiratory protection, relaxing its...

---

**Rocky Mountain Region COVID-19 Update (CO, ID, MT, NE, NM, UT, WY)**

**Gordon Rees Scully Mansukhani**

The Rocky Mountain Region COVID-19 Employment Update provides information about COVID-19 orders in Colorado, Idaho, Montana, Nebraska, New Mexico...

---

**Mayor Garcetti Signs Modified Los Angeles Ordinance Allowing Up To 80 Hours Of Supplemental COVID-19 Paid Sick Leave**

**Fisher Phillips**

Los Angeles Mayor Eric Garcetti just signed into law the City Council's proposed Supplemental Paid Sick Leave ordinance. He made some modifications...

---

**OFCCP's New Scheduling Letters Result in Few Changes for Contractors**

**Jackson Lewis PC**

As we previously reported, OFCCP finally received approval of its new scheduling letters - and as a result federal contractors and subcontractors...

---

**Outlook of Congress' "Phase 4" COVID-19 Stimulus Package**

**Akin Gump Strauss Hauer & Feld LLP**

In response to the COVID-19 outbreak, Congress has passed three major pieces of legislation to provide relief to families and the U.S. economy. On...

---

**OSHA to Employers: Some Relief from Respiratory Protection Rules in the Face of N95 Shortages**

**Jenner & Block LLP**

On April 3, 2020, U.S. OSHA issued two Enforcement Guidance memos which, for the first time, provide guidance to all industries, including healthcare...

---

**Los Angeles Mayor Signs COVID-19 Supplemental Paid Sick Leave Order**

**Ogletree Deakins**

The Los Angeles City Council recently passed an ordinance providing supplemental paid sick leave to employees affected by COVID-19 who were employed...

---

**New Guidance from the Federal Government on Unemployment Benefits -- \$600 Payment**

**Clingen Callow & McLean LLC**

Many of our clients have been faced with the Hobson's choice of furloughs, layoffs, or shutting down...

---

## **US Department of Labor Clarifies Employer Obligations to Record COVID-19 Cases (US)**

### **Squire Patton Boggs**

On April 10, 2020, the US Department of Labor's ("DOL") Occupational Safety and Health Administration ("OSHA") issued interim guidance on employers'...

---

## **Complying with the Evolving and Conflicting COVID-19 State Closure Landscape; CISA Updates List of Essential Critical Infrastructure Workers**

### **Womble Bond Dickinson (US) LLP**

Over the last two weeks, COVID-19 state business closure orders, which we are tracking on our 50-State interactive guide, and their related stay at...

---

## **CAL/OSHA Provides Guidance On COVID-19 Infection Prevention For Agricultural Industry**

California

### **Fisher Phillips**

The California Department of Industrial Relations Division of Occupational Safety & Health (DOSH), or Cal/OSHA, just issued guidance for employers on...

---

## **Department of Labor Regulations on the FFCRA: Summary**

### **Breazeale Sachse & Wilson LLP**

The Department of Labor ("DOL") has issued regulations codifying the DOL's prior guidance on the Families First Coronavirus Response Act, summaries...

---

## **DOL Final Rule: Paid Leave Under the Families First Coronavirus Response Act**

### **Haynsworth Sinkler Boyd PA**

The U.S. Department of Labor (DOL) issued a Final Rule regarding the paid leave provisions of the Families First Coronavirus Response Act (FFCRA)...

---

## **Your Construction Job Has Been Shut Down or Access Limited Due to the COVID-19 Pandemic, What Should You Do?**

### **Gordon Rees Scully Mansukhani**

Time is money. Costs on a construction project increase the longer it takes to complete. Project delays are common and costs associated therewith are...

---

## **OSHA Expands Guidance on Respirator Fit-Testing to Cover all Industries**

### **Jackson Lewis PC**

Due to the evolving coronavirus ("COVID-19") pandemic and emergence of outbreaks across the country, there have been widespread reports of critical...

---

## **Employers Can Provide Tax-Free Assistance to Employees Impacted by COVID-19**

### **Frost Brown Todd LLC**

Code section 139 excludes from taxable income "qualified disaster relief payments" made to reimburse or pay reasonable and necessary personal, family...

---

## **Pandemic Class Action Refund Lawsuits Against Airlines Ignore Long-Standing**



## **Precedent**

### **Stinson LLP**

Class action plaintiffs lawyers have reacted to the COVID-19 pandemic by filing putative class actions against Airlines which, in order to conserve...

---

## **NLRA Implications Amid COVID-19**

### **Frost Brown Todd LLC**

The COVID-19 pandemic has raised many labor issues for employers dealing with their workforces. State issued stay-at-home orders have forced employers...

---

## **IRS Offers Advance Funding of Employee Retention Tax Credit**

### **Baker & Hostetler LLP**

Businesses searching for immediate cash should not overlook the fully refundable employee retention tax credit (ERTC), which permits employers to...

---

## **Unemployment Insurance Benefits: A COVID-19 Update for California Employers**

### **Sheppard Mullin Richter & Hampton LLP**

As a result of the COVID-19 pandemic, more than 16 million Americans have filed for unemployment in the last three weeks—approximately 10% of the...

---

## **OSHA Issues Enforcement Guidance on Recording COVID-19 Cases**

### **Jackson Lewis PC**

Today, OSHA issued long over due guidance relating to the recordability of COVID-19 cases for employers. In short, OSHA has stated that it will not...

---

## **Troutman Sanders Weekly Consumer Financial Services COVID-19 Newsletter - April 13, 2020**

[West Virginia](#)

### **Troutman Sanders LLP**

Like most industries today, consumer finance services businesses are being significantly impacted COVID-19. Troutman Sanders and Pepper Hamilton have...

---

## **EEOC Updates COVID-19 Guidance**

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

On April 9, the Equal Employment Opportunity Commission (EEOC) posted additional, updated guidance for employers regarding COVID-19, the ADA, and...

---

## **Check Please: Paying for COVID-19**

### **Leech Tishman Fuscaldo & Lampl LLC**

Coronavirus ("COVID-19") has wreaked havoc on workplaces and communities. One of the first questions clients ask amid government shutdowns, forced...

---

## **The Emergency Paid Sick Leave Act - A Comprehensive Overview**

### **Brooks Pierce McLendon Humphrey & Leonard LLP**

On March 18, 2020, President Trump signed the Families First Coronavirus Response Act (FFCRA) into law. The FFCRA contains two key provisions for...

---

## **New York State Enacts Broad Paid Sick Leave Law**

New York

**Morgan Lewis**

New York Governor Andrew Cuomo signed legislation on April 3 creating a statewide paid sick leave requirement (the Paid Sick Leave Law), which allows...

---

## **CDC Significantly Relaxes Essential Worker Return-To-Work Standards After COVID-19 Exposure**

**Fisher Phillips**

The Centers for Disease Controls and Prevention (CDC) significantly relaxed its previous guidance on returning critical infrastructure workers to...

---

## **EEOC Answers Key Questions for Employers, Including Whether Employers Can Identify an Employee Diagnosed With COVID-19 to a Public Health Agency**

**Jackson Lewis PC**

Employers have been struggling with exactly what information they are permitted to disclose to a public health agency when an employee is diagnosed...

---

## **The Emergency Family and Medical Leave Expansion Act - A Comprehensive Overview**

**Brooks Pierce McLendon Humphrey & Leonard LLP**

On March 18, 2020, President Trump signed the Families First Coronavirus Response Act (FFCRA) into law. The FFCRA contains two key provisions for...

---

## **New EEOC Technical Assistance on COVID-19**

**Hall Render Killian Heath & Lyman PC**

EEOC states that EEO laws do not prevent employers from following guidelines and suggestions made by the CDC or state/local public health authorities...

---

## **States Adapt Workers' Compensation Systems Under COVID-19**

**Frost Brown Todd LLC**

As states continue to respond to the challenges presented by COVID-19, many are adapting their workers' compensation systems. Changes include virtual...

---

## **Summary of Recent Agency Activity on Employment-Related COVID-19 Issues**

**Spencer Fane LLP**

Last week (April 4-12), several federal agencies issued updated guidance for employers on issues relating to COVID-19, including...

---

## **OSHA Unmasks New Pandemic Respirator Guidance**

**Venable LLP**

The Respiratory Protection standard contains various requirements, including a written program, medical evaluation, fit-testing, and training, that...

---

## **First Employee Lawsuit Filed Seeking to Avoid the Workers' Compensation Exclusivity Bar for COVID-19-Related Injuries**

New Jersey

**Lowenstein Sandler LLP**

Among the many issues employers are struggling with in the midst of the current



COVID-19 crisis is the risk of harm to an essential employee who is...

---

#### **Remote Work Increases Data Security Risks**

##### **Vorys Sater Seymour and Pease LLP**

Your employees are sheltering in place and working remotely. They now communicate with each other, business partners and customers via email, Zoom...

---

#### **Essential Services Guide to Keeping Workplaces and Employees Safe During COVID-19**

##### **Haynsworth Sinkler Boyd PA**

Businesses operating on-site during the COVID-19 pandemic must take extra precautions to ensure they are not subjecting their employees and others...

---

#### **COVID-19 Impacts LCA Compliance**

##### **Troutman Sanders LLP**

The place of employment remains a critical consideration for employers sponsoring foreign nationals in H-1B, H-1B1, and E-3 status. In addition to...

---

#### **Tax Exemptions and Implications of Employee COVID-19 Hardship Payments**

##### **Faegre Drinker Biddle & Reath LLP**

Employers providing support to employees during the COVID-19 pandemic can do so without triggering tax requirements in many cases — but executives...

---

#### **FAQs: COVID-19 - General Labor and Employment Legal Concerns - April 13, 2020 Update**

##### **Baker & Hostetler LLP**

BakerHostetler's COVID-19 Labor and Employment Issues Task Force issued a set of FAQs on March 18, 2020, March 30, 2020 and April 6, 2020 regarding...

---

#### **CDC: Asymptomatic Critical Infrastructure Workers Can Continue Working after Potential COVID-19 Exposure**

##### **Jackson Lewis PC**

When can employees who may have been exposed to COVID-19 return to work? Guidance from the Centers for Disease Control and Prevention (CDC) advises...

---

#### **OSHA Relaxes Requirement for Work-related Assessment for COVID-19 Recordkeeping for Certain Employers**

##### **Haynes and Boone LLP**

OSHA requires that covered employers record certain work-related injuries and illnesses on their OSHA 300 log. Under OSHA's recordkeeping...

---

#### **OSHA Considerations for Employers Deciding Whether to Require or Allow Use of Face Masks in the Workplace**

##### **Stinson LLP**

The Centers for Disease Control and Prevention (CDC) recently recommended the use of cloth face coverings in public as an "additional, voluntary...

---

## **OSHA Issues Interim Enforcement Guidance on the Meaning of “Work Related” for Recording Cases of COVID-19**

**Ogletree Deakins**

On April 10, 2020, the federal Occupational Safety and Health Administration (OSHA) issued interim enforcement guidance for recording cases of the...

---

## **Getting Back to Work After Confirmed COVID-19: The Importance of Response Planning**

**Womble Bond Dickinson (US) LLP**

By now, every segment of our economy and industrial sector has been touched by the novel coronavirus, COVID-19. A recent supply management survey...

---

## **COVID-19: COVID-19 Considerations: Employer Sponsored Health and Welfare Plans**

**K&L Gates**

In the wake of the COVID-19 pandemic and the resulting economic uncertainty, many employers are searching for ways to be financially prepared in the...

---

## **COVID-19: Frequently Asked Questions For You and Your Business**

**Breazeale Sachse & Wilson LLP**

Is my business required to shut down because of the statewide Stay-at-Home order issued by Governor John Bel Edwards? The Stay at Home order issued...

---

## **Preparing to Return U.S. Employees to the Workplace**

**Bryan Cave Leighton Paisner LLP**

As we approach the one month anniversary of the first “stay-at-home” orders, many are asking when we can get back to work and what will it look like...

---

## **New CISA Essential Business Guidance for Exposed Workers; Fed Reserve Issues Relief; Administration Looking at Calls for Expensing**

**Michael Best & Friedrich LLP**

Interim Guidance for Critical Infrastructure Workers Who MAY HAVE BEEN EXPOSED to COVID-19 Please find below an important update from the Centers for...

---

## **Expansion of Unemployment Benefits in the CARES Act**

**Breazeale Sachse & Wilson LLP**

The Coronavirus Aid, Relief, and Economic Security Act or the "CARES Act" was signed into law on March 27, 2020 and provides \$2 trillion in funds...

---

## **Benefit Plan Implications of the CARES Act**

**Dykema Gossett PLLC**

The Act allows tax-qualified retirement plans to provide Coronavirus-related distributions (“CRDs”)...

---

## **Louisiana Workers' Compensation Law and COVID-19 as a Potential**

---



## **Compensable Occupational Disease**

Louisiana

### **Breazeale Sachse & Wilson LLP**

To understand the potential to employers for possible compensability of COVID-19 infections of its employees under Louisiana Worker's Compensation law...

---

## **NLRB Reaffirms Limitations on Employers' Ability to Solicit Employee Assistance in Anti-Union Campaigning and Confidentiality Restrictions**

### **Proskauer Rose LLP**

In maintaining business as usual as best it can amidst the ongoing COVID-19 crisis, the Board recently decided an issue concerning limitations on...

---

## **Some Clarity to the Murky: Temporary Rules Relative to the Families First Coronavirus Response Act Have Been Issued**

### **Foster Garvey**

The U.S. Department of Labor (the "DOL") issued, effective April 6, 2020, temporary rules ("Rules") relative to the Families First Coronavirus...

---

## **COVID-19: Handling a Positive Diagnosis in the Workforce**

### **Mintz**

As the COVID-19 outbreak continues to disrupt normal workplace operations, an increasing number of employers are facing the reality of employees...

---

## **FDA Releases Best Practices for Retail Food Establishments During the COVID-19 Pandemic**

### **Faegre Drinker Biddle & Reath LLP**

On April 9, 2020, the Food and Drug Administration (FDA) issued Best Practices for Retail Food Stores, Restaurants, and Food Pick-Up and Delivery...

---

## **Implementing Coronavirus Leave under New Federal Laws: Frequently Asked Questions**

### **Akin Gump Strauss Hauer & Feld LLP**

On April 1, 2020, the Families First Coronavirus Response Act (FFCRA) became effective, enabling employees to take paid sick leave under...

---

## **COVID-19 Wage Subsidy Bill Received Royal Assent On April 11, 2020**

### **Dickinson Wright**

Bill C-14: A second Act respecting certain measures in response to COVID-19 (the "COVID-19 Wage Subsidy Bill") - the second piece of emergency...

---

## **Novel coronavirus - How employers should dispose of personal protective equipment**

### **Reed Smith LLP**

The Occupational Safety and Health Administration (OSHA) and the California Department of Occupational Safety and Health (Cal/OSHA) have issued...

---

## **Claiming Federal Relief Tax Credits and Deferring Payroll Tax Payments**

### **Vorys Sater Seymour and Pease LLP**

Recent Federal COVID-19 legislation provides employers with a number of new potential tax credits. The FFCRA (Phase II relief) requires certain...

---

### **US COVID-19: Workplace Temperature Screening: How To Develop and Implement A Screening Protocol**

**Bryan Cave Leighton Paisner LLP**

The notion that U.S. employers would engage in broad-scale temperature screening of employees would have once been essentially unthinkable. But the...

---

### **Business Court Waives 90-Day Waiting Period For All Derivative Claims Where At Least One Claim Seeks Emergency Relief**

**Womble Bond Dickinson (US) LLP**

Where at least one derivative claim asserted "irreparable harm" to the LLC if the member waited 90 days after its demand before filing suit, the...

---

### **Puerto Rico Enacts Five-Day Paid Emergency Leave for Pandemic Illness**

**Jackson Lewis PC**

Puerto Rico's Law 37-2020 provides certain employees up to five days of paid leave once they exhaust other paid leave. Law 37-2020 amends Puerto Rico...

---

### **Employers Take Note of the CARES Act: More Paid Sick and Family Leave Legislation in Response to Coronavirus**

**Robinson & Cole LLP**

As the novel coronavirus (COVID-19) continues to sweep the nation, the "Families First Coronavirus Response Act" (FFCRA) was approved by Congress and...

---

### **Paid Sick and Family Leave Legislation in Response to Coronavirus**

**Robinson & Cole LLP**

Please note that this summary has been updated to reflect guidance issued by the U.S. Department of Labor (DOL) on March 29, 2020. The recent...

---

### **Turf War Update: Sixth Circuit Weighs In on Dispute Between Bankruptcy Courts and FERC Over Rejection of Power Contracts**

**Jones Day**

The recent chapter 11 filings by PG&E Corp. and its Pacific Gas & Electric Co. utility subsidiary (collectively, "PG&E") and FirstEnergy Solutions...

---

### **FAQs Clarify COVID-19 Testing and Diagnosis Requirements for Employer Health Plans**

**Ogletree Deakins**

Employers now have greater clarity on how the new federal requirements covering COVID-19 testing and diagnosis apply to their group health plans...

---

### **California Offers Some Clarity Regarding Revised Notice Requirements Under Cal-WARN**

California

**Ogletree Deakins**



On March 23, 2020, the California Department of Industrial Relations (DIR) issued "Guidance on [the] Conditional Suspension of California WARN Act..."

---

### **U.S. Fifth Circuit Clarifies Position: Later-Verified Charge Can Relate Back To Filing Date**

#### **Proskauer Rose LLP**

On April 3, 2020, a three-judge panel of the U.S. Fifth Circuit in *EEOC v. Vantage Energy Services, Inc.*, No. 19-20541, clarified its interpretation...

---

### **OSHA tries to simplify recording of COVID-19 cases on employers' OSHA 300 Logs**

#### **Constangy Brooks Smith & Prophete LLP**

In an Interim Guidance Memorandum issued on Friday, the Occupational Health and Safety Administration has attempted to simplify the decision making...

---

### **Employer Update on the FFCRA**

#### **Greenspoon Marder LLP**

First and foremost, we hope each of you and your families are well as we continue to navigate through this difficult period for all of us. Many of...

---

### **Recent Amendments to Home Care Worker Wage Parity Law**

#### **Robinson & Cole LLP**

On April 3, 2020, New York State passed legislation implementing amendments to the Home Care Worker Wage Parity Law, contained in section 3614-c of...

---

### **Does Your Company Timely Respond to All Reports of Potential Misconduct?**

#### **Jones Day**

The Securities and Exchange Commission ("SEC") awards \$450,000 to a whistleblower who had compliance-related responsibilities. On March 30, 2020, the...

---

### **FFCRA documentation requirements for employers: What to ask for, what to document, and what to keep**

#### **Greensfelder, Hemker & Gale, P.C.**

Almost two weeks after the effective date of the Families First Coronavirus Response Act (FFCRA), many employers are still not certain what...

---

### **OSHA Update: Recording Cases of COVID-19**

#### **Frost Brown Todd LLC**

The Occupational Health and Safety Administration (OSHA) requires covered employers to record certain workplace injuries and illnesses on their OSHA...

---

### **US COVID-19: Workplace Temperature Screening: How To Develop and Implement A Screening Protocol**

#### **Bryan Cave Leighton Paisner LLP**

The notion that U.S. employers would engage in broad-scale temperature screening of employees would have once been essentially unthinkable. But the...

---

## **Emergency Rule: Seattle Employers Cannot Ask For Doctor's Notes For Paid Sick Time**

**Fisher Phillips**

Seattle's Office of Labor Standards just issued a temporary emergency rule that prohibits employers from requesting a doctor's note to verify...

---

## **The FRA Provides Guidance on Best Practices and Reporting Cases of COVID-19 Among Railroad Employees**

**Duane Morris LLP**

The Federal Railroad Administration (the "FRA") has recently issued regulatory guidance regarding safety precautions related to COVID-19 and whether...

---

## **DOL Issues Corrections to FFCRA Regulations - What Employers Need to Know**

**Proskauer Rose LLP**

On April 10, 2020, the Department of Labor ("DOL") released corrections to the regulations implementing the Emergency Family and Medical Leave...

---

## **Ohio House of Representatives Has Introduced Legislation to Include COVID-19 in the List of Scheduled Occupational Diseases**

**Taft Stettinius & Hollister LLP**

In light of the ongoing COVID-19 pandemic, the Ohio House of Representatives has introduced legislation that would amend section 4123.68 of the...

---

## **A Guide To Unemployment Benefits In California During Covid-19**

**Fisher Phillips**

California's Unemployment Insurance (UI) program pays benefits to individuals who have become unemployed or partially unemployed and who meet the...

---

### **Environment & Climate Change**



## **Keeping Current on COVID-19 Challenges for the Water Industry**

**Nossaman LLP**

There is no question that the COVID-19 pandemic has significantly disrupted business operations in virtually every business sector, and the water...

---

## **EPA Provides Flexibilities to Manufacturers of "List N" Disinfectants for Use Against Coronavirus**

**Covington & Burling LLP**

EPA on March 31 provided a formal relaxation of certain FIFRA requirements for pesticides listed on EPA's "List N" of products expected to be...

---

## **US Public Water Systems During the COVID-19 Pandemic**

**Morgan Lewis**

The virus that causes the coronavirus (COVID-19) disease is highly susceptible to standard treatment and disinfectant processes practiced by the...

---



## **Amid COVID-19, US EPA loosens its enforcement policies on the regulated community**

### **DLA Piper**

On March 26, 2020, the Environmental Protection Agency (EPA) announced that it will exercise enforcement discretion in Policing businesses and other...

---

## **Forests Recognized as Contributors to Washington State's Response to Climate Change**

Washington

### **Beveridge & Diamond PC**

On March 25, 2020, Governor Jay Inslee signed HB 2528 into law which recognizes the contributions of the State's forests and forest products sector...

---

## **EPA Finalizes SAFER Part 2**

### **Sidley Austin LLP**

On March 31, 2020, the U.S. Environmental Protection Agency (EPA) and the National Highway Traffic Safety Administration (NHTSA) finalized Part 2 of...

---

## **EPA responds to criticisms of its new temporary enforcement discretion policy**

### **Reed Smith LLP**

In response to the backlash regarding the EPA's implementation of a temporary enforcement discretion policy, the EPA administrator, Andrew Wheeler...

---

## **State Environmental Agencies Announce Expanded Compliance Assistance, New Enforcement Policies in Light of COVID-19**

Wisconsin

### **Michael Best & Friedrich LLP**

In the wake of the Environmental Protection Agency's (EPA) recent announcement of temporary enforcement discretion for certain environmental...

---

## **Second District Reaffirms Rule That Filing of Facially Valid NOD Triggers Short CEQA Statute of Limitations And Plaintiff May Not "Go Behind" Agency's Declarations In Document To Challenge Validity of Project Approval**

California

### **Miller Starr Regalia**

On April 2, 2020, the Second Appellate District Court of Appeal (Division 5) filed its published opinion in Coalition for an Equitable...

---

## **Ozone's Cure is Climate's Scourge—Northeast States to Ban Use of Hydrofluorocarbons**

### **Hunton Andrews Kurth LLP**

Joining a growing chorus of states, several Northeastern states, including Massachusetts, Maine and Rhode Island, have recently announced their...

---

## **U.S. EPA and NHTSA Finalize Rollback of Obama-Era CO2 emissions and CAFE Standards**

### **Baker McKenzie**

On March 30, 2020, the United States Environmental Protection Agency ("EPA") and the National Highway Traffic Safety Administration ("NHTSA"), on...

---

## **U.S. EPA Issues Enforcement Discretion Policy in Response to COVID-19**

### **Lewis Rice LLC**

Last month, the United States Environmental Protection Agency (the “U.S. EPA”) released a temporary enforcement discretion policy in response to the...

---

## **Quadruple Threat: EPA Joins Fight to Prevent Sales of Bogus Virus Fighters**

### **Frankfurt Kurnit Klein & Selz PC**

I blogged yesterday about a joint effort of the FTC and FCC to prevent robocalls marketing fraudulent home coronavirus testing kits and HVAC cleaning...

---

## **Wisconsin Department of Natural Resources Outlines its COVID-19**

### **Environmental Compliance Process** Wisconsin

### **Quarles & Brady LLP**

The Wisconsin Department of Natural Resources (WDNR) recognizes that compliance with certain environmental regulations may be difficult for some...

---

## **EPA Extends Deadline For Chemical Data Reporting Filings Under Toxic Substances Control Act**

### **Nelson Mullins Riley & Scarborough LLP**

Effective April 9, 2020, EPA is amending the Toxic Substances Control Act (TSCA) Chemical Data Reporting (CDR) regulations by extending the submission...

---

## **US EPA Offers Advice to NPDES Permittees on Documenting COVID-Related Noncompliance While Environmental Groups Seek More Stringent Reporting Requirements**

### **Squire Patton Boggs**

On March 26, 2020, US EPA issued a temporary policy regarding enforcement of routine monitoring, recordkeeping, and reporting violations caused by the...

---

## **Challenges to Environmental Investigations and Cleanups During the COVID-19 Crisis** New York

### **Morgan Lewis**

The rapidly evolving coronavirus (COVID-19) crisis has given rise to several immediate impacts to ongoing cleanups of contaminated sites under state...

---

## **COVID-19 Unsympathetic to TSCA Compliance**

### **Keller and Heckman LLP**

On March 26, 2020, the U.S. Environmental Protection Agency (EPA) released a memorandum (“Policy”) announcing the temporary exercise of enforcement...

---

## **Massachusetts Department of Environmental Protection: COVID-19 Guidance For Waste Site Cleanup Activities** Massachusetts

### **Gordon Rees Scully Mansukhani**

Massachusetts Department of Environmental Protection's (MassDEP) Bureau of Waste Site Cleanup (BWSC) is continuing to operate during the State of...

---



## **Autonomous and Connected Multimodal Transportation: A Global Game Changer**

California

### **Beveridge & Diamond PC**

Autonomous and connected vehicles are on the brink of changing global transportation and land use forever. These types of vehicles will, among other...

---

## **COVID-19 - U.S. Environmental Update: EPA Issues New "Temporary" Enforcement Policy**

### **Baker McKenzie**

Earlier this week, we provided guidance on the development of an "Environmental Action Plan" to address potential environmental regulatory and...

---

## **COVID-19: EPA, Other Federal Agencies Continue Processing FOIA Requests—For Now**

### **Morgan Lewis**

In response to heightened Freedom of Information Act (FOIA) activity since 2012, federal agencies have increased their FOIA staff by 21%. This...

---

## **District Court Holds CERCLA Preempts ELA's Statute of Limitations**

### **Taft Stettinius & Hollister LLP**

Refined Metals first filed its claims in 2017 under CERCLA and the ELA seeking response costs related to environmental contamination but CERCLA's...

---

## **EPA Lifts TSCA Risk Evaluation Fees Requirement for Most of Retail Industry**

### **Hunton Andrews Kurth LLP**

The United States Environmental Protection Agency (EPA) has announced that it will provide retail companies with significant relief from its Toxic...

---

## **Federal Agencies Crack Down on Coronavirus Advertising**

### **Patterson Belknap Webb & Tyler LLP**

As coronavirus (COVID-19) spreads across the country, some companies are advertising their products' usefulness in preventing or treating the disease...

---

## **EPA Administrator Andrew Wheeler Talks Disinfectant Products and False Claims of Effectiveness Against COVID-19**

### **Taft Stettinius & Hollister LLP**

On April 3, 2020, U.S. Environmental Protection Agency (EPA) Administrator Andrew Wheeler hosted a call with retailers and third-party marketplace...

---

## **EPA Issues Interim Guidance for Managing COVID-19 Impacts at Superfund, RCRA, and Other Remediation Projects**

### **Spencer Fane LLP**

Following on the March 19 internal memorandum from the Office of Land and Emergency Management (available here), and the March 26 COVID-19...

---

## **EPA Releases COVID-19 Guidance for Superfund and Other Field Work**

### **Sidley Austin LLP**

On April 10, the U.S. Environmental Protection Agency (EPA) issued its anticipated guidance to its regional administrators regarding whether field...

---

### **Environmental Regulatory Implications of New Jersey Executive Order (EO) 122 Halting All Non-Essential Construction**

New Jersey

#### **Manko Gold Katcher & Fox**

On April 8, Governor Murphy issued Executive Order No. 122 (EO 122) suspending all non-essential construction in the State of New Jersey, effective...

---

### **EPA Requests SAB And SAB Standing Committee Nominations**

#### **Bergeson & Campbell PC**

On April 1, 2020, the U.S. Environmental Protection Agency (EPA) announced that it is now accepting nominations of scientific experts to be considered...

---

### **EPA Issues Interim Guidance on Site Field Work Decisions at Superfund and RCRA Sites in Light of COVID-19 Emergency**

#### **Manko Gold Katcher & Fox**

On April 10, 2020, EPA issued its Interim Guidance on Site Field Work Decisions Due to Impacts of COVID-19 (the Guidance), concerning the potential...

---

### **Trump administration releases final SAFE vehicles rule**

#### **Hogan Lovells**

On 31 March 2020, the U.S. Environmental Protection Agency (EPA) and the Department of Transportation National Highway Traffic Safety Administration...

---

### **EPA Extends Comment Period on Supplement to Proposed Rule on Strengthening Transparency in Regulatory Science**

#### **Bergeson & Campbell PC**

On March 3, 2020, the U.S. Environmental Protection Agency (EPA) announced the availability of a supplemental notice of proposed rulemaking (SNPRM) to...

---

### **EPA Sets Stage for Future Asbestos Regulations in New Draft Risk Evaluation**

#### **Hunton Andrews Kurth LLP**

On March 30, 2020, the United States Environment Protection Agency (EPA) issued its long-awaited draft risk evaluation for asbestos. In it, EPA...

---

### **EPA Announces Clarification on Its Temporary Compliance Guidance**

#### **Bergeson & Campbell PC**

On March 30, 2020, the U.S. Environmental Protection Agency (EPA) issued a Press Release to clarify its Temporary Policy released on March 26, 2020...

---

### **EPA Announces and Clarifies Temporary Enforcement Discretion Policy**

#### **Bergeson & Campbell PC**

EPA announced on March 26, 2020, a temporary policy regarding enforcement of environmental legal obligations during the COVID-19 pandemic. EPA states...

---

### **Misconceptions About EPA's Temporary Enforcement Discretion Policy for**



## **COVID-19**

### **Hunton Andrews Kurth LLP**

Commentary regarding the US Environmental Protection Agency's (EPA) Office of Enforcement and Compliance Assurance (OECA) memorandum articulating a...

---

### **EPA Guidance Concludes COVID-19 Can Constitute Force Majeure Event for Parties Performing CERCLA/RCRA Remediation**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The U.S. Environmental Protection Agency (EPA), in response to the COVID-19 pandemic, has announced Interim Guidance for the...

---

### **USEPA Releases Draft Guidance which would allow additional construction activities in advance of obtaining a pre-construction permit**

#### **Vorys Sater Seymour and Pease LLP**

On March 25, 2020, USEPA released draft guidance regarding its interpretation of "begin actual construction" under the regulations implementing the...

---

### **EPA Highlights Enforcement Against Disinfectant Products Making Fraudulent Coronavirus Claims**

#### **Beveridge & Diamond PC**

What Happened: On an April 3, 2020 call with retailers and marketplace platforms, EPA identified enforcement against sales of...

---

### **Update: How "Stay at Home" Orders are Impacting the Waste Industry Across the Country**

#### **Freeborn & Peters**

In a matter of days, Americans have been asked to stay home as states across the country issue orders requiring non-essential businesses to cease...

---

### **The RESPONSE: Federal and State Actions Affecting the Financial Services Industry - Edition 4**

#### **Holland & Knight LLP**

Like our clients, Holland & Knight's Financial Services Industry Group is committed to actively contributing to our nation's response to the...

---

### **EPA Letter to Congress "Correct[s] the Record on the Temporary Enforcement Policy"**

#### **Bergeson & Campbell PC**

The U.S. Environmental Protection Agency (EPA) announced on April 2, 2020, that it sent a letter to all members of Congress to correct the record on...

---

### **New York Approves \$3 Billion 2020 Conservation Bond Act**

New York

#### **Beveridge & Diamond PC**

The New York State Legislature passed Governor Cuomo's Restore Mother Nature Bond Act on April 1st as part of the state's 2020-2021 budget. The Act...

---

## **Environmental Cleanup During A Pandemic - Q&A Summary of EPA's Guidance Crowell & Moring LLP**

On April 10, 2020, EPA released an interim guidance document on response field activities under CERCLA, RCRA, and other EPA response programs during...

---

## **EPA Issues Interim Guidance for Remedial Field Work During the COVID-19 Pandemic**

### **Lowenstein Sandler LLP**

On April 10, the U.S. Environmental Protection Agency (EPA) issued interim guidance to determine when, and how, to suspend field work under certain...

---

## **Environmental Professional Work in the D.C. Metro Area During the COVID-19 Pandemic**

[District of Columbia](#)

### **Holland & Knight LLP**

All jurisdictions in the D.C. Metro Area are currently subject to Orders prohibiting business activities that are not deemed essential. Neither...

---

## **Environmental Protection Agency Issues Temporary Enforcement Discretion Policy in Response to COVID-19**

### **Gordon Rees Scully Mansukhani**

The U.S. Environmental Protection Agency's ("EPA") response to the COVID-19 pandemic includes a temporary policy of enforcement discretion relative...

---

## **Amid COVID-19 Pandemic, NJDEP Publishes Key Remediation Standard Proposal**

[New Jersey](#)

### **Lowenstein Sandler LLP**

On April 6, 2020, the New Jersey Department of Environmental Protection (NJDEP) published to the New Jersey Register, 52 N.J.R. 566(a), a rule...

---

## **New U.S. EPA Guidance for Site Field Work Decisions Impacted by COVID-19**

### **Vorys Sater Seymour and Pease LLP**

On April 10th, U.S. EPA published an interim guidance memorandum titled "Site Field Work Decisions Due to Impacts of COVID-19" (Field Work...

---

## **EPA Issues Interim Guidance on Site Field Work Decisions Due to Impacts of COVID-19**

### **Nelson Mullins Riley & Scarborough LLP**

General Instructions On April 10, EPA issued an interim guidance memo ("Interim Guidance") to all EPA Regional Administrators aimed at addressing how...

---

## **EPA Inspector General Finds Declining Enforcement and Compliance Resources and Outcomes**

### **Greenberg Traurig LLP**

An EPA Inspector General (IG) report issued on March 31 found that agency enforcement and compliance activity and resources have generally declined -...

---

## **Beware of Dirty Dirt: New Jersey Enacts Stringent Licensing Requirements for**



**Soil and Recycle Fill Providers; Providers of Soil and Fill Recycling Services Must Register with the DEP by April 20, 2020 for a Temporary License**

**Greenbaum, Rowe, Smith & Davis LLP**

Nearly a decade has passed since the New Jersey State Commission of Investigation (SCI) first reported on soil and fill providers circumventing New...

---

**D.C.'s Department of Energy & Environment Proposes Major Changes to Flood Hazard Regulations**

[District of Columbia](#)

**Holland & Knight LLP**

The Department of Energy & Environment (DOEE) in Washington, D.C., has announced its intent to propose significant changes to its flood hazard...

---

**EPA and NHTSA Finalize Rollback of Vehicle Fuel Economy and GHG Standards**

**Beveridge & Diamond PC**

Regulatory Action: Vehicle fuel economy and greenhouse gas emissions standards will increase in stringency by 1.5 percent per year from...

---

**Retailers Working with EPA to Protect Consumers from Fraudulent COVID-19 Disinfectant Claims**

**Hunton Andrews Kurth LLP**

On April 3, 2020, the United States Environmental Protection Agency (EPA) and leading retailers participated in a conference call to discuss ways to...

---

**COVID-19 in Australia and US: A tale of two environmental regulators**

**Clyde & Co LLP**

The United States Environmental Protection Agency (US EPA) caused a wave a controversy when it announced in February 2020 suspension of some...

---

**NGOs Petition U.S. EPA for "Emergency Rule" to Require Disclosure of Environmental Noncompliance Due to COVID-19**

**Goldberg Segalla LLP**

On April 1, a group of twenty-one organizations sent a petition to the U.S. Environmental Protection Agency seeking accountability for companies that...

---

**EPA Releases Interim Guidance for Cleanup and Emergency Response Actions During COVID-19**

**Winston & Strawn LLP**

On April 10, 2020, the Assistant Administrators of the U.S. Environmental Protection Agency's (EPA or Agency) Office of Land and Emergency Management...

---

**EPA's COVID-19 Guidance for Superfund and RCRA Operations Expected Soon**

**Taft Stettinius & Hollister LLP**

Property owners conducting Superfund or Resource Conservation and Recovery Act (RCRA) clean-up operations are waiting to hear how the U.S...

---

**Eroding Investor Protections: Managing CSR and Political Risk in the**

## **Sustainable Brave New World**

### **Hunton Andrews Kurth LLP**

Facing growing criticism that they impede sustainable development goals, investment protections afforded by traditional international investment...

---

## **EPA Issues Guidance for Cleanup and Emergency Response Field Work During COVID-19 Pandemic**

### **Brownstein Hyatt Farber Schreck LLP**

As a follow-up to our recent alert regarding the U.S. Environmental Protection Agency's (EPA) enforcement discretion memo, last Friday EPA published...

---

## **EPA Issues Guidance on COVID-19 Impacts for Ongoing Cleanups**

### **Jenner & Block LLP**

Building on its March 26, 2020 temporary enforcement policy, on April 10, 2020, the U.S. Environmental Protection Agency ("EPA") issued its interim...

---

## **Will Pipeline Spill Response Plans Require a Biological Opinion or NEPA Review?**

### **Troutman Sanders LLP**

On April 9, the United States Court of Appeals for the Sixth Circuit heard arguments in *National Wildlife Federation v. Secretary of the Department of...*

---

## **EPA Leaves COVID-19 Decision-Making for On-Site Cleanup Work to Regional Offices**

### **Sidley Austin LLP**

On April 10, the U.S. Environmental Protection Agency (EPA) released guidance to its regional offices regarding how on-site cleanup work may be...

---

## **Montana District Court Interprets Local Controversy Exception to Class Action Fairness Act** [Montana](#)

### **Goldberg Segalla LLP**

Plaintiff Korey L. Aarstad, along with 191 other plaintiffs moved to remand their case back to state court in Montana on the basis that the case had...

---

## **Proactively Adopting a Poison Pill in Response to the COVID-19 Crisis**

### **Latham & Watkins LLP**

Tailored considerations for boards of directors and management in the current environment...

---

## **Real Estate Developers Grapple with CEQA's Vehicle Miles Traveled Metric for Measuring Transportation Impacts** [California](#)

### **K&L Gates**

The metric by which transportation impacts are analyzed under the California Environmental Quality Act ("CEQA") has changed, and real estate...

---

## **EPA Issues COVID-19 Enforcement Discretion Policy**

### **Robinson & Cole LLP**



Having been "inundated with questions from both state regulators and the regulated community about how to handle the current extraordinary situation...

---

### **New York Significantly Overhauls Siting Process to Boost Renewable Energy Development**

New York

#### **Holland & Knight LLP**

New York's recently passed 2020-2021 budget contains a significant overhaul to the siting process for large-scale renewable energy projects, including...

---

### **EPA Takes Steps to Address Site Cleanup and Enforcement Matters During COVID-19 Pandemic**

#### **McCarter & English LLP**

On Friday, April 10, 2020, the U.S. Environmental Protection Agency (EPA) issued guidance regarding the impact of the COVID-19 pandemic on site...

---

### **Nationwide Permit 12 (NWP 12) Vacated on ESA Grounds**

#### **Nossaman LLP**

On April 15, 2020, the U.S. District Court for the District of Montana issued an order that could impact energy and development projects across the...

---

### **California Rules of Court Amendments Lead to Requests for Clarification Regarding CEQA Lawsuits**

California

#### **Holland & Knight LLP**

In response to the COVID-19 pandemic, the California Judicial Council on April 6, 2020, introduced amendments to the California Rules of Court, which...

---

### **NJ Appellate Court Affirms Dismissal of State's Trespass Claim in NRD Lawsuit**

New Jersey

#### **Manko Gold Katcher & Fox**

On April 7, 2020, the Appellate Division of the New Jersey Superior Court rendered its decision in New Jersey Department of Environmental Protection...

---

### **To Sample Or Not: EPA Issues Interim Guidance on Site Field Work During the COVID-19 Pandemic**

#### **Holland & Knight LLP**

On April 10, 2020, the U.S. Environmental Protection Agency (EPA) issued Interim Guidance on Site Field Work Decisions Due to Impacts of the COVID-19...

---

### **EPA Enforcement Discretion and COVID-19**

#### **Reed Smith LLP**

The Environmental Protection Agency has announced an unprecedented level of enforcement discretion related to environmental obligations and...

---

### **COVID-19 and Environmental Remediation: Guidance and Practical Tips on Whether Remediation is "Essential"**

#### **Riker Danzig Scherer Hyland & Perretti LLP**

New Jersey and many other states continue to issue directives outlining which businesses may continue to operate during the COVID-19 pandemic. The...

---

**Manufacturer Alert - The Environmental Impact of a Suspension or Shut Down in Operations**

**Vedder Price PC**

If you are operating in a state where your governor has issued a stay at home order (NY, NJ, CT, CA, PA, IL, OH, MI, LA, DE, KY, WI)<sup>1</sup> and you have...

---

**COVID-19 Implications for the U.S. EPA's Enforcement and Compliance Assurance Program**

**Vedder Price PC**

On Thursday, March 26, 2020, the United States Environmental Protection Agency (U.S. EPA) announced an Enforcement Discretion Policy for the COVID-19...

---

**EPA Inspector General sends message to EPA: Communities must have better access to health risk information**

**Thompson Coburn LLP**

On March 31, 2020, the United States Environmental Protection Agency, Office of the Inspector General (OIG) released a report addressing community...

---

**EPA Issues Interim Guidance for Site Field Work Decisions Due to the COVID-19 Pandemic**

**Phillips Lytle LLP**

On April 10, 2020, the United States Environmental Protection Agency (EPA) issued its anticipated Interim Guidance (Guidance) to regional offices on...

---

**EPA Issues Guidance for On-Site Cleanup Activity Suspension, Reduction or Continuation in Response to COVID-19**

**Troutman Sanders LLP**

On April 10, the U.S. Environmental Protection Agency's (EPA's) Office of Land and Emergency Management (OLEM) and Office of Enforcement and...

---

**U.S. Environmental Protection Agency Creates New Code for NetDMR Reporting**

**Holland & Knight LLP**

On March 31, David A. Hindin, the director of the U.S. Environmental Protection Agency (EPA) Office of Enforcement and Compliance Assurance, issued a...

---

**US EPA's COVID-19 Interim Guidance on Site Field Work Decisions**

**Sheppard Mullin Richter & Hampton LLP**

On April 10, 2020, the U.S. Environmental Protection Agency (EPA) issued Interim Guidance regarding EPA decision-making with respect to the potential...

---

**EPA Cleanup Site Guidance Recognizes COVID-19 Challenges for Response Activities**

**Hunton Andrews Kurth LLP**



Today, April 10, 2020, the U.S. Environmental Protection Agency (EPA) issued its anticipated Interim Guidance on impacts to operations at cleanup...

---

### **"Recycling Victoria: A New Economy" and The Future of Waste to Energy**

#### **DLA Piper**

The Victorian Government recently released Recycling Victoria, a circular economy policy and 10 year action plan. The policy and action plan...

---

### **The Phase I Environmental Site Assessment: Unexpected COVID-19 Victim?**

#### **Akin Gump Strauss Hauer & Feld LLP**

The COVID-19 crisis has left consultants, lenders, servicers, investors and other users struggling to assess environmental conditions of...

---

### **Covid-19 & international investment protection**

#### **Shearman & Sterling LLP**

Governments around the world will adopt profound and unprecedented measures to tackle the COVID-19 pandemic crisis and keep their economies afloat...

---

### **National Academies Publish Quadrennial Review of NNI**

#### **Bergeson & Campbell PC**

The National Academies of Sciences, Engineering, and Medicine (National Academies) have published a prepublication copy of A Quadrennial Review of the...

---

### **COVID-19 Policy Update- April 8, 2020**

Wisconsin

#### **Akin Gump Strauss Hauer & Feld LLP**

Congress, Administration Call for Additional Emergency Coronavirus Relief - Differences Remain...

---

## **Internet & Social Media**



---

### **The Children's Online Privacy Protection Act and Online Learning**

#### **Cozen O'Connor**

With schools across the nation closing their physical locations and moving to an online learning environment, it is important for school officials to...

---

### **FTC Sends Warning Letters to VOIP Companies Over COVID-19 Robocalls**

#### **Reed Smith LLP**

The Federal Trade Commission ("FTC") issued warning letters to nine Voice over Internet Protocol ("VoIP") service providers to warn them that...

---

### **Focus on Children's Privacy Intensifies as Daily Life Moves Online**

#### **Baker & Hostetler LLP**

With physical schools closed indefinitely, classrooms have moved online, either introducing or significantly expanding children's use of virtual...

---

**If a consumer sends a request for deletion or a request for access via Twitter or**

**other social media, does a business have to respond?**

**Bryan Cave Leighton Paisner LLP**

Yes, if currently pending regulations are made final. As an initial matter, the statutory text of the CCPA is somewhat unclear regarding a business's...

---

**City of LA Email Blunder Exposes COVID-19 Test Results to All Recipients**

California

**Robinson & Cole LLP**

Although email seems to be the preferred method of communication during the coronavirus pandemic, an error made by a City of Los Angeles employee is...

---

**FTC: 2 - OTA: 0**

**Frankfurt Kurnit Klein & Selz PC**

In the latest showdown between the FTC and Online Training Academy ("OTA"), the FTC was again victorious as the Central District Court of California...

---

**A Big Zooming Mess: A Cautionary Tale**

**Frankfurt Kurnit Klein & Selz PC**

Over the last several weeks, while Americans have grown accustomed to working from home, home schooling, and life in lockdown during the COVID-19...

---

**FBI offers new warning, tips for avoiding business email scams**

**Greensfelder, Hemker & Gale, P.C.**

As if life is not difficult enough these days with the impact of the COVID-19 pandemic, this week the FBI issued a warning related to an increase in...

---

**Governor Cuomo's Updated Guidance Clarifies That Notaries Must Execute in Ink**

New York

**Venable LLP**

This article reports on the New York Department of State's Guidance to Notaries Concerning Executive Order 202.7, a revised version of which was...

---

**COVID-19 Exploitations: Malicious Cyber Actors Strike with Pandemic-Related Scams**

**Quarles & Brady LLP**

The U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) shared an alert on April 9, 2020, issued a day earlier by the U.S...

---

**European Court of Justice Holds Amazon Not Liable for Storing Third-Party Sellers' Infringing Products, Another Reason Why Brands Must Take Greater Control In The European Market**

**Vorys Sater Seymour and Pease LLP**

The potential liability of online platforms such as Amazon for third-party content is a hot issue all around the world. The most recent court decision...

---

**Two Emails Don't Always Equal One Contract: Contracts in the World of COVID-**

19 Texas



### **Bradley Arant Boult Cummings LLP**

The coronavirus (COVID-19) has changed many of our personal and professional lives. This includes working from home and increased communication by...

---

### **Is the Platform You're Using a Potential Threat to Protecting Your Trade Secret?**

#### **Crowell & Moring LLP**

The COVID-19 pandemic presents unique and unprecedented challenges to the ongoing need to protect confidential information and trade secrets. With...

---

### **A New Approach to Telecom Regulation in the Times of Covid-19**

#### **Squire Patton Boggs**

As the coronavirus pandemic spreads across the world, forcing people into their homes, electronic communications have played and will continue to play...

---

### **Protecting Your Online Business and Assets in the Age of COVID-19**

#### **Procopio Cory Hargreaves & Savitch LLP**

With COVID-19 prompting stay-at-home orders from state and local officials across the United States, both business owners and consumers are online...

---

### **FCC Waives Gift Rules for Rural Health Care, E-Rate Entities in COVID-19 Response**

#### **Morgan Lewis**

The Federal Communications Commission is easing gift rules for participants in the RHC and E-Rate programs so that broadband providers can help...

---

### **Videoconferencing: Tips for Fund Managers to Navigate Security, Privacy and Compliance Risks**

#### **Schulte Roth & Zabel LLP**

The COVID-19 pandemic has resulted in a dramatic increase in the use of web-based video and audio conferencing ("WC") services by private fund...

---

### **FBI Issues Warning of Increased BEC During COVID-19 Pandemic**

#### **Robinson & Cole LLP**

On April 6, 2020, the Federal Bureau of Investigation (FBI) issued a warning to companies to be aware of an increase in business email compromises...

---

### **US and UK cybersecurity agencies publish a joint statement warning of a rise in Covid-related cybercrime**

#### **Kingsley Napley**

On 8 April 2020, GCHQ's National Cyber Security Centre and the US Department of Homeland Security's Cybersecurity and Infrastructure Agency published...

---

### **What are Interpol Red Notices and how can you challenge them?**

#### **Kingsley Napley**

Over 13,000 Interpol Red Notices were issued last year. Even if a person is not arrested pursuant to a Red Notice, the notice itself will cause...

---

### **Who's Zoomin' Who?**

#### **Womble Bond Dickinson (US) LLP**

The Coronavirus has forced millions of people around the world to work from home, and adapt to a professional and social culture...

---

### **The U.K. and U.S. Security Agencies Issue Joint COVID-19 Cyber Threat Update**

#### **Paul Hastings LLP**

On 8 April 2020, the U.K.'s National Cyber Security Centre ("NCSC") and the U.S. Department of Homeland Security ("DHS") Cybersecurity and...

---

### **Class Actions Follow Universities' Moves to Online Learning**

#### **Ogletree Deakins**

After switching to online learning in response to the COVID-19 pandemic and sending students home, colleges and universities are beginning to face...

---

### **A First Amendment Win for YouTube!**

#### **Saiber LLC**

The January 16, 2019 post - Will Social Media Websites Become State Actors? - wondered how the U.S. Supreme Court would rule in Community Access Corp...

---

### **Zoom, Online Meetings, and Privacy in Today's WFH Environment**

#### **Newmeyer Dillion**

As a result of the COVID-19 (commonly referred to as the Coronavirus) pandemic, remote working arrangements have become the new norm. For those...

---

### **COVID-19: The legislative framework for the security and use of electronic signatures in Singapore**

#### **Duane Morris LLP**

For most of us working from home and actively telecommuting to help stem the tide of local transmissions of COVID-19 during this crucial period of...

---

### **'Wet' Ink Signatures Requirements May Fade After Coronavirus, Says Pera in Bloomberg Law**

#### **Adams and Reese LLP**

The spread of the coronavirus and social distancing are posing challenges to requirements for wet signatures on documents. Even though it may expose...

---

### **Computer Service Providers Face Implied Limits on CDA Immunity**

#### **Morrison & Foerster LLP**

Often lauded as the most important law for online speech, Section 230 of the Communications Decency Act (CDA) does not just protect popular websites...

---

### **Videoconferencing: Tips for Schools to Navigate Security and Privacy Risks**

#### **Schulte Roth & Zabel LLP**

The COVID-19 pandemic has resulted in a dramatic increase in the use of web-based video and audio conferencing ("WC") services by schools, as most...



---

## Episode 310: Is Twitter using the health emergency to settle political scores?

Audio

### **Steptoe & Johnson LLP**

Nate Jones and I dig deep into Twitter's decision to delete Rudy Giuliani's tweet (quoting Charlie Kirk of Turning Point) to the effect that...

---

## **InfoWars takedown over coronavirus misinformation illustrates value of Internet oversight**

### **Thompson Coburn LLP**

Google's recent removal of Alex Jones' InfoWars from its Google Play service, because of false and misleading information it had been transmitting...

---

## **Privacy Tip #234 - Children's Privacy During the Pandemic**

### **Robinson & Cole LLP**

Kids are at home all day now, remote learning and surfing the web more than ever before. Parents are working from home too, and understandably are...

---

## **FTC Settles Alleged Deceptive Privacy and Infosec Practices with Canadian Maker of First Smart Fingerprint Padlock**

### **Troutman Sanders LLP**

On April 6, the Federal Trade Commission announced a settlement with Tapplock, Inc. for falsely claiming in its privacy policy that its...

---

## **What's New in 5G - April 2020**

### **Mintz**

The next-generation of wireless technologies - known as 5G - is here. Not only is it expected to offer network speeds that are up to 100 times faster...

---

## **The FTC's Response to the Coronavirus Pandemic: Consumer Protection Priorities and Initial Actions**

### **Covington & Burling LLP**

The FTC's Response to the Coronavirus Pandemic: Consumer Protection Priorities and Initial Actions April 7, 2020 Advertising and Consumer Protection...

---

## **U.S. and U.K. Agencies Warn of Increased COVID-19 Related Cyber Threats**

### **Pepper Hamilton LLP**

As we reported in March, the COVID-19 pandemic is being leveraged by malicious cyber actors to make various cybersecurity attacks. In a...

---

## **Federal Agencies Warn of COVID-19 Implications for Energy Sector Cybersecurity**

### **Michael Best & Friedrich LLP**

Federal agencies tasked with various aspects of energy regulation are encouraging situational awareness and coordination in light of increasingly...

---

## **Canadian Maker of Smart Locks Settles with FTC Over Deceptive Security Claims**

### **Hunton Andrews Kurth LLP**

A Canadian maker of Internet-connected padlocks, Tapplock, Inc. ("Tapplock"), settled Federal Trade Commission ("FTC") allegations that the company...

### **U.S. and U.K. Agencies Warn of Increased COVID-19 Related Cyber Threats**

#### **Troutman Sanders LLP**

As we reported in March, the COVID-19 pandemic is being leveraged by malicious cyber actors to make various cybersecurity attacks. In a joint alert...

#### **Legal Practice**



### **COVID-19 Response: NY Executive Order Permits Video Execution of Wills and Other Documents**

**New York**

#### **Day Pitney LLP**

On April 7, New York Governor Andrew Cuomo issued Executive Order 202.14, permitting remote witnessing of wills, powers of attorney, health care...

### **North Carolina State and Federal Court Filing Deadline Extensions and Continuances of Proceedings**

#### **Brooks Pierce McLendon Humphrey & Leonard LLP**

As the COVID-19 crisis continues, state and federal courts in North Carolina have extended certain filing deadlines and continued various proceedings...

### **Restatement to the Rescue: 20-Year-Old Treatise May Help Ease Work-at-Home Privilege Problems**

#### **Holland & Knight LLP**

In a time of crisis, thoughtful lawyers look for ways to apply pre-existing authority to evolving situations. Since so many lawyers and clients are...

### **"How the Science of Memory Can Be Used in Fact Witness Questioning"**

#### **Quarles & Brady LLP**

In personal injury and wrongful death litigation, memory plays a central role, forming the foundation on which the "facts" needed to determine...

### **Lawyer's Advocacy in Arbitrations: No. 2 of the Top 10 Horrible, Terrible, No Good Mistakes Lawyers Make**

#### **Bradley Arant Boult Cummings LLP**

David K. Taylor, Bradley Arant Boult Cummings, Nashville, TN  
dtaylor@bradley.com 615-252-2396 This post is a continuation of the Top 10 most horrible...

### **Attorneys are counselors at law**

#### **Stange Law Firm PC**

Attorneys rarely forget that they have a role in serving as a legal advocate for their clients. As legal advocates, lawyers file pleadings, issue and...

### **Better Call Saul: Legal ethics you can use**

**Video**



### **Thompson Hine LLP**

Kim's take on Model Rule 7.1 ("Communications Concerning a Lawyer's Services") and Model Rule 7.3 ("Solicitation of Clients") is timely because we all...

---

### **Voluntary Dismissal With Prejudice Does Not Preclude Attorney's Fees**

#### **Knobbe Martens**

Keith Manufacturing filed a lawsuit against its former employee, Larry Butterfield, relating to a patent Mr. Butterfield had obtained. After...

---

### **Take Care in Settling During a Crisis**

#### **Holland & Hart LLP**

Those of us who work in trial preparation and case assessment are in a remarkable new reality as trials across the country are on indefinite hold...

---

### **More Courts Disagree About Common Interest Doctrine Requirements**

#### **McGuireWoods LLP**

The common interest doctrine can sometimes avoid the normal waiver implications of separately represented clients sharing privileged communications...

---

### **Pennsylvania Superior Court Holds that a Court Cannot Compel Production of Allegedly Privileged Materials for "Attorneys' Eyes Only"**

[Pennsylvania](#)

#### **K&L Gates**

Last week, the Superior Court of Pennsylvania issued a decision that strengthens the work-product and attorney-client privileges in Pennsylvania. In...

---

### **How to Choose the Best Car Wreck Attorney for your Case**

[California](#)

#### **Rosenfeld Injury Lawyers LLC**

Going through a car wreck is difficult enough. Dealing with a lawyer shouldn't be. If you choose to have a lawyer represent you, you'll want somebody...

---

### **Is it really worth it to get a lawyer for a car wreck?**

#### **Rosenfeld Injury Lawyers LLC**

A car wreck happens in a split second, but it can alter your whole life. Unfortunately, there's no reversing an accident. That's why you deserve a...

---

### **COVID-19: The Chief Justice of the Family Court releases guidance for families**

#### **HopgoodGanim**

Last week, the Chief Justice of the Family Court of Australia released a media statement providing general guidance to families and the Australian...

---

### **The Intersection of International Arbitration and Construction Disputes: A Review of the 2019 Queen Mary University of London International Arbitration Survey**

#### **Pepper Hamilton LLP**

Over the past decade, the annual Queen Mary University of London International Arbitration Survey (QMUL Survey) has become an invaluable resource for...

---

## **Cyber Security 101: What Every Defense Lawyer Should Know**

### **Bradley Arant Boult Cummings LLP**

"The Package" The day begins like any other. Your client opens for business at 9:00 a.m. All employees are at their desks as customers begin calling...

---

## **Recovering Attorney's Fees Under Georgia Law Just Got Easier**

Georgia

### **Barnes & Thornburg LLP**

One of the advantages to business litigation in the state of Georgia is the ability for experienced litigators to wield the State's statute for the...

---

## **Prior Work Conflicts in the Age of COVID-19**

### **Goulston & Storrs PC**

It is always the case that lawyers and law firms must stay attuned to the possibility of prior work conflicts: conflicts of interest that arise when...

---

## **Criminal Statutes of Limitations and Speedy Trial Act Considerations During the COVID-19 Pandemic**

### **Covington & Burling LLP**

COVID-19 (hereinafter, "the coronavirus") is causing significant interruptions to the legal system across the United States, with implications for...

---

## **Internal Corporate Investigations May Deserve Work Product Protection If They Differ From The Corporation's Normal Procedures: Part I**

### **McGuireWoods LLP**

The work product doctrine can protect documents primarily motivated by a corporation's involvement in or reasonable anticipation of litigation...

---

## **Projects & Procurement**



## **OFCCP Says AAP Data Safe While the Agency Works Remotely**

### **Jackson Lewis PC**

When federal contractors share sensitive data - including pay data - with the OFCCP, data security is always a concern. Is your data any less secure...

---

## **Utility-Scale Solar Expected to Weather COVID-19 Impacts**

### **McGuireWoods LLP**

Industry observers report 2019 as a record year for utility-scale solar contracts, with the market increase driven by economic competitiveness...

---

## **The Sovereign Acts Doctrine: Understanding COVID-19 Implications For Your Government Contract**

### **Morrison & Foerster LLP**

The COVID-19 pandemic has introduced significant uncertainty for government contractors as agencies prepare for substantial disruptions, including...

---

## **OFCCP Addresses Data Security and FAAP Approvals In Light of the COVID-19**



## **Pandemic**

### **Proskauer Rose LLP**

As we previously reported, OFCCP has already informed contractors that it “remains fully operational during the COVID-19 pandemic” and provided the...

---

## **FEMA Opens a Door and Closes a Window: A Primer on FEMA’s Broad Efforts to Obtain and Retain Medical Supplies to Combat COVID-19**

### **McCarter & English LLP**

Through its website, the Federal Emergency Management Association (“FEMA”) is encouraging the private sector to step up and suppo...

---

## **Another False Start for the Long Awaited Infrastructure Bill**

### **Nossaman LLP**

Last Tuesday, President Donald Trump tweeted his support for a “very big and bold” \$2 trillion infrastructure package to be included in Congress’...

---

## **New Guidelines for New Jersey Construction, Retail, Warehouse and Manufacturing Sectors**

New Jersey

### **Duane Morris LLP**

Per the order, all nonessential construction operations in New Jersey shut down at 8:00 p.m. on April 10, 2020...

---

## **Top Ten Things Government Contractors Should Know Regarding the Coronavirus (as of April 2, 2020)**

### **Morrison & Foerster LLP**

Contractors who are unable to perform or complete work under a contract as a result of the pandemic should be able to get schedule relief and avoid...

---

## **Biopharmaceutical Company Agrees to Pay \$6.5 Million to Resolve False Claims Act Allegations of False Commercial Pricing Disclosures in Government Contracts**

### **Stinson LLP**

On Monday, April 6, the U.S. Department of Justice (DOJ) announced that MiMedx Group Inc. (MiMedx or the company), an advanced wound care and...

---

## **UPDATE: Georgia Governor Issues Executive Order Clarifying Who Has Authority to Stop Construction Projects**

Georgia

### **Smith Currie & Hancock**

On April 2, 2020, Brian Kemp, Governor of Georgia, issued Executive Order 04.02.20.01 stating that “only those officials deputized by the Governor or...

---

## **A Gov’t Contractor’s Guide to Excusable, Compensable Delays**

### **Bradley Arant Boult Cummings LLP**

With the recent and rapid spread of COVID-19 in the U.S., government contractors have already started experiencing contract performance delays...

---

## **COVID-19 and the Construction Industry: Looking Beyond Force Majeure To**

## **Recover Time and Costs For Delay**

### **Troutman Sanders LLP**

Much has been written about whether and how COVID-19 qualifies as a force majeure event, and some additional information can be found here. But...

---

## **General Services Administration Issues Class-Wide Waiver of Trade Agreements Act and Buy American Act for All GSA Contracts and Schedules**

### **McCarter & English LLP**

In a Class Determination and Findings (CD&F) published on April 3, 2020, the GSA's Senior Procurement Executive directed that certain limited...

---

## **March Bid Protest Roundup (Law360 Spotlight)**

### **Morrison & Foerster LLP**

Neither rain nor sleet nor quarantine restrictions stop bid protests or our monthly roundup. Thus far the virus has not resulted in dramatic changes...

---

## **False Claims Act Liability for Lenders Participating in the CARES Act Paycheck Protection Program**

### **Manatt Phelps & Phillips LLP**

Although federal regulators repeatedly have assured banks that they can make Paycheck Protection Program ("PPP") loans without fear of later...

---

## **Proposed Lehigh County, PA Regulation Changes May Restrict GOVT Contract Bidding**

### **Green and Spiegel LLC**

Lehigh County, PA commissioners have introduced a regulation change which, if enacted, would limit which construction companies can bid for government...

---

## **Update: DoD Provides Guidance On Equitable Adjustments to Contract Price for Impacts of COVID-19**

### **Smith Currie & Hancock**

On March 30, 2020, Kim Herrington, Acting Principal Director of Defense Pricing...

---

## **GAO Report Reveals New Insights Into Lobbying Disclosure Act Compliance and Enforcement**

### **Covington & Burling LLP**

The 2020 annual report from the Government Accountability Office ("GAO") provides new details regarding the state of Lobbying Disclosure Act ("LDA")...

---

## **Dealing with COVID-19 in the Construction Industry - An Update**

### **Duane Morris LLP**

On Friday 3 April 2020, to reduce the risk of further local transmission of COVID-19, the Building and Construction Authority (BCA) released an...

---

## **Coronavirus: The Defense Production Act's authorities and limitations in the fight against COVID-19**



### **DLA Piper**

On March 18, 2020, the President issued an Executive Order invoking the Defense Production Act (DPA) to prioritize and allocate health and medical...

---

### **The CARES Act and Risk of FCA Exposure**

#### **Bass, Berry & Sims PLC**

The financial relief programs enacted by the Coronavirus Aid, Relief, and Economic Security (CARES) Act stand ready to provide crucial financial...

---

### **New Jersey Closes all Non-Essential Construction Projects**

New Jersey

#### **Ogletree Deakins**

On April 8, 2020, New Jersey Governor Phil Murphy signed Executive Order No. 122, requiring the closure of all non-essential construction projects...

---

### **DoD Issues Class Commercial Item Determination for Critical Supplies & Services to Aid COVID-19 Response**

#### **Thompson Hine LLP**

The Department of Defense (DoD) issued a Commercial Item Determination (CID) dated March 27, 2020, for essential supplies and services procured in the...

---

### **COVID-19: The Federal Landscape, States' Response and Issues Businesses Are Facing Now**

#### **McGuireWoods Consulting LLC**

In this webinar, hear from MWC professionals on the ground, talking with state and federal leaders and working with businesses on their most pressing...

---

### **An Overview of Recent Land Use Guidance and Legislation in New Jersey in Response to COVID-19**

New Jersey

#### **Greenbaum, Rowe, Smith & Davis LLP**

In the midst of the ongoing COVID-19 public health emergency, New Jersey-based builders, developers, contractors, municipal entities, and other...

---

### **Government Agencies Work to Flatten the Curve by Taking Over Hotels**

#### **Holland & Knight LLP**

While hotels struggle with low occupancy rates and municipalities deal with overcrowding at hospitals with an inverse capacity issue...

---

### **Renewed Importance of False Claims Act Enforcement Under the CARES Act**

#### **Katz Marshall & Banks LLP**

The False Claims Act, 31 U.S.C. § 3729 et seq. ("FCA"), is one of the federal Government's most powerful tools for recovering fraudulently obtained...

---

### **DoD Issues Class Deviation Regarding Implementation of Section 3610 of the CARES Act**

#### **Crowell & Moring LLP**

On April 8, 2020, the Office of the Under Secretary of Defense, Acting Principal Director, Defense Pricing and Contracting (DPC) issued Class...

---

## **San Francisco Bay Area Shelter-In-Place Orders Impact Construction Projects** **Greenberg Traurig LLP**

In response to the Coronavirus Disease 2019 (COVID-19) crisis, California Gov. Newsom issued Executive Order N-33-20, referred to as the Safer at...

---

## **COVID-19: Getting Compensated for Delays and Disruptions**

### **Morrison & Foerster LLP**

Government contractors continue to face disruptions from COVID-19 and the attempts to halt its spread: closures of government and contractor...

---

## **DOD Clarifies Progress Payments Deviation**

### **Morrison & Foerster LLP**

In one of its earliest moves to shore up cash flow for contractors that may be affected by the COVID-19, the DOD issued a deviation on March 20, 2020...

---

## **Federal Government Adopts New Process for States and Tribes to Request Ventilators from the Limited Federal Supply**

### **Seyfarth Shaw LLP**

On April 1, 2020, a FEMA advisory issued that announced a new, more formalized process for distributing the limited available supply of ventilators...

---

## **Meet OFCCP's New Scheduling Letters, Same As The Old Scheduling Letters?**

### **Proskauer Rose LLP**

As faithful readers of this blog know, OFCCP proposed significant changes to its audit scheduling letters in April 2019, and then scaled back those...

---

## **Congress, DoD Encourage Use of Other Transaction Authority in Response to COVID-19**

### **Morrison & Foerster LLP**

Department of Defense ("DoD") acquisition chief Ellen Lord earlier this week issued a memorandum reducing internal approvals required to issue other...

---

## **Limits on a Contractor's Ability to Recover for Unforeseen Risks in the Age of COVID-19**

### **Morrison & Foerster LLP**

Communities across the country and around the world are fighting a war against COVID-19. This is also true - maybe even especially true - for...

---

## **DoD Issues Class Deviation to Address Contractor Reimbursement for Paid Leave Required to Maintain a Mission-Ready Workforce During the COVID-19 Outbreak Pursuant to Section 3610 of the CARES Act**

### **Sheppard Mullin Richter & Hampton LLP**

To further assist the contractor community with the effects of the unprecedented Coronavirus Disease 2019 (COVID-19), the U.S. Department of Defense...

---



### **Mayer Brown**

Nick looks at the Government's Emergency Volunteering Leave Scheme and the responsibilities of employers towards those who wish to volunteer under it...

---

### **Guidance Issued for CARES Act Relief For Contractors**

#### **Morrison & Foerster LLP**

In an earlier post concerning contractor relief under the CARES Act, we noted Section 3610 as one of the provisions most likely to benefit government...

---

### **The Paycheck Protection Program: FOIA and Potential Implications for Applicants and Investors**

#### **Lowenstein Sandler LLP**

The Paycheck Protection Program (PPP) has now seen three days of frenzy over application uncertainties, eligibility questions, and employee count/loan...

---

### **US Supreme Court Declines to Consider DOJ Dismissal Power in FCA Cases**

#### **Morgan Lewis**

In a recent denial of a petition for certiorari, the US Supreme Court declined to resolve the standard courts should use when evaluating government...

---

### **Local Impact of the CARES Act and Potential New Infrastructure Bill**

#### **Bilzin Sumberg**

The Act created \$500 billion in aid for state and local governments, and these funds could directly impact major projects on the horizon in...

---

### **Seven tips for companies or organizations seeking or receiving federal funds to fight COVID-19**

#### **Thompson Coburn LLP**

Entities working with the Federal Government to address the novel coronavirus (COVID-19) may encounter a number of issues in performance of the...

---

### **DOD Issues Class Deviation and Implementation Guidance for CARES Act Section 3610 Authorizing Potential Recovery by Federal Contractors Due to COVID-19**

#### **Seyfarth Shaw LLP**

On April 8, 2020, the Department of Defense ("DOD") issued Class Deviation Number: 2020-00013 authorizing Contracting Officers ("COs") to deviate...

---

### **CMMC in the Age of COVID-19**

#### **Step toe & Johnson LLP**

While attention is necessarily focused on the nation's response to COVID-19, defense contractors should not put aside the need to prepare to meet...

---

### **D.C. Circuit Reverses FERC's Rejection of "Incremental Plus" Rates for Gas Pipeline Expansion Project**

#### **Troutman Sanders LLP**

On April 10, 2020, the United States Court of Appeals for the District of Columbia

Circuit ("D.C. Circuit") granted Gulf South Pipeline Company, LP's...

---

### **Update on N.J. and Pa. Restrictions on Construction Activities — Utility and Other Projects**

New Jersey

#### **Cozen O'Connor**

We earlier reported that while New Jersey's state of emergency order (Executive Order No. 107) did not halt the construction indust...

---

### **New York State Supercharges Clean Energy Development**

New York

#### **Phillips Lytle LLP**

With only 10 years to reach New York State's nation-leading goal of 70 percent renewable electricity by 2030, the State took groundbreaking action to...

---

### **DoD Issues Class Deviation and Guidance to Implement CARES Act Relief for DoD Contractors under Section 3610**

#### **Stinson LLP**

Section 3610 of the CARES Act provides for funding to aid government contractors whose employees or subcontractors "cannot perform work on a site...

---

### **DFARS Final Rule Establishes Goal of 15-Day Accelerated Payments for Small Business Contractors**

#### **McCarter & English LLP**

On April 8, 2020, a final rule (the Rule) was issued amending the Defense Federal Acquisition Regulation Supplement (DFARS) and implementing Section...

---

### **Congressional, Executive, and Legal Developments for Government Contractors to Consider - March 2020**

#### **Venable LLP**

With the COVID-19 pandemic front and center, this month has seen several developments that impact government contractors, including notable...

---

### **Department of Defense Releases Further Guidance for Implementing Section 3610 of the CARES Act**

#### **Holland & Knight LLP**

The U.S. Department of Defense (DoD) has released additional information relative to implementation of Section 3610 of the recently passed Coronavirus...

---

### **Emergency Public Contracting Procedures, Part 3: Other South Florida Jurisdictions**

Florida

#### **Bilzin Sumberg**

As discussed in our previous posts on emergency contracting procedures in Miami-Dade County and the State of Florida, the spread of COVID-19 has...

---

### **Office of Management and Budget Issues COVID-19 Guidance for Contractors**

#### **Holland & Knight LLP**

On March 20, the U.S. Office of Management and Budget (OMB) issued guidance



regarding contractor expectations and performance in the wake of the...

---

### **Force Majeure: COVID-19 Pandemic Issues That Could Impact Electricity Contracts**

#### **Holland & Knight LLP**

As the current health crisis from COVID-19 grows, electricity market participants may benefit from developing strategies to assess their risks and...

---

### **The Case for Adequate Public Transportation Funding during the COVID-19 Pandemic**

#### **Nossaman LLP**

In his Infra Insight Blog of April 9, Frank Liu reported on the uncertain status of the long awaited federal Infrastructure bill. As the federal...

---

### **GSA Leases Under Unusual and Compelling Urgency**

#### **Holland & Knight LLP**

The General Services Administration (GSA) released Lease Acquisition Circular, LAC-2020-01, issuing Leasing Desk Guide, Chapter 23, Lease Acquisitions...

---

### **Ninth Circuit Joins Several Others in Finding that Lack of Medical Necessity Claims Can Proceed Under the False Claims Act**

#### **Mintz**

The Ninth Circuit Court of Appeals recently allowed a False Claims Act (FCA) case based on an alleged lack of medical necessity to proceed, rejecting...

---

### **Ongoing Impacts of the Coronavirus Pandemic on Construction Projects in Major Markets**

#### **Robinson & Cole LLP**

As we began to describe on March 18, the economic impacts of the ongoing coronavirus/COVID-19 pandemic on the construction industry are becoming more...

---

### **CARES Act Benefits are Not Risk-Free: Understanding and Minimizing False Claims Act Liability Under the CARES Act**

#### **Hunton Andrews Kurth LLP**

On March 27, President Donald Trump signed into law the Coronavirus Aid, Relief, and Economic Security Act, also known as the CARES Act, which...

---

### **Unprecedented Discovery Orders Vacated: Fourth Circuit Confirms Government Contractors Do Not Waive Privilege by Disclosing Facts Uncovered during an Internal Investigation under the FAR's Mandatory Disclosure Rule**

#### **Morrison & Foerster LLP**

Lawyers often view a writ of mandamus to a Court of Appeals as a last-gasp—indeed, almost hopeless—stratagem. But sometimes they are granted...

---

### **Insights About False Claim Act Cases and Qui Tams from Joseph “Jody” Hunt and Michael Granston from the U.S. Department of Justice at the Federal Bar**

## **Association's 2020 Qui Tam Conference**

### **Phelps Dunbar LLP**

Two key representatives of the U.S. Department of Justice - Joseph "Jody" Hunt, Assistant Attorney General for Civil Division, and Michael Granston...

---

## **Revised Scheduling Letters released**

### **Constangy Brooks Smith & Prophete LLP**

The Office of Management and Budget has approved the Office of Federal Contract Compliance Programs' request to revise the Scheduling Letters that in...

---

## **Key legal issues for project finance transactions in USA**

### **Debevoise & Plimpton LLP**

This article highlights some of the key legal issues surrounding project finance transactions in USA, including government approvals, financing registration and governing law.

Public



## **Antitrust agencies' COVID-19 response: federal and state authorities warn against price gouging**

### **Norton Rose Fulbright LLP**

In the wake of COVID-19, some sellers of essential goods and services have tried to greatly increase the cost of their products to take advantage of...

---

## **CARES Act Provides Aid and Regulatory Relief to Students and Educational Institutions**

### **Faegre Drinker Biddle & Reath LLP**

On Friday, March 27, 2020, the President signed into law a \$2 trillion stimulus package to combat the coronavirus pandemic and its systemic effects...

---

## **Past as Prologue: The Wave of Investigations to Follow the Pandemic Recovery and Actions that Companies Can Take Now to Prepare**

### **Covington & Burling LLP**

On March 30, 2020, the inspectors general of several major agencies selected the Department of Defense Inspector General, Glenn Fine, to lead a newly...

---

## **Public legislative processes and public meetings during the time of COVID-19**

### **DLA Piper**

All states have open meetings laws that provide for transparency in decision-making by deliberative governmental bodies. In light of public health...

---

## **AGs Target Health Clubs for Charging Fees While Closed**

### **Frankfurt Kurnit Klein & Selz PC**

The Attorneys General of New York, Pennsylvania, and the District of Columbia recently wrote to Town Sports International Holdings -- the owner of New...

---

## **COVID-19: Getting your cross-border deal done and documents notarized and**



## **legalized in the age of coronavirus (United States)**

### **DLA Piper**

Under normal circumstances, executing corporate documents for purposes of implementing international corporate transactions is not an overly...

---

## **Florida Governor Issues Stay-at-Home Order, Designates Essential Services During COVID-19 Pandemic**

Florida

### **Day Pitney LLP**

On April 1, Florida Governor Ron DeSantis signed Executive Order Number 20-91 (EO 20-91), which became effective at 12:01 a.m. On April 3 and...

---

## **Lamont Executive Order Grants Partial Immunity to Health Care Providers Responding to COVID-19**

### **Day Pitney LLP**

On April 5, Connecticut's Governor Ned Lamont issued Executive Order No. 7U (Order) providing healthcare professionals and healthcare facilities with...

---

## **Gov. Kemp issues "Shelter in Place" Executive Order for Georgia**

Georgia

### **Constangy Brooks Smith & Prophete LLP**

Gov. Brian Kemp (R) has placed the State of Georgia under a shelter-in-place Executive Order. The order took effect Friday evening and is currently...

---

## **Congress Should Authorize Removal of Counterclaims and Third-Party Claims Pleaded as Class Actions**

### **Bradley Arant Boult Cummings LLP**

For over 240 years, Congress has allowed citizens of different states to litigate in federal court and, for equally as long, has permitted defendants...

---

## **South Carolina Becomes 42nd State to Issue 'Stay at Home' Order**

South Carolina

### **Ogletree Deakins**

On April 6, 2020, South Carolina Governor Henry McMaster issued Executive Order No. 2020-21 (E.O. 2020-21), which implemented a "home or work"...

---

## **White House Establishes Committee on Foreign Participation in U.S. Telecommunications**

### **Cadwalader Wickersham & Taft LLP**

Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (the "Committee")...

---

## **New Jersey Extends State of Emergency for 30 Days**

New Jersey

### **Jackson Lewis PC**

New Jersey Governor Phil Murphy has signed Executive Order 119 (EO), extending the state of emergency due to the COVID-19 crisis, originally...

---

## **Schools Accepting COVID-19 Loans Must Be Aware Of Workplace Law Consequences**

### **Fisher Phillips**

Many independent and private schools are contemplating applying for Paycheck Protection Program (PPP) and/or Economic Injury Disaster (EIDL) loans...

---

## **Intellectual Property and Technology News (North America), Issue 45, Q1 2020**

California

### **DLA Piper**

The world is always changing, sometimes in unforeseeable ways, and we understand that and are working hard...

---

## **No Free Lunch: Additional Regulatory Concerns in Healthcare Relief Funds**

### **Bradley Arant Boult Cummings LLP**

This week the Department of Health and Human Services announced distribution of the first \$30 billion of CARES Act funds for healthcare providers...

---

## **Targeted Options for Increasing Medicaid Payments to Providers During COVID-19 Crisis**

### **Manatt Phelps & Phillips LLP**

The COVID-19 pandemic is causing dramatic changes in utilization that threaten the financial stability of providers and may jeopardize access to care...

---

## **CFIUS During COVID-19 Pandemic**

### **Squire Patton Boggs**

The European Union (EU) recognised the unprecedented situation, which has arisen as a result of the Coronavirus disease 2019 (COVID-19) outbreak and...

---

## **COVID-19: New York Issues Updated Guidance on the definition of “Essential Business” and “Non-Essential Business” - Executive Order 202.6**

New York

### **Duane Morris LLP**

On April 9, the Governor issued and updated Executive Order (202.6) to provide further guidance on determining whether a business is “Essential” (and...

---

## **Provisions in Federal COVID-19 Legislation Benefiting Nonprofit Organizations**

### **Squire Patton Boggs**

Provisions in Federal COVID-19 Legislation Benefiting Nonprofit Organizations Congress, so far, has enacted three pieces of legislation designed to...

---

## **California Counties and Cities Begin to Mandate Face Coverings in Further Efforts to Slow the Spread of COVID-19**

California

### **Jackson Lewis PC**

The Center for Disease Control (“CDC”) recently began recommending the use of non-medical masks or “cloth face coverings” to help stem the spread of...

---

## **Indiana Governor Orders Extension of Property Tax Exemption filing deadline from April 1st to June 30th**

Indiana

### **Faegre Drinker Biddle & Reath LLP**

Indiana’s real and personal property tax exemption petitions (Form 136) are normally due on or before April 1st annually. On March 26, 2020, Indiana...



---

## **Governor Baker Extends Order on Non-Essential Business Closure Through May 4, 2020**

### **Nutter McClennen & Fish LLP**

On March 31, 2020, Governor Baker extended his March 23, 2020 order mandating the temporary closure of all “non-essential” workplaces through May 4...

---

## **What You Need to Know: State and Federal Updates Related to COVID-19**

### **Mintz**

As the coronavirus pandemic spreads across the nation, your team at ML Strategies continues to monitor legislative and regulatory updates at the...

---

## **Missouri Enacts Stay-At-Home Order**

Missouri

### **Constangy Brooks Smith & Prophete LLP**

Effective April 6, 2020, Missouri implemented an order directing residents to stay at home to combat the spread of COVID-19. The order instructs...

---

## **Protecting Student Privacy during a Pandemic**

### **Michael Best & Friedrich LLP**

Last week, the U.S. Department of Education (DOE) issued guidance, by way of Frequently Asked Questions, about what circumstances are permissible for...

---

## **Client Alert: Congress Passes Phase 3 of Coronavirus Response**

### **Baker McKenzie**

Congress Passes Phase 3 of Coronavirus Response Earlier this week, the Senate passed the nearly \$2 trillion Coronavirus Aid, Relief, and Economic...

---

## **Seattle Mayor's Office Proposes Emergency Action to Keep City's Land Use Process Moving During COVID-19 Slowdown**

### **Foster Garvey**

In an effort to keep Master Use Permit applications moving through the review process during the COVID-19 emergency, on April 2, Seattle Mayor Jenny...

---

## **New York State Legislature Grants Unprecedented Powers to Executive to Maintain Balanced Budget**

New York

### **Greenberg Traurig LLP**

Given the state of uncertainty resulting from the Coronavirus Disease 2019 (COVID-19) pandemic, the recently enacted 2020-21 New York State Budget...

---

## **Governor Newsom Suspends Some Brown Act Requirements in Light of COVID-19 Public Health Crisis**

### **Holland & Knight LLP**

In an effort to implement public health officials' recommendations to slow the spread of the coronavirus (COVID-19), California Gov. Gavin Newsom...

---

## **U.S. Department of Education Q&A on Use of Federal Grant Funds During**

## **COVID-19**

### **Duane Morris LLP**

On April 8, 2020, the U.S. Department of Education published a Q&A that answers questions related to use of Department grant funds during the novel...

---

## **CA Legislature to Reopen Capitol for Oversight Hearings**

California

### **Manatt Phelps & Phillips LLP**

In response to the growing spread of COVID-19, California Senate President Pro Tempore Toni G. Atkins (D-San Diego) and Assembly Speaker Anthony...

---

## **COVID-19: Kentucky Passes HB 150**

### **Graydon Head & Ritchey LLP**

Last week the Kentucky legislature passed HB 150 which, in addition to codifying many of Governor Beshear's executive actions, includes a number of...

---

## **Even Golf, the "Sport of Social Distancers," Has Been Affected by the Coronavirus**

### **Holland & Knight LLP**

Last weekend, President Donald Trump extended "social distancing" guidelines related to the COVID-19 pandemic until April 30, 2020. While some critics...

---

## **May 4, 2020 Deadline for Public Comment on Important Distance Education Rulemaking**

### **Duane Morris LLP**

On April 1, the U.S. Department of Education ("USDE") published a long-awaited Notice of Proposed Rulemaking (NPRM) for Distance Education and...

---

## **Can He Do That? The Governor's Authority to Suspend or Modify Statutes in an Emergency Like the Covid-19 Pandemic**

### **Day Pitney LLP**

Like many Governors, Connecticut Governor Ned Lamont has responded to the COVID-19 pandemic with a series of Executive Orders implementing a variety...

---

## **Key Takeaways for Indian Country From the Coronavirus Relief Package**

### **Faegre Drinker Biddle & Reath LLP**

On March 25, 2020, the Senate passed the Coronavirus Aid, Relief, and Economic Security Act, which the House passed and President Trump signed into...

---

## **CARES Act Expands Rules Related to Cost-Free Coverage of COVID-19 Testing**

### **Day Pitney LLP**

On March 27, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) was passed by Congress and signed by President Donald Trump. The...

---

## **Governor J. B. Pritzker Signs Executive Order Approving Remote Notarization in Illinois**

Illinois

### **Masuda Funai Eifert & Mitchell Ltd**



Governor J. B. Pritzker, through COVID-19 Executive Order No. 14 signed March 26, 2020, has approved Remote Notarization in Illinois for as long as...

---

**William Kishman Discusses Legality of Large-scale Lockdown and Quarantine in Wake of Coronavirus Disease 2019 (COVID-19)** [Video](#)

**Squire Patton Boggs**

Labor & Employment partner William Kishman appeared on Fox News Channel's March 11, 2020, edition of "The Ingraham Angle" to discuss the legal...

---

**Funding opportunities and changed requirements for education institutions in the CARES act**

**DLA Piper**

On March 25, the US Senate passed Phase 3 of the monumental coronavirus disease 2019 (COVID-19) economic rescue package, the Coronavirus Aid, Relief...

---

**New York State Issues Updated Guidance on Essential (And Non-Essential) Businesses** [New York](#)

**Proskauer Rose LLP**

On April 9, 2020, Empire State Development ("ESD") released updated guidance for determining whether a business or service is "essential" under...

---

**U.S. Department of Education Delivering \$6 Billion in Student Emergency Grants via Institutions**

**Duane Morris LLP**

On April 9, 2020, the Secretary of Education announced the availability of more than \$6 billion for immediate distributed to colleges and...

---

**COVID-19: Washington State Institutes Statewide "Stay Home - Stay Healthy" Order to Combat COVID-19** [Washington](#)

**K&L Gates**

The State of Washington has ordered its residents to stay home until midnight on April 6, 2020, in a strong effort to stem the spread of COVID-19. On...

---

**Appellate Litigation in the Age of COVID-19**

**Paul Weiss**

The United States Supreme Court and other federal and state appellate courts are adjusting their practices in response to the COVID-19 pandemic...

---

**Lighthouse - March 2020 | US edition**

**Morrow Sodali**

Shareholder proposals for the 2020 proxy season will cover many familiar topics, including independent board and committee Chairs, the right of...

---

**DOJ Ramps Up Enforcement of Coronavirus Scams**

**Frankfurt Kurnit Klein & Selz PC**

In recent weeks, regulators such as the FDA, the FTC and the New York Attorney

General have started to crack down on possible illegal or fraudulent...

---

### **Managing COVID-19 Disruption: ED Updates and Consolidates Guidance**

#### **Cooley LLP**

On April 3, the US Department of Education released additional guidance for institutions responding to the COVID-19 pandemic. The guidance provides...

---

### **What are the requirements for remote notarization in Missouri?**

Missouri

#### **Greensfelder, Hemker & Gale, P.C.**

Due to the outbreak of COVID-19, many Missourians are finding it difficult to carry on a modicum of "business as usual." One of the many difficulties...

---

### **Banking litigation in the next decade: A look ahead**

#### **Linklaters LLP**

Change and uncertainty have always fuelled litigation. Altered conditions can show agreed contractual terms as not being up to their intended task...

---

### **Who's in Charge? Making Sense of Government Orders in the COVID-19 Response**

New York

#### **Faegre Drinker Biddle & Reath LLP**

All levels of government are issuing declarations, orders, and guidance directing individuals and businesses to socially distance, isolate, and...

---

### **Conducting Public Meetings During the COVID-19 Pandemic**

Tennessee

#### **Bradley Arant Boult Cummings LLP**

On March 30th and April 2nd, Tennessee Gov. Bill Lee issued Executive Orders No. 22 and No. 23, respectively, which instituted a statewide Safer at...

---

### **COVID-19 Impact on Florida Real Estate - Suspending Foreclosures and Residential Evictions for 45 Days**

Florida

#### **Day Pitney LLP**

State mandated closures and other governmental regulations issued to mitigate the spread of COVID-19 are drastically impacting the real estate world...

---

### **Georgia Issues Shelter In Place Order**

Georgia

#### **Greenberg Traurig LLP**

On April 2, 2020, Georgia Governor Brian Kemp issued Executive Order, 04-02-20.01, requiring all residents and visitors to the State of Georgia to...

---

### **Wisconsin Issues Emergency Order Temporarily Banning Evictions and Stalling Foreclosure Actions on Commercial and Residential Properties in Wisconsin**

Wisconsin

#### **Michael Best & Friedrich LLP**

Pursuant to Emergency Order No. 15 issued by Governor Tony Evers and Secretary of Wisconsin Department of Health Services Andrea Palm on March 27...

---



## **US DOE Invites States to Submit Fiscal Spending Waiver Requests Under CARES Act**

### **Nelson Mullins Riley & Scarborough LLP**

The first round of flexibility waivers under the CARES Act has begun. On Friday, April 3, 2020, the US DOE sent a letter to all State DOE Chief School...

---

## **California's Crackdown on the Price Gouging Gold Rush** California

### **Proskauer Rose LLP**

In early March, California Attorney General Xavier Becerra issued a consumer alert on price gouging. Two weeks later, police in San Diego arrested...

---

## **COVID-19: Federal Election Commission Makes Adjustments to Operations Amid COVID-19 Mitigation Measures**

### **K&L Gates**

Like many other government agencies, those responsible for implementing state and federal campaign finance disclosure requirements are adjusting...

---

## **CARES Act Provides Economic Relief for State and Local Governments**

### **Haynsworth Sinkler Boyd PA**

The Coronavirus (COVID-19) pandemic has significantly impacted state and local governments across the United States. The additional service demands...

---

## **Kentucky Attorney General weighs in on Open Meetings Act video conferencing requirements** Kentucky

### **Graydon Head & Ritchey LLP**

The COVID-19 pandemic has presented governments throughout the world with unprecedented challenges, sparking a flurry of legislation, Executive...

---

## **Client Alert: Premises Liability in a Pandemic—Be Reasonable and Take Precautions**

### **Brouse McDowell**

Ohio's Stay at Home Order has been amended to extend through May 1, 2020. Now is a good time for businesses to review their safety precautions and...

---

## **COVID-19 Update: FDA Deputy Commissioner Yiannas Issues PSA and FDA Updates COVID-19 Food Safety Guidance**

### **Hogan Lovells**

This memorandum summarizes recent actions the U.S. Food and Drug Administration (FDA) has taken in response to the COVID-19 outbreak. First, FDA...

---

## **SBA Releases Interim Final Rule Implementing Paycheck Protection Program**

### **Kramer Levin Naftalis & Frankel LLP**

On April 2, the Small Business Administration (SBA) issued an interim final rule on the implementation of the Paycheck Protection Program (PPP), which...

---

## **North Carolina Order Places New Social Distancing Restrictions on Retailers**

North Carolina

### **Fox Rothschild LLP**

On April 9, 2020, North Carolina Governor Roy Cooper signed a new Executive Order that implements new requirements for retail establishments that are...

### **Oversight of the CARES Act: Regulatory and Litigation Issues to Consider**

#### **Kramer Levin Naftalis & Frankel LLP**

The Coronavirus Aid, Relief, and Economic Security (CARES) Act was signed into law on March 27 in order to address the economic crisis caused by the...

### **DOJ Signs Off On First COVID-19 Competitor Collaboration**

#### **Robins Kaplan LLP**

On April 4, 2020, the Department of Justice announced its first blessing of a competitor collaboration aimed at fighting the COVID-19 pandemic. On...

### **Department of Education Delivers More Than \$6 Billion in Emergency Grants**

#### **Akerman LLP**

On April 9, 2020, U.S. Secretary of Education Betsy DeVos announced the immediate availability of over \$6 billion in emergency funding to...

### **Providers Gain Substantial Flexibility under New 1135 Waivers**

#### **Manatt Phelps & Phillips LLP**

On March 30, the Centers for Medicare & Medicaid Services (CMS) swept aside dozens of federal healthcare requirements using its emergency waiver...

### **Several U.S. Retailers Forced to Close by Law Enforcement as Non-Essential**

#### **Bryan Cave Leighton Paisner LLP**

Several U.S. retailers that remained open in the face of state and local shutdown orders have now been forced to close by local law enforcement...

### **Emergencies and the Coastal Act**

#### **Nossaman LLP**

In the past, the Coastal Commission has taken a very negative view on any limitations of public beach access. In fact, one can say that the...

### **Executive Order 202.14 Allows Audio-Video Witnessing for Execution of Wills, Trusts, Powers of Attorney, Health Care Proxies, and Appointments of Agent for Disposition of Remains**

#### **Frankfurt Kurnit Klein & Selz PC**

On April 7, 2020, Governor Cuomo issued Executive Order No. 202.14, which allows for audio-video witnessing of Wills, Trusts, Powers of Attorney...

### **North Carolina General Assembly — Coronavirus (COVID-19) Update**

Carolina

#### **McGuireWoods Consulting LLC**

As of Thursday morning, in the state of North Carolina, there were 3,651 confirmed cases of COVID-19, 47,809 tests completed, 391 hospitalizations...



---

**New York budget bill passes legislature****Eversheds Sutherland (US) LLP**

The New York Legislature has approved budget legislation for the Fiscal Year 2021 (the Budget Bill). Consistent with Governor Andrew Cuomo's earlier...

---

**FEMA Restricts Export of PPE in Temporary Final Rule****Hall Render Killian Heath & Lyman PC**

On April 10, 2020, FEMA published a temporary final rule giving the Agency the authority to block the export of critical PPE during the COVID-19...

---

**Senate Majority Leader McConnell Aims for Additional Funding for Paycheck Protection Program by Voice Vote this Thursday****Michael Best & Friedrich LLP**

Senate Majority Leader Mitch McConnell announced today that he hopes to approve further funding for the Paycheck Protection Program (PPP) during this...

---

**Proposed Federal Pandemic Risk Reinsurance Program: What We Know So Far****McDermott Will & Emery**

Development of legislation to establish a Federal Pandemic Risk Reinsurance Program appears to be progressing. It has been reported that a bill could...

---

**New SBA Loan Guidance Issued****Michael Best & Friedrich LLP**

U.S. Treasury Dept just release updated guidance on how \$349b in federal loans for small businesses reeling from the economic fallout of the...

---

**Indiana Governor Extends Stay At Home Order to April 20th: Legal and Real Estate / Appraisal / Title Services should be conducted virtually**[Indiana](#)**Faegre Drinker Biddle & Reath LLP**

Indiana Governor Eric Holcomb has extended the State's Stay at Home Order in Executive Order 20-18 until April 20, 2020. In the Order, the Governor...

---

**CARES Act Includes New Route to Recovery for Contractors Affected By COVID-19****Covington & Burling LLP**

Contractors sidelined by facility closures and stay-at-home orders in the wake of the COVID-19 pandemic may now have a new pathway to recovering idle...

---

**NJ Issues Guidance on Holding Land Use Hearings During COVID-19 Pandemic**[New Jersey](#)**Pepper Hamilton LLP**

April 2, the Division of Local Government Affairs in the New Jersey Department of Community Affairs (DCA) issued an operational...

---

**Resources and Assistance for Institutes of Higher Education under the CARES Act**

### **Steptoe & Johnson LLP**

On March 27, 2020, President Trump signed the “Coronavirus Aid, Relief, and Economic Security Act” (the CARES Act), after the US House of...

---

### **COVID-19 and Public Assistance under the Stafford Act**

#### **Ice Miller LLP**

In March, President Trump declared a national emergency in response to the coronavirus outbreak, or COVID-19, in the United States. Among the many...

---

### **Securing Mechanic’s Liens in Rhode Island During the COVID-19 Crisis** Rhode Island

#### **Pierce Atwood LLP**

The current COVID-19 crisis has complicated all facets of life, including securing mechanic’s liens. Properly notarizing your lien and recording the...

---

### **Higher Education & Immigration: Five Evolving Areas to Watch** Video

#### **Thompson Coburn LLP**

Webinar In 2020, immigration regulation, policy, and practice, are in a state of constant evolution. Institutions of higher education are focused on...

---

### **Don’t Let Your Brand’s Goodwill Fall Victim to COVID-19 Scams**

#### **Fredrikson & Byron PA**

By Courtney A. H. Thompson Consumers rely on the brands they trust to keep their families safe, healthy and happy. However, pandemic profiteers and...

---

### **Ohio’s Amended Stay-at-Home Order** Ohio

#### **Thompson Hine LLP**

On April 2, 2020, Ohio Governor Mike DeWine announced that Ohio Department of Health Director Dr. Amy Acton issued an Amended Stay-at-Home Order...

---

### **Regulators Continue to Modify Lobbying and Campaign Finance Reporting and Enforcement Practices and Requirements**

#### **Venable LLP**

Federal and state regulators continue to modify their lobbying and campaign finance reporting and enforcement practices and requirements in response...

---

### **Oklahoma governor issues stay at home order** Oklahoma

#### **Buckley LLP**

On April 8, the Oklahoma governor issued an Executive Order closing all businesses that are not within a critical infrastructure or considered...

---

### **Sunshine, Electronic Meetings, and H.B. 197**

#### **Graydon Head & Ritchey LLP**

Described as the “Robin Hood of Law” during his years of private practice, attorney and United States Supreme Court Justice Louis Brandeis’s enduring...

---

### **HHS Initiates Initial \$30 Billion Distribution of the \$100 Billion Public Health and**



## **Social Services Emergency Fund**

### **Ropes & Gray LLP**

On April 10, 2020, the Department of Health & Human Services (HHS) announced it would immediately begin to distribute the first \$30 billion of the...

---

## **Compliance Considerations for Companies and Individuals Donating Funds, Goods, or Services to Domestic Government Entities**

### **Covington & Burling LLP**

As the coronavirus pandemic continues across the country, many corporations, organizations, and individuals are looking for ways they can help fight...

---

## **The Special Inspector General for Pandemic Recovery - Crisis Funding Comes with Heightened Investigation Risk**

### **Bass, Berry & Sims PLC**

On March 27, President Trump signed into law the \$2 trillion coronavirus stimulus bill, named the Coronavirus Aid, Relief, and Economic Security Act...

---

## **ED Releases CARES Act Stimulus Funding for Emergency Student Grants, Subject to Institutional Certification**

### **Cooley LLP**

On April 9, the US Department of Education released the Funding Certification and Agreement and expected allocations for institutional funding under...

---

## **Ten Topics for College and University Senior Administrator Teams Navigating COVID-19**

### **Pepper Hamilton LLP**

Last spring, I was in my seventh year as General Counsel and chief of staff at a private university with a close-knit senior leadership...

---

## **Resources and Assistance for Institutions of Higher Education under the CARES Act**

### **Step toe & Johnson LLP**

On March 27, 2020, President Trump signed the "Coronavirus Aid, Relief, and Economic Security Act" (the CARES Act), after the US House of...

---

## **Strings Attached: COVID-19 Funds and the New House Select Committee**

### **Jenner & Block LLP**

Now that Congress has passed, and the President has signed, historic stimulus bills in response to the COVID-19 pandemic, the practical realities of...

---

## **DOJ and FTC Issue Joint Antitrust Statement Regarding Collaboration During COVID-19 Crisis**

### **Dykema Gossett PLLC**

Even though the COVID-19 crisis has shuttered many government and commercial activities, the nation's antitrust regulators are still very much open...

---

## **Legal Alert: New York budget bill passes legislature**

### **Eversheds Sutherland (US) LLP**

The New York Legislature has approved budget legislation for the Fiscal Year 2021 (the Budget Bill). Consistent with Governor Andrew Cuomo's earlier...

---

### **Illinois Food and Beverage COVID-19 Update**

Illinois

#### **Taft Stettinius & Hollister LLP**

Below are important updates covering COVID-19 related information as it pertains to the food and beverage industry...

---

### **Client Alert: Child Support in Times of Uncertainty**

#### **Bowditch & Dewey LLP**

With Governor Baker extending the Stay-at-Home Advisory through May 4, the anxieties and uncertainties people are facing as a result of COVID-19 are...

---

### **Governor Temporarily Suspends Certain FOIA Deadlines**

#### **Foster Swift Collins & Smith PC**

Since the state of emergency was declared, many public bodies have been grappling with how to fulfill Freedom of Information Act ("FOIA") requests...

---

### **The Bay Area Extends Shelter-In-Place Orders, Adding New Obligations For Employers and New Restrictions on Residents**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis. Eight California counties—San Francisco, Alameda, Contra Costa, San Mateo, Santa Clara, Marin, Sonoma, and Santa Cruz—

---

### **New York State Governor Signs Law Protecting Health Care Workers, Facilities and Administrators from COVID-19-Related Liability**

New York

#### **Paul Weiss**

On April 3, New York Governor Andrew Cuomo signed into law an act that immunizes health care facilities and professionals from certain forms of...

---

### **Basics of FEMA Public Assistance Program Funding for the COVID-19 Pandemic**

#### **Manatt Phelps & Phillips LLP**

The coronavirus disease 2019 (COVID-19) pandemic's effects on states and communities have had a significant financial impact on organizations and...

---

### **US Department of Justice Announces That It Will Not Challenge Collaborative Effort to Manufacture and Distribute COVID-19-Related Medical Supplies**

#### **Mayer Brown**

The Antitrust Division of the US Department of Justice has determined in a business review letter that it will not challenge a plan for several...

---

### **Special Otten Johnson Alert: Part 6 - Is Social Distancing the New Urban Sprawl?**

Colorado

#### **Otten Johnson Robinson Neff + Ragonetti PC**

Next in our series of alerts on the COVID-19 crisis and our work comes a look at



housing and, more specifically, what effects we think this pandemic...

---

### **FAQs: The Affiliation Rules' Impact on PPP Loans to Private Equity and Venture Firms**

#### **Baker & Hostetler LLP**

We have been getting tons of questions from our private fund clients about whether they (and their portfolio companies) can access funds through the...

---

### **Special Otten Johnson Alert: Part 7 - What Does the Pandemic Mean for the Retail Apocalypse?** Colorado

#### **Otten Johnson Robinson Neff + Ragonetti PC**

Entering 2020, uncertainty characterized the retail sector due in part to the impact of tariffs on costs and supply chain Reliability. Consumer...

---

### **DOE Releases Guidance for Accessing Higher Education CARES Act Funding** **Nelson Mullins Riley & Scarborough LLP**

On April 9, the Department of Education released highly-anticipated guidance on the process higher education institutions will use to access portions...

---

### **HHS Distributes \$30 Billion from CARES Act Provider Relief Fund**

#### **Winston & Strawn LLP**

On April 10, 2020, the U.S. Department of Health and Human Services ("HHS") announced an immediate infusion of \$30 billion into the health care...

---

### **Today in Washington - April 13, 2020: COVID-19 Updates** Washington

#### **Hall Render Killian Heath & Lyman PC**

The Senate held a proforma session today without taking any action on providing an interim funding bill...

---

### **Understanding COVID-19 Public Assistance Funds**

#### **Faegre Drinker Biddle & Reath LLP**

On March 13, 2020, President Trump declared that the ongoing COVID-19 pandemic warranted an emergency declaration for all states, tribes, territories...

---

### **Federal Student Loans Under the CARES Act: Borrower and Employer Guidance**

#### **Frost Brown Todd LLC**

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act), a sweeping third-wave relief package in response to the COVID-19 pandemic, became...

---

### **Stay Home for Nevada: Nevada Emergency Directive 013 Tightens Sanitization/Social Distancing and Adds Enforcement Teeth** Nevada

#### **Dickinson Wright**

On March 11, 2020, the World Health Organization declared the rapidly spreading coronavirus disease of 2019 (COVID-19 or the "coronavirus") a...

---

### **Relief for Wholesalers and Distributors**

### **McBrayer McGinnis Leslie & Kirkland PLLC**

After a flurry of executive orders and legislative action by Kentucky's Governor and General Assembly to provide relief for hard hit alcohol retailers...

---

### **Nationwide Implications of CDC and NJ Updated Workplace Requirements** New

Jersey

### **Bryan Cave Leighton Paisner LLP**

Recent state and federal developments are a reminder that the COVID-19 landscape is continually changing and demonstrate that businesses must remain...

---

### **Overview of Major COVID-19 Relief Programs Potentially Applicable to Healthcare Providers As of 4.4.20**

### **Holland & Knight LLP**

The APP is an expanded version of the Periodic Interim Payment (PIP) program that has existed for hospitals; this expansion was authorized under the...

---

### **"To Shield Thee From Diseases of the World": The Past, Present, and Possible Future of Immunization Policy**

### **Bradley Arant Boult Cummings LLP**

The World Health Organization named "vaccine hesitancy" as one of the top global health threats in 2019. In the United States, widespread utilization...

---

### **Student and Borrower Relief Under the CARES Act**

### **Cooley LLP**

In addition to providing institutions relief from certain federal student aid requirements, as discussed in our previous post, the CARES Act relaxes...

---

### **U.S. Department of Education Releases Details on CARES Act Emergency Assistance for Higher Education Students**

### **Faegre Drinker Biddle & Reath LLP**

On Thursday, April 9, 2020, the U.S. Department of Education (ED) released details regarding its distribution of approximately \$6 billion in...

---

### **No Delay? What To Expect on CCPA Enforcement Timing**

### **Kelley Drye & Warren LLP**

The CCPA grants the California Attorney General (AG) the authority to enforce the CCPA starting on July 1, 2020. Last month, the AG confirmed no...

---

### **SECURE Notarization Act Would Allow Remote Notarization**

### **Morrison & Foerster LLP**

One of the impediments to conducting "business as usual" while offices have shut down and work has transitioned to a remote environment has been the...

---

### **Focusing on Resilience**

### **Winston & Strawn LLP**

As we begin our fourth week of remote work, the newness has worn off and a



new normal is forming for most of us. A new way of managing work, life...

---

### **Newly Issued Interim Rules Update Paycheck Protection Program Loan Eligibility Considerations**

#### **Morrison & Foerster LLP**

Late Friday evening, the Small Business Administration (SBA) issued an Interim Final Rule on affiliation, which was posted to the U.S. Treasury...

---

### **Summary of Developments in the Student Loan Market in Reaction to the COVID-19 Emergency**

#### **Lowenstein Sandler LLP**

Under the Coronavirus Aid, Relief and Economic Security Act (CARES Act), all principal and interest payments on federally held student loans are...

---

### **COVID-19: Governor Baker Issues Order Closing All "Non-Essential" Businesses Until April 7, 2020**

[Massachusetts](#)

[New York](#)

#### **Robinson & Cole LLP**

In response to the COVID-19 pandemic, as of this writing, a growing number of states, including California, Illinois, Connecticut, New York, New...

---

### **The CARES Act: Guidance For Servicing Federal and Private Student Loans in the U.S. During the COVID-19 Pandemic**

#### **Bryan Cave Leighton Paisner LLP**

The Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136 (the "CARES Act") was signed into law on March 27, 2020. Although much...

---

### **South Carolina Order Suspending Enforcement of Certain PA and APRN Requirements**

[South Carolina](#)

#### **Nelson Mullins Riley & Scarborough LLP**

On April 10, 2020, the Board of Nursing and Board of Medical Examiners issued a joint order significantly loosening the APRN Practice Agreement and PA...

---

### **COVID-19 class actions forecast**

#### **Borden Ladner Gervais LLP**

As the COVID-19 pandemic continues to ripple across the globe, greatly affecting the global economy, proposed class actions relating to the pandemic...

---

### **COVID-19 and Business Interruption Coverage: what's next?**

#### **Baker McKenzie**

What people are learning at an ever-increasing pace is that besides the thousands of victims by Covid-19, the financial consequences of this pandemic...

---

### **Scaling Up in Baltimore: Why a Nonprofit Helped Found a Startup**

[Video](#)

#### **Vinson & Elkins LLP**

The Baltimore-based nonprofit helps connect at-risk students with a group of volunteers that serves as a powerful support...

---

## **Helping At-Risk Students in Baltimore: The Power of Human Connections** Video

### **Vinson & Elkins LLP**

Everyone could use a person to lean on — someone to seek advice from and confide in. But for too many, that human connection is hard to find. That's...

---

## **Some States Relax Regulation of Medical and Recreational Cannabis During COVID-19 Crisis**

### **McGuireWoods LLP**

Amid a sea of regulatory changes occurring in response to the novel coronavirus (COVID-19) pandemic, several states have temporarily suspended...

---

## **Defense Production Act Update: FEMA Exercises Control over PPE Exports**

### **Mayer Brown**

The Federal Emergency Management Agency ("FEMA") has issued a temporary rule that enables FEMA to regulate exports over shipments of certain personal...

---

## **Governor Cuomo Revises E-Signature Executive Order** New York

### **Klein Moynihan Turco LLP**

Previously, we blogged about federal and state e-signature and notarization laws that apply in this time of working remotely from home. On March 31...

---

## **COVID-19: Update to Various State Construction Closure Orders - Continued Shifting Sands as States Refine and Modify Closure Orders and Essential Business Definitions**

### **Duane Morris LLP**

This list is current as of April 14, 2020 (4:00 p.m. EST) and is an Update to an earlier Alert we posted on April 3rd. Please note that these...

---

## **Tennessee Governor Bill Lee Extends Stay-At-Home Order** Tennessee

### **Nelson Mullins Riley & Scarborough LLP**

Governor Bill Lee's Executive Order 27 has extended Tennessee's Stay at Home Order, requiring that all persons in Tennessee stay at home (except for...

---

## **Give Us A Break: Students Filing Tuition Refund Class Actions Against Universities Over COVID-19 Disruptions**

### **Crowell & Moring LLP**

Many colleges and universities have transitioned to on-line courses and have asked students to vacate campus housing, in response to the COVID-19...

---

## **During Mandated Social Distancing, in Louisiana, "The pen [stroked before a Notary and Two Witnesses, still appears to be] Mightier than the Sword"**

Louisiana

### **Breazeale Sachse & Wilson LLP**

A cursory review of the Remote Online Notarization Procedures included in Emergency Proclamation 37-JBE-2020; what they authorize, and more...

---

## **The impact of the COVID-19 crisis and government measures in relation to the**



capacity of parties to perform their contractual obligations - force majeure, revision of contracts for unforeseen circumstances and MAC clauses

**Hogan Lovells**

The crisis linked to the Covid-19 epidemic and the measures taken by governments to limit the propagation of the virus, has resulted in a number of...

---

**Financial Daily Dose 4.14.2020 | Top Story: SoftBank warns of likely \$17 billion loss for its tech-focused Vision Fund**

**Robins Kaplan LLP**

All is not coming up roses for Masayoshi Son and his faltering SoftBank empire, which warned investors on Monday of a coming \$16.7 billion loss to its...

---

**Assessment of CISA "Memorandum on identification of essential critical infrastructure workers during COVID-19 response" guidance version 2.0**

**Hogan Lovells**

The U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) first widely promoted and published its Essential...

---

**Colleges and Universities: What to Know When You Accept and Distribute CARES Act Emergency COVID-19 Funds**

**Jenner & Block LLP**

Colleges and universities adapting to COVID-19 will soon receive billions of dollars authorized by Congress through the CARES Act. Attendant with that...

---

**CARES Act: Business Relief Provisions, State, Local, and Tribal Government and Individual Assistance Breakdown**

**Barnes & Thornburg LLP**

The Coronavirus Aid, Relief and Economic Security Act (CARES Act) is a \$2 trillion stimulus package intended to provide financial aid to businesses...

---

**OCR Guidance on Disability Rights and Distance Learning During the COVID-19 Pandemic**

**Duane Morris LLP**

On April 3, 2020, the Office for Civil Rights continued its guidance on how institutions can implement distance learning while complying with federal...

---

**COVID-19: Providing Disaster Assistance to Students**

**Michael Best & Friedrich LLP**

With educational campuses - including dormitories, school cafeterias, and locations of work study opportunities - closed due to the COVID-19 pandemic...

---

**Agricultural Eligibility under the CARES Act - EIDL and PPP**

**Michael Best & Friedrich LLP**

In the nearly two weeks since President Trump signed the CARES Act, there has been tremendous confusion surrounding the eligibility of agricultural...

---

**Key Provisions in the CARES Act for Higher Education Institutions**

### **Michael Best & Friedrich LLP**

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) provides educational institutions with financial assistance and contains...

---

### **Alaska governor announces temporary suspension of state regulations as part of Covid-19 emergency measures**

Alaska

### **Buckley LLP**

On April 10, Alaska Governor Mike Dunleavy announced a temporary suspension of certain state fees, statutes, and regulations through May 11...

---

### **COVID-19: Federal Government of Mexico Declares State of Emergency and Suspends “Nonessential Activities”**

### **Wilmer Cutler Pickering Hale and Dorr LLP**

On March 30, 2020, the Mexican General Health Council declared a national state of sanitary emergency, caused by force majeure, in response to the...

---

### **Higher Education Relief in the CARES Act**

### **Taft Stettinius & Hollister LLP**

Recently, Congress passed the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) (Pub. L. No. 116-136 (H.R. 748)) in response to the...

---

### **Massachusetts Updates Essential Services List - See What Can Continue and What Must Stop**

Massachusetts

### **Bowditch & Dewey LLP**

Yesterday, on March 31, 2020, Governor Baker issued an order extending the closure of non-essential businesses and organizations for in-person...

---

### **Key Issues for Retailers Navigating Disparate Stay-at-Home Orders and Store Closure Requirements**

### **Akin Gump Strauss Hauer & Feld LLP**

All but a few states are now under some type of stay-at-home order that requires non-essential businesses to close to the public. Retailers...

---

### **New York Lawmakers Forgo Extension of Child Victims Act’s Look-Back Window ... For Now**

New York

### **Goldberg Segalla LLP**

As discussed in our March 31, 2020 alert, recent administrative orders arising from the COVID-19 pandemic, which preclude the initiation of new...

---

### **CARES Act: Treasury Identifies Businesses ‘Critical to Maintaining National Security’**

### **Morgan Lewis**

The US Department of the Treasury on April 10 released updated criteria outlining which businesses are eligible to apply for CARES Act loans out of...

---

### **Collaborative Efforts to Address COVID-19: A Cross-Jurisdictional Antitrust Enforcement Update**



### **Freshfields Bruckhaus Deringer**

The COVID-19 pandemic has threatened not only public health, but also economies around the world. Many companies are exploring ways to cope...

---

### **Texas Governor Announces \$50 Million Loan Program for Texas Small Businesses through Goldman Sachs/LiftFund Partnership**

Texas

#### **Hunton Andrews Kurth LLP**

As discussed in our previous alert on this issue, the CARES Act established a \$349 billion U.S. Small Business Administration (SBA) Paycheck...

---

### **Coronavirus Prompts Temporary Changes to Mississippi's In-Person Notary Requirement**

Mississippi

#### **Phelps Dunbar LLP**

Mississippi is adjusting its notary rules to allow business to happen while at the same time practicing social distancing. On April 7, 2020...

---

### **FAQs Regarding the Paycheck Protection Program**

#### **Riker Danzig Scherer Hyland & Perretti LLP**

On April 6, 2020, the Small Business Administration ("SBA"), in consultation with the Department of the Treasury, released a series of frequently...

---

### **"This lopsided Treaty..." Is the US/UK Extradition Treaty imbalanced?**

#### **6KBW**

Recent high-profile extradition cases have breathed new life into the old question of whether extradition relations between the US and the UK are...

---

### **Council of the District of Columbia Passes Second Coronavirus Relief Emergency Bill**

District of Columbia

#### **Venable LLP**

On March 17, 2020, The Council of the District of Columbia enacted, and the Mayor signed into law, the COVID-19 Response Emergency Amendment Act of...

---

### **Municipal Liquidity Facility**

#### **Holland & Knight LLP**

The MLF, a \$500 billion program, supplants the existing resources for banks on municipal debt that were available through the Money Market Mutual...

---

### **COVID-19 Bulletin: ZOOM Challenges Provide Timely Reminder about Need for Diligence in Managing Privacy and Security and Student Data**

#### **Taft Stettinius & Hollister LLP**

As we discussed before, educational institutions are closing campuses and are meeting legal obligations to educate their students by conducting...

---

### **Contingency Planning for Distressed Institutions of Higher Education**

Video

#### **Thompson Coburn LLP**

As we wrote in a recent blog post, "COVID-19 did not descend upon a higher education community that was in a place of strength and prosperity. Rather...

---

## **COVID-19 Washington Update: April 7, 2020**

### **Kelley Drye & Warren LLP**

Today, Congressional leaders and the Trump administration announced plans to quickly pass legislation to provide additional funding for the Paycheck...

---

## **COVID-19: Massachusetts Extends Non-Essential Business Closures and Gathering Restrictions**

Massachusetts

### **K&L Gates**

On March 31, 2020, Massachusetts Governor Charles D. Baker issued COVID-19 Order No. 21 (the "March 31 Order") extending his original March 23, 2020...

---

## **Michigan Temporarily Embraces 21st Century Virtual Technology Document Signing**

Michigan

### **Dykema Gossett PLLC**

On Wednesday, April 8, 2020, Michigan Governor Gretchen Whitmer issued Executive Order 2020-41 (the "Order"), which relaxes the witness and notary...

---

## **COVID-19: Maine Governor Janet Mills Extends State of Emergency**

Maine

### **Pierce Atwood LLP**

On Tuesday, April 14, 2020, Governor Janet Mills issued a proclamation extending Maine's state of civil emergency through May 15, 2020. The original...

---

## **Financial Daily Dose 4.15.2020 | Top Story: US and Airlines Reach Deal on Industry Bailout**

### **Robins Kaplan LLP**

The White House and the US airline industry have agreed in principle to a \$25 billion bailout after weeks of "haggling" over the terms, including...

---

## **Don't Mess With Texas: Price Gouging in the Lone Star State**

Texas

### **Proskauer Rose LLP**

When it comes to price gouging in the Lone Star State, Attorney General Ken Paxton is sending a message: don't mess with Texas. On March 26, 2020, AG...

---

## **Los Angeles County Provides Grocery, Drug, Food-Delivery Workers Additional Protections During Covid-19 Outbreak**

### **Fox Rothschild LLP**

Following the April 7, 2020 Worker Protection Order issued by Los Angeles Mayor Eric Garcetti, the Los Angeles County Board of Supervisors passed an...

---

## **Proving a Real Signature in a Surreal World: Notarization Concerns in a Pandemic (Part 2)**

### **McGuireWoods LLP**

On April 6, 2020, McGuireWoods issued an alert analyzing issues facing attorneys, clients and Notaries in the execution of documents during a global...

---

## **The CARES Act: Key Funding Provisions for Institutions of Higher Education**



### **Holland & Knight LLP**

The recently enacted Coronavirus Aid, Relief, and Economic Security Act (CARES Act) includes several sources of funds for postsecondary educational...

---

### **Key Considerations for COVID-19 Emergency Triage Policies in Georgia** Georgia

#### **Ropes & Gray LLP**

Ropes & Gray offers immediate practical guidance on how to navigate the legal and ethical issues raised by the need to have a clear plan for...

---

### **Key Considerations for COVID-19 Emergency Triage Policies in Maryland**

Maryland

#### **Ropes & Gray LLP**

Ropes & Gray offers immediate practical guidance on how to navigate the legal and ethical issues raised by the need to have a clear plan for...

---

### **Five Tips for Making Virtual Compliance a Reality**

#### **Brownstein Hyatt Farber Schreck LLP**

The COVID-19 pandemic is impacting every type of organization, from large, multinational corporations to small nonprofits. But just because the old...

---

### **Elder Law Webinar Recording - New Visitation Guidelines and Useful Technology Tips to Minimize the Social Distancing Gap** Video

#### **Riker Danzig Scherer Hyland & Perretti LLP**

As many of you are aware, there are new visitation restrictions in long term care facilities. It is important that you know what the new visitation...

---

### **Unified Patent Court ratification declared unconstitutional by German court**

#### **Womble Bond Dickinson (US) LLP**

Following on from the announcement that the German Federal Constitutional Court (the "FCC") has upheld the complaint that, as it stands, the...

---

### **First Tranche of Payments from the \$100B CARES Funding Relief Being Delivered**

#### **Hall Render Killian Heath & Lyman PC**

HHS announced that it will begin to deliver the initial \$30 billion of the \$100 billion from the CARES Act Provider Relief Funding on April 10...

---

### **New Statement of Changes to Immigration Rules Effective 6 April 2020**

#### **Faegre Drinker Biddle & Reath LLP**

The U.K. Government published a Statement of Changes to the Immigration Rules on 12 March 2020, and this comes into force on 6 April 2020. The main...

---

### **HHS Begins Delivery of Cares Act Provider Relief Funding - What Providers Should Consider**

#### **Crowell & Moring LLP**

The Department of Health and Human Services (HHS) released on Friday the initial terms and conditions related to the distribution of the first...

---

## HHS Sends Out First \$30B of Provider Relief Fund - What Providers Need to Know about the Funds

**Sheppard Mullin Richter & Hampton LLP**

On Friday, April 10, 2020, the Department of Health and Human Services ("HHS") began distributing \$30B of the \$100B appropriated in the Coronavirus...

---

## Jones Day Global Privacy & Cybersecurity Update | Vol. 25 California

**Jones Day**

Jones Day Cybersecurity, Privacy & Data Protection Lawyer Spotlight: Lisa Ropple Cyberattacks remain among the most feared events confronting...

---

## CARES Act Provider Relief Fund

**Taft Stettinius & Hollister LLP**

On April 10, the U.S. Department of Health & Human Services (HHS) announced that it had begun making payments of an initial tranche of funds from the...



## Global

Employment & Labor



## COVID-19: A guide for the TMT sector

**Baker McKenzie**

With the COVID-19 pandemic quickly spreading across the globe and forcing entire countries to shut down all but essential services, businesses in all...

---

## COVID-19 - Guidance for International Employers

**White & Case LLP**

Companies and their workforces are facing extraordinary challenges during the period of disruption caused by COVID-19, and Governments around the...

---

## Coronavirus: Guide for International Employers

**Ius Laboris**

The coronavirus is spreading very fast, so we have been looking at the steps you can take to keep your employees and your business as safe as...

---

## EU governments responding with dynamic measures to support employees and businesses in the face of COVID19

**CMS Legal**

In response to the COVID-19 epidemic currently gripping much of the world, governments - particularly those in Europe - have responded with...

---

## Covid-19 coronavirus and global employment law: key risks you need to be aware of - part 3 Audio

**Allen & Overy LLP**



Allen & Overy's Global Employment team held the third in a series of calls on the major developments of interest when workforce planning in light of...

---

### **COVID-19: Webinar series (Global)**

#### **Herbert Smith Freehills LLP**

The COVID-19 pandemic is creating significant health, social and economic challenges world-wide, forcing governments and businesses to critically...

---

### Internet & Social Media



---

### **The Seoul Protocol: Guidelines for Remote Arbitration Hearings During the COVID-19 Outbreak**

#### **Pepper Hamilton LLP**

As the COVID-19 pandemic continues to upend carefully choreographed arbitration schedules, parties, counsel and arbitrators have expressed interest...

---

### **Coronavirus: Cyber hygiene practices**

#### **DLA Piper**

During a crisis, bad actors often seek to take advantage by exploiting an already stressful and demanding...

---

### **Intellectual Property rights in the platform economy: A chance to rise or fall**

#### **Denemeyer – The IP Group**

"If you're teaching today what you were teaching five years ago, either the field is dead, or you are" (Noam Chomsky). In our speedy and tech-driven...

---

### **How COVID-19 might change our world**

#### **Baker McKenzie**

The COVID-19 situation presents an unprecedented challenge to the global community as we know it, and it is yet to stabilise. Various governments are...

---

### **Deciphering International Telemedicine Regulations**

#### **Hogan Lovells**

As the world responds to COVID-19, physicians and patients increasingly turn to telemedicine solutions as a central facet of health care. The rise of...

---

### **COVID-19 and the international crime threats: INTERPOL's perspective**

#### **Nyman Gibson Miralis**

As the COVID-19 virus spreads around the globe, criminals are looking for ways to exploit the fear and uncertainty surrounding the virus to generate...

---

### Legal Practice



---

### **Estate Planning in a Global Pandemic - Ontario Permits Virtual Witnessing of Wills**

**Ontario**

#### **Sotos LLP**

Pursuant to an emergency order passed by the Lieutenant Governor in Council

on April 7, 2020, the Ontario government will permit legal professionals...

## Projects & Procurement



### Impact of COVID-19 on Public Procurement

#### CMS Legal

The COVID-19 crisis is having a serious impact on the economy and businesses. In these circumstances, public procurement can be of even greater...

### The digital war to COVID-19: possible solutions at the crossroads of competition, privacy and regulatory checkpoints

#### Hogan Lovells

A worldwide race. Researchers and technologists in these days are scrambling to build apps that Alert users when they have come into contact with...

## Public



### Preserve, Protect and Defend: Global Nationalization Risk

#### Baker McKenzie

The extent of governmental involvement in their national economies goes to the very heart of political and economic debates that have raged since...

### COVID-19: Developments in the Caribbean

#### Squire Patton Boggs

As the coronavirus disease 2019 (COVID-19) pandemic continues to impact business globally, Latin America has not been spared. As of the date of this...

### Alcance 74 de la Gaceta 70 del sábado 4 de abril de 2020 publica normas relacionadas al COVID-19

#### Consortium Legal

La declaraci&oslash;n de estado de emergencia a raz&oslash;n de la pandemia del Coronavirus, hace necesario que el Gobierno Central emita normativas...

### Domestic Abuse during Covid-19: Support & Guidance

#### Anthony Gold

Nazia Rashid, senior associate at Anthony Gold speaks about the increase numbers of domestic abuse being reported worldwide and provides some guidance...

### Client Alert: Could the COVID-19 pandemic inspire the development of a United Nations Convention on Pandemic Suppression?

#### Volterra Fietta

The COVID-19 pandemic poses unprecedented global challenges. States have adopted disparate measures in response to the COVID-19 pandemic. These...

### Domestic Abuse during Covid-19: Support & Guidance

#### Anthony Gold



Nazia Rashid, Senior Associate at Anthony Gold speaks about the increase numbers of domestic abuse being reported worldwide and provides some...

---

## **COVID-19: Pressure Points: A Catalyst for Collaboration (Global)**

### **Herbert Smith Freehills LLP**

As COVID-19 infiltrates every aspect of our daily lives and the world races to respond and to address the pandemic, there is a consistent theme which...

## **Other top stories**

### **Global Toolkit: Force Majeure (COVID-19)**

---

### **Update on CARES Act Small Business Loans and Analysis of the Affiliation Rules as Applied to PE Portfolio Companies**

---

### **The Impact of COVID-19 on the California Consumer Privacy Act**

---

### **CDC's Updated Return-To-Work Standards May Be Helpful To Businesses**

---

### **Commercial Leases in the Age of COVID-19 - A Menu of Options for Landlords and Tenants**

---

### **A Crash Course on Unemployment Benefits During the COVID-19 Pandemic**

---

### **Confusion surrounding 2020 deadline for Form 3520**

---

### **Protecting Intellectual Property and Data if Employee Separation is Anticipated**

---

### **New DOL Guidance Clarifies Eligibility for \$600 Payments under CARES Act**

---

### **Williams-Sonoma Reaches \$1M Settlement With FTC**

---

## **International developments**

### **Summary of response to Covid-19 employment issues across Europe**

---

### **The future of commercial real estate after Covid-19**

---

### **South Africa: Coronavirus (COVID-19) TERS: A guide to the updated memorandum of agreement for employers**

---

### **Hogan Lovells Asia Pacific Data Protection and Cyber Security Guide 2020**

---

### **Supreme Court of Canada Bulletin - April 2020**

---

### **COVID-19: What does it mean for the Financial Services Industry?**

---

### **Summary of new and proposed legislation (UK construction focus)**

---

### **Validity of Electronic Signatures | Overview of the E-signatures Regime in Southeast Asia**

---

### **The EDPB gives its view on connected car technology - but will it reach the chequered flag?**

---

### **Foreign investment issues for project companies in India**

---

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law  
[Contact Lexology](#)

[About Lexology](#)



© 2006-2020 Law Business Research



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fggurina@sunnyvale.ca.gov](mailto:fggurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for April 13, 2020  
**Date:** Monday, April 13, 2020 5:03:22 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)



## **Officials must work to release low-risk, non-violent offenders during COVID**

The COVID-19 pandemic is a moment of intense crisis that has impacted everyone across the country in a variety of ways. But one of the more under-reported aspects of how coronavirus is affecting our society is how the lack of social distancing in the criminal justice system can impact public health. While the nation's focus has primarily been on the developments in Washington, officials in Los Angeles County have been mobilizing to meet the moment and help curb the spread of the coronavirus.

[The Hill](#)

## **COVID-19 makes 'strange bedfellows' of LA defenders, DAs**

Nikhil Ramnaney felt Los Angeles courthouses hadn't done enough to protect attorneys and their clients from the spread of the coronavirus. So the self-professed "bleeding-heart" assistant public defender did something unusual - he called up a prosecutor to commiserate. Ramnaney, who serves as the L.A. public defender union's president, found a receptive audience in a lawyer who would normally be an adversary - Michele Hanisee, president of the Association of Deputy District Attorneys.

[Law360](#)

## **Wearing face covers in courthouses is encouraged, presiding judge says**

Judges of the Los Angeles Superior Court and court staff members are encouraged to wear face covers during the present coronavirus epidemic, Presiding Judge Kevin Brazile said yesterday, announcing that masks will be supplied over the next few days. This follows last week's advisory that all persons who are authorized to be in courthouses may adopt "business casual attire," which includes jeans, but excludes tee-shirts and shorts.

[Metropolitan News-Enterprise](#)

## **Judicial council adopts new rules to lower jail population, suspend evictions and foreclosures**

At its meeting today, the Judicial Council approved 11 temporary emergency rules, including setting bail statewide at \$0 for misdemeanors and lower-level felonies to "safely reduce jail populations" and staying eviction and foreclosure proceedings to protect Californians from losing their homes during the COVID-19 pandemic.

[Judicial Branch of California](#)

## **District Attorney Jackie Lacey responds to judicial council's decision to set zero bail amid COVID-19 pandemic**

Los Angeles County District Attorney Jackie Lacey issued the following statement after today's decision by the Judicial Council of California to set zero bail in response to the COVID-19 pandemic: "I applaud the

Chief Justice and the Judicial Council for adopting a statewide zero bail for people charged with most misdemeanors and low-level felonies," District Attorney Lacey said.

[Los Angeles County District Attorney's Office](#)

### **Courts, plagues and politics**

To the conspiracy minded, one might think when it comes to jurisprudence, the coronavirus plague is a scheme thought up by criminal justice reformers to advance their agenda. Consider the movements of late to reduce the number of prisoners and eliminate bail. Because of the coronavirus those things are happening now in California.

[Fox & Hounds](#)

### **US judge won't block gun store closures in Los Angeles**

A federal judge on Monday refused to block Los Angeles officials from shutting down gun stores as nonessential businesses during the coronavirus pandemic. It's at least the second time federal judges in California have declined to intervene in shutdown orders even as similar orders are being challenged nationwide.

[AP](#)

### **U.S. prosecutors resist calls to free inmates as coronavirus spreads**

Five inmates at a federal prison in Oakdale, Louisiana, have died since March 28 after contracting the coronavirus. Harold Lee's family fears he could be next. Lee, who was sentenced in 2018 for a bank fraud conviction, has asked a federal court for release on home confinement. The 59-year-old has hypertension and requires a breathing machine to sleep. Oakdale was the country's first federal prison to report fatalities from COVID-19, the respiratory illness caused by the coronavirus.

[New York Times](#)

### **Trial by video conference? Not yet, but coronavirus forces Bay Area courts to embrace more virtual proceedings**

Jurors can't sit alongside one another. Defendants can't confront their accusers in person. Judges, lawyers, clients and witnesses communicate electronically from a distance. Such is the new reality at courts across California, where the coronavirus pandemic, and its accompanying social distancing mandates, have forced the legal system to innovate and experiment with virtual and remote proceedings to keep cases moving forward.

[San Francisco Chronicle](#)

### **The coronavirus crisis is forcing the US Supreme Court to face its technology problem**

The US Supreme Court is still hard at work making decisions and publishing opinions during the coronavirus crisis, although these efforts now go mostly unnoticed while the people frantically scan the news for

answers to practical and pressing questions about the pandemic. Whether the nation's top jurists miss the attention is unclear because apart from oral arguments there are few opportunities to hear from them.

[Quartz](#)

### **Lawyers seek release of inmates amid contagion: 'prisons are a tinderbox'**

California's overcrowded state prisons are ripe for a devastating coronavirus outbreak, lawyers for inmates told a panel of three judges considering a motion for the emergency release of thousands of medically high-risk prisoners. "The conditions in the prisons are a tinderbox and will remain a tinderbox unless this court acts," said attorney Donald Specter with the Prison Law Office on Thursday.

[Courthouse News Service](#)

### **Judges reject bid to free California prisoners to slow coronavirus behind bars**

The federal three-judge panel that previously set a population cap for the California prison system has rejected an effort by activists to require further inmate releases to slow the spread of the coronavirus behind bars. In an order filed Saturday evening, the judges ruled that they did not have authority to consider the request because the panel had originally been convened to address a different issue: prisoners' lack of access to adequate medical and mental health care.

[San Francisco Chronicle](#)

### **SD presiding judge authorizes release of inmates: Coronavirus**

The presiding judge of the San Diego Superior Court signed orders this week authorizing the sheriff's department to release county jail inmates with under 60 days remaining on their sentences to stem the spread of COVID-19. Presiding Judge Lorna Alksne's order states "There is an immediate and continuing need to protect the health and safety of the jail population and staff by reducing the jail population in order to help prevent the spread of the coronavirus."

[San Diego Patch](#)

### **DA in `self-quarantine,' tests negative for coronavirus**

Los Angeles County District Attorney Jackie Lacey revealed Wednesday that she has tested negative for coronavirus but is in "self-quarantine" after coming in close contact with one of two employees in her office who tested positive. "I am writing this message from self-quarantine after coming in close contact with one of the two employees in my office who tested positive for COVID-19," Lacey wrote in her monthly newsletter.

[My News LA](#)

### **Stay-at-home orders and travel bans spur constitutional fights**

Last week, Kentucky Governor Andy Beshear signed an executive order



that prohibits Kentuckians from crossing state lines, save for a limited number of exceptions, including employment, trips for necessary supplies or to seek medical care. While the Democrat and neighboring Ohio Governor Mike DeWine, a Republican, have been lauded by political allies and opponents alike for their decisive action in response to the Covid-19 outbreak, the interstate travel ban marked a decisive shift in tactics.

[Courthouse News Service](#)

### **ICE evaluating vulnerable detainees for possible release due to virus risk**

Some immigrants held in federal detention facilities could be freed amid the outbreak of Covid-19 in immigration jails across the country as federal officials announced on Tuesday they are "reviewing cases" of people vulnerable to the virus. U.S. Immigration and Customs Enforcement says it has identified 600 "vulnerable" detainees, including people who are over 60 years old and women who are pregnant, that could be released from federal custody.

[Courthouse News Service](#)

### **Coronavirus lawsuits are coming to work, as health and privacy collide**

Can your employer ask if you are sick? And can you be fired if you are? Those questions, fraught in normal times, are coming to the fore as workers and businesses navigate a new environment where a sick colleague isn't just an inconvenience, but a potential threat to the company and the workforce. Federal law prohibits discrimination based on disabilities, and companies have to walk a fine line between protecting worker health and complying with labor laws.

[San Francisco Chronicle](#)

## **Courts & Rulings**

### **Supreme Court backs police in traffic stops**

Police can pull over a car when they know only that its owner's license is invalid, even if they don't know who's behind the wheel, the Supreme Court ruled Monday. The court said in an 8-1 decision that unless there's reason to believe otherwise, it's common sense for an officer to think the car's owner will be driving. "Empirical studies demonstrate what common experience readily reveals: Drivers with revoked licenses frequently continue to drive and therefore to pose safety risks to other motorists and pedestrians," Justice Clarence Thomas wrote for the court.

[AP](#)

### **Court: Undocumented immigrants fighting deportation entitled to hearing after six months in custody**

Undocumented immigrants challenging their deportation orders are entitled to a hearing for possible release on bond after six months in custody, a federal appeals court ruled Tuesday, with an appointee of

President Trump casting the deciding vote. The 2-1 ruling by the Ninth U.S. Circuit Court of Appeals in San Francisco applies to immigrants who have been arrested or turned themselves in after entering the United States and claim they would face persecution or torture in their homeland.

[San Francisco Chronicle](#)

### **Supreme Court hands federal worker major win in age discrimination case**

The U.S. Supreme Court sided with older federal workers on Monday, making it easier for those over 40 to sue for age discrimination. The 8-to-1 ruling rejected a Trump administration position that sought to dramatically limit the legal recourse available to federal workers. Justice Samuel Alito, writing for the majority, noted that federal law "demands that personnel actions be untainted by any consideration of age."

[NPR](#)

### **Why the criminal case against La Luz Del Mundo's leader got dismissed (for now)**

A California appeals court this week dismissed the criminal case against the leader of the Mexico-based religious group known as La Luz Del Mundo, or the Light of the World Church. Naason Joaquin Garcia was arrested in L.A. this past summer and charged with child sexual abuse and human trafficking. After the court determined he was a flight risk, Garcia's been held without bail in a downtown Los Angeles jail cell since.

[LAist](#)

### **Officer's warning that it would 'look worse' if omitted fact came out later was proper**

An admonition by a police officer that it would "look worse later" if a suspect did not presently make a full disclosure in connection with his crime was not coercive, the Ninth U.S. Circuit Court of Appeals has said, affirming the denial of a suppression motion. The ruling came in a memorandum opinion filed Tuesday. In that opinion, a three-judge panel reversed the conviction of Edward Cragg for receipt and distribution of child pornography, holding that the record shows he was not advised of possible penalties for his crime before he waived his right to counsel.

[Metropolitan News-Enterprise](#)

### **Wrongful death suit against San Diego, officers, to proceed**

The Ninth U.S. Circuit Court of Appeals yesterday rebuffed the second bid by the County of San Diego, the county Sheriff's Department, and individual sheriff's deputies to overturn a District Court judge's denial of qualified immunity in connection with the death of a psychotic man who became assaultive and was tasered, hogtied, and struck with a baton. A three-judge panel dismissed an appeal from the partial denial of summary judgment.

[Metropolitan News-Enterprise](#)

## **California appeals court upholds conviction in Samohi grad's murder**

A state appeals court on Wednesday upheld the conviction of a Santa Monica man for shooting to death a Samohi graduate after a brief run-in near a local liquor store. In 2018, a jury found Sherwin Mendoza Espinosa, 43, guilty of second degree murder for the killing of 18-year-old Juan Castillo on February 26, 2017. But Espinosa was acquitted of the more serious charge of first degree murder.

[Santa Monica Lookout](#)

## **Blind man sues LAPD, eight officers for excessive force during 2019 arrest**

The LAPD officer stood over Michael Moore and pressed a white towel against his face while hospital security guards strapped him onto a gurney. Moore, a 62-year-old blind man, began thrashing around. "I can't breathe! I can't breathe! I can't breathe!" he said in a muffled voice. "Take this off my face!" The guards kept working and the officer re-positioned his hands to push them firmly on Moore's face.

[Los Angeles Times](#)

## **C.A. won't disturb order forbidding supplying trial transcript to inmate**

The Sixth District Court of Appeal has rebuffed the writ challenge by a convicted slayer to an order that bars "anyone" from supplying him with a copy of his trial transcript. The petitioner, Juan Manuel Hernandez-Delgado, whose convictions on two counts of first degree murder were affirmed last year, has failed to show that denying him a copy of the transcript constitutes a denial of his right of access to the courts or that he has a property interest in the document, Justice Nathan D. Mihara said in an unpublished opinion filed Monday.

[Metropolitan News-Enterprise](#)

## **CA Appellate Court takes over City of Fullerton's lawsuit against local bloggers**

California's Fourth District Court of Appeal has barred Orange County's Superior Court from issuing any more orders regarding a City of Fullerton's lawsuit against two resident-bloggers while the appellate court considers the case. Joshua Ferguson and David Curlee were sued by the city after the blog, Friends for Fullerton's Future, began publishing secret city hall documents. The order, known as a writ of supersedeas, was issued last Thursday.

[Voice of OC](#)

## **California Supreme Court affirms LA Court decision in capital case**

On April 2, 2020, the Supreme Court of California affirmed the decision of the trial court in the case against James Michael Fayed. The trial court denied his application for a modification to the verdict in this capital

case, and the automatic appeal went to the CA Supreme Court. Fayed was sentenced to death for the murder of his estranged wife, Pamela Fayed, back in 2008.

[The Davis Vanguard](#)

### **Noncommercial use of dead girl's name, likeness not tortious**

Solicitation of funds for the purpose of promoting a cause is not commercial speech, and use of a deceased person's name and likeness in support of that effort does not give to a cause of action under California's Astaire Celebrity Image Protection Act in favor of successors-in-interest to the decedent's personality rights, the Sixth District Court of Appeal held yesterday.

[Metropolitan News-Enterprise](#)

### **Federal judge clears the way for portion of border wall lawsuit to proceed**

President Donald Trump was within his constitutional authority to declare a national emergency at the southern border last year, a federal judge ruled Thursday, but environmental groups can move forward on a central challenge in their lawsuit: whether the president can divert \$3.6 billion in military funds to build a border wall.

[Courthouse News Service](#)

### **Supreme Court upturns constitutional federalism, yet again**

The U.S. Supreme Court's March 23 ruling in *Allen v. Cooper* is its latest in empowering states at the expense of the federal government - in variance with all that our Constitution has to say about the matter. The court found states enjoy sweeping sovereign immunity from suits to enforce federal law, and that the federal government can do precious little about it.

[Bloomberg Law](#)

## **Prosecutors**

### **Additional sex assault charge filed against Harvey Weinstein**

Los Angeles County District Attorney Jackie Lacey announced today that film producer Harvey Weinstein was charged with an additional sexual assault count stemming from an incident that allegedly occurred at a Beverly Hills hotel in May 2010. Case BA483663 was amended to add one felony count of sexual battery by restraint. Weinstein was charged in January with one felony count each of forcible rape, forcible oral copulation, sexual penetration by use of force and sexual battery by restraint.

[Los Angeles County District Attorney's Office](#)

### **Los Angeles prosecutors charge 'non-essential' shops for staying open**

Los Angeles prosecutors hit four shops with criminal charges for refusing to close during the shutdown orders imposed to slow the spread of the



coronavirus, according to a report. The move marks the first time the city has filed charges against stores for violating the "Safer at Home" order requiring "non-essential" businesses to close during the pandemic, according to the Los Angeles Times. The stores - two smoke shops, a shoe store, and a discount electronics shop - were deemed non-essential by the order, the outlet said.

[New York Post](#)

### **LA City Attorney sues company, alleging unauthorized COVID-19 test kits**

The City Attorney's Office is suing a company for allegedly offering at-home test kits for coronavirus that have not been approved by the federal government. The Los Angeles Superior Court lawsuit was filed Friday and names as defendants Yikon Genomics Inc. and its CEO, Brandon Richard Hensinger. The company does business under the name of Yikon Global, the suit states. A representative for Yikon Global could not be immediately reached for comment.

[City News Service](#)

### **Youth baseball coach charged with lewd acts on three boys**

A Rowland Heights man who coached youth baseball is facing charges that he committed lewd acts on three boys, the Los Angeles County District Attorney's Office announced Friday. Carlton Murray Harris Jr., 47, is scheduled to be arraigned April 15 at the Pomona courthouse on one count each of committing a lewd act on a child under 14 and continuous sexual abuse, along with five counts of committing a lewd act on a child 14 or 15, according to Deputy District Attorney Leslie Bouvier.

[City News Service](#)

## **Policy/ Legal Issues**

### **Riverside County Sheriff Chad Bianco warns of taking COVID-19 seriously after losing two deputies on same day to disease**

One day, two dead deputies - victims of an invisible killer that is stalking the globe. In the tight-knit world of law enforcement, the deaths of two Riverside County Sheriff's Department deputies on Thursday, April 2, from complications related to COVID-19, has cut particularly deep. Terrell Young, 52, was a 15-year veteran of the RCSD.

[Behind the Badge](#)

### **Gov. Newsom's dilemma: More prisoner releases needed in coronavirus crisis**

The COVID-19 pandemic has reportedly infected fewer than a dozen men among California's 122,000 state prison inmates. These cases, all in Southern California, represent a remarkably low number, which is bound to grow dramatically very soon, when the prison system begins to do more testing. The former director of the California Department of Corrections and Rehabilitation, Scott Kernan, has called state prison a

"tinderbox of potential infection."

[San Francisco Chronicle](#)

### **Man convicted in Pittsburg cop killing gets slim chance at freedom, wants to be re-sentenced as a juvenile**

A man who is serving a life sentence for his role in the shooting death of a Pittsburg police officer is asking a Contra Costa County court to re-sentence him as a juvenile, a motion that would mean his immediate release if it's granted. Andrew Moffett, 32, was convicted of murdering Officer Larry Lasater and sentenced to life in 2008. He was just four days shy of his 18th birthday in 2005, when he helped plan a store robbery that led to his cohort, Alexander Rashad Hamilton, 33, fatally shooting Lasater while he attempted to arrest the pair.

[Bay Area News Group](#)

### **Crackdowns on lone surfers and paddleboarders threaten to erode respect for law enforcement even further**

I've been a cop for nearly 40 years. For the last 20 of them, I've had the good fortune of being granted the platform, first at National Review Online, later at City Journal, Ricochet, and here at PJ Media, to write on behalf of my fellow police officers when their actions came under what I considered to be unfair criticism. Police work has grown more difficult since I began, all the more so when cops' split-second decisions are scrutinized by an uninformed public after having been mischaracterized in the media, sometimes deliberately.

[PJ Media](#)

### **Probation and parole officers are rethinking their rules as COVID-19 spreads**

In the effort to release people from jails to stem coronavirus outbreaks behind bars, those jailed for probation and parole violations have been an obvious choice. They're locked up not for committing new crimes but for breaking the rules of their supervision, like drinking alcohol, traveling without permission, or missing appointments. In New York alone, Governor Andrew Cuomo last week ordered the release of more than 1,000 such people from jails around the state.

[The Marshall Project](#)

## **Los Angeles County/City**

### **Los Angeles County Sheriff's Department will increase rates costing cities hundreds of thousands**

Hews Media Group Los Cerritos Community News has learned that the Los Angeles County Sheriff's Department will increase rates on all contract cities; the hit to member city budgets will range from \$250,000 to over \$1 million annually. The March 27 letter indicated that the cities will see an increase of 5.57% for services, while increasing the Liability Trust Fund (LTF) by .05% to 11.5%.

[Los Cerritos News](#)

### **L.A. County Supervisors urge Sheriff Villanueva to correct record on coronavirus sick pay**

Los Angeles County Supervisors have sent a scathing letter to Sheriff Alex Villanueva, imploring him to correct the record after they said he falsely accused the county's chief executive of withholding pay from deputies he ordered to quarantine due to exposure to the coronavirus. "Your unfortunate and erroneous comments have been sowing confusion and controversy by raising doubts about pay for deputies you chose to put on leave last month," the supervisors said in the letter, dated Friday. [Los Angeles Times](#)

### **LAPD officer hit by object, possibly shot by pellet gun; 3 in custody**

A Los Angeles police officer was struck in the neck by what authorities believe was a pellet from a pellet gun in South Los Angeles and hospitalized Thursday with stable vital signs. Officers with South Traffic Division were patrolling the area of 69th Street and Denker Avenue about 11 p.m. Wednesday when one officer was hit, according to the Los Angeles Police Department. The officer was taken to a hospital with non-life-threatening injuries, police said. [City News Service](#)

### **Gun rights group sues L.A. over closure of firearms stores during coronavirus**

A gun rights group is suing the city of Los Angeles, arguing that an order that has shuttered stores selling firearms in L.A. during the COVID-19 pandemic is unconstitutional and preempted by state law. The lawsuit, whose plaintiffs include the California Rifle & Pistol Assn. and stores selling firearms in the San Fernando Valley, states that although Mayor Eric Garcetti did not expressly name gun stores in his written order, both Garcetti and City Atty. Mike Feuer have stated that the stores must close and the Police Department has ordered them to shut down. [Los Angeles Times](#)

### **Most of LA's homeless are left on the crowded streets during coronavirus crisis**

Despite promises of making thousands of shelter beds, hotel and motel rooms available so Los Angeles' homeless can come off the streets during the coronavirus crisis, NBC4's I-Team found most beds across the city are full or unavailable. "It's heartbreaking," Ken Craft, CEO of Hope of the Valley, said. "There's nothing worse than when you're at capacity and you know you just can't take on more person." [NBC4 Los Angeles](#)

### **Actor Gary Sinise aids busy L.A.P.D. officers who can't make it home (Video)**

Actor Gary Sinise and his foundation join others who give Los Angeles Police officers a place to rest and recharge while working long hours

during Covid-19 crisis.

[ABC7 Los Angeles](#)

### **Map: Where challengers forced runoff in District Attorney race**

Challengers George Gascón and Rachel Rossi combined to nab more than 50% of the vote in the race for Los Angeles County District Attorney. That denied incumbent D.A. Jackie Lacey the majority she needed to secure a third term, and sets up a rematch between Lacey and former San Francisco D.A. Gascón in November. With the election results certified, we've mapped the results at the precinct level. Green areas saw a majority for Lacey.

[LAist](#)

### **The investigation into City Hall corruption may soon take a new, bigger step**

If you follow local government, now is the perfect time to deploy a cliché that invokes a warning. A few options: City Council members should beware the Ides of April (March has passed); for politics as usual, the end is near; or, my personal favorite, for L.A. City Hall, winter is coming. That's the only logical take considering federal officials' recent moves. A public corruption investigation that the FBI launched years ago is in the hands of prosecutors and appears to be nearing a climax.

[Los Angeles Magazine](#)

## **Consumer**

### **Amazon vowed to crack down on coronavirus profiteering. Some sellers have figured out loopholes**

Amazon took a hard line against pandemic profiteering last month, vowing to remove product listings that claim to prevent the coronavirus. But third-party merchants that sell millions of items on the e-commerce giant's marketplace are already finding ways around that. The latest gambit: promising coronavirus protection in the gallery of images that shoppers see next to the product on the site.

[Washington Post](#)

### **FBI coronavirus warning: 'Significant spike' in COVID-19 scams targeting these three states**

As cybercriminals continue to exploit the coronavirus pandemic, the FBI has warned that three U.S. states need to be particularly alert to the cyber-attack threat. The FBI has warned of a significant spike in coronavirus scams, adding to concerns about an "unprecedented wave" of cyber-attacks voiced by United States Attorney Scott Brady. However, according to the FBI Cyber Division, threat actors from outside the U.S. are mainly targeting three states, those who have unusually high rates of COVID-19 infection.

[Forbes](#)

## **Public Safety/Crime**



---

## **Manager arrested after firearms go missing at LAPD academy gun store**

After more than three dozen firearms went missing from the gun store at the LAPD Police Academy, the store's civilian manager has been arrested, multiple sources confirm to Eyewitness News. Several law enforcement officers are on leave pending the investigation, Eyewitness News has also learned. And about a dozen weapons are still missing, sources say. The civilian manager of the gun store, 33-year-old Archi Duenas, was arrested for grand theft on March 19, according to the LAPD.

[ABC7 Los Angeles](#)

## **Police nationwide report rise in domestic violence calls**

Reports of domestic violence increased in March in many cities around the country as the coronavirus pandemic spread, according to law enforcement officials - raising concerns about families' safety as they isolate at home. Of the 22 law enforcement agencies across the United States that responded to requests for data on domestic violence calls, 18 departments said they had seen a rise in March. Houston police received about 300 more domestic violence calls in March than they did in February, a roughly 20 percent increase.

[PoliceOne](#)

## **Los Angeles crime plunges during the coronavirus stay at home order**

Los Angeles has seen a 23% drop in crime in the past month as California has been under a stay at home order to fight the spread of coronavirus, the city's police chief said. "People staying home in their neighborhoods, watching out for each other, and exercising social distancing is allowing us to have a safer city," Los Angeles Police Department Chief Michel Moore said.

[CNN](#)

## **LAPD files 37 complaints against businesses for violating coronavirus closure rules**

Los Angeles Police Chief Michel Moore said Monday that officers have filed 37 total complaints against businesses that have not complied with the city's sweeping coronavirus stay-at-home orders. Those complaints will lead to fines and potential criminal prosecutions, Moore said. "This is not just irresponsible," Moore said. "It is not only endangering themselves but their employees and everyone else in that community and I am proud of City Atty. [Mike] Feuer and of his work and the prosecution of those individuals."

[Los Angeles Times](#)

## **Long Beach man charged with kidnapping, sexually assaulting woman**

A man has been charged with kidnapping a woman from a Long Beach

parking structure and sexually assaulting her last month, the Los Angeles County District Attorney's Office announced today. Jacob William Brown (dob 5/12/80) of Long Beach faces one count each of carjacking, kidnapping during carjacking and kidnapping for a sex crime as well as three counts each of assault with intent to commit rape and forced oral copulation.

[Los Angeles County District Attorney's Office](#)

### **San Diego County authorities begin ticketing health order violators**

Dozens of San Diego-area residents and some local businesses received citations over the weekend for violating government social-distancing requirements designed to slow the spread of the deadly COVID-19 pandemic, authorities reported Monday. In the city of San Diego, police handed out 16 tickets to individual scofflaws on Saturday and Sunday - five in Balboa Park and 11 in the Ocean Beach area, including Sunset Cliffs and Robb Field park, SDPD public-affairs Lt. Shawn Takeuchi said.

[City News Service](#)

### **LAPD concerned about boarded-up businesses**

LAPD officers have been making lists of closed businesses that have boarded doors and windows, worried that the locations could become targets for burglars. "We will continue to monitor those locations and assure extra patrol," Chief Michel Moore said Tuesday. "We're watching our commercial burglaries carefully to see instances of those businesses, which are not opening, are falling victim to offenders that would want to prey on them."

[NBC4 Los Angeles](#)

### **On streets emptied by coronavirus, L.A. officials crack down on speeding**

With millions of Southern Californians hunkering down at home, traffic has been blissfully light - a rare positive in a time of sickness, death, unemployment and isolation. But in the age of coronavirus, people still venture out to the supermarket or to help elderly relatives. And some are succumbing to the temptations of wide-open roads. Speeds are up by as much as 30% on some Los Angeles streets, according to a preliminary analysis by the city's Department of Transportation that measured traffic at a subset of locations.

[Los Angeles Times](#)

### **Coronavirus crimes: San Francisco restaurants see trend in break-ins amid COVID-19 shelter-in-place**

Property crimes are down by double digits in San Francisco compared to the same time last year due to the novel coronavirus shelter-in-place. However, restaurant owners are discovering that during recent break-ins there is a new trend in what's being taken. Saira and Monica Gomez have a hard time watching the 20 different security videos recorded at

their restaurant, Crossroad Pizza from a rash of 5 break-ins spanning 3 days.

[ABC7 Los Angeles](#)

### **FBI anticipates rise in business email compromise schemes related to the COVID-19 pandemic**

Fraudsters will take advantage of any opportunity to steal your money, personal information, or both. Right now, they are using the uncertainty surrounding the COVID-19 pandemic to further their efforts. Business email compromise (BEC) is a scam that targets anyone who performs legitimate funds transfers. Recently, there has been an increase in BEC frauds targeting municipalities purchasing personal protective equipment or other supplies needed in the fight against COVID-19.

[FBI News Release](#)

### **Report: juvenile arrest rate in San Diego County hits new 10-year low**

The juvenile arrest rate in San Diego County declined 28 percent between 2017 and 2018, continuing a notable downward trend and reaching a new 10-year low, according to a new study. Over the past decade, the rate dropped 82 percent, according to a report that outlines the study by the San Diego Association of Governments, known as SANDAG. The downward trend has been seen across the state.

[San Diego Union-Tribune](#)

### **Unique California gun program clears fewer cases in 2019**

State authorities cleared 8.6% fewer cases last year regarding people who no longer are allowed to own firearms, down from a record high in 2018, through a unique California program. Records show officials last year also finally closed the program's pre-July 2013 backlog of nearly 21,000 cases - completing the final 538 cases in March 2019. The state Legislature in 2013 had appropriated \$24 million to close the gap within three years.

[AP](#)

### **Chicago mayor chooses former Dallas chief to lead CPD as next superintendent**

Mayor Lori Lightfoot announced Thursday that she selected Dallas' former police chief, David Brown, to be Chicago's next police superintendent. "David Brown's track record of integrity, honor and legitimacy exemplifies what it means to be a Chicago police officer," Lightfoot said. "Through his nationally-recognized leadership and years of on-the-ground work to create a culture rooted in transparency, accountability and community policing, he will build on our all-hands-on-deck effort to create real, widespread and lasting public safety in our communities."

[NBC5 Chicago](#)

### **I just remember being exhausted': LAPD commander recovers**

### **from COVID-19**

Los Angeles Police Department Commander Cory Palka has returned to work after testing positive for COVID-19 last month. "I just remember being exhausted," said Palka. "When I was originally infected we were in the very preliminary stages. There was some early discussion regarding washing your hands. We had just started the language regarding safe distance. We weren't even into the mask language at the time."

[CBS4 Los Angeles](#)

### **New LAFD recruits graduate early, join front-lines against COVID-19 pandemic**

Forty-nine Los Angeles Fire Department recruits graduated today, four weeks earlier than scheduled, to join on the front lines against the COVID-19 pandemic. The class of 44 men and five women is set to start work at their fire stations on Sunday, according to Peter Sanders, public information director for the Los Angeles Fire Department. The department accelerated the class timeline as preparation for a potential surge of COVID-19 patients in the next few weeks, Sanders said.

[City News Service](#)

## **California/National**

### **Three big Democratic clashes in California**

The coronavirus pandemic obviously overshadows this year's political contests, but we presumably will still have an election seven months hence, so we cannot completely ignore its potential outcomes. Will President Donald Trump's re-election chances, which were iffy before the pandemic struck, be enhanced by his handling of the crisis - so far erratic, at best - or diminished? Will Democrats ratify former Vice President Joe Biden's pre-crisis lock on their party's presidential nomination, or will they opt for someone else?

[Santa Maria Times](#)

### **Las Vegas Metro Sheriff Lombardo suspends collective bargaining contracts with police**

A spokesperson for Las Vegas Metropolitan Police confirms collective bargaining agreements with officers and other employees have been suspended as a precautionary measure in case more police are needed in the field. "At this time, the intent in suspending the collective bargaining contracts is to allow LVMPD management the ability to potentially bypass the restriction of a 14-day notice prior to any transfer of personnel, whether permanent or semi-permanent," the spokesperson said in a statement to the Current.

[Nevada Current](#)

### **Pandemic pushes U.S. gun sales to all-time high**

Firearms sales and federal background checks for purchases soared to all-time highs in March as the coronavirus pandemic brought buyers out



in record numbers, even though gun dealers were included in orders shutting down businesses in some states. The FBI conducted 3.7 million background checks last month, according to its latest figures, the highest total since the national instant check system for buyers was launched in 1998 and 1.1 million higher than the number conducted in March 2019.

[NBC News](#)

## Corrections

### **With social distancing impossible, what do we do about inmates?**

When Attorney General Bill Barr called for increased home confinement over incarceration to stem the spread of coronavirus in federal prison, it showed that bipartisan demands for inmate releases had gained significant momentum. "We don't want our institutions to become petri dishes," said Barr, who directed the Bureau of Prisons to identify prisoners who have shown good conduct, were convicted of lower level crimes and have plans for release that would not create greater risks for spreading the virus.

[MSNBC](#)

### **Dozens of California prison workers have tested positive for coronavirus**

Fifty-three people who work at California state prisons have tested positive for COVID-19, according to new figures released on Sunday. The California Institute for Men, in Chino, had 16 reported cases, the most among 18 state facilities - including prisons and other offices - where employees have reported positive tests, according to the Department of Corrections and Rehabilitation.

[Sacramento Bee](#)

### **California prisons on soft lockdown; prison nurses must work overtime, or else**

California has launched a 14-day statewide soft lockdown in its prisons amid the coronavirus and told exhausted prison nurses that if they're ordered to work 16-hour shifts, they must comply or face reprisal. Inmates will be fed in their cells but still given access to prison services, exercise yards, supply canteens and phone calls within their own housing groups, the California Department of Corrections and Rehabilitation said Tuesday.

[Los Angeles Times](#)

## Sentences/Convictions/Parole

### **Buena Park man convicted of sexually assaulting 2-year-old**

A man convicted of sexually assaulting a 2-year-old girl in a unique jury trial utilizing social distancing in the closed-to-the-public Central Justice Center in Santa Ana is facing 50 years to life in prison. Arthur William Robert Callender, 23, of Buena Park, was found guilty Wednesday of two

felony counts of sexual intercourse with a child younger than 10, according to the Orange County District Attorney's Office.

[City News Service](#)

### **Simpson Thacher helps upend Calif. murder conviction**

Up to the moment last month when a judge told him he was a free man, Jeremy Puckett refused to believe freedom was a real possibility. Puckett, 43, sat inside jail cells in California for more than 18 years, convicted in February 2002 of a murder that he did not commit. His own long-standing efforts to secure his release had failed, and some of the evidence from the murder case had been destroyed.

[Law360](#)

### **Paso Robles woman who helped daughter kidnap son from county worker sentenced**

The mother of a Paso Robles woman who kidnapped her son from a San Luis Obispo County Child Welfare Services employee at knifepoint, sparking a multi-county Amber Alert, was sentenced for her role as getaway driver on Monday. Serbina Bullock, 50, had pleaded no contest in late February to a single felony count of kidnapping for the July 2019 incident in Paso Robles that involved Bullock's daughter, Rashawna Bullock, and Rashawna's 1-year-old son.

[The Tribune](#)

### **Redwood City murderer granted parole date**

James Harold Ward, 70, convicted of first degree murder in the 1982 stabbing of his girlfriend in an apartment near Woodside Road in Redwood City, was granted a parole date Tuesday after a hearing at the California State Prison at Solano. An administrative review now follows and the matter is then sent to the governor, San Mateo County District Attorney Steve Wagstaffe said. It's expected to take up to five months before the governor's decision Wagstaffe said.

[The Daily Journal](#)

## **Articles of Interest**

### **Amazon's self-publishing arm is a haven for white supremacists**

"Give me, a white man, a reason to live," a user posted to the anonymous message board 4chan in the summer of 2017. "Should I get a hobby. What interests can I pursue to save myself from total despair. How do you go on living." A fellow user had a suggestion: "Please write a concise book of only factual indisputable information exposing the Jews," focusing on "their selling of our high tech secrets to China/Russia" and "their long track record of pedophilia and perversion etc."

[ProPublica](#)

### **How New York City's emergency ventilator stockpile ended up on the auction block**

In July 2006, with an aggressive and novel strain of the flu circulating in

Asia and the Middle East, New York City Mayor Michael Bloomberg unveiled a sweeping pandemic preparedness plan. Using computer models to calculate how a disease could spread rapidly through the city's five boroughs, experts concluded New York needed a substantial stockpile of both masks and ventilators.

[ProPublica](#)

## Pensions

### **Recent stock market losses may spike local pension costs, but not immediately**

The recent stock market crash caused by the COVID-19 pandemic threatens to sharply increase pension costs for local cities, school districts and other government agencies. Those higher pension costs will worsen an already ongoing financial crisis for local governments, which have been grappling with sharp drops in tax revenue because so many parts of the economy have been forced to shut down.

[San Diego Union-Tribune](#)

### **Pension bomb fuse just got shorter**

Homeowners have enough to worry about in the current coronavirus crisis. They face an April 10 deadline for the second installment of their annual property tax bill and there is no relief - yet - coming from either the governor's office or the majority of county treasurer/tax collectors. Many taxpayers have been furloughed or laid off and the chances are high that property values throughout America will take a hit - even in California. How could things possibly get worse?

[Torrance Daily Breeze](#)

### **Does multiemployer pension reform belong in a 'phase 4' coronavirus bill?**

The short answer: maybe. In the days preceding the passage of the "CARES Act" economic relief/stimulus bill, there were numerous complaints about the House version's many unrelated provisions. I myself objected, in a personal blog post, to such provisions as an aircraft version of "cash for clunkers," a \$15 minimum wage mandate, and a requirement that large corporate recipients' boards of directors include employee-elected directors.

[Forbes](#)

### **CARES Act establishes rules for coronavirus-related distributions from 457(b) plans**

One provision of the recently signed \$2.2 trillion federal economic rescue package allows public employers to grant employees access to their retirement-savings accounts during the coronavirus epidemic. The Coronavirus Aid, Relief, and Economic Security Act (or CARES Act) created a new emergency retirement plan distribution option, labeled a coronavirus-related distribution, providing affected workers access to their 401(k)s, 403(b)s, IRAs and governmental 457(b)s under certain

circumstances.

[ProPublica](#)

### **No bailout for broke pensions**

At a time when Americans need to pull together to contain the coronavirus as well as the economic devastation it has unleashed, too many politicians are exploiting the moment to advance unrelated agendas. One egregious example is the renewed effort in the House to attach a multiemployer pension bailout to possible additional coronavirus relief legislation. The provision would be a taxpayer-funded giveaway to corporate and union leaders who failed to finance their pension promises long before the coronavirus appeared.

[Wall Street Journal](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Los Angeles Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)



**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of March 30, 2020  
**Date:** Monday, April 06, 2020 2:26:28 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of March 30, 2020](#)

04/06/2020 07:33 AM EDT

Original release date: April 6, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accenture -- mercury	An XXE issue exists in Accenture Mercury before 1.12.28 because of the platformlambda/core/serializers/SimpleXmlParser.java component.	2020-03-27	7.5	<a href="#">CVE-2020-10990</a> <a href="#">MISC</a> <a href="#">MISC</a>
alienform2 -- alienform2	Jon Hedley AlienForm2 (typically installed as af.cgi or alienform.cgi) 2.0.2 is vulnerable to Remote Command Execution via eval injection, a different issue than CVE-2002-0934. An unauthenticated, remote attacker can exploit this via a series of crafted requests.	2020-04-01	10	<a href="#">CVE-2020-10948</a> <a href="#">MISC</a>
apache -- http_server	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.	2020-04-01	7.5	<a href="#">CVE-2020-1934</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
	A memory corruption issue was			

apple -- macos_catalina	addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.4. An application may be able to execute arbitrary code with system privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3903</a> <a href="#">MISC</a>
apple -- macos_catalina	Multiple issues were addressed by updating to version 8.1.1850. This issue is fixed in macOS Catalina 10.15.4. Multiple issues in Vim.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-9769</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to leak memory.	2020-04-01	<a href="#">10</a>	<a href="#">CVE-2020-3847</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3892</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3893</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3904</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-3849</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3905</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-3850</a> <a href="#">MISC</a>
	A memory corruption issue was			

apple -- macos_catalina_and_tvos_10.15.3_and_higher	addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3 and higher. An attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	7.5	<a href="#">CVE-2020-3848</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3911</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3910</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3909</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	9.3	<a href="#">CVE-2020-9785</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to execute arbitrary code with system privileges.	2020-04-01	9.3	<a href="#">CVE-2020-9768</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to	2020-04-01	9.3	<a href="#">CVE-2020-3919</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	execute arbitrary code with kernel privileges.			<a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3895</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3899</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3897</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to bypass intended access restrictions on tasks from an untrusted process, when Self Defense is enabled.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-10867</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
azkaban -- azkaban	Azkaban through 3.84.0 allows XXE, related to validator/XmlValidatorManager.java and user/XmlUserManager.java.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10992</a> <a href="#">MISC</a>
bubblewrap -- bubblewrap	Bubblewrap (bwrap) before version 0.4.1, if installed in setuid mode and the kernel supports unprivileged user namespaces, then the `bwrap --users2` option can be used to make the setuid process keep running as root while being traceable. This can in turn be used to gain root permissions. Note that this only affects the combination of bubblewrap in setuid mode (which is typically used when unprivileged user namespaces are not supported) and the support of unprivileged user namespaces. Known to	2020-03-31	<a href="#">8.5</a>	<a href="#">CVE-2020-5291</a> <a href="#">MISC</a>



	be affected are: * Debian testing/unstable, if unprivileged user namespaces enabled (not default) * Debian buster-backports, if unprivileged user namespaces enabled (not default) * Arch if using `linux-hardened`, if unprivileged user namespaces enabled (not default) * Centos 7 flatpak COPR, if unprivileged user namespaces enabled (not default) This has been fixed in the 0.4.1 release, and all affected users should update.			<a href="#">CONFIRM</a>
buildah -- buildah	A path traversal flaw was found in Buildah in versions before 1.14.5. This flaw allows an attacker to trick a user into building a malicious container image hosted on an HTTP(s) server and then write files to the user's system anywhere that the user has permissions.	2020-03-31	<a href="#">9.3</a>	<a href="#">CVE-2020-10696</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
cacagoo -- tv-288zd-2mp_devices	CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 has weak authentication of TELNET access, leading to root privileges without any password required.	2020-04-02	<a href="#">10</a>	<a href="#">CVE-2020-6852</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- emc_idrac_devices	Dell EMC iDRAC7, iDRAC8 and iDRAC9 versions prior to 2.65.65.65, 2.70.70.70, 4.00.00.00 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may exploit this vulnerability to crash the affected process or execute arbitrary code on the system by sending specially crafted input data.	2020-03-31	<a href="#">10</a>	<a href="#">CVE-2020-5344</a> <a href="#">MISC</a>
effect -- effect	effect through 1.0.4 is vulnerable to Command Injection. It allows execution of arbitrary command via the options argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7624</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- elasticsearch	Elasticsearch versions from 6.7.0 before 6.8.8 and 7.0.0 before 7.6.2 contain a privilege escalation flaw if an attacker is able to create API keys. An attacker who is able to generate an API key can perform a series of steps that result in an API key being generated with elevated privileges.	2020-03-31	<a href="#">7.5</a>	<a href="#">CVE-2020-7009</a> <a href="#">N/A</a> <a href="#">CONFIRM</a> <a href="#">N/A</a>
f5 -- nginx_controller	In NGINX Controller versions prior to 3.2.0, an unauthenticated attacker with network access to the Controller API can create unprivileged user accounts. The user which is created is only able to upload a new license to the system but cannot view or modify any other components of the system.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-5863</a> <a href="#">MISC</a>
	git-add-remote through 1.0.0 is vulnerable			<a href="#">CVE-2020-</a>

git-add-remote -- git-add-remote	to Command Injection. It allows execution of arbitrary commands via the name argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">7630 MISC MISC</a>
gitlab -- gitlab	GitLab 8.10 and later through 12.9 is vulnerable to an SSRF in a project import note feature.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10956 CONFIRM MISC</a>
hiproxy -- op-broswer	op-browser through 1.0.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the url function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7625 MISC MISC</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to execute arbitrary commands on the system in the context of root user, caused by improper validation of user-supplied input. IBM X-Force ID: 174966.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4206 XF CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174975.	2020-03-31	<a href="#">7.5</a>	<a href="#">CVE-2020-4208 XF CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175418.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4241 XF CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175419.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4242 XF CONFIRM</a>
install-package -- install-package	install-package through 0.4.0 is vulnerable to Command Injection. It allows execution of arbitrary commands via the options argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7629 MISC MISC</a>
install-package -- install-package	install-package through 1.1.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the device function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7628 MISC MISC</a>

karma-mojo -- karma-mojo	karma-mojo through 1.0.1 is vulnerable to Command Injection. It allows execution of arbitrary commands via the config argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7626</a> <a href="#">MISC</a> <a href="#">MISC</a>
ksh -- ksh	In ksh version 20120801, a flaw was found in the way it evaluates certain environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Services and applications that allow remote unauthenticated attackers to provide one of those environment variables could allow them to exploit this issue remotely.	2020-04-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14868</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
laminar_research -- x-plane	X-Plane before 11.41 allows Arbitrary Memory Write via crafted network packets, which could cause a denial of service or arbitrary code execution.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2019-19605</a> <a href="#">MISC</a>
laminar_research -- x-plane	X-Plane before 11.41 has multiple improper path validations that could allow reading and writing files from/to arbitrary paths (or a leak of OS credentials to a remote system) via crafted network packets. This could be used to execute arbitrary commands on the system.	2020-03-30	<a href="#">10</a>	<a href="#">CVE-2019-19606</a> <a href="#">MISC</a>
lenovo -- multiple_notebooks	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A buffer overflow vulnerability was reported, (fixed and publicly disclosed in 2015) in the Lenovo Service Engine (LSE), affecting various versions of BIOS for Lenovo Notebooks, that could allow a remote user to execute arbitrary code on the system.	2020-03-27	<a href="#">10</a>	<a href="#">CVE-2015-5684</a> <a href="#">MISC</a>
lenovo -- multiple_products	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type COMMAND type could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-7334</a> <a href="#">MISC</a>
lenovo -- multiple_products	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type INF and INF_BY_COMPATIBLE_ID	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-7333</a> <a href="#">MISC</a>

	command types could allow a user to execute arbitrary code with elevated privileges.			
lenovo -- solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-8534</a> <a href="#">MISC</a>
lenovo -- solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A directory traversal vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-8535</a> <a href="#">MISC</a>
march_networks -- command_client	The connection initiation process in March Networks Command Client before 2.7.2 allows remote attackers to execute arbitrary code via crafted XAML objects.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2019-9163</a> <a href="#">CONFIRM</a>
mongodb -- js-bson	All versions of bson before 1.1.4 are vulnerable to Deserialization of Untrusted Data. The package will ignore an unknown value for an object's _bsotype, leading to cases where an object is serialized as a document rather than the intended BSON type.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2020-7610</a> <a href="#">MISC</a>
mulesoft -- apikit	Mulesoft APIkit through 1.3.0 allows XXE because of validation/RestXmlSchemaValidator.java	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10991</a> <a href="#">MISC</a>
node-key-sender -- node-key-sender	node-key-sender through 1.0.11 is vulnerable to Command Injection. It allows execution of arbitrary commands via the 'arrParams' argument in the 'execute()' function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7627</a> <a href="#">MISC</a> <a href="#">MISC</a>
objectcomputing -- micronaut	All versions of io.micronaut:micronaut-http-client before 1.2.11 and all versions from 1.3.0 before 1.3.2 are vulnerable to HTTP Request Header Injection due to not validating request headers passed to the client.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2020-7611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
odata4j -- odata4j	odata4j 0.7.0 allows ExecuteJPQLQueryCommand.java SQL injection. NOTE: this product is apparently discontinued.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2016-11024</a> <a href="#">MISC</a>
odata4j -- odata4j	odata4j 0.7.0 allows ExecuteCountQueryCommand.java SQL injection. NOTE: this product is	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2016-11023</a> <a href="#">MISC</a>



	apparently discontinued.			
paessler -- prtg_network_monitor	A webserver component in Paessler PRTG Network Monitor 19.2.50 to PRTG 20.1.56 allows unauthenticated remote command execution via a crafted POST request or the what parameter of the screenshot function in the Contact Support form.	2020-03-30	7.5	<a href="#">CVE-2020-10374</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
pam-krb5 -- pam-krb5	pam-krb5 before 4.9 has a buffer overflow that might cause remote code execution in situations involving supplemental prompting by a Kerberos library. It may overflow a buffer provided by the underlying Kerberos library by a single ' ' byte if an attacker responds to a prompt with an answer of a carefully chosen length. The effect may range from heap corruption to stack corruption depending on the structure of the underlying Kerberos library, with unknown effects but possibly including code execution. This code path is not used for normal authentication, but only when the Kerberos library does supplemental prompting, such as with PKINIT or when using the non-standard no_prompt PAM configuration option.	2020-03-31	7.5	<a href="#">CVE-2020-10595</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows Remote Code Execution.	2020-04-01	9	<a href="#">CVE-2020-10204</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows JavaEL Injection (issue 1 of 2).	2020-04-01	9	<a href="#">CVE-2020-10199</a> <a href="#">CONFIRM</a>
unisocon -- ultralog_express	UltraLog Express device management interface does not properly filter user inputted string in some specific parameters, attackers can inject arbitrary SQL command.	2020-03-27	7.5	<a href="#">CVE-2020-3936</a> <a href="#">MISC</a>
university_of_southern_california -- innovation_in_integrated_informatics_lab_cereal	An issue was discovered in USC iLab cereal through 1.3.0. It employs caching of std::shared_ptr values, using the raw pointer address as a unique identifier. This becomes problematic if an std::shared_ptr variable goes out of scope and is freed, and a new std::shared_ptr is allocated at the same address. Serialization fidelity thereby becomes dependent upon memory layout. In short, serialized std::shared_ptr variables cannot always be expected to serialize back into their original values. This can have any number of consequences,	2020-03-30	7.5	<a href="#">CVE-2020-11105</a> <a href="#">MISC</a>

	depending on the context within which this manifests.			
vertiv -- avocent_umg-400_devices	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to command injection because the application incorrectly neutralizes code syntax before executing. Since all commands within the web application are executed as root, this could allow a remote attacker authenticated with an administrator account to execute arbitrary commands as root.	2020-03-30	9	<a href="#">CVE-2019-9507</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. It has numerous fields that can contain data that is pulled from different sources. One issue with this is that the data isn't sanitized, and no input validation is performed, before the exporting of the user data. This can lead to (at least) CSV injection if a crafted Excel document is uploaded.	2020-04-01	7.5	<a href="#">CVE-2020-7947</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	LearnDash Wordpress plugin version below 3.1.6 is vulnerable to Unauthenticated SQL Injection.	2020-04-01	7.5	<a href="#">CVE-2020-6009</a> <a href="#">MISC</a>
wordpress -- wordpress	LifterLMS Wordpress plugin version below 3.37.15 is vulnerable to arbitrary file write leading to remote code execution	2020-03-31	7.5	<a href="#">CVE-2020-6008</a> <a href="#">MISC</a>
yamaha -- multiple_products	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors.	2020-04-01	7.8	<a href="#">CVE-2020-5548</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoom -- client_for_meetings	Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process	2020-04-01	7.2	<a href="#">CVE-2020-11469</a> <a href="#">MISC</a>

	(with the user's privileges) to obtain root access by replacing runwithroot.			<a href="#">MISC</a>
--	--	--	--	----------------------

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.3, the X-Content-Type-Options Header is missing in the HTTP response, potentially causing the response body to be interpreted and displayed as different content type other than declared. A possible attack scenario would be unauthorized code execution via text interpreted as JavaScript.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19089</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the X-Frame-Options header is not configured in HTTP response. This can potentially allow 'ClickJacking' attacks where an attacker can frame parts of the application on a malicious web site, revealing sensitive user information such as authentication credentials.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19001</a> <a href="#">CONFIRM</a>
abb -- esoms	Lack of input checks for SQL queries in ABB eSOMS versions 3.9 to 6.0.3 might allow an attacker SQL injection attacks against the backend database.	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2019-19094</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the HTTPOnly flag is not set. This can allow Javascript to access the cookie contents, which in turn might enable Cross Site Scripting.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19003</a> <a href="#">CONFIRM</a>
abb -- esoms	ABB eSOMS versions 4.0 to 6.0.3 accept connections using medium strength ciphers. If a connection is enabled using such a cipher, an attacker might be able to eavesdrop and/or intercept the connection.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19097</a> <a href="#">CONFIRM</a>
abb -- esoms	eSOMS versions 4.0 to 6.0.3 do not enforce password complexity settings, potentially resulting in lower access security due to insecure user passwords.	2020-04-02	<a href="#">6.4</a>	<a href="#">CVE-2019-19093</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS 4.0 to 6.0.3, the Cache-Control and Pragma HTTP header(s) have not been properly configured within the application response. This can potentially allow browsers and proxies to	2020-04-02	<a href="#">6.4</a>	<a href="#">CVE-2019-19000</a> <a href="#">CONFIRM</a>

	cache sensitive information.			
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.3, HTTPS responses contain comments with sensitive information about the application. An attacker might use this detail information to specifically craft the attack.	2020-04-02	<a href="#">4</a>	<a href="#">CVE-2019-19091</a> <a href="#">CONFIRM</a>
advantech -- webaccess	In Advantech WebAccess, Versions 8.4.2 and prior. A stack-based buffer overflow vulnerability caused by a lack of proper validation of the length of user-supplied data may allow remote code execution.	2020-03-27	<a href="#">6.5</a>	<a href="#">CVE-2020-10607</a> <a href="#">MISC</a>
advantech -- webaccess	Advantech WebAccess 8.3.4 does not properly restrict an RPC call that allows unauthenticated, remote users to read files. An attacker can use this vulnerability to recover the administrator password.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2019-3942</a> <a href="#">MISC</a>
apache -- dubbo	Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. This issue affected Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.x versions.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2019-17564</a> <a href="#">MISC</a>
apache -- http_server	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.	2020-04-02	<a href="#">5.8</a>	<a href="#">CVE-2020-1927</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apache -- netbeans	The "Apache NetBeans" autoupdate system does not validate SSL certificates and hostnames for https based downloads. This allows an attacker to intercept downloads of autoupdates and modify the download, potentially injecting malicious code. "Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	2020-03-30	<a href="#">6.4</a>	<a href="#">CVE-2019-17560</a> <a href="#">MISC</a>
apache -- netbeans	The "Apache NetBeans" autoupdate system does not fully validate code signatures. An attacker could modify the downloaded nbm and include additional code. "Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2019-17561</a> <a href="#">MISC</a>
apache -- ofbiz	Data sent with contentId to /control/stream is not sanitized, allowing	2020-04-	<a href="#">4.3</a>	<a href="#">CVE-2020-1943</a>



	XSS attacks in Apache OFBiz 16.11.01 to 16.11.07.	01		<a href="#">MISC</a>
apache -- sling_cms	Scripts in Sling CMS before 0.16.0 do not properly escape the Sling Selector from URLs when generating navigational elements for the administrative consoles and are vulnerable to reflected XSS attacks.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-1949</a> <a href="#">MISC</a>
apache -- solr	In Apache Solr, the cluster can be partitioned into multiple collections and only a subset of nodes actually host any given collection. However, if a node receives a request for a collection it does not host, it proxies the request to a relevant node and serves the request. Solr bypasses all authorization settings for such requests. This affects all Solr versions prior to 7.7 that use the default authorization mechanism of Solr (RuleBasedAuthorizationPlugin).	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2018-11802</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4. An attacker in a privileged network position may be able to intercept Bluetooth traffic.	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2020-9770</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the selection of video file by Mail. The issue was fixed by selecting the latest version of a video. This issue is fixed in iOS 13.4 and iPadOS 13.4. Cropped videos may not be shared properly via Mail.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9777</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4. A maliciously crafted page may interfere with other web contexts.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3888</a> <a href="#">MISC</a>
apple -- ios_and_ipados	The issue was addressed by clearing website permission prompts after navigation. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user may grant website permissions to a site they didn't intend to.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9781</a> <a href="#">MISC</a>
apple -- ios_and_ipados	The issue was addressed with improved deletion. This issue is fixed in iOS 13.4 and iPadOS 13.4. Deleted messages groups may still be suggested as an autocompletion.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-3890</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the handling of tabs displaying picture in picture video. The issue was corrected with improved state handling. This issue is fixed in iOS 13.4	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9775</a>

	and iPadOS 13.4. A user's private browsing activity may be unexpectedly saved in Screen Time.			MISC
apple -- macos_catalina	This issue was addressed with a new entitlement. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to access a user's call history.	2020-04-01	4.3	<a href="#">CVE-2020-9776</a> MISC
apple -- macos_high_sierra_and_catalina	An injection issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A remote attacker may be able to cause arbitrary javascript code execution.	2020-04-01	4.3	<a href="#">CVE-2020-3884</a> MISC
apple -- macos_mojave_and_catalina	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.4. A maliciously crafted application may be able to bypass code signing enforcement.	2020-04-01	6.8	<a href="#">CVE-2020-3906</a> MISC
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	6.6	<a href="#">CVE-2020-3908</a> MISC
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	6.6	<a href="#">CVE-2020-3912</a> MISC
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	6.6	<a href="#">CVE-2020-3907</a> MISC
apple -- multiple_devices	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution.	2020-04-01	6.8	<a href="#">CVE-2020-9783</a> MISC MISC MISC MISC MISC
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to read restricted memory.	2020-04-01	4.3	<a href="#">CVE-2020-3914</a> MISC MISC MISC MISC

apple -- multiple_products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A download's origin may be incorrectly associated.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3887</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	The issue was addressed with improved handling of icon caches. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to identify what other applications a user has installed.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-9773</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, watchOS 6.2. A malicious application may be able to elevate privileges.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-3913</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to a cross site scripting attack.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3902</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-3900</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. Setting an alternate app icon may disclose a photo without needing permission to access photos.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-3916</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-3901</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	7.18. Processing maliciously crafted web content may lead to arbitrary code execution.			<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- safari	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1. A malicious iframe may use another website's download settings.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-9784</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to make arbitrary changes to the Components section of the Stats.ini file via RPC from a Low Integrity process.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10865</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Arbitrary File Deletion from Avast Program Path via RPC, when Self Defense is Enabled.	2020-04-01	<a href="#">6.4</a>	<a href="#">CVE-2020-10861</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to launch the Repair App RPC call from a Low Integrity process.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. An Arbitrary Memory Address Overwrite vulnerability in the aswAvLog Log Library results in Denial of Service of the Avast Service (AvastSvc.exe).	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10860</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a shutdown via RPC from a Low Integrity process via TempShutDownMachine.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Local Privilege Escalation (LPE) via RPC.	2020-04-01	<a href="#">4.6</a>	<a href="#">CVE-2020-10862</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a reboot via RPC from	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10864</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	a Low Integrity process.			
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to enumerate the network interfaces and access points from a Low Integrity process via RPC.	2020-04-01	5	<a href="#">CVE-2020-10866</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacagoo -- cloud_storage_intelligent_camera_tv_288zd-2mp	The CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 allows access to the RTSP service without a password.	2020-04-02	5	<a href="#">CVE-2020-9349</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/people endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve sensitive information about all users registered on the system. This includes their full name, privilege, email address, phone number, etc.	2020-04-01	4	<a href="#">CVE-2020-11464</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/tickets endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve arbitrary information about all helpdesk tickets stored in database with numerous filters. This leaked sensitive information to unauthorized parties. Additionally, it leaked ticket authentication code, making it possible to make changes to a ticket.	2020-04-01	4	<a href="#">CVE-2020-11466</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/email_accounts endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve cleartext credentials of all helpdesk email accounts, including incoming and outgoing email credentials. This enables an attacker to get full access to all emails sent or received by the system including password reset emails, making it possible to reset any user's password.	2020-04-01	5	<a href="#">CVE-2020-11463</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/apps/* endpoints failed to properly validate a user's privilege, allowing an attacker to control/install helpdesk applications and leak current applications' configurations, including applications used as user sources (used for authentication). This enables an attacker to forge valid authentication models that resembles any	2020-04-01	6.5	<a href="#">CVE-2020-11465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	user on the system.			
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. This product enables administrators to modify the helpdesk interface by editing /portal/api/style/edit-theme-set/template-sources theme templates, and uses TWIG as its template engine. While direct access to self and _self variables was not permitted, one could abuse the accessible variables in one's context to reach a native unserialize function via the code parameter. There, one could pass a crafted payload to trigger a set of POP gadgets in order to achieve remote code execution.	2020-04-01	<a href="#">6.5</a>	<a href="#">CVE-2020-11467</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5859</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5857</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.2, under certain conditions, TMM may crash or stop processing new traffic with the DPDK/ENA driver on AWS systems while sending traffic. This issue does not affect any other platforms, hardware or virtual, or any other cloud provider since the affected driver is specific to AWS.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5862</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 12.1.0-12.1.5, the TMM process may produce a core file in some cases when Ram Cache incorrectly optimizes stored data resulting in memory errors.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5861</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.2, 14.1.0-14.1.2.2, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, users with non-administrator roles (for example, Guest or Resource Administrator) with tmsh shell access can execute arbitrary commands with elevated privilege via a crafted tmsh command.	2020-03-27	<a href="#">4.6</a>	<a href="#">CVE-2020-5858</a> <a href="#">MISC</a>
f5 -- big-ip_and_big-iq	On BIG-IP 15.0.0-15.1.0.2, 14.1.0-14.1.2.3, 13.1.0-13.1.3.2, 12.1.0-12.1.5.1, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, in a High Availability (HA) network failover in Device Service Cluster (DSC), the failover service does not require a strong form of	2020-03-27	<a href="#">6.8</a>	<a href="#">CVE-2020-5860</a> <a href="#">MISC</a>

	authentication and HA network failover traffic is not encrypted by Transport Layer Security (TLS).			
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.activemq.* (aka activemq-jms, activemq-core, activemq-pool, and activemq-pool-jms).	2020-03-31	6.8	<a href="#">CVE-2020-11111</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.openjpa.ee.WASRegistryManagedRuntime (aka openjpa).	2020-03-31	6.8	<a href="#">CVE-2020-11113</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.proxy.provider.remoting.RmiProvider (aka apache/commons-proxy).	2020-03-31	6.8	<a href="#">CVE-2020-11112</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- fortios	An external control of system vulnerability in FortiOS may allow an authenticated, regular user to change the routing settings of the device via connecting to the ZebOS component.	2020-04-02	6.5	<a href="#">CVE-2018-13371</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab through 12.9 is affected by a potential DoS in repository archive download.	2020-03-27	5	<a href="#">CVE-2020-10954</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and_enterprise_editions	GitLab EE/CE 8.11 through 12.9.1 allows blocked users to pull/push docker images.	2020-03-27	5.8	<a href="#">CVE-2020-10952</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and_enterprise_editions	GitLab EE/CE 11.1 through 12.9 is vulnerable to parameter tampering on an enterprise edition that allows an unauthorized user to read content available under specific folders.	2020-03-27	4	<a href="#">CVE-2020-10955</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	In GitLab EE 11.7 through 12.9, the NPM feature is vulnerable to a path traversal issue.	2020-03-27	5	<a href="#">CVE-2020-10953</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
grandstream -- ucm6200_series_devices	The UCM6200 series 1.0.20.22 and below stores unencrypted user passwords in an SQLite database. This could allow an attacker to retrieve all passwords and possibly gain elevated privileges.	2020-03-30	5	<a href="#">CVE-2020-5723</a> <a href="#">CONFIRM</a>
	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL			

grandstream -- ucm6200_series_devices	injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords.	2020-03-30	<a href="#">4.3</a>	<a href="#">CVE-2020-5725</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grandstream -- ucm6200_series_devices	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-5726</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grandstream -- ucm6200_series_devices	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-5724</a> <a href="#">CONFIRM</a>
gststreamer -- gst-rtsp-server	An exploitable denial of service vulnerability exists in the GstRTSPAuth functionality of GStreamer/gst-rtsp-server 1.14.5. A specially crafted RTSP setup request can cause a null pointer deference resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-6095</a> <a href="#">MISC</a> <a href="#">MISC</a>
haproxy -- haproxy	In hpack_dht_insert in hpack-tbl.c in the HPACK decoder in HAProxy 1.8 through 2.x before 2.1.4, a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing remote code execution.	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2020-11100</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
huawei -- multiple_smartax_devices	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include: SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800	2020-04-02	<a href="#">5.2</a>	<a href="#">CVE-2020-9067</a> <a href="#">CONFIRM</a>



	versions V100R018C00, V100R018C10, V100R019C10.			
ibm -- process_federation_server	The IBM Process Federation Server 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, and 19.0.0.3 Global Teams REST API does not properly shutdown the thread pools that it creates to retrieve Global Teams information from the federated systems. As a consequence, the Java Virtual Machine can't recover the memory used by those thread pools, which leads to an OutOfMemory exception when the Process Federation Server Global Teams REST API is used extensively. IBM X-Force ID: 177596.	2020-04-02	4	<a href="#">CVE-2020-4325</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request to overwrite or create arbitrary files on the system. IBM X-Force ID: 175417.	2020-03-31	6.4	<a href="#">CVE-2020-4240</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to arbitrary delete a directory caused by improper validation of user-supplied input. IBM X-Force ID: 175026.	2020-03-31	6.4	<a href="#">CVE-2020-4214</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 175412.	2020-03-31	5	<a href="#">CVE-2020-4239</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175411.	2020-03-31	6.8	<a href="#">CVE-2020-4238</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175410.	2020-03-31	6.8	<a href="#">CVE-2020-4237</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 could allow an authenticated user to cause a denial of service due to improper content parsing in the project	2020-03-31	4	<a href="#">CVE-2020-4236</a> <a href="#">XF</a>

	management module. IBM X-Force ID: 175409.			<a href="#">CONFIRM</a>
ibm -- websphere_application_server --liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 20.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176670.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2020-4304</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server --liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 20.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176668.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2020-4303</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intland_software -- codebeamer	codeBeamer before 9.5.0-RC3 does not properly restrict the ability to execute custom Java code and access the Java class loader via computed fields.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20635</a> <a href="#">MISC</a>
kubernetes -- api_server	The Kubernetes API server component in versions prior to 1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via successful API requests.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-8552</a> <a href="#">MISC</a> <a href="#">MISC</a>
kubernetes -- api_server	The Kubernetes API Server component in versions 1.1-1.14, and versions prior to 1.15.10, 1.16.7 and 1.17.3 allows an authorized user who sends malicious YAML payloads to cause the kube-apiserver to consume excessive CPU cycles while parsing YAML.	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2019-11254</a> <a href="#">MISC</a> <a href="#">MISC</a>
leantime -- leantime	Leantime before versions 2.0.15 and 2.1-beta3 has a SQL Injection vulnerability. The impact is high. Malicious users/attackers can execute arbitrary SQL queries negatively affecting the confidentiality, integrity, and availability of the site. Attackers can exfiltrate data like the users' and administrators' password hashes, modify data, or drop tables. The unescaped parameter is "searchUsers" when sending a POST request to "/tickets/showKanban" with a valid session. In the code, the parameter is named "users" in class.tickets.php. This issue is fixed in versions 2.0.15 and 2.1.0 beta 3.	2020-03-31	<a href="#">6.5</a>	<a href="#">CVE-2020-5292</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

lenovo -- lenovo_solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow cross-site request forgery.	2020-03-27	<a href="#">6.8</a>	<a href="#">CVE-2015-8536</a> <a href="#">MISC</a>
lenovo -- multiple_devices	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A race condition was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">6.9</a>	<a href="#">CVE-2015-7335</a> <a href="#">MISC</a>
lenovo -- multiple_devices	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow the signature check of an update to be bypassed.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2015-7336</a> <a href="#">MISC</a>
limesurvey -- limesurvey	LimeSurvey before 4.1.12+200324 contains a path traversal vulnerability in application/controllers/admin/LimeSurveyFileManager.php.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-11455</a> <a href="#">MISC</a>
limesurvey -- limesurvey	LimeSurvey before 4.1.12+200324 has stored XSS in application/views/admin/surveysgroups/surveySettings.php and application/models/SurveysGroups.php (aka survey groups).	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-11456</a> <a href="#">MISC</a>
microstrategy -- web_services	The Upload Visualization plugin in the Microstrategy Web 10.4 admin panel allows an administrator to upload a ZIP archive containing files with arbitrary extensions and data. (This is also exploitable via SSRF.)	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2020-11451</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy -- web_services	Microstrategy Web 10.4 is vulnerable to Server-Side Request Forgery in the Test Web Service functionality exposed through the path /MicroStrategyWS/. The functionality requires no authentication and, while it is not possible to pass parameters in the SSRF request, it is still possible to exploit it to conduct port scanning. An attacker could exploit this vulnerability to enumerate the resources allocated in the network (IP addresses and services exposed).	2020-04-02	<a href="#">5</a>	<a href="#">CVE-2020-11453</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy --	Microstrategy Web 10.4 exposes the JVM configuration, CPU architecture, installation folder, and other information			<a href="#">CVE-2020-11450</a>

web_services	through the URL /MicroStrategyWS/happyaxis.jsp. An attacker could use this vulnerability to learn more about the environment the application is running in.	2020-04-02	5	MISC <a href="#">FULLDISC</a> MISC <a href="#">MISC</a>
microstrategy -- web_services	Microstrategy Web 10.4 includes functionality to allow users to import files or data from external resources such as URLs or databases. By providing an external URL under attacker control, it's possible to send requests to external resources (aka SSRF) or leak files from the local system using the file:// stream wrapper.	2020-04-02	4	<a href="#">CVE-2020-11452</a> MISC <a href="#">FULLDISC</a> MISC <a href="#">MISC</a>
misp_project -- misp	app/Model/feed.php in MISP before 2.4.124 allows administrators to choose arbitrary files that should be ingested by MISP. This does not cause a leak of the full contents of a file, but does cause a leaks of strings that match certain patterns. Among the data that can leak are passwords from database.php or GPG key passphrases from config.php.	2020-04-02	4	<a href="#">CVE-2020-11458</a> MISC <a href="#">MISC</a>
mongodb -- js-bson	Incorrect parsing of certain JSON input may result in js-bson not correctly serializing BSON. This may cause unexpected application behaviour including data disclosure.	2020-03-31	5.5	<a href="#">CVE-2019-2391</a> <a href="#">CONFIRM</a>
moodle -- moodle	A vulnerability was found in Moodle versions 3.7 before 3.7.3, 3.6 before 3.6.7, 3.5 before 3.5.9 and earlier. OAuth 2 providers who do not verify users' email address changes require additional verification during sign-up to reduce the risk of account compromise.	2020-03-31	6.4	<a href="#">CVE-2019-14880</a> <a href="#">CONFIRM</a> MISC
open_source_social_network -- open_source_social_network	An issue was discovered in Open Source Social Network (OSSN) through 5.3. A user-controlled file path with a weak cryptographic rand() can be used to read any file with the permissions of the webserver. This can lead to further compromise. The attacker must conduct a brute-force attack against the SiteKey to insert into a crafted URL for components/OssnComments/ossn_com.php and/or libraries/ossn.lib.upgrade.php.	2020-03-30	4.3	<a href="#">CVE-2020-10560</a> MISC <a href="#">MISC</a>
osmand -- osmand	Osmand through 2.0.0 allow XXE because of binary/BinaryMapIndexReader.java.	2020-03-27	6.4	<a href="#">CVE-2020-10993</a> <a href="#">MISC</a>
	An attacker with the ability to generate session IDs or password reset tokens, either by being able to authenticate or by			



otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	exploiting OSA-2020-09, may be able to predict other users session IDs, password tokens and authentication system passwords. This issue affects ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	5.5	<a href="#">CVE-2020-1773</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	In the login screens (in agent and customer interface), Username and Password fields use autocomplete, which might be considered as security issue. This issue affects ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	4	<a href="#">CVE-2020-1769</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	It's possible to craft Lost Password requests with wildcards in the Token value, which allows attacker to retrieve valid Token(s), generated by users which already requested new passwords. This issue affects: ((OTRS)) Community Edition 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	5	<a href="#">CVE-2020-1772</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	Support bundle generated files could contain sensitive information that might be unwanted to be disclosed. This issue affects: ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	4	<a href="#">CVE-2020-1770</a> <a href="#">MISC</a>
phoenix_contact -- pc_worx_srt	Insecure, default path permissions in PHOENIX CONTACT PC WORX SRT through 1.14 allow for local privilege escalation.	2020-03-27	4.6	<a href="#">CVE-2020-10939</a> <a href="#">CONFIRM</a>
phoenix_contact -- portico_server	Local Privilege Escalation can occur in PHOENIX CONTACT PORTICO SERVER through 3.0.7 when installed to run as a service.	2020-03-27	4.6	<a href="#">CVE-2020-10940</a> <a href="#">CONFIRM</a>
php -- php	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.	2020-04-01	5.8	<a href="#">CVE-2020-7064</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
php -- php	In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using mb_strtolower() function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated	2020-04-01	6.8	<a href="#">CVE-2020-7065</a> <a href="#">MISC</a>

	buffer. This could lead to memory corruption, crashes and potentially code execution.			<a href="#">CONFIRM</a>
php -- php	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using get_headers() with user-supplied URL, if the URL contains zero ( ) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-7066</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
progress_software -- telerik_ui_for_silverlight	An issue was discovered in Progress Telerik UI for Silverlight before 2020.1.330. The RadUploadHandler class in RadUpload for Silverlight expects a web request that provides the file location of the uploading file along with a few other parameters. The uploading file location should be inside the directory where the upload handler class is defined. Before 2020.1.330, a crafted web request could result in uploads to arbitrary locations.	2020-03-31	<a href="#">5</a>	<a href="#">CVE-2020-11414</a> <a href="#">MISC</a>
proofpoint -- email_protection	An issue was discovered in Proofpoint Email Protection through 2019-09-08. By collecting scores from Proofpoint email headers, it is possible to build a copy-cat Machine Learning Classification model and extract insights from this model. The insights gathered allow an attacker to craft emails that receive preferable scores, with a goal of delivering malicious emails.	2020-03-30	<a href="#">6.4</a>	<a href="#">CVE-2019-20634</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible_engine	A vulnerability was found in Ansible Engine versions 2.9.x before 2.9.3, 2.8.x before 2.8.8, 2.7.x before 2.7.16 and earlier, where in Ansible's nxos_file_copy module can be used to copy files to a flash or bootflash on NXOS devices. Malicious code could craft the filename parameter to perform OS command injections. This could result in a loss of confidentiality of the system among other issues.	2020-03-31	<a href="#">4.6</a>	<a href="#">CVE-2019-14905</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a>
red_hat -- openshift/apb-base	An insecure modification vulnerability in the /etc/passwd file was found in the container openshift/apb-base, affecting versions before the following 4.3.5, 4.2.21, 4.1.37, and 3.11.188-4. An attacker with access to the container	2020-04-02	<a href="#">4.4</a>	<a href="#">CVE-2019-19348</a> <a href="#">CONFIRM</a>

	could use this flaw to modify /etc/passwd and escalate their privileges.			
red_hat -- openshift/mariadb-apb	An insecure modification vulnerability in the /etc/passwd file was found in the container openshift/mariadb-apb, affecting versions before the following 4.3.5, 4.2.21, 4.1.37, and 3.11.188-4 . An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	2020-04-02	<a href="#">4.4</a>	<a href="#">CVE-2019-19346</a> <a href="#">CONFIRM</a>
redpwn -- redpwnctf	In RedpwnCTF before version 2.3, there is a session fixation vulnerability in exploitable through the `#token=\$ssid` hash when making a request to the `/verify` endpoint. An attacker team could potentially steal flags by, for example, exploiting a stored XSS payload in a CTF challenge so that victim teams who solve the challenge are unknowingly (and against their will) signed into the attacker team's account. Then, the attacker can gain points / value off the backs of the victims. This is patched in version 2.3.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-5290</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
responsive_filemanager -- responsive_filemanager	An issue was discovered in Responsive Filemanager through 9.14.0. In the dialog.php page, the session variable \$_SESSION['RF']['view_type'] wasn't sanitized if it was already set. This made stored XSS possible if one opens ajax_calls.php and uses the "view" action and places a payload in the type parameter, and then returns to the dialog.php page. This occurs because ajax_calls.php was also able to set the \$_SESSION['RF']['view_type'] variable, but there it wasn't sanitized.	2020-03-30	<a href="#">4.3</a>	<a href="#">CVE-2020-11106</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, improperly stores system files. Attackers can use a specific URL and capture confidential information.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-10508</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, contains vulnerability of Cross-Site Scripting (XSS), attackers can inject arbitrary command into the system and launch XSS attack.	2020-03-27	<a href="#">4.3</a>	<a href="#">CVE-2020-10509</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, contains a vulnerability of Broken Access Control. After login, attackers can use a specific URL, access unauthorized	2020-03-27	<a href="#">4</a>	<a href="#">CVE-2020-10510</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	functionality and data.			
symfony -- symfony	In Symfony before versions 4.4.7 and 5.0.7, when a `Response` does not contain a `Content-Type` header, affected versions of Symfony can fallback to the format defined in the `Accept` header of the request, leading to a possible mismatch between the response's content and `Content-Type` header. When the response is cached, this can prevent the use of the website by other users. This has been patched in versions 4.4.7 and 5.0.7.	2020-03-30	4	<a href="#">CVE-2020-5255</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
symfony -- symfony	In symfony/security-http before versions 4.4.7 and 5.0.7, when a `Firewall` checks access control rule, it iterate overs each rule's attributes and stops as soon as the accessDecisionManager decides to grant access on the attribute, preventing the check of next attributes that should have been take into account in an unanimous strategy. The accessDecisionManager is now called with all attributes at once, allowing the unanimous strategy being applied on each attribute. This issue is patched in versions 4.4.7 and 5.0.7.	2020-03-30	5.5	<a href="#">CVE-2020-5275</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
symfony -- symfony	In Symfony before versions 5.0.5 and 4.4.5, some properties of the Exception were not properly escaped when the `ErrorHandler` rendered it stacktrace. In addition, the stacktrace were displayed even in a non-debug configuration. The ErrorHandler now escape all properties of the exception, and the stacktrace is only display in debug configuration. This issue is patched in symfony/http-foundation versions 4.4.5 and 5.0.5	2020-03-30	5.5	<a href="#">CVE-2020-5274</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
technicolor -- tc7337_devices	An issue was discovered on Technicolor TC7337 8.89.17 devices. An attacker can discover admin credentials in the backup file, aka backupsettings.conf.	2020-04-01	5	<a href="#">CVE-2020-11449</a> <a href="#">MISC</a>
tikiwiki -- groupware_and_cms	There is an Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in php webpages of Tiki-Wiki Groupware. Tiki-Wiki CMS all versions through 20.0 allows malicious users to cause the injection of malicious code fragments (scripts) into a legitimate web page.	2020-04-01	4.3	<a href="#">CVE-2020-8966</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
totemo -- totemomail	An insecure direct object reference in webmail in totemo totemomail 7.0.0 allows an authenticated remote user to	2020-03-27	5.5	<a href="#">CVE-2020-7918</a> <a href="#">MISC</a>



	read and modify mail folder names of other users via enumeration.			<a href="#">MISC</a>
toyota -- model_year_2017_display_control_unit	Toyota 2017 Model Year DCU (Display Control Unit) allows an unauthenticated attacker within Bluetooth range to cause a denial of service attack and/or execute an arbitrary command. The affected DCUs are installed in Lexus (LC, LS, NX, RC, RC F), TOYOTA CAMRY, and TOYOTA SIENNA manufactured in the regions other than Japan from Oct. 2016 to Oct. 2019. An attacker with certain knowledge on the target vehicle control system may be able to send some diagnostic commands to ECUs with some limited availability impacts; the vendor states critical vehicle controls such as driving, turning, and stopping are not affected.	2020-03-30	<a href="#">5.4</a>	<a href="#">CVE-2020-5551</a> <a href="#">MISC</a> <a href="#">MISC</a>
ubiquiti -- unifi_video_controller	The UniFi Video Server (Windows) web interface configuration restore functionality at the “backup” and “wizard” endpoints does not implement sufficient privilege checks. Low privileged users, belonging to the PUBLIC_GROUP or CUSTOM_GROUP groups, can access these endpoints and overwrite the current application configuration. This can be abused for various purposes, including adding new administrative users. Affected Products: UniFi Video Controller v3.9.3 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.9.6 and newer.	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2020-8145</a> <a href="#">CONFIRM</a>
ubiquiti -- unifi_video_controller	In UniFi Video v3.10.1 (for Windows 7/8/10 x64) there is a Local Privileges Escalation to SYSTEM from arbitrary file deletion and DLL hijack vulnerabilities. The issue was fixed by adjusting the .tsExport folder when the controller is running on Windows and adjusting the SafeDllSearchMode in the windows registry when installing UniFi-Video controller. Affected Products: UniFi Video Controller v3.10.2 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.10.3 and newer.	2020-04-01	<a href="#">6.9</a>	<a href="#">CVE-2020-8146</a> <a href="#">CONFIRM</a>
ubiquiti --	The UniFi Video Server v3.9.3 and prior (for Windows 7/8/10 x64) web interface Firmware Update functionality, under certain circumstances, does not validate firmware download destinations to ensure they are within the intended destination directory tree. It accepts a request with a	2020-04-		<a href="#">CVE-2020-</a>

unifi_video_controller	URL to firmware update information. If the version field contains ..\ character sequences, the destination file path to save the firmware can be manipulated to be outside the intended destination directory tree. Fixed in UniFi Video Controller v3.10.3 and newer.	01	<a href="#">5.2</a>	<a href="#">8144</a> <a href="#">CONFIRM</a>
unisoan -- ultralog_express	UltraLog Express device management software stores user's information in cleartext. Any user can obtain accounts information through a specific page.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-3921</a> <a href="#">MISC</a>
unisoan -- ultralog_express	UltraLog Express device management interface does not properly perform access authentication in some specific pages/functions. Any user can access the privileged page to manage accounts through specific system directory.	2020-03-27	<a href="#">5.5</a>	<a href="#">CVE-2020-3920</a> <a href="#">MISC</a>
university_of_southern_california -- innovation_in_integrated_informatics_lab_cereal	An issue was discovered in USC iLab cereal through 1.3.0. Serialization of an (initialized) C/C++ long double variable into a BinaryArchive or PortableBinaryArchive leaks several bytes of stack or heap memory, from which sensitive information (such as memory layout or private keys) can be gleaned if the archive is distributed outside of a trusted context.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-11104</a> <a href="#">MISC</a>
vertiv -- avocent_universal_management_gateway	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to stored XSS. A remote attacker authenticated with an administrator account could store a maliciously named file within the web application that would execute each time a user browsed to the page.	2020-03-30	<a href="#">6</a>	<a href="#">CVE-2019-9508</a> <a href="#">MISC</a> <a href="#">MISC</a>
vertiv -- avocent_universal_management_gateway	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to reflected XSS in an HTTP POST parameter. The web application does not sanitize user-controllable input before displaying to users in a web page, which could allow a remote attacker authenticated with a user account to execute arbitrary code.	2020-03-30	<a href="#">6.5</a>	<a href="#">CVE-2019-9509</a> <a href="#">MISC</a> <a href="#">MISC</a>
weberp -- weberp	In webERP 4.15, the Import Bank Transactions function fails to sanitize the content of imported MT940 bank statement files, resulting in the execution of arbitrary SQL queries, aka SQL Injection.	2020-03-30	<a href="#">6.5</a>	<a href="#">CVE-2019-7755</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A stored cross-site scripting (XSS)			<a href="#">CVE-2020-</a>

wordpress -- wordpress	vulnerability exists in the Auth0 plugin before 4.0.0 for WordPress via the settings page.	2020-04-01	<a href="#">4.3</a>	<a href="#">5392</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The custom-searchable-data-entry-system (aka Custom Searchable Data Entry System) plugin through 1.7.1 for WordPress allows SQL Injection. NOTE: this product is discontinued.	2020-03-27	<a href="#">6.5</a>	<a href="#">CVE-2020-10817</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. A user can perform an insecure direct object reference.	2020-04-01	<a href="#">6.5</a>	<a href="#">CVE-2020-7948</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerabilities exist in the Auth0 plugin before 4.0.0 for WordPress via the domain field.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-5391</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The Login by Auth0 plugin before 4.0.0 for WordPress allows stored XSS on multiple pages, a different issue than CVE-2020-5392.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-6753</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
yahoo -- elide	In Elide before 4.5.14, it is possible for an adversary to "guess and check" the value of a model field they do not have access to assuming they can read at least one other field in the model. The adversary can construct filter expressions for an inaccessible field to filter a collection. The presence or absence of models in the returned collection can be used to reconstruct the value of the inaccessible field. Resolved in Elide 4.5.14 and greater.	2020-03-30	<a href="#">4</a>	<a href="#">CVE-2020-5289</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zeit -- next.js	Next.js versions before 9.3.2 have a directory traversal vulnerability. Attackers could craft special requests to access files in the dist directory (.next). This does not affect files outside of the dist directory (.next). In general, the dist directory only holds build assets unless your application intentionally stores other assets under this directory. This issue is fixed in version 9.3.2.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-5284</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zevenet -- zen_load_balancer	Monitoring::Logs in Zen Load Balancer 3.10.1 allows remote authenticated admins to conduct absolute path traversal attacks, as demonstrated by a filelog=/etc/shadow request to index.cgi.	2020-04-02	<a href="#">4</a>	<a href="#">CVE-2020-11491</a> <a href="#">MISC</a> <a href="#">MISC</a>

zoho -- manageengine_desktop_central	Zoho ManageEngine Desktop Central allows unauthenticated users to access PDF Generation Servlet, leading to sensitive information disclosure.	2020-03-30	5	<a href="#">CVE-2020-8509</a> <a href="#">CONFIRM</a>
---	---	------------	---	--

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- esoms	The Redis data structure component used in ABB eSOMS versions 6.0 to 6.0.2 stores credentials in clear text. If an attacker has file system access, this can potentially compromise the credentials' confidentiality.	2020-04-02	<a href="#">3.6</a>	<a href="#">CVE-2019-19096</a> <a href="#">CONFIRM</a>
abb -- esoms	Lack of adequate input/output validation for ABB eSOMS versions 4.0 to 6.0.2 might allow an attacker to attack such as stored cross-site scripting by storing malicious content in the database.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19095</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the X-XSS-Protection HTTP response header is not set in responses from the web server. For older web browser not supporting Content Security Policy, this might increase the risk of Cross Site Scripting.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19002</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the Secure Flag is not set in the HTTP response header. Unencrypted connections might access the cookie information, thus making it susceptible to eavesdropping.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19090</a> <a href="#">CONFIRM</a>
abb -- esoms	ABB eSOMS versions 4.0 to 6.0.3 use ASP.NET Viewstate without Message Authentication Code (MAC). Alterations to Viewstate might thus not be noticed.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19092</a> <a href="#">CONFIRM</a>
apache -- cxf	Apache CXF has the ability to integrate with JMX by registering an InstrumentationManager extension with the CXF bus. If the 'createMBServerConnectorFactory' property of the default InstrumentationManagerImpl is not disabled, then it is vulnerable to a man-in-the-middle (MITM) style attack. An attacker on the same host can connect to the registry and rebind the entry to	2020-04-01	<a href="#">2.9</a>	<a href="#">CVE-2020-1954</a> <a href="#">MISC</a>





bd -- pyxis_medstation_es_system_and_pyxis_anesthesia_es_system	In BD Pyxis MedStation ES System v1.6.1 and Pyxis Anesthesia (PAS) ES System v1.6.1, a restricted desktop environment escape vulnerability exists in the kiosk mode functionality of affected devices. Specially-crafted inputs could allow the user to escape the restricted environment, resulting in access to sensitive data.	2020-04-01	<a href="#">3.6</a>	<a href="#">CVE-2020-10598</a> <a href="#">MISC</a>
gradle -- plugin_portal	All versions of com.gradle.plugin-publish before 0.11.0 are vulnerable to Insertion of Sensitive Information into Log File. When a plugin author publishes a Gradle plugin while running Gradle with the --info log level flag, the Gradle Logger logs an AWS pre-signed URL. If this build log is publicly visible (as it is in many popular public CI systems like TravisCI) this AWS pre-signed URL would allow a malicious actor to replace a recently uploaded plugin with their own.	2020-03-30	<a href="#">3.3</a>	<a href="#">CVE-2020-7599</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 175408.	2020-03-31	<a href="#">3.5</a>	<a href="#">CVE-2020-4235</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intland_software -- codebeamer_alm	In Intland codeBeamer ALM 9.5 and earlier, there is stored XSS via the Trackers Title parameter.	2020-03-30	<a href="#">3.5</a>	<a href="#">CVE-2019-19913</a> <a href="#">MISC</a>
intland_software -- codebeamer_alm	In Intland codeBeamer ALM 9.5 and earlier, a cross-site scripting (XSS) vulnerability in the Upload Flash File feature allows authenticated remote attackers to inject arbitrary scripts via an active script embedded in an SWF file.	2020-03-30	<a href="#">3.5</a>	<a href="#">CVE-2019-19912</a> <a href="#">MISC</a>
kubernetes -- kubelet	The Kubelet component in versions 1.15.0-1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via the kubelet API, including the unauthenticated HTTP read-only API typically served on port 10255, and the authenticated HTTPS API typically served on port 10250.	2020-03-27	<a href="#">3.3</a>	<a href="#">CVE-2020-8551</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy -- web_services	Microstrategy Web 10.4 is vulnerable to Stored XSS in the HTML Container and Insert Text features in the window, allowing for the creation of a new dashboard. In order to exploit this vulnerability, a user needs to get access	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2020-11454</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>

	to a shared dashboard or have the ability to create a dashboard on the application.			<a href="#">MISC</a>
otrs -- open_ticket_request_system	Attacker is able craft an article with a link to the customer address book with malicious content (JavaScript). When agent opens the link, JavaScript code is executed due to the missing parameter encoding. This issue affects: ((OTRS)) Community Edition: 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	3.5	<a href="#">CVE-2020-1771</a> <a href="#">MISC</a>
pfsense -- pfsense	pfSense before 2.4.5 has stored XSS in system_usermanager_addprivs.php in the WebGUI via the descr parameter (aka full name) of a user.	2020-04-01	3.5	<a href="#">CVE-2020-11457</a> <a href="#">MISC</a> <a href="#">MISC</a>
pki-core -- pki-core	A vulnerability was found in all pki-core 10.x.x version, where the Token Processing Service (TPS) did not properly sanitize several parameters stored for the tokens, possibly resulting in a Stored Cross Site Scripting (XSS) vulnerability. An attacker able to modify the parameters of any token could use this flaw to trick an authenticated user into executing arbitrary JavaScript code.	2020-03-31	3.5	<a href="#">CVE-2019-10180</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows XSS.	2020-04-01	3.5	<a href="#">CVE-2020-10203</a> <a href="#">CONFIRM</a>
versiant -- lynx_customer_service_portal	Versiant LYNX Customer Service Portal (CSP), version 3.5.2, is vulnerable to stored cross-site scripting, which could allow a local, authenticated attacker to insert malicious JavaScript that is stored and displayed to the end user. This could lead to website redirects, session cookie hijacking, or information disclosure.	2020-03-30	3.5	<a href="#">CVE-2020-9055</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
zoom -- zoom_client_for_meetings	Zoom Client for Meetings through 4.6.8 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Zoom Client's microphone and camera access.	2020-04-01	2.1	<a href="#">CVE-2020-11470</a> <a href="#">MISC</a> <a href="#">MISC</a>
zyxel -- xgs221-52hp_devices	In firmware version 4.50 of Zyxel XGS2210-52HP, multiple stored cross-site scripting (XSS) issues allows remote authenticated users to inject arbitrary web script via an rpSys.html Name or Location field.	2020-03-31	3.5	<a href="#">CVE-2019-13495</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3xlogic -- infinias_eidc32_devices	3xLOGIC Infinias eIDC32 2.213 devices with Web 1.107 allow Authentication Bypass via CMD.HTM?CMD= because authentication depends on the client side's interpretation of the <KEY>MYKEY</KEY> substring.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11542</a> <a href="#">MISC</a>
apple -- macos_catalina	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to read arbitrary files.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3889</a> <a href="#">MISC</a>
apple -- multiple_products	This issue was addressed with improved checks. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary entitlements.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3883</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3885</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bit2spr -- bit2spr	bit2spr 1992-06-07 has a stack-based buffer overflow (129-byte write) in conv_bitmap in bit2spr.c via a long line in a bitmap file.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11528</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- emc_isilon_onefs	Dell EMC Isilon OneFS versions 8.2.2 and earlier contain a denial of service vulnerability. SmartConnect had an error condition that may be triggered to loop, using CPU and potentially preventing other SmartConnect DNS responses.	2020-04-04	not yet calculated	<a href="#">CVE-2020-5347</a> <a href="#">MISC</a>
dell -- latitude_7202_rugged	Dell Latitude 7202 Rugged Tablet BIOS versions prior to A28 contain a UAF vulnerability in EFI_BOOT_SERVICES in system management mode. A local authenticated attacker may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in system management mode.	2020-04-04	not yet calculated	<a href="#">CVE-2020-5348</a> <a href="#">MISC</a>
	A flaw was found in the Eclipse Che up to			



eclipse -- che	version 7.8.x, where it did not properly restrict access to workspace pods. An authenticated user can exploit this flaw to bypass JWT proxy and gain access to the workspace pods of another user. Successful exploitation requires knowledge of the service name and namespace of the target pod.	2020-04-03	not yet calculated	<a href="#">CVE-2020-10689</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
firmware_analysis_and_comparison -- firmware_analysis_and_comparison	Firmware Analysis and Comparison Tool (FACT) has stored XSS when updating analysis details via a localhost web request and demonstrated by mishandling of the tags and version fields in helperFunctions/mongo_task_conversion.py.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11499</a> <a href="#">MISC</a> <a href="#">MISC</a>
get-git-data -- get-git-data	get-git-data through 1.3.1 is vulnerable to Command Injection. It is possible to inject arbitrary commands as part of the arguments provided to get-git-data.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7619</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu_glibc -- gnu_glibc	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.	2020-04-01	not yet calculated	<a href="#">CVE-2020-6096</a> <a href="#">MISC</a>
gnutls -- gnutls	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected version is 3.6.3 (2018-07-16) because of an error in a 2017-10-06 commit. The DTLS client always uses 32 ' ' bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol.	2020-04-03	not yet calculated	<a href="#">CVE-2020-11501</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
grav -- grav	Common/Grav.php in Grav before 1.6.23 has an Open Redirect.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11529</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A buffer overflow vulnerability was found			

hirschmann_automation_and_control -- hios_and_hisecos	in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30.	2020-04-03	not yet calculated	<a href="#">CVE-2020-6994</a> MISC
ibm -- spectrum_scale	IBM Spectrum Scale 4.2 and 5.0 could allow a local unprivileged attacker with intimate knowledge of the environment to execute commands as root using specially crafted input. IBM X-Force ID: 175977.	2020-04-03	not yet calculated	<a href="#">CVE-2020-4273</a> XF CONFIRM
ibm -- strongloop_strong-nginx-controller	strong-nginx-controller through 1.0.2 is vulnerable to Command Injection. It allows execution of arbitrary command as part of the '_nginxCmd()' function.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7621</a> MISC MISC
ini-parser -- ini-parser	ini-parser through 0.0.2 is vulnerable to Prototype Pollution. The library could be tricked into adding or modifying properties of Object.prototype using a '__proto__' payload.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7617</a> CONFIRM CONFIRM
ivanti -- workspace_control	Ivanti Workspace Control before 10.4.30.0, when SCCM integration is enabled, allows local users to obtain sensitive information (keying material).	2020-04-04	not yet calculated	<a href="#">CVE-2020-11533</a> MISC
jscover -- jscover	jscover through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary command via the source argument.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7623</a> MISC MISC
linux -- linux_kernel	An issue was discovered in slc_bump in drivers/net/can/slc.c in the Linux kernel through 5.6.2. It allows attackers to read uninitialized can_frame data, potentially containing sensitive information from kernel stack memory, if the configuration lacks CONFIG_INIT_STACK_ALL, aka CID-b9258a2cece4.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11494</a> MISC
linux -- linux_kernel	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was	2020-04-02	not yet calculated	<a href="#">CVE-2020-8835</a> CONFIRM CONFIRM FEDORA CONFIRM UBUNTU

	backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780)			<a href="#">UBUNTU CONFIRM CONFIRM</a>
mcafee -- endpoint_security_for_windows	Improper access control vulnerability in ESConfigTool.exe in ENS for Windows all current versions allows a local administrator to alter the ENS configuration up to and including disabling all protection offered by ENS via insecurely implemented encryption of configuration for export and import.	2020-04-01	not yet calculated	<a href="#">CVE-2020-7263 CONFIRM</a>
mediawiki -- mediawiki	In MediaWiki before 1.34.1, users can add various Cascading Style Sheets (CSS) classes (which can affect what content is shown or hidden in the user interface) to arbitrary DOM nodes via HTML content within a MediaWiki page. This occurs because jquery.makeCollapsible allows applying an event handler to any Cascading Style Sheets (CSS) selector. There is no known way to exploit this for cross-site scripting (XSS).	2020-04-03	not yet calculated	<a href="#">CVE-2020-10960 CONFIRM CONFIRM</a>
mitsubishi -- multiple_products	When MELSOFT transmission port (UDP/IP) of Mitsubishi Electric MELSEC iQ-R series (all versions), MELSEC iQ-F series (all versions), MELSEC Q series (all versions), MELSEC L series (all versions), and MELSEC F series (all versions) receives massive amount of data via unspecified vectors, resource consumption occurs and the port does not process the data properly. As a result, it may fall into a denial-of-service (DoS) condition. The vendor states this vulnerability only affects Ethernet communication functions.	2020-03-30	not yet calculated	<a href="#">CVE-2020-5527 MISC MISC</a>
netgear -- multiple_products	NETGEAR has released fixes for a pre-authentication command injection in request_handler.php security vulnerability on the following product models: WC7500, running firmware versions prior to 6.5.3.5; WC7520, running firmware versions prior to 2.5.0.46; WC7600v1, running firmware versions prior to 6.5.3.5; WC7600v2, running firmware versions prior to 6.5.3.5; and WC9500, running firmware versions prior to 6.5.3.5.	2020-04-01	not yet calculated	<a href="#">CVE-2018-11106 CONFIRM</a>
parrot -- anafi_drone	Web server running on Parrot ANAFI can be crashed due to the SDK command "Common_CurrentDateTime" being sent to control service with larger than	2020-04-01	not yet calculated	<a href="#">CVE-2019-3945 MISC</a>

	expected date length.			
parrot -- anafi_drone	Parrot ANAFI is vulnerable to Wi-Fi deauthentication attack, allowing remote and unauthenticated attackers to disconnect drone from controller during mid-flight.	2020-04-01	not yet calculated	<a href="#">CVE-2019-3944</a> <a href="#">MISC</a>
pomelo-monitor -- pomelo-monitor	pomelo-monitor through 0.3.7 is vulnerable to Command Injection.It allows injection of arbitrary commands as part of 'pomelo-monitor' params.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7620</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive_adserver -- revive_adserver	An Open Redirect vulnerability was discovered in Revive Adserver version < 5.0.5 and reported by HackerOne user hoangn144. A remote attacker could trick logged-in users to open a specifically crafted link and have them redirected to any destination.The CSRF protection of the “/www/admin/*-modify.php” could be skipped if no meaningful parameter was sent. No action was performed, but the user was still redirected to the target page, specified via the “returnurl” GET parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8143</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive_adserver -- revive_adserver	A security restriction bypass vulnerability has been discovered in Revive Adserver version < 5.0.5 by HackerOne user hoangn144. Revive Adserver, like many other applications, requires the logged in user to type the current password in order to change the e-mail address or the password. It was however possible for anyone with access to a Revive Adserver admin user interface to bypass such check and change e-email address or password of the currently logged in user by altering the form payload.The attack requires physical access to the user interface of a logged in user. If the POST payload was altered by turning the “pwold” parameter into an array, Revive Adserver would fetch and authorise the operation even if no password was provided.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8142</a> <a href="#">MISC</a> <a href="#">MISC</a>
slack -- nebula	Slack Nebula through 1.1.0 contains a relative path vulnerability that allows a low-privileged attacker to execute code in the context of the root user via tun_darwin.go or tun_windows.go. A user can also use Nebula to execute arbitrary code in the user's own context, e.g., for user-level persistence or to bypass security controls. NOTE: the vendor	2020-04-02	not yet calculated	<a href="#">CVE-2020-11498</a> <a href="#">MISC</a> <a href="#">MISC</a>



	states that this "requires a high degree of access and other preconditions that are tough to achieve."			
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3.x up to and including 3.21.2 has Incorrect Access Control.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11444</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
starface -- ucc_client	STARFACE UCC Client before 6.7.1.204 on WIndows allows binary planting to execute code with System rights, aka usd-2020-0006.	2020-04-02	not yet calculated	<a href="#">CVE-2020-10515</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
suse -- linux_enterprise_server	A Insufficient Verification of Data Authenticity vulnerability in autoyast2 of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15 allows remote attackers to MITM connections when deprecated and unused functionality of autoyast2 and its derivatives. This issue affects: SUSE Linux Enterprise Server 12 autoyast2 version 4.1.9-3.9.1 and prior versions. SUSE Linux Enterprise Server 15 autoyast2 version 4.0.70-3.20.1 and prior versions.	2020-04-03	not yet calculated	<a href="#">CVE-2019-18905</a> <a href="#">CONFIRM</a>
suse -- multiple_products	A Race Condition Enabling Link Following vulnerability in the packaging of texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users to corrupt files or potentially escalate privileges. This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8016</a> <a href="#">CONFIRM</a>
	A Race Condition Enabling Link Following vulnerability in the cron job shipped with texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-			

suse -- multiple_products	SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users in group mktx to delete arbitrary files on the system This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8017</a> <a href="#">CONFIRM</a>
suse -- multiple_products	A Uncontrolled Resource Consumption vulnerability in rmt of SUSE Linux Enterprise High Performance Computing 15-ESPOS, SUSE Linux Enterprise High Performance Computing 15-LTSS, SUSE Linux Enterprise Module for Public Cloud 15-SP1, SUSE Linux Enterprise Module for Server Applications 15, SUSE Linux Enterprise Module for Server Applications 15-SP1, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1 allows remote attackers to cause DoS against rmt by requesting migrations. This issue affects: SUSE Linux Enterprise High Performance Computing 15-ESPOS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise High Performance Computing 15-LTSS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Module for Public Cloud 15-SP1 rmt-server versions prior to 2.5.2-3.9.1. SUSE Linux Enterprise Module for Server Applications 15 rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Module for Server Applications 15-SP1 rmt-server versions prior to 2.5.2-3.9.1. SUSE Linux Enterprise Server 15-LTSS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Server for SAP 15 rmt-server versions prior to 2.5.2-3.26.1. openSUSE Leap 15.1 rmt-server versions prior to 2.5.2-lp151.2.9.1.	2020-04-03	not yet calculated	<a href="#">CVE-2019-18904</a> <a href="#">CONFIRM</a>
	A Least Privilege Violation vulnerability in crowbar of SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE			

suse -- openstack_cloud_and_ardana	OpenStack Cloud 9, SUSE OpenStack Cloud Crowbar 8, SUSE OpenStack Cloud Crowbar 9 allows root users on any crowbar managed node to cause become root on any other node. This issue affects: SUSE OpenStack Cloud 7 crowbar-core versions prior to 4.0+git.1578392992.fabfd186c-9.63.1, crowbar-. SUSE OpenStack Cloud 8 crowbar-core versions prior to 8.0+git.1579279939.ee7da88-3.39.3, ardana-. SUSE OpenStack Cloud 9 ardana-ansible versions prior to 9.0+git.1581611758.f694f7d-3.16.1, ardana-. SUSE OpenStack Cloud Crowbar 8 crowbar-core versions prior to 5.0+git.1582968668.1a55c77c5-3.35.4, crowbar-. SUSE OpenStack Cloud Crowbar 9 crowbar-core versions prior to 6.0+git.1582892022.cbd70e833-3.19.3, crowbar-.	2020-04-03	not yet calculated	<a href="#">CVE-2018-17954</a> <a href="#">CONFIRM</a>
suse -- opensuse_factory	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of exim in openSUSE Factory allows local attackers to escalate from user mail to root. This issue affects: openSUSE Factory exim versions prior to 4.93.0.4-3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8015</a> <a href="#">CONFIRM</a>
systemd -- systemd	A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.	2020-03-31	not yet calculated	<a href="#">CVE-2020-1712</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
testlink -- testlink	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in planUrgency.php via the urgency parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8638</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
testlink -- testlink	An unrestricted file upload vulnerability in keywordsImport.php in TestLink 1.9.20 allows remote attackers to execute arbitrary code by uploading a file with an executable extension. This allows an authenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to a publicly accessible directory of the application.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8639</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

testlink -- testlink	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in dragdroptreenodes.php via the node_id parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8637</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tp-link -- cloud_camera	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855.	2020-04-01	not yet calculated	<a href="#">CVE-2020-11445</a> <a href="#">MISC</a>
tp-link -- multiple_devices	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference.	2020-04-01	not yet calculated	<a href="#">CVE-2020-10231</a> <a href="#">MISC</a> <a href="#">MISC</a>
tp-link -- tl-wr841n_devices	A buffer overflow in the httpd daemon on TP-Link TL-WR841N V10 (firmware version 3.16.9) devices allows an authenticated remote attacker to execute arbitrary code via a GET request to the page for the configuration of the Wi-Fi network.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8423</a> <a href="#">MISC</a> <a href="#">MISC</a>
utils-extend -- utils-extend	Flaw in input validation in npm package utils-extend version 1.0.8 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using utils-extend.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8147</a> <a href="#">MISC</a>
viewvc -- viewvc	ViewVC before versions 1.1.28 and 1.2.1 has a XSS vulnerability in CVS show_subdir_lastmod support. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a CVS repository exposed by an otherwise trusted ViewVC instance that also has the `show_subdir_lastmod` feature enabled. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. This vulnerability is patched in versions 1.2.1 and 1.1.28.	2020-04-03	not yet calculated	<a href="#">CVE-2020-5283</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow a vulnerable ActiveX component to be exploited resulting in a buffer overflow,	2020-04-03	not yet calculated	<a href="#">CVE-2020-10599</a> <a href="#">MISC</a>



	which may lead to a denial-of-service condition and execution of arbitrary code.			
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow weak or insecure permissions on the VBASE directory resulting in elevation of privileges or malicious effects on the system the next time a privileged user runs the application.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7004 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow an unauthenticated attacker to discover the cryptographic key from the web server and gain information about the login and the encryption/decryption mechanism, which may be exploited to bypass authentication of the HTML5 HMI web interface.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7000 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow user input passed in the URL that is not properly verified before use, which may allow an attacker to read arbitrary files from local resources.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7008 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module allow weak hashing algorithm and insecure permissions which may allow a local attacker to bypass the password-protected mechanism through brute-force attacks, cracking techniques, or overwriting the password hash.	2020-04-03	not yet calculated	<a href="#">CVE-2020-10601 MISC</a>
wordpress -- wordpress	includes/theme-functions.php in the OneTone theme through 3.0.6 for WordPress allows unauthenticated options changes.	2020-04-03	not yet calculated	<a href="#">CVE-2019-17230 MISC</a>
wordpress -- wordpress	includes/theme-functions.php in the OneTone theme through 3.0.6 for WordPress has multiple stored XSS issues.	2020-04-03	not yet calculated	<a href="#">CVE-2019-17231 MISC</a>
xampp -- xampp	An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-contol.ini for all users (including admins) to enable arbitrary command execution.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11107 CONFIRM</a>
zevenet -- zen_load_balancer	Manage::Certificates in Zen Load Balancer 3.10.1 allows remote authenticated admins to execute arbitrary OS commands via shell metacharacters	2020-04-	not yet	<a href="#">CVE-2020-11490</a>

	in the index.cgi cert_issuer, cert_division, cert_organization, cert_locality, cert_state, cert_country, or cert_email parameter.	02	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
zoho -- manageengine_ad_sel	Zoho ManageEngine ADSelfService Plus before 5.8.15 allows unauthenticated remote code execution.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11518</a> <a href="#">MISC</a>
zoho -- manageengine_op_manager	In Zoho ManageEngine OpManager before 12.4.181, an unauthenticated remote attacker can send a specially crafted URI to read arbitrary files.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11527</a> <a href="#">MISC</a>
zoom -- client_for_meetings	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.	2020-04-03	not yet calculated	<a href="#">CVE-2020-11500</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [edigiovanna@sunnyvale.ca.gov](mailto:edigiovanna@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of March 30, 2020  
**Date:** Monday, April 06, 2020 2:26:03 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of March 30, 2020](#)

04/06/2020 07:33 AM EDT

Original release date: April 6, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accenture -- mercury	An XXE issue exists in Accenture Mercury before 1.12.28 because of the platformlambda/core/serializers/SimpleXmlParser.java component.	2020-03-27	7.5	<a href="#">CVE-2020-10990</a> <a href="#">MISC</a> <a href="#">MISC</a>
alienform2 -- alienform2	Jon Hedley AlienForm2 (typically installed as af.cgi or alienform.cgi) 2.0.2 is vulnerable to Remote Command Execution via eval injection, a different issue than CVE-2002-0934. An unauthenticated, remote attacker can exploit this via a series of crafted requests.	2020-04-01	10	<a href="#">CVE-2020-10948</a> <a href="#">MISC</a>
apache -- http_server	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.	2020-04-01	7.5	<a href="#">CVE-2020-1934</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
	A memory corruption issue was			

apple -- macos_catalina	addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.4. An application may be able to execute arbitrary code with system privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3903</a> <a href="#">MISC</a>
apple -- macos_catalina	Multiple issues were addressed by updating to version 8.1.1850. This issue is fixed in macOS Catalina 10.15.4. Multiple issues in Vim.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-9769</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to leak memory.	2020-04-01	<a href="#">10</a>	<a href="#">CVE-2020-3847</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3892</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3893</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3904</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-3849</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3905</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-3850</a> <a href="#">MISC</a>
	A memory corruption issue was			



apple -- macos_catalina_and_tvos_10.15.3_and_higher	addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3 and higher. An attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	7.5	<a href="#">CVE-2020-3848</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3911</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3910</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3909</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	9.3	<a href="#">CVE-2020-9785</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to execute arbitrary code with system privileges.	2020-04-01	9.3	<a href="#">CVE-2020-9768</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to	2020-04-01	9.3	<a href="#">CVE-2020-3919</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	execute arbitrary code with kernel privileges.			<a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3895</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3899</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3897</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to bypass intended access restrictions on tasks from an untrusted process, when Self Defense is enabled.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-10867</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
azkaban -- azkaban	Azkaban through 3.84.0 allows XXE, related to validator/XmlValidatorManager.java and user/XmlUserManager.java.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10992</a> <a href="#">MISC</a>
bubblewrap -- bubblewrap	Bubblewrap (bwrap) before version 0.4.1, if installed in setuid mode and the kernel supports unprivileged user namespaces, then the `bwrap --users2` option can be used to make the setuid process keep running as root while being traceable. This can in turn be used to gain root permissions. Note that this only affects the combination of bubblewrap in setuid mode (which is typically used when unprivileged user namespaces are not supported) and the support of unprivileged user namespaces. Known to	2020-03-31	<a href="#">8.5</a>	<a href="#">CVE-2020-5291</a> <a href="#">MISC</a>

	be affected are: * Debian testing/unstable, if unprivileged user namespaces enabled (not default) * Debian buster-backports, if unprivileged user namespaces enabled (not default) * Arch if using `linux-hardened`, if unprivileged user namespaces enabled (not default) * Centos 7 flatpak COPR, if unprivileged user namespaces enabled (not default) This has been fixed in the 0.4.1 release, and all affected users should update.			<a href="#">CONFIRM</a>
buildah -- buildah	A path traversal flaw was found in Buildah in versions before 1.14.5. This flaw allows an attacker to trick a user into building a malicious container image hosted on an HTTP(s) server and then write files to the user's system anywhere that the user has permissions.	2020-03-31	<a href="#">9.3</a>	<a href="#">CVE-2020-10696</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
cacagoo -- tv-288zd-2mp_devices	CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 has weak authentication of TELNET access, leading to root privileges without any password required.	2020-04-02	<a href="#">10</a>	<a href="#">CVE-2020-6852</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- emc_idrac_devices	Dell EMC iDRAC7, iDRAC8 and iDRAC9 versions prior to 2.65.65.65, 2.70.70.70, 4.00.00.00 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may exploit this vulnerability to crash the affected process or execute arbitrary code on the system by sending specially crafted input data.	2020-03-31	<a href="#">10</a>	<a href="#">CVE-2020-5344</a> <a href="#">MISC</a>
effect -- effect	effect through 1.0.4 is vulnerable to Command Injection. It allows execution of arbitrary command via the options argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7624</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- elasticsearch	Elasticsearch versions from 6.7.0 before 6.8.8 and 7.0.0 before 7.6.2 contain a privilege escalation flaw if an attacker is able to create API keys. An attacker who is able to generate an API key can perform a series of steps that result in an API key being generated with elevated privileges.	2020-03-31	<a href="#">7.5</a>	<a href="#">CVE-2020-7009</a> <a href="#">N/A</a> <a href="#">CONFIRM</a> <a href="#">N/A</a>
f5 -- nginx_controller	In NGINX Controller versions prior to 3.2.0, an unauthenticated attacker with network access to the Controller API can create unprivileged user accounts. The user which is created is only able to upload a new license to the system but cannot view or modify any other components of the system.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-5863</a> <a href="#">MISC</a>
	git-add-remote through 1.0.0 is vulnerable			<a href="#">CVE-2020-</a>

git-add-remote -- git-add-remote	to Command Injection. It allows execution of arbitrary commands via the name argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">7630 MISC MISC</a>
gitlab -- gitlab	GitLab 8.10 and later through 12.9 is vulnerable to an SSRF in a project import note feature.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10956 CONFIRM MISC</a>
hiproxy -- op-broswer	op-browser through 1.0.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the url function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7625 MISC MISC</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to execute arbitrary commands on the system in the context of root user, caused by improper validation of user-supplied input. IBM X-Force ID: 174966.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4206 XF CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174975.	2020-03-31	<a href="#">7.5</a>	<a href="#">CVE-2020-4208 XF CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175418.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4241 XF CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175419.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4242 XF CONFIRM</a>
install-package -- install-package	install-package through 0.4.0 is vulnerable to Command Injection. It allows execution of arbitrary commands via the options argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7629 MISC MISC</a>
install-package -- install-package	install-package through 1.1.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the device function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7628 MISC MISC</a>



karma-mojo -- karma-mojo	karma-mojo through 1.0.1 is vulnerable to Command Injection. It allows execution of arbitrary commands via the config argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7626</a> <a href="#">MISC</a> <a href="#">MISC</a>
ksh -- ksh	In ksh version 20120801, a flaw was found in the way it evaluates certain environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Services and applications that allow remote unauthenticated attackers to provide one of those environment variables could allow them to exploit this issue remotely.	2020-04-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14868</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
laminar_research -- x-plane	X-Plane before 11.41 allows Arbitrary Memory Write via crafted network packets, which could cause a denial of service or arbitrary code execution.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2019-19605</a> <a href="#">MISC</a>
laminar_research -- x-plane	X-Plane before 11.41 has multiple improper path validations that could allow reading and writing files from/to arbitrary paths (or a leak of OS credentials to a remote system) via crafted network packets. This could be used to execute arbitrary commands on the system.	2020-03-30	<a href="#">10</a>	<a href="#">CVE-2019-19606</a> <a href="#">MISC</a>
lenovo -- multiple_notebooks	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A buffer overflow vulnerability was reported, (fixed and publicly disclosed in 2015) in the Lenovo Service Engine (LSE), affecting various versions of BIOS for Lenovo Notebooks, that could allow a remote user to execute arbitrary code on the system.	2020-03-27	<a href="#">10</a>	<a href="#">CVE-2015-5684</a> <a href="#">MISC</a>
lenovo -- multiple_products	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type COMMAND type could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-7334</a> <a href="#">MISC</a>
lenovo -- multiple_products	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type INF and INF_BY_COMPATIBLE_ID	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-7333</a> <a href="#">MISC</a>

	command types could allow a user to execute arbitrary code with elevated privileges.			
lenovo -- solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-8534</a> <a href="#">MISC</a>
lenovo -- solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A directory traversal vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-8535</a> <a href="#">MISC</a>
march_networks -- command_client	The connection initiation process in March Networks Command Client before 2.7.2 allows remote attackers to execute arbitrary code via crafted XAML objects.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2019-9163</a> <a href="#">CONFIRM</a>
mongodb -- js-bson	All versions of bson before 1.1.4 are vulnerable to Deserialization of Untrusted Data. The package will ignore an unknown value for an object's _bsotype, leading to cases where an object is serialized as a document rather than the intended BSON type.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2020-7610</a> <a href="#">MISC</a>
mulesoft -- apikit	Mulesoft APIkit through 1.3.0 allows XXE because of validation/RestXmlSchemaValidator.java	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10991</a> <a href="#">MISC</a>
node-key-sender -- node-key-sender	node-key-sender through 1.0.11 is vulnerable to Command Injection. It allows execution of arbitrary commands via the 'arrParams' argument in the 'execute()' function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7627</a> <a href="#">MISC</a> <a href="#">MISC</a>
objectcomputing -- micronaut	All versions of io.micronaut:micronaut-http-client before 1.2.11 and all versions from 1.3.0 before 1.3.2 are vulnerable to HTTP Request Header Injection due to not validating request headers passed to the client.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2020-7611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
odata4j -- odata4j	odata4j 0.7.0 allows ExecuteJPQLQueryCommand.java SQL injection. NOTE: this product is apparently discontinued.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2016-11024</a> <a href="#">MISC</a>
odata4j -- odata4j	odata4j 0.7.0 allows ExecuteCountQueryCommand.java SQL injection. NOTE: this product is	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2016-11023</a> <a href="#">MISC</a>

	apparently discontinued.			
paessler -- prtg_network_monitor	A webserver component in Paessler PRTG Network Monitor 19.2.50 to PRTG 20.1.56 allows unauthenticated remote command execution via a crafted POST request or the what parameter of the screenshot function in the Contact Support form.	2020-03-30	7.5	<a href="#">CVE-2020-10374</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
pam-krb5 -- pam-krb5	pam-krb5 before 4.9 has a buffer overflow that might cause remote code execution in situations involving supplemental prompting by a Kerberos library. It may overflow a buffer provided by the underlying Kerberos library by a single ' ' byte if an attacker responds to a prompt with an answer of a carefully chosen length. The effect may range from heap corruption to stack corruption depending on the structure of the underlying Kerberos library, with unknown effects but possibly including code execution. This code path is not used for normal authentication, but only when the Kerberos library does supplemental prompting, such as with PKINIT or when using the non-standard no_prompt PAM configuration option.	2020-03-31	7.5	<a href="#">CVE-2020-10595</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows Remote Code Execution.	2020-04-01	9	<a href="#">CVE-2020-10204</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows JavaEL Injection (issue 1 of 2).	2020-04-01	9	<a href="#">CVE-2020-10199</a> <a href="#">CONFIRM</a>
unisocon -- ultralog_express	UltraLog Express device management interface does not properly filter user inputted string in some specific parameters, attackers can inject arbitrary SQL command.	2020-03-27	7.5	<a href="#">CVE-2020-3936</a> <a href="#">MISC</a>
university_of_southern_california -- innovation_in_integrated_informatics_lab_cereal	An issue was discovered in USC iLab cereal through 1.3.0. It employs caching of std::shared_ptr values, using the raw pointer address as a unique identifier. This becomes problematic if an std::shared_ptr variable goes out of scope and is freed, and a new std::shared_ptr is allocated at the same address. Serialization fidelity thereby becomes dependent upon memory layout. In short, serialized std::shared_ptr variables cannot always be expected to serialize back into their original values. This can have any number of consequences,	2020-03-30	7.5	<a href="#">CVE-2020-11105</a> <a href="#">MISC</a>

	depending on the context within which this manifests.			
vertiv -- avocent_umg-400_devices	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to command injection because the application incorrectly neutralizes code syntax before executing. Since all commands within the web application are executed as root, this could allow a remote attacker authenticated with an administrator account to execute arbitrary commands as root.	2020-03-30	9	<a href="#">CVE-2019-9507</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. It has numerous fields that can contain data that is pulled from different sources. One issue with this is that the data isn't sanitized, and no input validation is performed, before the exporting of the user data. This can lead to (at least) CSV injection if a crafted Excel document is uploaded.	2020-04-01	7.5	<a href="#">CVE-2020-7947</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	LearnDash Wordpress plugin version below 3.1.6 is vulnerable to Unauthenticated SQL Injection.	2020-04-01	7.5	<a href="#">CVE-2020-6009</a> <a href="#">MISC</a>
wordpress -- wordpress	LifterLMS Wordpress plugin version below 3.37.15 is vulnerable to arbitrary file write leading to remote code execution	2020-03-31	7.5	<a href="#">CVE-2020-6008</a> <a href="#">MISC</a>
yamaha -- multiple_products	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors.	2020-04-01	7.8	<a href="#">CVE-2020-5548</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoom -- client_for_meetings	Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process	2020-04-01	7.2	<a href="#">CVE-2020-11469</a> <a href="#">MISC</a>



	(with the user's privileges) to obtain root access by replacing runwithroot.			<a href="#">MISC</a>
--	--	--	--	----------------------

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.3, the X-Content-Type-Options Header is missing in the HTTP response, potentially causing the response body to be interpreted and displayed as different content type other than declared. A possible attack scenario would be unauthorized code execution via text interpreted as JavaScript.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19089</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the X-Frame-Options header is not configured in HTTP response. This can potentially allow 'ClickJacking' attacks where an attacker can frame parts of the application on a malicious web site, revealing sensitive user information such as authentication credentials.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19001</a> <a href="#">CONFIRM</a>
abb -- esoms	Lack of input checks for SQL queries in ABB eSOMS versions 3.9 to 6.0.3 might allow an attacker SQL injection attacks against the backend database.	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2019-19094</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the HTTPOnly flag is not set. This can allow Javascript to access the cookie contents, which in turn might enable Cross Site Scripting.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19003</a> <a href="#">CONFIRM</a>
abb -- esoms	ABB eSOMS versions 4.0 to 6.0.3 accept connections using medium strength ciphers. If a connection is enabled using such a cipher, an attacker might be able to eavesdrop and/or intercept the connection.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19097</a> <a href="#">CONFIRM</a>
abb -- esoms	eSOMS versions 4.0 to 6.0.3 do not enforce password complexity settings, potentially resulting in lower access security due to insecure user passwords.	2020-04-02	<a href="#">6.4</a>	<a href="#">CVE-2019-19093</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS 4.0 to 6.0.3, the Cache-Control and Pragma HTTP header(s) have not been properly configured within the application response. This can potentially allow browsers and proxies to	2020-04-02	<a href="#">6.4</a>	<a href="#">CVE-2019-19000</a> <a href="#">CONFIRM</a>

	cache sensitive information.			
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.3, HTTPS responses contain comments with sensitive information about the application. An attacker might use this detail information to specifically craft the attack.	2020-04-02	<a href="#">4</a>	<a href="#">CVE-2019-19091</a> <a href="#">CONFIRM</a>
advantech -- webaccess	In Advantech WebAccess, Versions 8.4.2 and prior. A stack-based buffer overflow vulnerability caused by a lack of proper validation of the length of user-supplied data may allow remote code execution.	2020-03-27	<a href="#">6.5</a>	<a href="#">CVE-2020-10607</a> <a href="#">MISC</a>
advantech -- webaccess	Advantech WebAccess 8.3.4 does not properly restrict an RPC call that allows unauthenticated, remote users to read files. An attacker can use this vulnerability to recover the administrator password.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2019-3942</a> <a href="#">MISC</a>
apache -- dubbo	Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. This issue affected Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.x versions.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2019-17564</a> <a href="#">MISC</a>
apache -- http_server	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.	2020-04-02	<a href="#">5.8</a>	<a href="#">CVE-2020-1927</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apache -- netbeans	The "Apache NetBeans" autoupdate system does not validate SSL certificates and hostnames for https based downloads. This allows an attacker to intercept downloads of autoupdates and modify the download, potentially injecting malicious code. "Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	2020-03-30	<a href="#">6.4</a>	<a href="#">CVE-2019-17560</a> <a href="#">MISC</a>
apache -- netbeans	The "Apache NetBeans" autoupdate system does not fully validate code signatures. An attacker could modify the downloaded nbm and include additional code. "Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2019-17561</a> <a href="#">MISC</a>
apache -- offbiz	Data sent with contentId to /control/stream is not sanitized, allowing	2020-04-	<a href="#">4.3</a>	<a href="#">CVE-2020-1943</a>

	XSS attacks in Apache OFBiz 16.11.01 to 16.11.07.	01		<a href="#">MISC</a>
apache -- sling_cms	Scripts in Sling CMS before 0.16.0 do not properly escape the Sling Selector from URLs when generating navigational elements for the administrative consoles and are vulnerable to reflected XSS attacks.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-1949</a> <a href="#">MISC</a>
apache -- solr	In Apache Solr, the cluster can be partitioned into multiple collections and only a subset of nodes actually host any given collection. However, if a node receives a request for a collection it does not host, it proxies the request to a relevant node and serves the request. Solr bypasses all authorization settings for such requests. This affects all Solr versions prior to 7.7 that use the default authorization mechanism of Solr (RuleBasedAuthorizationPlugin).	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2018-11802</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4. An attacker in a privileged network position may be able to intercept Bluetooth traffic.	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2020-9770</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the selection of video file by Mail. The issue was fixed by selecting the latest version of a video. This issue is fixed in iOS 13.4 and iPadOS 13.4. Cropped videos may not be shared properly via Mail.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9777</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4. A maliciously crafted page may interfere with other web contexts.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3888</a> <a href="#">MISC</a>
apple -- ios_and_ipados	The issue was addressed by clearing website permission prompts after navigation. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user may grant website permissions to a site they didn't intend to.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9781</a> <a href="#">MISC</a>
apple -- ios_and_ipados	The issue was addressed with improved deletion. This issue is fixed in iOS 13.4 and iPadOS 13.4. Deleted messages groups may still be suggested as an autocompletion.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-3890</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the handling of tabs displaying picture in picture video. The issue was corrected with improved state handling. This issue is fixed in iOS 13.4	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9775</a>

	and iPadOS 13.4. A user's private browsing activity may be unexpectedly saved in Screen Time.			MISC
apple -- macos_catalina	This issue was addressed with a new entitlement. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to access a user's call history.	2020-04-01	4.3	<a href="#">CVE-2020-9776</a> MISC
apple -- macos_high_sierra_and_catalina	An injection issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A remote attacker may be able to cause arbitrary javascript code execution.	2020-04-01	4.3	<a href="#">CVE-2020-3884</a> MISC
apple -- macos_mojave_and_catalina	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.4. A maliciously crafted application may be able to bypass code signing enforcement.	2020-04-01	6.8	<a href="#">CVE-2020-3906</a> MISC
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	6.6	<a href="#">CVE-2020-3908</a> MISC
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	6.6	<a href="#">CVE-2020-3912</a> MISC
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	6.6	<a href="#">CVE-2020-3907</a> MISC
apple -- multiple_devices	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution.	2020-04-01	6.8	<a href="#">CVE-2020-9783</a> MISC MISC MISC MISC MISC
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to read restricted memory.	2020-04-01	4.3	<a href="#">CVE-2020-3914</a> MISC MISC MISC MISC



apple -- multiple_products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A download's origin may be incorrectly associated.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3887</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	The issue was addressed with improved handling of icon caches. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to identify what other applications a user has installed.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-9773</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A permissions issue existed. This issue was addressed with improved permission validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, watchOS 6.2. A malicious application may be able to elevate privileges.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-3913</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to a cross site scripting attack.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3902</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-3900</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. Setting an alternate app icon may disclose a photo without needing permission to access photos.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-3916</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-3901</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	7.18. Processing maliciously crafted web content may lead to arbitrary code execution.			<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- safari	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1. A malicious iframe may use another website's download settings.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-9784</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to make arbitrary changes to the Components section of the Stats.ini file via RPC from a Low Integrity process.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10865</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Arbitrary File Deletion from Avast Program Path via RPC, when Self Defense is Enabled.	2020-04-01	<a href="#">6.4</a>	<a href="#">CVE-2020-10861</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to launch the Repair App RPC call from a Low Integrity process.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. An Arbitrary Memory Address Overwrite vulnerability in the aswAvLog Log Library results in Denial of Service of the Avast Service (AvastSvc.exe).	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10860</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a shutdown via RPC from a Low Integrity process via TempShutDownMachine.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Local Privilege Escalation (LPE) via RPC.	2020-04-01	<a href="#">4.6</a>	<a href="#">CVE-2020-10862</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a reboot via RPC from	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10864</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	a Low Integrity process.			
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to enumerate the network interfaces and access points from a Low Integrity process via RPC.	2020-04-01	5	<a href="#">CVE-2020-10866</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacagoo -- cloud_storage_intelligent_camera_tv_288zd-2mp	The CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 allows access to the RTSP service without a password.	2020-04-02	5	<a href="#">CVE-2020-9349</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/people endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve sensitive information about all users registered on the system. This includes their full name, privilege, email address, phone number, etc.	2020-04-01	4	<a href="#">CVE-2020-11464</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/tickets endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve arbitrary information about all helpdesk tickets stored in database with numerous filters. This leaked sensitive information to unauthorized parties. Additionally, it leaked ticket authentication code, making it possible to make changes to a ticket.	2020-04-01	4	<a href="#">CVE-2020-11466</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/email_accounts endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve cleartext credentials of all helpdesk email accounts, including incoming and outgoing email credentials. This enables an attacker to get full access to all emails sent or received by the system including password reset emails, making it possible to reset any user's password.	2020-04-01	5	<a href="#">CVE-2020-11463</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/apps/* endpoints failed to properly validate a user's privilege, allowing an attacker to control/install helpdesk applications and leak current applications' configurations, including applications used as user sources (used for authentication). This enables an attacker to forge valid authentication models that resembles any	2020-04-01	6.5	<a href="#">CVE-2020-11465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	user on the system.			
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. This product enables administrators to modify the helpdesk interface by editing /portal/api/style/edit-theme-set/template-sources theme templates, and uses TWIG as its template engine. While direct access to self and _self variables was not permitted, one could abuse the accessible variables in one's context to reach a native unserialize function via the code parameter. There, one could pass a crafted payload to trigger a set of POP gadgets in order to achieve remote code execution.	2020-04-01	<a href="#">6.5</a>	<a href="#">CVE-2020-11467</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5859</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5857</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.2, under certain conditions, TMM may crash or stop processing new traffic with the DPDK/ENA driver on AWS systems while sending traffic. This issue does not affect any other platforms, hardware or virtual, or any other cloud provider since the affected driver is specific to AWS.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5862</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 12.1.0-12.1.5, the TMM process may produce a core file in some cases when Ram Cache incorrectly optimizes stored data resulting in memory errors.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-5861</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.2, 14.1.0-14.1.2.2, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, users with non-administrator roles (for example, Guest or Resource Administrator) with tmsh shell access can execute arbitrary commands with elevated privilege via a crafted tmsh command.	2020-03-27	<a href="#">4.6</a>	<a href="#">CVE-2020-5858</a> <a href="#">MISC</a>
f5 -- big-ip_and_big-iq	On BIG-IP 15.0.0-15.1.0.2, 14.1.0-14.1.2.3, 13.1.0-13.1.3.2, 12.1.0-12.1.5.1, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, in a High Availability (HA) network failover in Device Service Cluster (DSC), the failover service does not require a strong form of	2020-03-27	<a href="#">6.8</a>	<a href="#">CVE-2020-5860</a> <a href="#">MISC</a>



	authentication and HA network failover traffic is not encrypted by Transport Layer Security (TLS).			
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.activemq.* (aka activemq-jms, activemq-core, activemq-pool, and activemq-pool-jms).	2020-03-31	6.8	<a href="#">CVE-2020-11111</a> MISC MISC CONFIRM
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.openjpa.ee.WASRegistryManagedRuntime (aka openjpa).	2020-03-31	6.8	<a href="#">CVE-2020-11113</a> MISC MISC CONFIRM
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.proxy.provider.remoting.RmiProvider (aka apache/commons-proxy).	2020-03-31	6.8	<a href="#">CVE-2020-11112</a> MISC MISC CONFIRM
fortinet -- fortios	An external control of system vulnerability in FortiOS may allow an authenticated, regular user to change the routing settings of the device via connecting to the ZebOS component.	2020-04-02	6.5	<a href="#">CVE-2018-13371</a> MISC
gitlab -- gitlab	GitLab through 12.9 is affected by a potential DoS in repository archive download.	2020-03-27	5	<a href="#">CVE-2020-10954</a> CONFIRM MISC
gitlab -- gitlab_community_and_enterprise_editions	GitLab EE/CE 8.11 through 12.9.1 allows blocked users to pull/push docker images.	2020-03-27	5.8	<a href="#">CVE-2020-10952</a> CONFIRM MISC
gitlab -- gitlab_community_and_enterprise_editions	GitLab EE/CE 11.1 through 12.9 is vulnerable to parameter tampering on an upload feature that allows an unauthorized user to read content available under specific folders.	2020-03-27	4	<a href="#">CVE-2020-10955</a> CONFIRM MISC
gitlab -- gitlab_enterprise_edition	In GitLab EE 11.7 through 12.9, the NPM feature is vulnerable to a path traversal issue.	2020-03-27	5	<a href="#">CVE-2020-10953</a> CONFIRM MISC
grandstream -- ucm6200_series_devices	The UCM6200 series 1.0.20.22 and below stores unencrypted user passwords in an SQLite database. This could allow an attacker to retrieve all passwords and possibly gain elevated privileges.	2020-03-30	5	<a href="#">CVE-2020-5723</a> CONFIRM
	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL			

grandstream -- ucm6200_series_devices	injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the login action with a crafted username and, through the use of timing attacks, can discover user passwords.	2020-03-30	<a href="#">4.3</a>	<a href="#">CVE-2020-5725</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grandstream -- ucm6200_series_devices	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-5726</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grandstream -- ucm6200_series_devices	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-5724</a> <a href="#">CONFIRM</a>
gststreamer -- gst-rtsp-server	An exploitable denial of service vulnerability exists in the GstRTSPAuth functionality of GStreamer/gst-rtsp-server 1.14.5. A specially crafted RTSP setup request can cause a null pointer deference resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-6095</a> <a href="#">MISC</a> <a href="#">MISC</a>
haproxy -- haproxy	In hpack_dht_insert in hpack-tbl.c in the HPACK decoder in HAProxy 1.8 through 2.x before 2.1.4, a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing remote code execution.	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2020-11100</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
huawei -- multiple_smartax_devices	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include: SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800	2020-04-02	<a href="#">5.2</a>	<a href="#">CVE-2020-9067</a> <a href="#">CONFIRM</a>

	versions V100R018C00, V100R018C10, V100R019C10.			
ibm -- process_federation_server	The IBM Process Federation Server 18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, and 19.0.0.3 Global Teams REST API does not properly shutdown the thread pools that it creates to retrieve Global Teams information from the federated systems. As a consequence, the Java Virtual Machine can't recover the memory used by those thread pools, which leads to an OutOfMemory exception when the Process Federation Server Global Teams REST API is used extensively. IBM X-Force ID: 177596.	2020-04-02	4	<a href="#">CVE-2020-4325</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request to overwrite or create arbitrary files on the system. IBM X-Force ID: 175417.	2020-03-31	6.4	<a href="#">CVE-2020-4240</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to arbitrary delete a directory caused by improper validation of user-supplied input. IBM X-Force ID: 175026.	2020-03-31	6.4	<a href="#">CVE-2020-4214</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 175412.	2020-03-31	5	<a href="#">CVE-2020-4239</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175411.	2020-03-31	6.8	<a href="#">CVE-2020-4238</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175410.	2020-03-31	6.8	<a href="#">CVE-2020-4237</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 could allow an authenticated user to cause a denial of service due to improper content parsing in the project	2020-03-31	4	<a href="#">CVE-2020-4236</a> <a href="#">XE</a>

	management module. IBM X-Force ID: 175409.			<a href="#">CONFIRM</a>
ibm -- websphere_application_server --liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 20.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176670.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2020-4304</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server --liberty	IBM WebSphere Application Server - Liberty 17.0.0.3 through 20.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176668.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2020-4303</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intland_software -- codebeamer	codeBeamer before 9.5.0-RC3 does not properly restrict the ability to execute custom Java code and access the Java class loader via computed fields.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20635</a> <a href="#">MISC</a>
kubernetes -- api_server	The Kubernetes API server component in versions prior to 1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via successful API requests.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-8552</a> <a href="#">MISC</a> <a href="#">MISC</a>
kubernetes -- api_server	The Kubernetes API Server component in versions 1.1-1.14, and versions prior to 1.15.10, 1.16.7 and 1.17.3 allows an authorized user who sends malicious YAML payloads to cause the kube-apiserver to consume excessive CPU cycles while parsing YAML.	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2019-11254</a> <a href="#">MISC</a> <a href="#">MISC</a>
leantime -- leantime	Leantime before versions 2.0.15 and 2.1-beta3 has a SQL Injection vulnerability. The impact is high. Malicious users/attackers can execute arbitrary SQL queries negatively affecting the confidentiality, integrity, and availability of the site. Attackers can exfiltrate data like the users' and administrators' password hashes, modify data, or drop tables. The unescaped parameter is "searchUsers" when sending a POST request to "/tickets/showKanban" with a valid session. In the code, the parameter is named "users" in class.tickets.php. This issue is fixed in versions 2.0.15 and 2.1.0 beta 3.	2020-03-31	<a href="#">6.5</a>	<a href="#">CVE-2020-5292</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



lenovo -- lenovo_solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow cross-site request forgery.	2020-03-27	<a href="#">6.8</a>	<a href="#">CVE-2015-8536</a> <a href="#">MISC</a>
lenovo -- multiple_devices	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A race condition was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">6.9</a>	<a href="#">CVE-2015-7335</a> <a href="#">MISC</a>
lenovo -- multiple_devices	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow the signature check of an update to be bypassed.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2015-7336</a> <a href="#">MISC</a>
limesurvey -- limesurvey	LimeSurvey before 4.1.12+200324 contains a path traversal vulnerability in application/controllers/admin/LimeSurveyFileManager.php.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-11455</a> <a href="#">MISC</a>
limesurvey -- limesurvey	LimeSurvey before 4.1.12+200324 has stored XSS in application/views/admin/surveysgroups/surveySettings.php and application/models/SurveysGroups.php (aka survey groups).	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-11456</a> <a href="#">MISC</a>
microstrategy -- web_services	The Upload Visualization plugin in the Microstrategy Web 10.4 admin panel allows an administrator to upload a ZIP archive containing files with arbitrary extensions and data. (This is also exploitable via SSRF.)	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2020-11451</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy -- web_services	Microstrategy Web 10.4 is vulnerable to Server-Side Request Forgery in the Test Web Service functionality exposed through the path /MicroStrategyWS/. The functionality requires no authentication and, while it is not possible to pass parameters in the SSRF request, it is still possible to exploit it to conduct port scanning. An attacker could exploit this vulnerability to enumerate the resources allocated in the network (IP addresses and services exposed).	2020-04-02	<a href="#">5</a>	<a href="#">CVE-2020-11453</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy --	Microstrategy Web 10.4 exposes the JVM configuration, CPU architecture, installation folder, and other information			<a href="#">CVE-2020-11450</a>

web_services	through the URL /MicroStrategyWS/happyaxis.jsp. An attacker could use this vulnerability to learn more about the environment the application is running in.	2020-04-02	5	MISC <a href="#">FULLDISC</a> MISC <a href="#">MISC</a>
microstrategy -- web_services	Microstrategy Web 10.4 includes functionality to allow users to import files or data from external resources such as URLs or databases. By providing an external URL under attacker control, it's possible to send requests to external resources (aka SSRF) or leak files from the local system using the file:// stream wrapper.	2020-04-02	4	<a href="#">CVE-2020-11452</a> MISC <a href="#">FULLDISC</a> MISC <a href="#">MISC</a>
misp_project -- misp	app/Model/feed.php in MISP before 2.4.124 allows administrators to choose arbitrary files that should be ingested by MISP. This does not cause a leak of the full contents of a file, but does cause a leaks of strings that match certain patterns. Among the data that can leak are passwords from database.php or GPG key passphrases from config.php.	2020-04-02	4	<a href="#">CVE-2020-11458</a> MISC <a href="#">MISC</a>
mongodb -- js-bson	Incorrect parsing of certain JSON input may result in js-bson not correctly serializing BSON. This may cause unexpected application behaviour including data disclosure.	2020-03-31	5.5	<a href="#">CVE-2019-2391</a> <a href="#">CONFIRM</a>
moodle -- moodle	A vulnerability was found in Moodle versions 3.7 before 3.7.3, 3.6 before 3.6.7, 3.5 before 3.5.9 and earlier. OAuth 2 providers who do not verify users' email address changes require additional verification during sign-up to reduce the risk of account compromise.	2020-03-31	6.4	<a href="#">CVE-2019-14880</a> <a href="#">CONFIRM</a> MISC
open_source_social_network -- open_source_social_network	An issue was discovered in Open Source Social Network (OSSN) through 5.3. A user-controlled file path with a weak cryptographic rand() can be used to read any file with the permissions of the webserver. This can lead to further compromise. The attacker must conduct a brute-force attack against the SiteKey to insert into a crafted URL for components/OssnComments/ossn_com.php and/or libraries/ossn.lib.upgrade.php.	2020-03-30	4.3	<a href="#">CVE-2020-10560</a> MISC <a href="#">MISC</a>
osmand -- osmand	Osmand through 2.0.0 allow XXE because of binary/BinaryMapIndexReader.java.	2020-03-27	6.4	<a href="#">CVE-2020-10993</a> <a href="#">MISC</a>
	An attacker with the ability to generate session IDs or password reset tokens, either by being able to authenticate or by			

otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	exploiting OSA-2020-09, may be able to predict other users session IDs, password hashes and automatically generate passwords. This issue affects ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	5.5	<a href="#">CVE-2020-1773</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	In the login screens (in agent and customer interface), Username and Password fields use autocomplete, which might be considered as security issue. This issue affects ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	4	<a href="#">CVE-2020-1769</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	It's possible to craft Lost Password requests with wildcards in the Token value, which allows attacker to retrieve valid Token(s), generated by users which already requested new passwords. This issue affects: ((OTRS)) Community Edition 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	5	<a href="#">CVE-2020-1772</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_tokens_and_authentication_system_community_comr27	Support bundle generated files could contain sensitive information that might be unwanted to be disclosed. This issue affects: ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	4	<a href="#">CVE-2020-1770</a> <a href="#">MISC</a>
phoenix_contact -- pc_worx_srt	Insecure, default path permissions in PHOENIX CONTACT PC WORX SRT through 1.14 allow for local privilege escalation.	2020-03-27	4.6	<a href="#">CVE-2020-10939</a> <a href="#">CONFIRM</a>
phoenix_contact -- portico_server	Local Privilege Escalation can occur in PHOENIX CONTACT PORTICO SERVER through 3.0.7 when installed to run as a service.	2020-03-27	4.6	<a href="#">CVE-2020-10940</a> <a href="#">CONFIRM</a>
php -- php	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.	2020-04-01	5.8	<a href="#">CVE-2020-7064</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
php -- php	In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using mb_strtolower() function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated	2020-04-01	6.8	<a href="#">CVE-2020-7065</a> <a href="#">MISC</a>

	buffer. This could lead to memory corruption, crashes and potentially code execution.			<a href="#">CONFIRM</a>
php -- php	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using get_headers() with user-supplied URL, if the URL contains zero ( ) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-7066</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
progress_software -- telerik_ui_for_silverlight	An issue was discovered in Progress Telerik UI for Silverlight before 2020.1.330. The RadUploadHandler class in RadUpload for Silverlight expects a web request that provides the file location of the uploading file along with a few other parameters. The uploading file location should be inside the directory where the upload handler class is defined. Before 2020.1.330, a crafted web request could result in uploads to arbitrary locations.	2020-03-31	<a href="#">5</a>	<a href="#">CVE-2020-11414</a> <a href="#">MISC</a>
proofpoint -- email_protection	An issue was discovered in Proofpoint Email Protection through 2019-09-08. By collecting scores from Proofpoint email headers, it is possible to build a copy-cat Machine Learning Classification model and extract insights from this model. The insights gathered allow an attacker to craft emails that receive preferable scores, with a goal of delivering malicious emails.	2020-03-30	<a href="#">6.4</a>	<a href="#">CVE-2019-20634</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible_engine	A vulnerability was found in Ansible Engine versions 2.9.x before 2.9.3, 2.8.x before 2.8.8, 2.7.x before 2.7.16 and earlier, where in Ansible's nxos_file_copy module can be used to copy files to a flash or bootflash on NXOS devices. Malicious code could craft the filename parameter to perform OS command injections. This could result in a loss of confidentiality of the system among other issues.	2020-03-31	<a href="#">4.6</a>	<a href="#">CVE-2019-14905</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a>
red_hat -- openshift/apb-base	An insecure modification vulnerability in the /etc/passwd file was found in the container openshift/apb-base, affecting versions before the following 4.3.5, 4.2.21, 4.1.37, and 3.11.188-4. An attacker with access to the container	2020-04-02	<a href="#">4.4</a>	<a href="#">CVE-2019-19348</a> <a href="#">CONFIRM</a>



	could use this flaw to modify /etc/passwd and escalate their privileges.			
red_hat -- openshift/mariadb-apb	An insecure modification vulnerability in the /etc/passwd file was found in the container openshift/mariadb-apb, affecting versions before the following 4.3.5, 4.2.21, 4.1.37, and 3.11.188-4 . An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	2020-04-02	<a href="#">4.4</a>	<a href="#">CVE-2019-19346</a> <a href="#">CONFIRM</a>
redpwn -- redpwnctf	In RedpwnCTF before version 2.3, there is a session fixation vulnerability in exploitable through the `#token=\$ssid` hash when making a request to the `/verify` endpoint. An attacker team could potentially steal flags by, for example, exploiting a stored XSS payload in a CTF challenge so that victim teams who solve the challenge are unknowingly (and against their will) signed into the attacker team's account. Then, the attacker can gain points / value off the backs of the victims. This is patched in version 2.3.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-5290</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
responsive_filemanager -- responsive_filemanager	An issue was discovered in Responsive Filemanager through 9.14.0. In the dialog.php page, the session variable \$_SESSION['RF']['view_type'] wasn't sanitized if it was already set. This made stored XSS possible if one opens ajax_calls.php and uses the "view" action and places a payload in the type parameter, and then returns to the dialog.php page. This occurs because ajax_calls.php was also able to set the \$_SESSION['RF']['view_type'] variable, but there it wasn't sanitized.	2020-03-30	<a href="#">4.3</a>	<a href="#">CVE-2020-11106</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, improperly stores system files. Attackers can use a specific URL and capture confidential information.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-10508</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, contains vulnerability of Cross-Site Scripting (XSS), attackers can inject arbitrary command into the system and launch XSS attack.	2020-03-27	<a href="#">4.3</a>	<a href="#">CVE-2020-10509</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, contains a vulnerability of Broken Access Control. After login, attackers can use a specific URL, access unauthorized	2020-03-27	<a href="#">4</a>	<a href="#">CVE-2020-10510</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	functionality and data.			
symfony -- symfony	In Symfony before versions 4.4.7 and 5.0.7, when a `Response` does not contain a `Content-Type` header, affected versions of Symfony can fallback to the format defined in the `Accept` header of the request, leading to a possible mismatch between the response's content and `Content-Type` header. When the response is cached, this can prevent the use of the website by other users. This has been patched in versions 4.4.7 and 5.0.7.	2020-03-30	4	<a href="#">CVE-2020-5255</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
symfony -- symfony	In symfony/security-http before versions 4.4.7 and 5.0.7, when a `Firewall` checks access control rule, it iterate overs each rule's attributes and stops as soon as the accessDecisionManager decides to grant access on the attribute, preventing the check of next attributes that should have been take into account in an unanimous strategy. The accessDecisionManager is now called with all attributes at once, allowing the unanimous strategy being applied on each attribute. This issue is patched in versions 4.4.7 and 5.0.7.	2020-03-30	5.5	<a href="#">CVE-2020-5275</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
symfony -- symfony	In Symfony before versions 5.0.5 and 4.4.5, some properties of the Exception were not properly escaped when the `ErrorHandler` rendered it stacktrace. In addition, the stacktrace were displayed even in a non-debug configuration. The ErrorHandler now escape all properties of the exception, and the stacktrace is only display in debug configuration. This issue is patched in symfony/http-foundation versions 4.4.5 and 5.0.5	2020-03-30	5.5	<a href="#">CVE-2020-5274</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
technicolor -- tc7337_devices	An issue was discovered on Technicolor TC7337 8.89.17 devices. An attacker can discover admin credentials in the backup file, aka backupsettings.conf.	2020-04-01	5	<a href="#">CVE-2020-11449</a> <a href="#">MISC</a>
tikiwiki -- groupware_and_cms	There is an Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in php webpages of Tiki-Wiki Groupware. Tiki-Wiki CMS all versions through 20.0 allows malicious users to cause the injection of malicious code fragments (scripts) into a legitimate web page.	2020-04-01	4.3	<a href="#">CVE-2020-8966</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
totemo -- totemomail	An insecure direct object reference in webmail in totemo totemomail 7.0.0 allows an authenticated remote user to	2020-03-27	5.5	<a href="#">CVE-2020-7918</a> <a href="#">MISC</a>

	read and modify mail folder names of other users via enumeration.			<a href="#">MISC</a>
toyota -- model_year_2017_display_control_unit	Toyota 2017 Model Year DCU (Display Control Unit) allows an unauthenticated attacker within Bluetooth range to cause a denial of service attack and/or execute an arbitrary command. The affected DCUs are installed in Lexus (LC, LS, NX, RC, RC F), TOYOTA CAMRY, and TOYOTA SIENNA manufactured in the regions other than Japan from Oct. 2016 to Oct. 2019. An attacker with certain knowledge on the target vehicle control system may be able to send some diagnostic commands to ECUs with some limited availability impacts; the vendor states critical vehicle controls such as driving, turning, and stopping are not affected.	2020-03-30	<a href="#">5.4</a>	<a href="#">CVE-2020-5551</a> <a href="#">MISC</a> <a href="#">MISC</a>
ubiquiti -- unifi_video_controller	The UniFi Video Server (Windows) web interface configuration restore functionality at the “backup” and “wizard” endpoints does not implement sufficient privilege checks. Low privileged users, belonging to the PUBLIC_GROUP or CUSTOM_GROUP groups, can access these endpoints and overwrite the current application configuration. This can be abused for various purposes, including adding new administrative users. Affected Products: UniFi Video Controller v3.9.3 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.9.6 and newer.	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2020-8145</a> <a href="#">CONFIRM</a>
ubiquiti -- unifi_video_controller	In UniFi Video v3.10.1 (for Windows 7/8/10 x64) there is a Local Privileges Escalation to SYSTEM from arbitrary file deletion and DLL hijack vulnerabilities. The issue was fixed by adjusting the .tsExport folder when the controller is running on Windows and adjusting the SafeDllSearchMode in the windows registry when installing UniFi-Video controller. Affected Products: UniFi Video Controller v3.10.2 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.10.3 and newer.	2020-04-01	<a href="#">6.9</a>	<a href="#">CVE-2020-8146</a> <a href="#">CONFIRM</a>
ubiquiti --	The UniFi Video Server v3.9.3 and prior (for Windows 7/8/10 x64) web interface Firmware Update functionality, under certain circumstances, does not validate firmware download destinations to ensure they are within the intended destination directory tree. It accepts a request with a	2020-04-		<a href="#">CVE-2020-</a>

unifi_video_controller	URL to firmware update information. If the version field contains ..\ character sequences, the destination file path to save the firmware can be manipulated to be outside the intended destination directory tree. Fixed in UniFi Video Controller v3.10.3 and newer.	01	<a href="#">5.2</a>	<a href="#">8144</a> <a href="#">CONFIRM</a>
unisoan -- ultralog_express	UltraLog Express device management software stores user's information in cleartext. Any user can obtain accounts information through a specific page.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2020-3921</a> <a href="#">MISC</a>
unisoan -- ultralog_express	UltraLog Express device management interface does not properly perform access authentication in some specific pages/functions. Any user can access the privileged page to manage accounts through specific system directory.	2020-03-27	<a href="#">5.5</a>	<a href="#">CVE-2020-3920</a> <a href="#">MISC</a>
university_of_southern_california -- innovation_in_integrated_informatics_lab_cereal	An issue was discovered in USC iLab cereal through 1.3.0. Serialization of an (initialized) C/C++ long double variable into a BinaryArchive or PortableBinaryArchive leaks several bytes of stack or heap memory, from which sensitive information (such as memory layout or private keys) can be gleaned if the archive is distributed outside of a trusted context.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-11104</a> <a href="#">MISC</a>
vertiv -- avocent_universal_management_gateway	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to stored XSS. A remote attacker authenticated with an administrator account could store a maliciously named file within the web application that would execute each time a user browsed to the page.	2020-03-30	<a href="#">6</a>	<a href="#">CVE-2019-9508</a> <a href="#">MISC</a> <a href="#">MISC</a>
vertiv -- avocent_universal_management_gateway	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to reflected XSS in an HTTP POST parameter. The web application does not sanitize user-controllable input before displaying to users in a web page, which could allow a remote attacker authenticated with a user account to execute arbitrary code.	2020-03-30	<a href="#">6.5</a>	<a href="#">CVE-2019-9509</a> <a href="#">MISC</a> <a href="#">MISC</a>
weberp -- weberp	In webERP 4.15, the Import Bank Transactions function fails to sanitize the content of imported MT940 bank statement files, resulting in the execution of arbitrary SQL queries, aka SQL Injection.	2020-03-30	<a href="#">6.5</a>	<a href="#">CVE-2019-7755</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A stored cross-site scripting (XSS)			<a href="#">CVE-2020-</a>



wordpress -- wordpress	vulnerability exists in the Auth0 plugin before 4.0.0 for WordPress via the settings page.	2020-04-01	<a href="#">4.3</a>	<a href="#">5392</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The custom-searchable-data-entry-system (aka Custom Searchable Data Entry System) plugin through 1.7.1 for WordPress allows SQL Injection. NOTE: this product is discontinued.	2020-03-27	<a href="#">6.5</a>	<a href="#">CVE-2020-10817</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. A user can perform an insecure direct object reference.	2020-04-01	<a href="#">6.5</a>	<a href="#">CVE-2020-7948</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerabilities exist in the Auth0 plugin before 4.0.0 for WordPress via the domain field.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-5391</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The Login by Auth0 plugin before 4.0.0 for WordPress allows stored XSS on multiple pages, a different issue than CVE-2020-5392.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-6753</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
yahoo -- elide	In Elide before 4.5.14, it is possible for an adversary to "guess and check" the value of a model field they do not have access to assuming they can read at least one other field in the model. The adversary can construct filter expressions for an inaccessible field to filter a collection. The presence or absence of models in the returned collection can be used to reconstruct the value of the inaccessible field. Resolved in Elide 4.5.14 and greater.	2020-03-30	<a href="#">4</a>	<a href="#">CVE-2020-5289</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zeit -- next.js	Next.js versions before 9.3.2 have a directory traversal vulnerability. Attackers could craft special requests to access files in the dist directory (.next). This does not affect files outside of the dist directory (.next). In general, the dist directory only holds build assets unless your application intentionally stores other assets under this directory. This issue is fixed in version 9.3.2.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-5284</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zevenet -- zen_load_balancer	Monitoring::Logs in Zen Load Balancer 3.10.1 allows remote authenticated admins to conduct absolute path traversal attacks, as demonstrated by a filelog=/etc/shadow request to index.cgi.	2020-04-02	<a href="#">4</a>	<a href="#">CVE-2020-11491</a> <a href="#">MISC</a> <a href="#">MISC</a>

zoho -- manageengine_desktop_central	Zoho ManageEngine Desktop Central allows unauthenticated users to access PDF Generation Servlet, leading to sensitive information disclosure.	2020-03-30	5	<a href="#">CVE-2020-8509</a> <a href="#">CONFIRM</a>
---	---	------------	---	--

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- esoms	The Redis data structure component used in ABB eSOMS versions 6.0 to 6.0.2 stores credentials in clear text. If an attacker has file system access, this can potentially compromise the credentials' confidentiality.	2020-04-02	<a href="#">3.6</a>	<a href="#">CVE-2019-19096</a> <a href="#">CONFIRM</a>
abb -- esoms	Lack of adequate input/output validation for ABB eSOMS versions 4.0 to 6.0.2 might allow an attacker to attack such as stored cross-site scripting by storing malicious content in the database.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19095</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the X-XSS-Protection HTTP response header is not set in responses from the web server. For older web browser not supporting Content Security Policy, this might increase the risk of Cross Site Scripting.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19002</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the Secure Flag is not set in the HTTP response header. Unencrypted connections might access the cookie information, thus making it susceptible to eavesdropping.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19090</a> <a href="#">CONFIRM</a>
abb -- esoms	ABB eSOMS versions 4.0 to 6.0.3 use ASP.NET Viewstate without Message Authentication Code (MAC). Alterations to Viewstate might thus not be noticed.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19092</a> <a href="#">CONFIRM</a>
apache -- cxf	Apache CXF has the ability to integrate with JMX by registering an InstrumentationManager extension with the CXF bus. If the 'createMBServerConnectorFactory' property of the default InstrumentationManagerImpl is not disabled, then it is vulnerable to a man-in-the-middle (MITM) style attack. An attacker on the same host can connect to the registry and rebind the entry to	2020-04-01	<a href="#">2.9</a>	<a href="#">CVE-2020-1954</a> <a href="#">MISC</a>



bd -- pyxis_medstation_es_system_and_pyxis_anesthesia_es_system	In BD Pyxis MedStation ES System v1.6.1 and Pyxis Anesthesia (PAS) ES System v1.6.1, a restricted desktop environment escape vulnerability exists in the kiosk mode functionality of affected devices. Specially-crafted inputs could allow the user to escape the restricted environment, resulting in access to sensitive data.	2020-04-01	<a href="#">3.6</a>	<a href="#">CVE-2020-10598</a> <a href="#">MISC</a>
gradle -- plugin_portal	All versions of com.gradle.plugin-publish before 0.11.0 are vulnerable to Insertion of Sensitive Information into Log File. When a plugin author publishes a Gradle plugin while running Gradle with the --info log level flag, the Gradle Logger logs an AWS pre-signed URL. If this build log is publicly visible (as it is in many popular public CI systems like TravisCI) this AWS pre-signed URL would allow a malicious actor to replace a recently uploaded plugin with their own.	2020-03-30	<a href="#">3.3</a>	<a href="#">CVE-2020-7599</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 175408.	2020-03-31	<a href="#">3.5</a>	<a href="#">CVE-2020-4235</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intland_software -- codebeamer_alm	In Intland codeBeamer ALM 9.5 and earlier, there is stored XSS via the Trackers Title parameter.	2020-03-30	<a href="#">3.5</a>	<a href="#">CVE-2019-19913</a> <a href="#">MISC</a>
intland_software -- codebeamer_alm	In Intland codeBeamer ALM 9.5 and earlier, a cross-site scripting (XSS) vulnerability in the Upload Flash File feature allows authenticated remote attackers to inject arbitrary scripts via an active script embedded in an SWF file.	2020-03-30	<a href="#">3.5</a>	<a href="#">CVE-2019-19912</a> <a href="#">MISC</a>
kubernetes -- kubelet	The Kubelet component in versions 1.15.0-1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via the kubelet API, including the unauthenticated HTTP read-only API typically served on port 10255, and the authenticated HTTPS API typically served on port 10250.	2020-03-27	<a href="#">3.3</a>	<a href="#">CVE-2020-8551</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy -- web_services	Microstrategy Web 10.4 is vulnerable to Stored XSS in the HTML Container and Insert Text features in the window, allowing for the creation of a new dashboard. In order to exploit this vulnerability, a user needs to get access	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2020-11454</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>



	to a shared dashboard or have the ability to create a dashboard on the application.			<a href="#">MISC</a>
otrs -- open_ticket_request_system	Attacker is able craft an article with a link to the customer address book with malicious content (JavaScript). When agent opens the link, JavaScript code is executed due to the missing parameter encoding. This issue affects: ((OTRS)) Community Edition: 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	3.5	<a href="#">CVE-2020-1771</a> <a href="#">MISC</a>
pfsense -- pfsense	pfSense before 2.4.5 has stored XSS in system_usermanager_addprivs.php in the WebGUI via the descr parameter (aka full name) of a user.	2020-04-01	3.5	<a href="#">CVE-2020-11457</a> <a href="#">MISC</a> <a href="#">MISC</a>
pki-core -- pki-core	A vulnerability was found in all pki-core 10.x.x version, where the Token Processing Service (TPS) did not properly sanitize several parameters stored for the tokens, possibly resulting in a Stored Cross Site Scripting (XSS) vulnerability. An attacker able to modify the parameters of any token could use this flaw to trick an authenticated user into executing arbitrary JavaScript code.	2020-03-31	3.5	<a href="#">CVE-2019-10180</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows XSS.	2020-04-01	3.5	<a href="#">CVE-2020-10203</a> <a href="#">CONFIRM</a>
versiant -- lynx_customer_service_portal	Versiant LYNX Customer Service Portal (CSP), version 3.5.2, is vulnerable to stored cross-site scripting, which could allow a local, authenticated attacker to insert malicious JavaScript that is stored and displayed to the end user. This could lead to website redirects, session cookie hijacking, or information disclosure.	2020-03-30	3.5	<a href="#">CVE-2020-9055</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
zoom -- zoom_client_for_meetings	Zoom Client for Meetings through 4.6.8 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Zoom Client's microphone and camera access.	2020-04-01	2.1	<a href="#">CVE-2020-11470</a> <a href="#">MISC</a> <a href="#">MISC</a>
zyxel -- xgs221-52hp_devices	In firmware version 4.50 of Zyxel XGS2210-52HP, multiple stored cross-site scripting (XSS) issues allows remote authenticated users to inject arbitrary web script via an rpSys.html Name or Location field.	2020-03-31	3.5	<a href="#">CVE-2019-13495</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3xlogic -- infinias_eidc32_devices	3xLOGIC Infinias eIDC32 2.213 devices with Web 1.107 allow Authentication Bypass via CMD.HTM?CMD= because authentication depends on the client side's interpretation of the <KEY>MYKEY</KEY> substring.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11542</a> <a href="#">MISC</a>
apple -- macos_catalina	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to read arbitrary files.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3889</a> <a href="#">MISC</a>
apple -- multiple_products	This issue was addressed with improved checks. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary entitlements.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3883</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3885</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bit2spr -- bit2spr	bit2spr 1992-06-07 has a stack-based buffer overflow (129-byte write) in conv_bitmap in bit2spr.c via a long line in a bitmap file.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11528</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- emc_isilon_onefs	Dell EMC Isilon OneFS versions 8.2.2 and earlier contain a denial of service vulnerability. SmartConnect had an error condition that may be triggered to loop, using CPU and potentially preventing other SmartConnect DNS responses.	2020-04-04	not yet calculated	<a href="#">CVE-2020-5347</a> <a href="#">MISC</a>
dell -- latitude_7202_rugged	Dell Latitude 7202 Rugged Tablet BIOS versions prior to A28 contain a UAF vulnerability in EFI_BOOT_SERVICES in system management mode. A local authenticated attacker may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in system management mode.	2020-04-04	not yet calculated	<a href="#">CVE-2020-5348</a> <a href="#">MISC</a>
	A flaw was found in the Eclipse Che up to			

eclipse -- che	version 7.8.x, where it did not properly restrict access to workspace pods. An authenticated user can exploit this flaw to bypass JWT proxy and gain access to the workspace pods of another user. Successful exploitation requires knowledge of the service name and namespace of the target pod.	2020-04-03	not yet calculated	<a href="#">CVE-2020-10689</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
firmware_analysis_and_comparison -- firmware_analysis_and_comparison	Firmware Analysis and Comparison Tool (FACT) has stored XSS when updating analysis details via a localhost web request and demonstrated by mishandling of the tags and version fields in helperFunctions/mongo_task_conversion.py.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11499</a> <a href="#">MISC</a> <a href="#">MISC</a>
get-git-data -- get-git-data	get-git-data through 1.3.1 is vulnerable to Command Injection. It is possible to inject arbitrary commands as part of the arguments provided to get-git-data.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7619</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu_glibc -- gnu_glibc	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.	2020-04-01	not yet calculated	<a href="#">CVE-2020-6096</a> <a href="#">MISC</a>
gnutls -- gnutls	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected version is 3.6.3 (2018-07-16) because of an error in a 2017-10-06 commit. The DTLS client always uses 32 ' ' bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol.	2020-04-03	not yet calculated	<a href="#">CVE-2020-11501</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
grav -- grav	Common/Grav.php in Grav before 1.6.23 has an Open Redirect.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11529</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A buffer overflow vulnerability was found			

hirschmann_automation_and_control -- hios_and_hisecos	in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30.	2020-04-03	not yet calculated	<a href="#">CVE-2020-6994</a> MISC
ibm -- spectrum_scale	IBM Spectrum Scale 4.2 and 5.0 could allow a local unprivileged attacker with intimate knowledge of the environment to execute commands as root using specially crafted input. IBM X-Force ID: 175977.	2020-04-03	not yet calculated	<a href="#">CVE-2020-4273</a> XF CONFIRM
ibm -- strongloop_strong-nginx-controller	strong-nginx-controller through 1.0.2 is vulnerable to Command Injection. It allows execution of arbitrary command as part of the '_nginxCmd()' function.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7621</a> MISC MISC
ini-parser -- ini-parser	ini-parser through 0.0.2 is vulnerable to Prototype Pollution. The library could be tricked into adding or modifying properties of Object.prototype using a '__proto__' payload.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7617</a> CONFIRM CONFIRM
ivanti -- workspace_control	Ivanti Workspace Control before 10.4.30.0, when SCCM integration is enabled, allows local users to obtain sensitive information (keying material).	2020-04-04	not yet calculated	<a href="#">CVE-2020-11533</a> MISC
jscover -- jscover	jscover through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary command via the source argument.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7623</a> MISC MISC
linux -- linux_kernel	An issue was discovered in slc_bump in drivers/net/can/slc.c in the Linux kernel through 5.6.2. It allows attackers to read uninitialized can_frame data, potentially containing sensitive information from kernel stack memory, if the configuration lacks CONFIG_INIT_STACK_ALL, aka CID-b9258a2cece4.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11494</a> MISC
linux -- linux_kernel	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was	2020-04-02	not yet calculated	<a href="#">CVE-2020-8835</a> CONFIRM CONFIRM FEDORA CONFIRM UBUNTU



	backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780)			<a href="#">UBUNTU CONFIRM CONFIRM</a>
mcafee -- endpoint_security_for_windows	Improper access control vulnerability in ESConfigTool.exe in ENS for Windows all current versions allows a local administrator to alter the ENS configuration up to and including disabling all protection offered by ENS via insecurely implemented encryption of configuration for export and import.	2020-04-01	not yet calculated	<a href="#">CVE-2020-7263 CONFIRM</a>
mediawiki -- mediawiki	In MediaWiki before 1.34.1, users can add various Cascading Style Sheets (CSS) classes (which can affect what content is shown or hidden in the user interface) to arbitrary DOM nodes via HTML content within a MediaWiki page. This occurs because jquery.makeCollapsible allows applying an event handler to any Cascading Style Sheets (CSS) selector. There is no known way to exploit this for cross-site scripting (XSS).	2020-04-03	not yet calculated	<a href="#">CVE-2020-10960 CONFIRM CONFIRM</a>
mitsubishi -- multiple_products	When MELSOFT transmission port (UDP/IP) of Mitsubishi Electric MELSEC iQ-R series (all versions), MELSEC iQ-F series (all versions), MELSEC Q series (all versions), MELSEC L series (all versions), and MELSEC F series (all versions) receives massive amount of data via unspecified vectors, resource consumption occurs and the port does not process the data properly. As a result, it may fall into a denial-of-service (DoS) condition. The vendor states this vulnerability only affects Ethernet communication functions.	2020-03-30	not yet calculated	<a href="#">CVE-2020-5527 MISC MISC</a>
netgear -- multiple_products	NETGEAR has released fixes for a pre-authentication command injection in request_handler.php security vulnerability on the following product models: WC7500, running firmware versions prior to 6.5.3.5; WC7520, running firmware versions prior to 2.5.0.46; WC7600v1, running firmware versions prior to 6.5.3.5; WC7600v2, running firmware versions prior to 6.5.3.5; and WC9500, running firmware versions prior to 6.5.3.5.	2020-04-01	not yet calculated	<a href="#">CVE-2018-11106 CONFIRM</a>
parrot -- anafi_drone	Web server running on Parrot ANAFI can be crashed due to the SDK command "Common_CurrentDateTime" being sent to control service with larger than	2020-04-01	not yet calculated	<a href="#">CVE-2019-3945 MISC</a>

	expected date length.			
parrot -- anafi_drone	Parrot ANAFI is vulnerable to Wi-Fi deauthentication attack, allowing remote and unauthenticated attackers to disconnect drone from controller during mid-flight.	2020-04-01	not yet calculated	<a href="#">CVE-2019-3944</a> <a href="#">MISC</a>
pomelo-monitor -- pomelo-monitor	pomelo-monitor through 0.3.7 is vulnerable to Command Injection.It allows injection of arbitrary commands as part of 'pomelo-monitor' params.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7620</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive_adserver -- revive_adserver	An Open Redirect vulnerability was discovered in Revive Adserver version < 5.0.5 and reported by HackerOne user hoangn144. A remote attacker could trick logged-in users to open a specifically crafted link and have them redirected to any destination.The CSRF protection of the “/www/admin/*-modify.php” could be skipped if no meaningful parameter was sent. No action was performed, but the user was still redirected to the target page, specified via the “returnurl” GET parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8143</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive_adserver -- revive_adserver	A security restriction bypass vulnerability has been discovered in Revive Adserver version < 5.0.5 by HackerOne user hoangn144. Revive Adserver, like many other applications, requires the logged in user to type the current password in order to change the e-mail address or the password. It was however possible for anyone with access to a Revive Adserver admin user interface to bypass such check and change e-email address or password of the currently logged in user by altering the form payload.The attack requires physical access to the user interface of a logged in user. If the POST payload was altered by turning the “pwold” parameter into an array, Revive Adserver would fetch and authorise the operation even if no password was provided.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8142</a> <a href="#">MISC</a> <a href="#">MISC</a>
slack -- nebula	Slack Nebula through 1.1.0 contains a relative path vulnerability that allows a low-privileged attacker to execute code in the context of the root user via tun_darwin.go or tun_windows.go. A user can also use Nebula to execute arbitrary code in the user's own context, e.g., for user-level persistence or to bypass security controls. NOTE: the vendor	2020-04-02	not yet calculated	<a href="#">CVE-2020-11498</a> <a href="#">MISC</a> <a href="#">MISC</a>

	states that this "requires a high degree of access and other preconditions that are tough to achieve."			
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3.x up to and including 3.21.2 has Incorrect Access Control.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11444</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
starface -- ucc_client	STARFACE UCC Client before 6.7.1.204 on WIndows allows binary planting to execute code with System rights, aka usd-2020-0006.	2020-04-02	not yet calculated	<a href="#">CVE-2020-10515</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
suse -- linux_enterprise_server	A Insufficient Verification of Data Authenticity vulnerability in autoyast2 of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15 allows remote attackers to MITM connections when deprecated and unused functionality of autoyast2 and its derivatives. This issue affects: SUSE Linux Enterprise Server 12 autoyast2 version 4.1.9-3.9.1 and prior versions. SUSE Linux Enterprise Server 15 autoyast2 version 4.0.70-3.20.1 and prior versions.	2020-04-03	not yet calculated	<a href="#">CVE-2019-18905</a> <a href="#">CONFIRM</a>
suse -- multiple_products	A Race Condition Enabling Link Following vulnerability in the packaging of texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users to corrupt files or potentially escalate privileges. This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8016</a> <a href="#">CONFIRM</a>
	A Race Condition Enabling Link Following vulnerability in the cron job shipped with texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-			

suse -- multiple_products	SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users in group mktx to delete arbitrary files on the system This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8017</a> <a href="#">CONFIRM</a>
suse -- multiple_products	A Uncontrolled Resource Consumption vulnerability in rmt of SUSE Linux Enterprise High Performance Computing 15-ESPOS, SUSE Linux Enterprise High Performance Computing 15-LTSS, SUSE Linux Enterprise Module for Public Cloud 15-SP1, SUSE Linux Enterprise Module for Server Applications 15, SUSE Linux Enterprise Module for Server Applications 15-SP1, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1 allows remote attackers to cause DoS against rmt by requesting migrations. This issue affects: SUSE Linux Enterprise High Performance Computing 15-ESPOS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise High Performance Computing 15-LTSS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Module for Public Cloud 15-SP1 rmt-server versions prior to 2.5.2-3.9.1. SUSE Linux Enterprise Module for Server Applications 15 rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Module for Server Applications 15-SP1 rmt-server versions prior to 2.5.2-3.9.1. SUSE Linux Enterprise Server 15-LTSS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Server for SAP 15 rmt-server versions prior to 2.5.2-3.26.1. openSUSE Leap 15.1 rmt-server versions prior to 2.5.2-lp151.2.9.1.	2020-04-03	not yet calculated	<a href="#">CVE-2019-18904</a> <a href="#">CONFIRM</a>
	A Least Privilege Violation vulnerability in crowbar of SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE			



suse -- openstack_cloud_and	OpenStack Cloud 9, SUSE OpenStack Cloud Crowbar 8, SUSE OpenStack Cloud Crowbar 9 allows root users on any crowbar managed node to cause become root on any other node. This issue affects: SUSE OpenStack Cloud 7 crowbar-core versions prior to 4.0+git.1578392992.fabfd186c-9.63.1, crowbar-. SUSE OpenStack Cloud 8 crowbar-core versions prior to 8.0+git.1579279939.ee7da88-3.39.3, ardana-. SUSE OpenStack Cloud 9 ardana-ansible versions prior to 9.0+git.1581611758.f694f7d-3.16.1, ardana-. SUSE OpenStack Cloud Crowbar 8 crowbar-core versions prior to 5.0+git.1582968668.1a55c77c5-3.35.4, crowbar-. SUSE OpenStack Cloud Crowbar 9 crowbar-core versions prior to 6.0+git.1582892022.cbd70e833-3.19.3, crowbar-.	2020-04-03	not yet calculated	<a href="#">CVE-2018-17954</a> <a href="#">CONFIRM</a>
suse -- opensuse_factory	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of exim in openSUSE Factory allows local attackers to escalate from user mail to root. This issue affects: openSUSE Factory exim versions prior to 4.93.0.4-3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8015</a> <a href="#">CONFIRM</a>
systemd -- systemd	A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.	2020-03-31	not yet calculated	<a href="#">CVE-2020-1712</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
testlink -- testlink	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in planUrgency.php via the urgency parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8638</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
testlink -- testlink	An unrestricted file upload vulnerability in keywordsImport.php in TestLink 1.9.20 allows remote attackers to execute arbitrary code by uploading a file with an executable extension. This allows an authenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to a publicly accessible directory of the application.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8639</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

testlink -- testlink	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in dragdroptreenodes.php via the node_id parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8637</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tp-link -- cloud_camera	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855.	2020-04-01	not yet calculated	<a href="#">CVE-2020-11445</a> <a href="#">MISC</a>
tp-link -- multiple_devices	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference.	2020-04-01	not yet calculated	<a href="#">CVE-2020-10231</a> <a href="#">MISC</a> <a href="#">MISC</a>
tp-link -- tl-wr841n_devices	A buffer overflow in the httpd daemon on TP-Link TL-WR841N V10 (firmware version 3.16.9) devices allows an authenticated remote attacker to execute arbitrary code via a GET request to the page for the configuration of the Wi-Fi network.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8423</a> <a href="#">MISC</a> <a href="#">MISC</a>
utils-extend -- utils-extend	Flaw in input validation in npm package utils-extend version 1.0.8 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using utils-extend.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8147</a> <a href="#">MISC</a>
viewvc -- viewvc	ViewVC before versions 1.1.28 and 1.2.1 has a XSS vulnerability in CVS show_subdir_lastmod support. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a CVS repository exposed by an otherwise trusted ViewVC instance that also has the `show_subdir_lastmod` feature enabled. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. This vulnerability is patched in versions 1.2.1 and 1.1.28.	2020-04-03	not yet calculated	<a href="#">CVE-2020-5283</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow a vulnerable ActiveX component to be exploited resulting in a buffer overflow,	2020-04-03	not yet calculated	<a href="#">CVE-2020-10599</a> <a href="#">MISC</a>

	which may lead to a denial-of-service condition and execution of arbitrary code.			
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow weak or insecure permissions on the VBASE directory resulting in elevation of privileges or malicious effects on the system the next time a privileged user runs the application.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7004 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow an unauthenticated attacker to discover the cryptographic key from the web server and gain information about the login and the encryption/decryption mechanism, which may be exploited to bypass authentication of the HTML5 HMI web interface.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7000 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow user input passed in the URL that is not properly verified before use, which may allow an attacker to read arbitrary files from local resources.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7008 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module allow weak hashing algorithm and insecure permissions which may allow a local attacker to bypass the password-protected mechanism through brute-force attacks, cracking techniques, or overwriting the password hash.	2020-04-03	not yet calculated	<a href="#">CVE-2020-10601 MISC</a>
wordpress -- wordpress	includes/theme-functions.php in the OneTone theme through 3.0.6 for WordPress allows unauthenticated options changes.	2020-04-03	not yet calculated	<a href="#">CVE-2019-17230 MISC</a>
wordpress -- wordpress	includes/theme-functions.php in the OneTone theme through 3.0.6 for WordPress has multiple stored XSS issues.	2020-04-03	not yet calculated	<a href="#">CVE-2019-17231 MISC</a>
xampp -- xampp	An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-contol.ini for all users (including admins) to enable arbitrary command execution.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11107 CONFIRM</a>
zevenet -- zen_load_balancer	Manage::Certificates in Zen Load Balancer 3.10.1 allows remote authenticated admins to execute arbitrary OS commands via shell metacharacters	2020-04-	not yet	<a href="#">CVE-2020-11490</a>

	in the index.cgi cert_issuer, cert_division, cert_organization, cert_locality, cert_state, cert_country, or cert_email parameter.	02	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
zoho -- manageengine_ad_sel	Zoho ManageEngine ADSelfService Plus before 5.8.15 allows unauthenticated remote code execution.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11518</a> <a href="#">MISC</a>
zoho -- manageengine_op_manager	In Zoho ManageEngine OpManager before 12.4.181, an unauthenticated remote attacker can send a specially crafted URI to read arbitrary files.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11527</a> <a href="#">MISC</a>
zoom -- client_for_meetings	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.	2020-04-03	not yet calculated	<a href="#">CVE-2020-11500</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870





**From:** [US-CERT](#)  
**To:** [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of March 30, 2020  
**Date:** Monday, April 06, 2020 2:22:37 PM



National Cyber Awareness System:

## [Vulnerability Summary for the Week of March 30, 2020](#)

04/06/2020 07:33 AM EDT

Original release date: April 6, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accenture -- mercury	An XXE issue exists in Accenture Mercury before 1.12.28 because of the platformlambda/core/serializers/SimpleXmlParser.java component.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10990</a> <a href="#">MISC</a> <a href="#">MISC</a>
alienform2 -- alienform2	Jon Hedley AlienForm2 (typically installed as af.cgi or alienform.cgi) 2.0.2 is vulnerable to Remote Command Execution via eval injection, a different issue than CVE-2002-0934. An unauthenticated, remote attacker can exploit this via a series of crafted requests.	2020-04-01	<a href="#">10</a>	<a href="#">CVE-2020-10948</a> <a href="#">MISC</a>
apache -- http_server	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-1934</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.4. An application may be able to execute arbitrary code with	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3903</a> <a href="#">MISC</a>

	system privileges.			
apple -- macos_catalina	Multiple issues were addressed by updating to version 8.1.1850. This issue is fixed in macOS Catalina 10.15.4. Multiple issues in Vim.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-9769</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to leak memory.	2020-04-01	<a href="#">10</a>	<a href="#">CVE-2020-3847</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3892</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3893</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3904</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-3849</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3905</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-3850</a> <a href="#">MISC</a>
apple -- macos_catalina_and_mojave_and_high_sierra	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.3. A remote attacker may be able to cause unexpected application termination	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-3848</a> <a href="#">MISC</a>

	or arbitrary code execution.			
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3911</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3910</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Multiple issues in libxml2.	2020-04-01	7.5	<a href="#">CVE-2020-3909</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	9.3	<a href="#">CVE-2020-9785</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to execute arbitrary code with system privileges.	2020-04-01	9.3	<a href="#">CVE-2020-9768</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. A malicious application may be able to execute arbitrary code with kernel privileges.	2020-04-01	9.3	<a href="#">CVE-2020-3919</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A memory corruption issue was addressed with improved memory			<a href="#">CVE-2020-3895</a>

apple -- multiple_products	handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3899</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.	2020-04-01	<a href="#">9.3</a>	<a href="#">CVE-2020-3897</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to bypass intended access restrictions on tasks from an untrusted process, when Self Defense is enabled.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2020-10867</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
azkaban -- azkaban	Azkaban through 3.84.0 allows XXE, related to validator/XmlValidatorManager.java and user/XmlUserManager.java.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10992</a> <a href="#">MISC</a>
bubblewrap -- bubblewrap	Bubblewrap (bwrap) before version 0.4.1, if installed in setuid mode and the kernel supports unprivileged user namespaces, then the `bwrap --users2` option can be used to make the setuid process keep running as root while being traceable. This can in turn be used to gain root permissions. Note that this only affects the combination of bubblewrap in setuid mode (which is typically used when unprivileged user namespaces are not supported) and the support of unprivileged user namespaces. Known to be affected are: * Debian testing/unstable, if unprivileged user namespaces enabled (not default) * Debian buster-backports, if unprivileged user namespaces enabled	2020-03-31	<a href="#">8.5</a>	<a href="#">CVE-2020-5291</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



	(not default) * Arch if using `linux-hardened`, if unprivileged user namespaces enabled (not default) * Centos 7 flatpak COPR, if unprivileged user namespaces enabled (not default) This has been fixed in the 0.4.1 release, and all affected users should update.			
buildah -- buildah	A path traversal flaw was found in Buildah in versions before 1.14.5. This flaw allows an attacker to trick a user into building a malicious container image hosted on an HTTP(s) server and then write files to the user's system anywhere that the user has permissions.	2020-03-31	9.3	<a href="#">CVE-2020-10696</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
cacagoo -- tv-288zd-2mp_devices	CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 has weak authentication of TELNET access, leading to root privileges without any password required.	2020-04-02	10	<a href="#">CVE-2020-6852</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- emc_idrac_devices	Dell EMC iDRAC7, iDRAC8 and iDRAC9 versions prior to 2.65.65.65, 2.70.70.70, 4.00.00.00 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may exploit this vulnerability to crash the affected process or execute arbitrary code on the system by sending specially crafted input data.	2020-03-31	10	<a href="#">CVE-2020-5344</a> <a href="#">MISC</a>
effect -- effect	effect through 1.0.4 is vulnerable to Command Injection. It allows execution of arbitrary command via the options argument.	2020-04-02	7.5	<a href="#">CVE-2020-7624</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- elasticsearch	Elasticsearch versions from 6.7.0 before 6.8.8 and 7.0.0 before 7.6.2 contain a privilege escalation flaw if an attacker is able to create API keys. An attacker who is able to generate an API key can perform a series of steps that result in an API key being generated with elevated privileges.	2020-03-31	7.5	<a href="#">CVE-2020-7009</a> <a href="#">N/A</a> <a href="#">CONFIRM</a> <a href="#">N/A</a>
f5 -- nginx_controller	In NGINX Controller versions prior to 3.2.0, an unauthenticated attacker with network access to the Controller API can create unprivileged user accounts. The user which is created is only able to upload a new license to the system but cannot view or modify any other components of the system.	2020-03-27	7.5	<a href="#">CVE-2020-5863</a> <a href="#">MISC</a>
git-add-remote -- git-add-remote	git-add-remote through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary commands via the name argument.	2020-04-02	7.5	<a href="#">CVE-2020-7630</a> <a href="#">MISC</a> <a href="#">MISC</a>

gitlab -- gitlab	GitLab 8.10 and later through 12.9 is vulnerable to an SSRF in a project import note feature.	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10956</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
hiproxy -- op-browser	op-browser through 1.0.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the url function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7625</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to execute arbitrary commands on the system in the context of root user, caused by improper validation of user-supplied input. IBM X-Force ID: 174966.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4206</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 174975.	2020-03-31	<a href="#">7.5</a>	<a href="#">CVE-2020-4208</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175418.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4241</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Scale and IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM X-Force ID: 175419.	2020-03-31	<a href="#">9</a>	<a href="#">CVE-2020-4242</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
install-package -- install-package	install-package through 0.4.0 is vulnerable to Command Injection. It allows execution of arbitrary commands via the options argument.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7629</a> <a href="#">MISC</a> <a href="#">MISC</a>
install-package -- install-package	install-package through 1.1.6 is vulnerable to Command Injection. It allows execution of arbitrary commands via the device function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7628</a> <a href="#">MISC</a> <a href="#">MISC</a>
karma-mojo -- karma-mojo	karma-mojo through 1.0.1 is vulnerable to Command Injection. It allows execution of arbitrary commands via the config	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7626</a> <a href="#">MISC</a>

	argument.			MISC
ksh -- ksh	In ksh version 20120801, a flaw was found in the way it evaluates certain environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Services and applications that allow remote unauthenticated attackers to provide one of those environment variables could allow them to exploit this issue remotely.	2020-04-02	<a href="#">7.2</a>	<a href="#">CVE-2019-14868</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
laminar_research -- x-plane	X-Plane before 11.41 allows Arbitrary Memory Write via crafted network packets, which could cause a denial of service or arbitrary code execution.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2019-19605</a> <a href="#">MISC</a>
laminar_research -- x-plane	X-Plane before 11.41 has multiple improper path validations that could allow reading and writing files from/to arbitrary paths (or a leak of OS credentials to a remote system) via crafted network packets. This could be used to execute arbitrary commands on the system.	2020-03-30	<a href="#">10</a>	<a href="#">CVE-2019-19606</a> <a href="#">MISC</a>
lenovo -- multiple_notebooks	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A buffer overflow vulnerability was reported, (fixed and publicly disclosed in 2015) in the Lenovo Service Engine (LSE), affecting various versions of BIOS for Lenovo Notebooks, that could allow a remote user to execute arbitrary code on the system.	2020-03-27	<a href="#">10</a>	<a href="#">CVE-2015-5684</a> <a href="#">MISC</a>
lenovo -- multiple_products	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type COMMAND type could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-7334</a> <a href="#">MISC</a>
lenovo -- multiple_products	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior where the SUService.exe /type INF and INF_BY_COMPATIBLE_ID command types could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-7333</a> <a href="#">MISC</a>

lenovo -- solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A local privilege escalation vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-8534</a> <a href="#">MISC</a>
lenovo -- solution_center	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A directory traversal vulnerability was discovered (fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">7.2</a>	<a href="#">CVE-2015-8535</a> <a href="#">MISC</a>
march_networks -- command_client	The connection initiation process in March Networks Command Client before 2.7.2 allows remote attackers to execute arbitrary code via crafted XAML objects.	2020-04-01	<a href="#">7.5</a>	<a href="#">CVE-2019-9163</a> <a href="#">CONFIRM</a>
mongodb -- js-bson	All versions of bson before 1.1.4 are vulnerable to Deserialization of Untrusted Data. The package will ignore an unknown value for an object's _bsotype, leading to cases where an object is serialized as a document rather than the intended BSON type.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2020-7610</a> <a href="#">MISC</a>
mulesoft -- apikit	Mulesoft APIkit through 1.3.0 allows XXE because of validation/RestXmlSchemaValidator.java	2020-03-27	<a href="#">7.5</a>	<a href="#">CVE-2020-10991</a> <a href="#">MISC</a>
node-key-sender -- node-key-sender	node-key-sender through 1.0.11 is vulnerable to Command Injection. It allows execution of arbitrary commands via the 'arrParams' argument in the 'execute()' function.	2020-04-02	<a href="#">7.5</a>	<a href="#">CVE-2020-7627</a> <a href="#">MISC</a> <a href="#">MISC</a>
objectcomputing -- micronaut	All versions of io.micronaut:micronaut-http-client before 1.2.11 and all versions from 1.3.0 before 1.3.2 are vulnerable to HTTP Request Header Injection due to not validating request headers passed to the client.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2020-7611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
odata4j -- odata4j	odata4j 0.7.0 allows ExecuteJPQLQueryCommand.java SQL injection. NOTE: this product is apparently discontinued.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2016-11024</a> <a href="#">MISC</a>
odata4j -- odata4j	odata4j 0.7.0 allows ExecuteCountQueryCommand.java SQL injection. NOTE: this product is apparently discontinued.	2020-03-30	<a href="#">7.5</a>	<a href="#">CVE-2016-11023</a> <a href="#">MISC</a>
	A webserver component in Paessler PRTG Network Monitor 19.2.50 to PRTG			<a href="#">CVE-2020-</a>



paessler -- prtg_network_monitor	20.1.56 allows unauthenticated remote command execution via a crafted POST request or the what parameter of the screenshot function in the Contact Support form.	2020-03-30	7.5	<a href="#">10374</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
pam-krb5 -- pam-krb5	pam-krb5 before 4.9 has a buffer overflow that might cause remote code execution in situations involving supplemental prompting by a Kerberos library. It may overflow a buffer provided by the underlying Kerberos library by a single ' ' byte if an attacker responds to a prompt with an answer of a carefully chosen length. The effect may range from heap corruption to stack corruption depending on the structure of the underlying Kerberos library, with unknown effects but possibly including code execution. This code path is not used for normal authentication, but only when the Kerberos library does supplemental prompting, such as with PKINIT or when using the non-standard no_prompt PAM configuration option.	2020-03-31	7.5	<a href="#">CVE-2020-10595</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows Remote Code Execution.	2020-04-01	9	<a href="#">CVE-2020-10204</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows JavaEL Injection (issue 1 of 2).	2020-04-01	9	<a href="#">CVE-2020-10199</a> <a href="#">CONFIRM</a>
unisocon -- ultracon_express	UltraLog Express device management interface does not properly filter user inputted string in some specific parameters, attackers can inject arbitrary SQL command.	2020-03-27	7.5	<a href="#">CVE-2020-3936</a> <a href="#">MISC</a>
university_of_southern_california -- innovation_in_integrated_informatics_lab_cereal	An issue was discovered in USC iLab cereal through 1.3.0. It employs caching of std::shared_ptr values, using the raw pointer address as a unique identifier. This becomes problematic if an std::shared_ptr variable goes out of scope and is freed, and a new std::shared_ptr is allocated at the same address. Serialization fidelity thereby becomes dependent upon memory layout. In short, serialized std::shared_ptr variables cannot always be expected to serialize back into their original values. This can have any number of consequences, depending on the context within which this manifests.	2020-03-30	7.5	<a href="#">CVE-2020-11105</a> <a href="#">MISC</a>
	The web interface of the Vertiv Avocent			

vertiv -- avocent_umg-400_devices	UMG-4000 version 4.2.1.19 is vulnerable to command injection because the application incorrectly neutralizes code syntax before executing. Since all commands within the web application are executed as root, this could allow a remote attacker authenticated with an administrator account to execute arbitrary commands as root.	2020-03-30	9	<a href="#">CVE-2019-9507</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. It has numerous fields that can contain data that is pulled from different sources. One issue with this is that the data isn't sanitized, and no input validation is performed, before the exporting of the user data. This can lead to (at least) CSV injection if a crafted Excel document is uploaded.	2020-04-01	7.5	<a href="#">CVE-2020-7947</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	LearnDash Wordpress plugin version below 3.1.6 is vulnerable to Unauthenticated SQL Injection.	2020-04-01	7.5	<a href="#">CVE-2020-6009</a> <a href="#">MISC</a>
wordpress -- wordpress	LifterLMS Wordpress plugin version below 3.37.15 is vulnerable to arbitrary file write leading to remote code execution	2020-03-31	7.5	<a href="#">CVE-2020-6008</a> <a href="#">MISC</a>
yamaha -- multiple_products	Yamaha LTE VoIP Router(NVR700W firmware Rev.15.00.15 and earlier), Yamaha Gigabit VoIP Router(NVR510 firmware Rev.15.01.14 and earlier), Yamaha Gigabit VPN Router(RTX810 firmware Rev.11.01.33 and earlier, RTX830 firmware Rev.15.02.09 and earlier, RTX1200 firmware Rev.10.01.76 and earlier, RTX1210 firmware Rev.14.01.33 and earlier, RTX3500 firmware Rev.14.00.26 and earlier, and RTX5000 firmware Rev.14.00.26 and earlier), Yamaha Broadband VoIP Router(NVR500 firmware Rev.11.00.38 and earlier), and Yamaha Firewall(FWX120 firmware Rev.11.03.27 and earlier) allow remote attackers to cause a denial of service via unspecified vectors.	2020-04-01	7.8	<a href="#">CVE-2020-5548</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoom -- client_for_meetings	Zoom Client for Meetings through 4.6.8 on macOS copies runwithroot to a user-writable temporary directory during installation, which allows a local process (with the user's privileges) to obtain root access by replacing runwithroot.	2020-04-01	7.2	<a href="#">CVE-2020-11469</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.3, the X-Content-Type-Options Header is missing in the HTTP response, potentially causing the response body to be interpreted and displayed as different content type other than declared. A possible attack scenario would be unauthorized code execution via text interpreted as JavaScript.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19089 CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the X-Frame-Options header is not configured in HTTP response. This can potentially allow 'ClickJacking' attacks where an attacker can frame parts of the application on a malicious web site, revealing sensitive user information such as authentication credentials.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19001 CONFIRM</a>
abb -- esoms	Lack of input checks for SQL queries in ABB eSOMS versions 3.9 to 6.0.3 might allow an attacker SQL injection attacks against the backend database.	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2019-19094 CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the HTTPOnly flag is not set. This can allow Javascript to access the cookie contents, which in turn might enable Cross Site Scripting.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19003 CONFIRM</a>
abb -- esoms	ABB eSOMS versions 4.0 to 6.0.3 accept connections using medium strength ciphers. If a connection is enabled using such a cipher, an attacker might be able to eavesdrop and/or intercept the connection.	2020-04-02	<a href="#">4.3</a>	<a href="#">CVE-2019-19097 CONFIRM</a>
abb -- esoms	eSOMS versions 4.0 to 6.0.3 do not enforce password complexity settings, potentially resulting in lower access security due to insecure user passwords.	2020-04-02	<a href="#">6.4</a>	<a href="#">CVE-2019-19093 CONFIRM</a>
abb -- esoms	For ABB eSOMS 4.0 to 6.0.3, the Cache-Control and Pragma HTTP header(s) have not been properly configured within the application response. This can potentially allow browsers and proxies to cache sensitive information.	2020-04-02	<a href="#">6.4</a>	<a href="#">CVE-2019-19000 CONFIRM</a>
	For ABB eSOMS versions 4.0 to 6.0.3, HTTPS responses contain comments with			<a href="#">CVE-2019-</a>

abb -- esoms	sensitive information about the application. An attacker might use this detail information to specifically craft the attack.	2020-04-02	<a href="#">4</a>	<a href="#">19091 CONFIRM</a>
advantech -- webaccess	In Advantech WebAccess, Versions 8.4.2 and prior. A stack-based buffer overflow vulnerability caused by a lack of proper validation of the length of user-supplied data may allow remote code execution.	2020-03-27	<a href="#">6.5</a>	<a href="#">CVE-2020-10607 MISC</a>
advantech -- webaccess	Advantech WebAccess 8.3.4 does not properly restrict an RPC call that allows unauthenticated, remote users to read files. An attacker can use this vulnerability to recover the administrator password.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2019-3942 MISC</a>
apache -- dubbo	Unsafe deserialization occurs within a Dubbo application which has HTTP remoting enabled. An attacker may submit a POST request with a Java object in it to completely compromise a Provider instance of Apache Dubbo, if this instance enables HTTP. This issue affected Apache Dubbo 2.7.0 to 2.7.4, 2.6.0 to 2.6.7, and all 2.5.x versions.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2019-17564 MISC</a>
apache -- http_server	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.	2020-04-02	<a href="#">5.8</a>	<a href="#">CVE-2020-1927 MLIST MLIST CONFIRM MLIST MLIST</a>
apache -- netbeans	The "Apache NetBeans" autoupdate system does not validate SSL certificates and hostnames for https based downloads. This allows an attacker to intercept downloads of autoupdates and modify the download, potentially injecting malicious code. "Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	2020-03-30	<a href="#">6.4</a>	<a href="#">CVE-2019-17560 MISC</a>
apache -- netbeans	The "Apache NetBeans" autoupdate system does not fully validate code signatures. An attacker could modify the downloaded nbm and include additional code. "Apache NetBeans" versions up to and including 11.2 are affected by this vulnerability.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2019-17561 MISC</a>
apache -- ofbiz	Data sent with contentId to /control/stream is not sanitized, allowing XSS attacks in Apache OFBiz 16.11.01 to 16.11.07.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-1943 MISC</a>
	Scripts in Sling CMS before 0.16.0 do not			



apache -- sling_cms	property escape the Sling Selector from URLs when generating navigational elements for the administrative consoles and are vulnerable to reflected XSS attacks.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-1949</a> <a href="#">MISC</a>
apache -- solr	In Apache Solr, the cluster can be partitioned into multiple collections and only a subset of nodes actually host any given collection. However, if a node receives a request for a collection it does not host, it proxies the request to a relevant node and serves the request. Solr bypasses all authorization settings for such requests. This affects all Solr versions prior to 7.7 that use the default authorization mechanism of Solr (RuleBasedAuthorizationPlugin).	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2018-11802</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4. An attacker in a privileged network position may be able to intercept Bluetooth traffic.	2020-04-01	<a href="#">4</a>	<a href="#">CVE-2020-9770</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the selection of video file by Mail. The issue was fixed by selecting the latest version of a video. This issue is fixed in iOS 13.4 and iPadOS 13.4. Cropped videos may not be shared properly via Mail.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9777</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4. A maliciously crafted page may interfere with other web contexts.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3888</a> <a href="#">MISC</a>
apple -- ios_and_ipados	The issue was addressed by clearing website permission prompts after navigation. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user may grant website permissions to a site they didn't intend to.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9781</a> <a href="#">MISC</a>
apple -- ios_and_ipados	The issue was addressed with improved deletion. This issue is fixed in iOS 13.4 and iPadOS 13.4. Deleted messages groups may still be suggested as an autocompletion.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-3890</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the handling of tabs displaying picture in picture video. The issue was corrected with improved state handling. This issue is fixed in iOS 13.4 and iPadOS 13.4. A user's private browsing activity may be unexpectedly saved in Screen Time.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-9775</a> <a href="#">MISC</a>

apple -- macos_catalina	This issue was addressed with a new entitlement. This issue is fixed in macOS Catalina 10.15.4. A malicious application may be able to access a user's call history.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-9776</a> <a href="#">MISC</a>
apple -- macos_high_sierra_and_catalina	An injection issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. A remote attacker may be able to cause arbitrary javascript code execution.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3884</a> <a href="#">MISC</a>
apple -- macos_mojave_and_catalina	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15.4. A maliciously crafted application may be able to bypass code signing enforcement.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-3906</a> <a href="#">MISC</a>
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	<a href="#">6.6</a>	<a href="#">CVE-2020-3908</a> <a href="#">MISC</a>
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	<a href="#">6.6</a>	<a href="#">CVE-2020-3912</a> <a href="#">MISC</a>
apple -- macos_mojave_and_catalina	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.4. A malicious user may be able to cause unexpected system termination or read kernel memory.	2020-04-01	<a href="#">6.6</a>	<a href="#">CVE-2020-3907</a> <a href="#">MISC</a>
apple -- multiple_devices	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to code execution.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-9783</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to read restricted memory.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-3914</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4,			<a href="#">CVE-2020-3887</a> <a href="#">MISC</a>



apple -- safari	A logic issue was addressed with improved restrictions. This issue is fixed in Safari 13.1. A malicious iframe may use another website's download settings.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-9784</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to make arbitrary changes to the Components section of the Stats.ini file via RPC from a Low Integrity process.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10865</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Arbitrary File Deletion from Avast Program Path via RPC, when Self Defense is Enabled.	2020-04-01	<a href="#">6.4</a>	<a href="#">CVE-2020-10861</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to launch the Repair App RPC call from a Low Integrity process.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. An Arbitrary Memory Address Overwrite vulnerability in the aswAvLog Log Library results in Denial of Service of the Avast Service (AvastSvc.exe).	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10860</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a shutdown via RPC from a Low Integrity process via TempShutDownMachine.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to achieve Local Privilege Escalation (LPE) via RPC.	2020-04-01	<a href="#">4.6</a>	<a href="#">CVE-2020-10862</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
avast -- avast_antivirus	An issue was discovered in Avast Antivirus before 20. The aswTask RPC endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to trigger a reboot via RPC from a Low Integrity process.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-10864</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in Avast Antivirus before 20. The aswTask RPC			<a href="#">CVE-2020-</a>



avast -- avast_antivirus	endpoint for the TaskEx library in the Avast Service (AvastSvc.exe) allows attackers to enumerate the network interfaces and access points from a Low Integrity process via RPC.	2020-04-01	5	10866 <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacagoo -- cloud_storage_intelligent_camera_tv_288zd-2mp	The CACAGOO Cloud Storage Intelligent Camera TV-288ZD-2MP with firmware 3.4.2.0919 allows access to the RTSP service without a password.	2020-04-02	5	<a href="#">CVE-2020-9349</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/people endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve sensitive information about all users registered on the system. This includes their full name, privilege, email address, phone number, etc.	2020-04-01	4	<a href="#">CVE-2020-11464</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/tickets endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve arbitrary information about all helpdesk tickets stored in database with numerous filters. This leaked sensitive information to unauthorized parties. Additionally, it leaked ticket authentication code, making it possible to make changes to a ticket.	2020-04-01	4	<a href="#">CVE-2020-11466</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/email_accounts endpoint failed to properly validate a user's privilege, allowing an attacker to retrieve cleartext credentials of all helpdesk email accounts, including incoming and outgoing email credentials. This enables an attacker to get full access to all emails sent or received by the system including password reset emails, making it possible to reset any user's password.	2020-04-01	5	<a href="#">CVE-2020-11463</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
deskpro -- deskpro	An issue was discovered in Deskpro before 2019.8.0. The /api/apps/* endpoints failed to properly validate a user's privilege, allowing an attacker to control/install helpdesk applications and leak current applications' configurations, including applications used as user sources (used for authentication). This enables an attacker to forge valid authentication models that resembles any user on the system.	2020-04-01	6.5	<a href="#">CVE-2020-11465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in Deskpro before 2019.8.0. This product enables			

deskpro -- deskpro	administrators to modify the helpdesk interface by editing /portal/api/style/edit-theme-set/template-sources theme templates, and uses TWIG as its template engine. While direct access to self and _self variables was not permitted, one could abuse the accessible variables in one's context to reach a native unserialize function via the code parameter. There, one could pass a crafted payload to trigger a set of POP gadgets in order to achieve remote code execution.	2020-04-01	6.5	<a href="#">CVE-2020-11467</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.1.0.1, specially formatted HTTP/3 messages may cause TMM to produce a core file.	2020-03-27	5	<a href="#">CVE-2020-5859</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1, 14.1.0-14.1.2.2, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, undisclosed HTTP behavior may lead to a denial of service.	2020-03-27	5	<a href="#">CVE-2020-5857</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.1.0-15.1.0.1, 15.0.0-15.0.1.1, and 14.1.0-14.1.2.2, under certain conditions, TMM may crash or stop processing new traffic with the DPDK/ENA driver on AWS systems while sending traffic. This issue does not affect any other platforms, hardware or virtual, or any other cloud provider since the affected driver is specific to AWS.	2020-03-27	5	<a href="#">CVE-2020-5862</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 12.1.0-12.1.5, the TMM process may produce a core file in some cases when Ram Cache incorrectly optimizes stored data resulting in memory errors.	2020-03-27	5	<a href="#">CVE-2020-5861</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.2, 14.1.0-14.1.2.2, 13.1.0-13.1.3.2, 12.1.0-12.1.5, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, users with non-administrator roles (for example, Guest or Resource Administrator) with tmsh shell access can execute arbitrary commands with elevated privilege via a crafted tmsh command.	2020-03-27	4.6	<a href="#">CVE-2020-5858</a> <a href="#">MISC</a>
f5 -- big-ip_and_big-iq	On BIG-IP 15.0.0-15.1.0.2, 14.1.0-14.1.2.3, 13.1.0-13.1.3.2, 12.1.0-12.1.5.1, and 11.5.2-11.6.5.1 and BIG-IQ 7.0.0, 6.0.0-6.1.0, and 5.2.0-5.4.0, in a High Availability (HA) network failover in Device Service Cluster (DSC), the failover service does not require a strong form of authentication and HA network failover traffic is not encrypted by Transport Layer Security (TLS).	2020-03-27	6.8	<a href="#">CVE-2020-5860</a> <a href="#">MISC</a>

fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.activemq.* (aka activemq-jms, activemq-core, activemq-pool, and activemq-pool-jms).	2020-03-31	6.8	<a href="#">CVE-2020-11111</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.openjpa.ee.WASRegistryManagedRuntime (aka openjpa).	2020-03-31	6.8	<a href="#">CVE-2020-11113</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.commons.proxy.provider.remoting.RmiProvider (aka apache/commons-proxy).	2020-03-31	6.8	<a href="#">CVE-2020-11112</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- fortios	An external control of system vulnerability in FortiOS may allow an authenticated, regular user to change the routing settings of the device via connecting to the ZebOS component.	2020-04-02	6.5	<a href="#">CVE-2018-13371</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab through 12.9 is affected by a potential DoS in repository archive download.	2020-03-27	5	<a href="#">CVE-2020-10954</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and_enterprise_editions	GitLab EE/CE 8.11 through 12.9.1 allows blocked users to pull/push docker images.	2020-03-27	5.8	<a href="#">CVE-2020-10952</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and_enterprise_editions	GitLab EE/CE 11.1 through 12.9 is vulnerable to parameter tampering on an enterprise edition that allows an unauthorized user to read content available under specific folders.	2020-03-27	4	<a href="#">CVE-2020-10955</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	In GitLab EE 11.7 through 12.9, the NPM feature is vulnerable to a path traversal issue.	2020-03-27	5	<a href="#">CVE-2020-10953</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
grandstream -- ucm6200_series_devices	The UCM6200 series 1.0.20.22 and below stores unencrypted user passwords in an SQLite database. This could allow an attacker to retrieve all passwords and possibly gain elevated privileges.	2020-03-30	5	<a href="#">CVE-2020-5723</a> <a href="#">CONFIRM</a>
grandstream -- ucm6200_series_devices	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websocket endpoint. A remote unauthenticated attacker can invoke the	2020-03-30	4.3	<a href="#">CVE-2020-5725</a> <a href="#">MISC</a>

	login action with a crafted username and, through the use of timing attacks, can discover user passwords.			<a href="#">CONFIRM</a>
grandstream -- ucm6200_series_devices	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the CTI server on port 8888. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	2020-03-30	5	<a href="#">CVE-2020-5726</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
grandstream -- ucm6200_series_devices	The Grandstream UCM6200 series before 1.0.20.22 is vulnerable to an SQL injection via the HTTP server's websockify endpoint. A remote unauthenticated attacker can invoke the challenge action with a crafted username and discover user passwords.	2020-03-30	5	<a href="#">CVE-2020-5724</a> <a href="#">CONFIRM</a>
gststreamer -- gst-rtsp-server	An exploitable denial of service vulnerability exists in the GstRTSPAuth functionality of GStreamer/gst-rtsp-server 1.14.5. A specially crafted RTSP setup request can cause a null pointer deference resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability.	2020-03-27	5	<a href="#">CVE-2020-6095</a> <a href="#">MISC</a> <a href="#">MISC</a>
haproxy -- haproxy	In hpack_dht_insert in hpack-tbl.c in the HPACK decoder in HAProxy 1.8 through 2.x before 2.1.4, a remote attacker can write arbitrary bytes around a certain location on the heap via a crafted HTTP/2 request, possibly causing remote code execution.	2020-04-02	6.5	<a href="#">CVE-2020-11100</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
huawei -- multiple_smartax_devices	There is a buffer overflow vulnerability in some Huawei products. The vulnerability can be exploited by an attacker to perform remote code execution on the affected products when the affected product functions as an optical line terminal (OLT). Affected product versions include: SmartAX MA5600T versions V800R013C10, V800R015C00, V800R015C10, V800R017C00, V800R017C10, V800R018C00, V800R018C10; SmartAX MA5800 versions V100R017C00, V100R017C10, V100R018C00, V100R018C10, V100R019C10; SmartAX EA5800 versions V100R018C00, V100R018C10, V100R019C10.	2020-04-02	5.2	<a href="#">CVE-2020-9067</a> <a href="#">CONFIRM</a>
	The IBM Process Federation Server			



ibm -- process_federation_server	18.0.0.1, 18.0.0.2, 19.0.0.1, 19.0.0.2, and 19.0.0.3 Global Teams REST API does not properly shutdown the thread pools that it creates to retrieve Global Teams information from the federated systems. As a consequence, the Java Virtual Machine can't recover the memory used by those thread pools, which leads to an OutOfMemory exception when the Process Federation Server Global Teams REST API is used extensively. IBM X-Force ID: 177596.	2020-04-02	4	<a href="#">CVE-2020-4325</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request to overwrite or create arbitrary files on the system. IBM X-Force ID: 175417.	2020-03-31	6.4	<a href="#">CVE-2020-4240</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect_plus	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow a remote attacker to arbitrary delete a directory caused by improper validation of user-supplied input. IBM X-Force ID: 175026.	2020-03-31	6.4	<a href="#">CVE-2020-4214</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 175412.	2020-03-31	5	<a href="#">CVE-2020-4239</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175411.	2020-03-31	6.8	<a href="#">CVE-2020-4238</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 175410.	2020-03-31	6.8	<a href="#">CVE-2020-4237</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 could allow an authenticated user to cause a denial of service due to improper content parsing in the project management module. IBM X-Force ID: 175409.	2020-03-31	4	<a href="#">CVE-2020-4236</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
	IBM WebSphere Application Server -			

ibm -- websphere_application	Liberty 17.0.0.3 through 20.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176670.	2020-04-02	4.3	<a href="#">CVE-2020-4304</a> XF CONFIRM
ibm -- websphere_application	IBM WebSphere Application Server - Liberty 17.0.0.3 through 20.0.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176668.	2020-04-02	4.3	<a href="#">CVE-2020-4303</a> XF CONFIRM
intland_software -- codebeamer	codeBeamer before 9.5.0-RC3 does not properly restrict the ability to execute custom Java code and access the Java class loader via computed fields.	2020-04-02	4.3	<a href="#">CVE-2019-20635</a> MISC
kubernetes -- api_server	The Kubernetes API server component in versions prior to 1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via successful API requests.	2020-03-27	5	<a href="#">CVE-2020-8552</a> MISC MISC
kubernetes -- api_server	The Kubernetes API Server component in versions 1.1-1.14, and versions prior to 1.15.10, 1.16.7 and 1.17.3 allows an authorized user who sends malicious YAML payloads to cause the kube-apiserver to consume excessive CPU cycles while parsing YAML.	2020-04-01	4	<a href="#">CVE-2019-11254</a> MISC MISC
leantime -- leantime	Leantime before versions 2.0.15 and 2.1-beta3 has a SQL Injection vulnerability. The impact is high. Malicious users/attackers can execute arbitrary SQL queries negatively affecting the confidentiality, integrity, and availability of the site. Attackers can exfiltrate data like the users' and administrators' password hashes, modify data, or drop tables. The unescaped parameter is "searchUsers" when sending a POST request to "/tickets/showKanban" with a valid session. In the code, the parameter is named "users" in class.tickets.php. This issue is fixed in versions 2.0.15 and 2.1.0 beta 3.	2020-03-31	6.5	<a href="#">CVE-2020-5292</a> MISC MISC CONFIRM
lenovo --	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was discovered	2020-03-		<a href="#">CVE-2015-</a>

lenovo_solution_center	(fixed and publicly disclosed in 2015) in Lenovo Solution Center (LSC) prior to version 3.3.002 that could allow cross-site request forgery.	27	<a href="#">6.8</a>	<a href="#">8536</a> <a href="#">MISC</a>
lenovo --multiple_devices	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A race condition was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow a user to execute arbitrary code with elevated privileges.	2020-03-27	<a href="#">6.9</a>	<a href="#">CVE-2015-7335</a> <a href="#">MISC</a>
lenovo --multiple_devices	MITRE is populating this ID because it was assigned prior to Lenovo becoming a CNA. A vulnerability was reported (fixed and publicly disclosed in 2015) in Lenovo System Update version 5.07.0008 and prior that could allow the signature check of an update to be bypassed.	2020-03-27	<a href="#">5</a>	<a href="#">CVE-2015-7336</a> <a href="#">MISC</a>
limesurvey --limesurvey	LimeSurvey before 4.1.12+200324 contains a path traversal vulnerability in application/controllers/admin/LimeSurveyFileManager.php.	2020-04-01	<a href="#">5</a>	<a href="#">CVE-2020-11455</a> <a href="#">MISC</a>
limesurvey --limesurvey	LimeSurvey before 4.1.12+200324 has stored XSS in application/views/admin/surveysgroups/surveySettings.php and application/models/SurveysGroups.php (aka survey groups).	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-11456</a> <a href="#">MISC</a>
microstrategy --web_services	The Upload Visualization plugin in the Microstrategy Web 10.4 admin panel allows an administrator to upload a ZIP archive containing files with arbitrary extensions and data. (This is also exploitable via SSRF.)	2020-04-02	<a href="#">6.5</a>	<a href="#">CVE-2020-11451</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy --web_services	Microstrategy Web 10.4 is vulnerable to Server-Side Request Forgery in the Test Web Service functionality exposed through the path /MicroStrategyWS/. The functionality requires no authentication and, while it is not possible to pass parameters in the SSRF request, it is still possible to exploit it to conduct port scanning. An attacker could exploit this vulnerability to enumerate the resources allocated in the network (IP addresses and services exposed).	2020-04-02	<a href="#">5</a>	<a href="#">CVE-2020-11453</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microstrategy --web_services	Microstrategy Web 10.4 exposes the JVM configuration, CPU architecture, installation folder, and other information through the URL /MicroStrategyWS/happyaxis.jsp. An attacker could use this vulnerability to learn more about the environment the	2020-04-02	<a href="#">5</a>	<a href="#">CVE-2020-11450</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	application is running in.			
microstrategy --web_services	Microstrategy Web 10.4 includes functionality to allow users to import files or data from external resources such as URLs or databases. By providing an external URL under attacker control, it's possible to send requests to external resources (aka SSRF) or leak files from the local system using the file:// stream wrapper.	2020-04-02	4	<a href="#">CVE-2020-11452</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
misp_project -- misp	app/Model/feed.php in MISP before 2.4.124 allows administrators to choose arbitrary files that should be ingested by MISP. This does not cause a leak of the full contents of a file, but does cause a leaks of strings that match certain patterns. Among the data that can leak are passwords from database.php or GPG key passphrases from config.php.	2020-04-02	4	<a href="#">CVE-2020-11458</a> <a href="#">MISC</a> <a href="#">MISC</a>
mongodb -- js-bson	Incorrect parsing of certain JSON input may result in js-bson not correctly serializing BSON. This may cause unexpected application behaviour including data disclosure.	2020-03-31	5.5	<a href="#">CVE-2019-2391</a> <a href="#">CONFIRM</a>
moodle -- moodle	A vulnerability was found in Moodle versions 3.7 before 3.7.3, 3.6 before 3.6.7, 3.5 before 3.5.9 and earlier. OAuth 2 providers who do not verify users' email address changes require additional verification during sign-up to reduce the risk of account compromise.	2020-03-31	6.4	<a href="#">CVE-2019-14880</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
open_source_social_network -- open_source_social_network	An issue was discovered in Open Source Social Network (OSSN) through 5.3. A user-controlled file path with a weak cryptographic rand() can be used to read any file with the permissions of the webserver. This can lead to further compromise. The attacker must conduct a brute-force attack against the SiteKey to insert into a crafted URL for components/OssnComments/ossn_com.php and/or libraries/ossn.lib.upgrade.php.	2020-03-30	4.3	<a href="#">CVE-2020-10560</a> <a href="#">MISC</a> <a href="#">MISC</a>
osmand -- osmand	Osmand through 2.0.0 allow XXE because of binary/BinaryMapIndexReader.java.	2020-03-27	6.4	<a href="#">CVE-2020-10993</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system	An attacker with the ability to generate session IDs or password reset tokens, either by being able to authenticate or by exploiting OSA-2020-09, may be able to predict other users session IDs, password reset tokens and automatically generate passwords. This issue affects ((OTRS))	2020-03-27	5.5	<a href="#">CVE-2020-1773</a> <a href="#">MISC</a>



	Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS; 7.0.15 and prior versions.			
otrs -- open_ticket_request_system_and_open_ticket_request_system_community_comr27	In the login screens (in agent and customer interface), Username and Password fields use autocomplete, which might be considered as security issue. This issue affects: ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	4	<a href="#">CVE-2020-1769</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_and_open_ticket_request_system_community_comr27	It's possible to craft Lost Password requests with wildcards in the Token value, which allows attacker to retrieve valid Token(s), generated by users which already requested new passwords. This issue affects: ((OTRS)) Community Edition 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	5	<a href="#">CVE-2020-1772</a> <a href="#">MISC</a>
otrs -- open_ticket_request_system_and_open_ticket_request_system_community_comr27	Support bundle generated files could contain sensitive information that might be unwanted to be disclosed. This issue affects: ((OTRS)) Community Edition: 5.0.41 and prior versions, 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	4	<a href="#">CVE-2020-1770</a> <a href="#">MISC</a>
phoenix_contact -- pc_worx_srt	Insecure, default path permissions in PHOENIX CONTACT PC WORX SRT through 1.14 allow for local privilege escalation.	2020-03-27	4.6	<a href="#">CVE-2020-10939</a> <a href="#">CONFIRM</a>
phoenix_contact -- portico_server	Local Privilege Escalation can occur in PHOENIX CONTACT PORTICO SERVER through 3.0.7 when installed to run as a service.	2020-03-27	4.6	<a href="#">CVE-2020-10940</a> <a href="#">CONFIRM</a>
php -- php	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.	2020-04-01	5.8	<a href="#">CVE-2020-7064</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
php -- php	In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using mb_strtolower() function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated buffer. This could lead to memory corruption, crashes and potentially code execution.	2020-04-01	6.8	<a href="#">CVE-2020-7065</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

php -- php	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.34, while using get_headers() with user-supplied URL, if the URL contains zero ( ) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-7066</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
progress_software -- telerik_ui_for_silverlight	An issue was discovered in Progress Telerik UI for Silverlight before 2020.1.330. The RadUploadHandler class in RadUpload for Silverlight expects a web request that provides the file location of the uploading file along with a few other parameters. The uploading file location should be inside the directory where the upload handler class is defined. Before 2020.1.330, a crafted web request could result in uploads to arbitrary locations.	2020-03-31	<a href="#">5</a>	<a href="#">CVE-2020-11414</a> <a href="#">MISC</a>
proofpoint -- email_protection	An issue was discovered in Proofpoint Email Protection through 2019-09-08. By collecting scores from Proofpoint email headers, it is possible to build a copy-cat Machine Learning Classification model and extract insights from this model. The insights gathered allow an attacker to craft emails that receive preferable scores, with a goal of delivering malicious emails.	2020-03-30	<a href="#">6.4</a>	<a href="#">CVE-2019-20634</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible_engine	A vulnerability was found in Ansible Engine versions 2.9.x before 2.9.3, 2.8.x before 2.8.8, 2.7.x before 2.7.16 and earlier, where in Ansible's nxos_file_copy module can be used to copy files to a flash or bootflash on NXOS devices. Malicious code could craft the filename parameter to perform OS command injections. This could result in a loss of confidentiality of the system among other issues.	2020-03-31	<a href="#">4.6</a>	<a href="#">CVE-2019-14905</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a>
red_hat -- openshift/apb-base	An insecure modification vulnerability in the /etc/passwd file was found in the container openshift/apb-base, affecting versions before the following 4.3.5, 4.2.21, 4.1.37, and 3.11.188-4. An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	2020-04-02	<a href="#">4.4</a>	<a href="#">CVE-2019-19348</a> <a href="#">CONFIRM</a>
	An insecure modification vulnerability in			

red_hat -- openshift/mariadb-apb	the /etc/passwd file was found in the container openshift/mariadb-apb, affecting versions before the following 4.3.5, 4.2.21, 4.1.37, and 3.11.188-4 . An attacker with access to the container could use this flaw to modify /etc/passwd and escalate their privileges.	2020-04-02	4.4	<a href="#">CVE-2019-19346</a> <a href="#">CONFIRM</a>
redpwn -- redpwnctf	In RedpwnCTF before version 2.3, there is a session fixation vulnerability in exploitable through the `#token=\$ssid` hash when making a request to the `/verify` endpoint. An attacker team could potentially steal flags by, for example, exploiting a stored XSS payload in a CTF challenge so that victim teams who solve the challenge are unknowingly (and against their will) signed into the attacker team's account. Then, the attacker can gain points / value off the backs of the victims. This is patched in version 2.3.	2020-04-01	4.3	<a href="#">CVE-2020-5290</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
responsive_filemanager -- responsive_filemanager	An issue was discovered in Responsive Filemanager through 9.14.0. In the dialog.php page, the session variable \$_SESSION['RF']['view_type'] wasn't sanitized if it was already set. This made stored XSS possible if one opens ajax_calls.php and uses the "view" action and places a payload in the type parameter, and then returns to the dialog.php page. This occurs because ajax_calls.php was also able to set the \$_SESSION['RF']['view_type'] variable, but there it wasn't sanitized.	2020-03-30	4.3	<a href="#">CVE-2020-11106</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, improperly stores system files. Attackers can use a specific URL and capture confidential information.	2020-03-27	5	<a href="#">CVE-2020-10508</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, contains vulnerability of Cross-Site Scripting (XSS), attackers can inject arbitrary command into the system and launch XSS attack.	2020-03-27	4.3	<a href="#">CVE-2020-10509</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sunnet_technology -- ehrd	Sunnet eHRD, a human training and development management system, contains a vulnerability of Broken Access Control. After login, attackers can use a specific URL, access unauthorized functionality and data.	2020-03-27	4	<a href="#">CVE-2020-10510</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
	In Symfony before versions 4.4.7 and 5.0.7, when a `Response` does not			

symfony -- symfony	contain a `Content-Type` header, affected versions of Symfony can fallback to the format defined in the `Accept` header of the request, leading to a possible mismatch between the response's content and `Content-Type` header. When the response is cached, this can prevent the use of the website by other users. This has been patched in versions 4.4.7 and 5.0.7.	2020-03-30	4	<a href="#">CVE-2020-5255</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
symfony -- symfony	In symfony/security-http before versions 4.4.7 and 5.0.7, when a `Firewall` checks access control rule, it iterate overs each rule's attributes and stops as soon as the accessDecisionManager decides to grant access on the attribute, preventing the check of next attributes that should have been take into account in an unanimous strategy. The accessDecisionManager is now called with all attributes at once, allowing the unanimous strategy being applied on each attribute. This issue is patched in versions 4.4.7 and 5.0.7.	2020-03-30	5.5	<a href="#">CVE-2020-5275</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
symfony -- symfony	In Symfony before versions 5.0.5 and 4.4.5, some properties of the Exception were not properly escaped when the `ErrorHandler` rendered it stacktrace. In addition, the stacktrace were displayed even in a non-debug configuration. The ErrorHandler now escape alls properties of the exception, and the stacktrace is only display in debug configuration. This issue is patched in symfony/http-foundation versions 4.4.5 and 5.0.5	2020-03-30	5.5	<a href="#">CVE-2020-5274</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
technicolor -- tc7337_devices	An issue was discovered on Technicolor TC7337 8.89.17 devices. An attacker can discover admin credentials in the backup file, aka backupsettings.conf.	2020-04-01	5	<a href="#">CVE-2020-11449</a> <a href="#">MISC</a>
tikiwiki -- groupware_and_cms	There is an Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in php webpages of Tiki-Wiki Groupware. Tiki-Wiki CMS all versions through 20.0 allows malicious users to cause the injection of malicious code fragments (scripts) into a legitimate web page.	2020-04-01	4.3	<a href="#">CVE-2020-8966</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
totemo -- totemomail	An insecure direct object reference in webmail in totemo totemomail 7.0.0 allows an authenticated remote user to read and modify mail folder names of other users via enumeration.	2020-03-27	5.5	<a href="#">CVE-2020-7918</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Toyota 2017 Model Year DCU (Display			



toyota -- model_year_2017_display_control_unit	Control Unit) allows an unauthenticated attacker within Bluetooth range to cause a denial of service attack and/or execute an arbitrary command. The affected DCUs are installed in Lexus (LC, LS, NX, RC, RC F), TOYOTA CAMRY, and TOYOTA SIENNA manufactured in the regions other than Japan from Oct. 2016 to Oct. 2019. An attacker with certain knowledge on the target vehicle control system may be able to send some diagnostic commands to ECUs with some limited availability impacts; the vendor states critical vehicle controls such as driving, turning, and stopping are not affected.	2020-03-30	5.4	<a href="#">CVE-2020-5551</a> <a href="#">MISC</a> <a href="#">MISC</a>
ubiquiti -- unifi_video_controller	The UniFi Video Server (Windows) web interface configuration restore functionality at the “backup” and “wizard” endpoints does not implement sufficient privilege checks. Low privileged users, belonging to the PUBLIC_GROUP or CUSTOM_GROUP groups, can access these endpoints and overwrite the current application configuration. This can be abused for various purposes, including adding new administrative users. Affected Products: UniFi Video Controller v3.9.3 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.9.6 and newer.	2020-04-01	4	<a href="#">CVE-2020-8145</a> <a href="#">CONFIRM</a>
ubiquiti -- unifi_video_controller	In UniFi Video v3.10.1 (for Windows 7/8/10 x64) there is a Local Privileges Escalation to SYSTEM from arbitrary file deletion and DLL hijack vulnerabilities. The issue was fixed by adjusting the .tsExport folder when the controller is running on Windows and adjusting the SafeDllSearchMode in the windows registry when installing UniFi-Video controller. Affected Products: UniFi Video Controller v3.10.2 (for Windows 7/8/10 x64) and prior. Fixed in UniFi Video Controller v3.10.3 and newer.	2020-04-01	6.9	<a href="#">CVE-2020-8146</a> <a href="#">CONFIRM</a>
ubiquiti -- unifi_video_controller	The UniFi Video Server v3.9.3 and prior (for Windows 7/8/10 x64) web interface Firmware Update functionality, under certain circumstances, does not validate firmware download destinations to ensure they are within the intended destination directory tree. It accepts a request with a URL to firmware update information. If the version field contains ..\ character sequences, the destination file path to	2020-04-01	5.2	<a href="#">CVE-2020-8144</a> <a href="#">CONFIRM</a>

	save the firmware can be manipulated to be outside the intended destination directory tree. Fixed in UniFi Video Controller v3.10.3 and newer.			
unisoona -- ultraa_log_express	UltraLog Express device management software stores user's information in cleartext. Any user can obtain accounts information through a specific page.	2020-03-27	5	<a href="#">CVE-2020-3921</a> <a href="#">MISC</a>
unisoona -- ultraa_log_express	UltraLog Express device management interface does not properly perform access authentication in some specific pages/functions. Any user can access the privileged page to manage accounts through specific system directory.	2020-03-27	5.5	<a href="#">CVE-2020-3920</a> <a href="#">MISC</a>
university_of_southern_california -- innovation_in_integrated_informatics_lab_cereal	An issue was discovered in USC iLab cereal through 1.3.0. Serialization of an (initialized) C/C++ long double variable into a BinaryArchive or PortableBinaryArchive leaks several bytes of stack or heap memory, from which sensitive information (such as memory layout or private keys) can be gleaned if the archive is distributed outside of a trusted context.	2020-03-30	5	<a href="#">CVE-2020-11104</a> <a href="#">MISC</a>
vertiv -- avocent_universal_management_gateway	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to stored XSS. A remote attacker authenticated with an administrator account can store a maliciously named file within the web application that would execute each time a user browsed to the page.	2020-03-30	6	<a href="#">CVE-2019-9508</a> <a href="#">MISC</a> <a href="#">MISC</a>
vertiv -- avocent_universal_management_gateway	The web interface of the Vertiv Avocent UMG-4000 version 4.2.1.19 is vulnerable to reflected XSS in an HTTP POST parameter. The web application does not sanitize user-controllable input before displaying to users in a web page, which could allow a remote attacker authenticated with a user account to execute arbitrary code.	2020-03-30	6.5	<a href="#">CVE-2019-9509</a> <a href="#">MISC</a> <a href="#">MISC</a>
weberp -- weberp	In webERP 4.15, the Import Bank Transactions function fails to sanitize the content of imported MT940 bank statement files, resulting in the execution of arbitrary SQL queries, aka SQL Injection.	2020-03-30	6.5	<a href="#">CVE-2019-7755</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	A stored cross-site scripting (XSS) vulnerability exists in the Auth0 plugin before 4.0.0 for WordPress via the settings page.	2020-04-01	4.3	<a href="#">CVE-2020-5392</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

wordpress -- wordpress	The custom-searchable-data-entry-system (aka Custom Searchable Data Entry System) plugin through 1.7.1 for WordPress allows SQL Injection. NOTE: this product is discontinued.	2020-03-27	<a href="#">6.5</a>	<a href="#">CVE-2020-10817</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An issue was discovered in the Login by Auth0 plugin before 4.0.0 for WordPress. A user can perform an insecure direct object reference.	2020-04-01	<a href="#">6.5</a>	<a href="#">CVE-2020-7948</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerabilities exist in the Auth0 plugin before 4.0.0 for WordPress via the domain field.	2020-04-01	<a href="#">6.8</a>	<a href="#">CVE-2020-5391</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The Login by Auth0 plugin before 4.0.0 for WordPress allows stored XSS on multiple pages, a different issue than CVE-2020-5392.	2020-04-01	<a href="#">4.3</a>	<a href="#">CVE-2020-6753</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
yahoo -- elide	In Elide before 4.5.14, it is possible for an adversary to "guess and check" the value of a model field they do not have access to assuming they can read at least one other field in the model. The adversary can construct filter expressions for an inaccessible field to filter a collection. The presence or absence of models in the returned collection can be used to reconstruct the value of the inaccessible field. Resolved in Elide 4.5.14 and greater.	2020-03-30	<a href="#">4</a>	<a href="#">CVE-2020-5289</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zeit -- next.js	Next.js versions before 9.3.2 have a directory traversal vulnerability. Attackers could craft special requests to access files in the dist directory (.next). This does not affect files outside of the dist directory (.next). In general, the dist directory only holds build assets unless your application intentionally stores other assets under this directory. This issue is fixed in version 9.3.2.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-5284</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zevenet -- zen_load_balancer	Monitoring::Logs in Zen Load Balancer 3.10.1 allows remote authenticated admins to conduct absolute path traversal attacks, as demonstrated by a filelog=/etc/shadow request to index.cgi.	2020-04-02	<a href="#">4</a>	<a href="#">CVE-2020-11491</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho -- manageengine_desktop_central	Zoho ManageEngine Desktop Central allows unauthenticated users to access PDFGenerationServlet, leading to sensitive information disclosure.	2020-03-30	<a href="#">5</a>	<a href="#">CVE-2020-8509</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- esoms	The Redis data structure component used in ABB eSOMS versions 6.0 to 6.0.2 stores credentials in clear text. If an attacker has file system access, this can potentially compromise the credentials' confidentiality.	2020-04-02	<a href="#">3.6</a>	<a href="#">CVE-2019-19096</a> <a href="#">CONFIRM</a>
abb -- esoms	Lack of adequate input/output validation for ABB eSOMS versions 4.0 to 6.0.2 might allow an attacker to attack such as stored cross-site scripting by storing malicious content in the database.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19095</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the X-XSS-Protection HTTP response header is not set in responses from the web server. For older web browser not supporting Content Security Policy, this might increase the risk of Cross Site Scripting.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19002</a> <a href="#">CONFIRM</a>
abb -- esoms	For ABB eSOMS versions 4.0 to 6.0.2, the Secure Flag is not set in the HTTP response header. Unencrypted connections might access the cookie information, thus making it susceptible to eavesdropping.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19090</a> <a href="#">CONFIRM</a>
abb -- esoms	ABB eSOMS versions 4.0 to 6.0.3 use ASP.NET Viewstate without Message Authentication Code (MAC). Alterations to Viewstate might thus not be noticed.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2019-19092</a> <a href="#">CONFIRM</a>
apache -- cxf	Apache CXF has the ability to integrate with JMX by registering an InstrumentationManager extension with the CXF bus. If the 'createMBServerConnectorFactory' property of the default InstrumentationManagerImpl is not disabled, then it is vulnerable to a man-in-the-middle (MITM) style attack. An attacker on the same host can connect to the registry and rebind the entry to another server, thus acting as a proxy to the original. They are then able to gain access to all of the information that is sent and received over JMX.	2020-04-01	<a href="#">2.9</a>	<a href="#">CVE-2020-1954</a> <a href="#">MISC</a>



apache -- druid	When LDAP authentication is enabled in Apache Druid 0.17.0, callers of Druid APIs with a valid set of LDAP credentials can bypass the <code>credentialsValidator.userSearch</code> filter barrier that determines if a valid LDAP user is allowed to authenticate with Druid. They are still subject to role-based authorization checks, if configured. Callers of Druid APIs can also retrieve any LDAP attribute values of users that exist on the LDAP server, so long as that information is visible to the Druid server. This information disclosure does not require the caller itself to be a valid LDAP user.	2020-04-01	3.5	<a href="#">CVE-2020-1958</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apple -- ios_and_ipados	The issue was resolved by clearing application previews when content is deleted. This issue is fixed in iOS 13.4 and iPadOS 13.4. A local user may be able to view deleted content in the app switcher.	2020-04-01	2.1	<a href="#">CVE-2020-9780</a> <a href="#">MISC</a>
apple -- macos_catalina	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to view sensitive user information.	2020-04-01	2.1	<a href="#">CVE-2020-3881</a> <a href="#">MISC</a>
apple -- multiple_products	This issue was addressed with a new entitlement. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2. An application may be able to use an SSH client provided by private frameworks.	2020-04-01	2.1	<a href="#">CVE-2020-3917</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.4 and iPadOS 13.4, watchOS 6.2. A person with physical access to a locked iOS device may be able to respond to messages even when replies are disabled.	2020-04-01	2.1	<a href="#">CVE-2020-3891</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. An application may be able to read restricted memory.	2020-04-01	2.6	<a href="#">CVE-2020-3894</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bd --	In BD Pyxis MedStation ES System v1.6.1 and Pyxis Anesthesia (PAS) ES System v1.6.1, a restricted desktop environment escape vulnerability exists in	2020-04-		<a href="#">CVE-2020-</a>

pyxis_medstation_es_system and pyxis_anesthesia_es_system	the kiosk mode functionality of affected devices. Specially-crafted inputs could allow the user to escape the restricted environment, resulting in access to sensitive data.	01	<a href="#">3.6</a>	<a href="#">10598 MISC</a>
gradle -- plugin_portal	All versions of com.gradle.plugin-publish before 0.11.0 are vulnerable to Insertion of Sensitive Information into Log File. When a plugin author publishes a Gradle plugin while running Gradle with the --info log level flag, the Gradle Logger logs an AWS pre-signed URL. If this build log is publicly visible (as it is in many popular public CI systems like TravisCI) this AWS pre-signed URL would allow a malicious actor to replace a recently uploaded plugin with their own.	2020-03-30	<a href="#">3.3</a>	<a href="#">CVE-2020-7599 MISC MISC</a>
ibm -- tivoli_netcool_impact	IBM Tivoli Netcool Impact 7.1.0.0 through 7.1.0.17 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 175408.	2020-03-31	<a href="#">3.5</a>	<a href="#">CVE-2020-4235 XE CONFIRM</a>
intland_software -- codebeamer_alm	In Intland codeBeamer ALM 9.5 and earlier, there is stored XSS via the Trackers Title parameter.	2020-03-30	<a href="#">3.5</a>	<a href="#">CVE-2019-19913 MISC</a>
intland_software -- codebeamer_alm	In Intland codeBeamer ALM 9.5 and earlier, a cross-site scripting (XSS) vulnerability in the Upload Flash File feature allows authenticated remote attackers to inject arbitrary scripts via an active script embedded in an SWF file.	2020-03-30	<a href="#">3.5</a>	<a href="#">CVE-2019-19912 MISC</a>
kubernetes -- kubelet	The Kubelet component in versions 1.15.0-1.15.9, 1.16.0-1.16.6, and 1.17.0-1.17.2 has been found to be vulnerable to a denial of service attack via the kubelet API, including the unauthenticated HTTP read-only API typically served on port 10255, and the authenticated HTTPS API typically served on port 10250.	2020-03-27	<a href="#">3.3</a>	<a href="#">CVE-2020-8551 MISC MISC</a>
microstrategy -- web_services	Microstrategy Web 10.4 is vulnerable to Stored XSS in the HTML Container and Insert Text features in the window, allowing for the creation of a new dashboard. In order to exploit this vulnerability, a user needs to get access to a shared dashboard or have the ability to create a dashboard on the application.	2020-04-02	<a href="#">3.5</a>	<a href="#">CVE-2020-11454 MISC FULLDISC MISC MISC</a>
	Attacker is able craft an article with a link to the customer address book with			

otrs -- open_ticket_request_system_and_open_ticket_request_system_community_edition	malicious content (JavaScript). When agent opens the link, JavaScript code is executed due to the missing parameter encoding. This issue affects: ((OTRS)) Community Edition: 6.0.26 and prior versions. OTRS: 7.0.15 and prior versions.	2020-03-27	3.5	<a href="#">CVE-2020-1771</a> <a href="#">MISC</a>
pfsense -- pfsense	pfSense before 2.4.5 has stored XSS in system_usermanager_addprivs.php in the WebGUI via the descr parameter (aka full name) of a user.	2020-04-01	3.5	<a href="#">CVE-2020-11457</a> <a href="#">MISC</a> <a href="#">MISC</a>
pki-core -- pki-core	A vulnerability was found in all pki-core 10.x.x version, where the Token Processing Service (TPS) did not properly sanitize several parameters stored for the tokens, possibly resulting in a Stored Cross Site Scripting (XSS) vulnerability. An attacker able to modify the parameters of any token could use this flaw to trick an authenticated user into executing arbitrary JavaScript code.	2020-03-31	3.5	<a href="#">CVE-2019-10180</a> <a href="#">CONFIRM</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository before 3.21.2 allows XSS.	2020-04-01	3.5	<a href="#">CVE-2020-10203</a> <a href="#">CONFIRM</a>
versiant -- lynx_customer_service_portal	Versiant LYNX Customer Service Portal (CSP), version 3.5.2, is vulnerable to stored cross-site scripting, which could allow a local, authenticated attacker to insert malicious JavaScript that is stored and displayed to the end user. This could lead to website redirects, session cookie hijacking, or information disclosure.	2020-03-30	3.5	<a href="#">CVE-2020-9055</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
zoom -- zoom_client_for_meetings	Zoom Client for Meetings through 4.6.8 on macOS has the disable-library-validation entitlement, which allows a local process (with the user's privileges) to obtain unprompted microphone and camera access by loading a crafted library and thereby inheriting Zoom Client's microphone and camera access.	2020-04-01	2.1	<a href="#">CVE-2020-11470</a> <a href="#">MISC</a> <a href="#">MISC</a>
zyxel -- xgs221-52hp_devices	In firmware version 4.50 of Zyxel XGS2210-52HP, multiple stored cross-site scripting (XSS) issues allows remote authenticated users to inject arbitrary web script via an rpSys.html Name or Location field.	2020-03-31	3.5	<a href="#">CVE-2019-13495</a> <a href="#">MISC</a>

[Back to top](#)

**Severity Not Yet Assigned**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3xlogic -- infinias_eidc32_devices	3xLOGIC Infinias eIDC32 2.213 devices with Web 1.107 allow Authentication Bypass via CMD.HTM?CMD= because authentication depends on the client side's interpretation of the <KEY>MYKEY</KEY> substring.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11542</a> <a href="#">MISC</a>
apple -- macos_catalina	A logic issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15.4. A local user may be able to read arbitrary files.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3889</a> <a href="#">MISC</a>
apple -- multiple_products	This issue was addressed with improved checks. This issue is fixed in iOS 13.4 and iPadOS 13.4, macOS Catalina 10.15.4, tvOS 13.4, watchOS 6.2. An application may be able to use arbitrary entitlements.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3883</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed.	2020-04-01	not yet calculated	<a href="#">CVE-2020-3885</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bit2spr -- bit2spr	bit2spr 1992-06-07 has a stack-based buffer overflow (129-byte write) in conv_bitmap in bit2spr.c via a long line in a bitmap file.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11528</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- emc_isilon_onefs	Dell EMC Isilon OneFS versions 8.2.2 and earlier contain a denial of service vulnerability. SmartConnect had an error condition that may be triggered to loop, using CPU and potentially preventing other SmartConnect DNS responses.	2020-04-04	not yet calculated	<a href="#">CVE-2020-5347</a> <a href="#">MISC</a>
dell -- latitude_7202_rugged_tablet	Dell Latitude 7202 Rugged Tablet BIOS versions prior to A28 contain a UAF vulnerability in EFI_BOOT_SERVICES in system management mode. A local authenticated attacker may exploit this vulnerability by overwriting the EFI_BOOT_SERVICES structure to execute arbitrary code in system management mode.	2020-04-04	not yet calculated	<a href="#">CVE-2020-5348</a> <a href="#">MISC</a>
eclipse -- che	A flaw was found in the Eclipse Che up to version 7.8.x, where it did not properly restrict access to workspace pods. An authenticated user can exploit this flaw to bypass JWT proxy and gain access to the	2020-04-03	not yet calculated	<a href="#">CVE-2020-10689</a> <a href="#">CONFIRM</a>



	workspace pods of another user. Successful exploitation requires knowledge of the service name and namespace of the target pod.			<a href="#">MISC</a>
firmware_analysis_and -- firmware_analysis_and	Firmware Analysis and Comparison Tool (FACT) has stored XSS when updating analysis details via a localhost web request, as demonstrated by mishandling of the tags and version fields in helperFunctions/mongo_task_conversion.py.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11499</a> <a href="#">MISC</a> <a href="#">MISC</a>
get-git-data -- get-git-data	get-git-data through 1.3.1 is vulnerable to Command Injection. It is possible to inject arbitrary commands as part of the arguments provided to get-git-data.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7619</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu_glibc -- gnu_glibc	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution and iterations of this code will be executed with this corrupted data.	2020-04-01	not yet calculated	<a href="#">CVE-2020-6096</a> <a href="#">MISC</a>
gnutls -- gnutls	GnuTLS 3.6.x before 3.6.13 uses incorrect cryptography for DTLS. The earliest affected version is 3.6.3 (2018-07-16) because of an error in a 2017-10-06 commit. The DTLS client always uses 32 '' bytes instead of a random value, and thus contributes no randomness to a DTLS negotiation. This breaks the security guarantees of the DTLS protocol.	2020-04-03	not yet calculated	<a href="#">CVE-2020-11501</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
grav -- grav	Common/Grav.php in Grav before 1.6.23 has an Open Redirect.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11529</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A buffer overflow vulnerability was found in some devices of Hirschmann Automation and Control HiOS and HiSecOS. The vulnerability is due to improper parsing of URL arguments. An			

hirschmann_automation_and_control -- hios_and_hisecos	attacker could exploit this vulnerability by specially crafting HTTP requests to overflow an internal buffer. The following devices using HiOS Version 07.0.02 and lower are affected: RSP, RSPE, RSPS, RSPL, MSP, EES, EESX, GRS, OS, RED. The following devices using HiSecOS Version 03.2.00 and lower are affected: EAGLE20/30.	2020-04-03	not yet calculated	<a href="#">CVE-2020-6994</a> <a href="#">MISC</a>
ibm -- spectrum_scale	IBM Spectrum Scale 4.2 and 5.0 could allow a local unprivileged attacker with intimate knowledge of the environment to execute commands as root using specially crafted input. IBM X-Force ID: 175977.	2020-04-03	not yet calculated	<a href="#">CVE-2020-4273</a> <a href="#">CONFIRM</a>
ibm -- strongloop_strong-nginx-controller	strong-nginx-controller through 1.0.2 is vulnerable to Command Injection. It allows execution of arbitrary command as part of the '_nginxCmd()' function.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7621</a> <a href="#">MISC</a> <a href="#">MISC</a>
ini-parser -- ini-parser	ini-parser through 0.0.2 is vulnerable to Prototype Pollution. The library could be tricked into adding or modifying properties of Object.prototype using a '__proto__' payload.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7617</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ivanti -- workspace_control	Ivanti Workspace Control before 10.4.30.0, when SCCM integration is enabled, allows local users to obtain sensitive information (keying material).	2020-04-04	not yet calculated	<a href="#">CVE-2020-11533</a> <a href="#">MISC</a>
jscover -- jscover	jscover through 1.0.0 is vulnerable to Command Injection. It allows execution of arbitrary command via the source argument.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7623</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in slc_bump in drivers/net/can/slcan.c in the Linux kernel through 5.6.2. It allows attackers to read uninitialized can_frame data, potentially containing sensitive information from kernel stack memory, if the configuration lacks CONFIG_INIT_STACK_ALL, aka CID-b9258a2cece4.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11494</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.5.0 and newer, the bpf verifier (kernel/bpf/verifier.c) did not properly restrict the register bounds for 32-bit operations, leading to out-of-bounds reads and writes in kernel memory. The vulnerability also affects the Linux 5.4 stable series, starting with v5.4.7, as the introducing commit was backported to that branch. This vulnerability was fixed in 5.6.1, 5.5.14, and 5.4.29. (issue is aka ZDI-CAN-10780)	2020-04-02	not yet calculated	<a href="#">CVE-2020-8835</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

mcafee -- endpoint_security_for_windows	Improper access control vulnerability in ESConfigTool.exe in ENS for Windows all current versions allows a local administrator to alter the ENS configuration up to and including disabling all protection offered by ENS via insecurely implemented encryption of configuration for export and import.	2020-04-01	not yet calculated	<a href="#">CVE-2020-7263</a> <a href="#">CONFIRM</a>
mediawiki -- mediawiki	In MediaWiki before 1.34.1, users can add various Cascading Style Sheets (CSS) classes (which can affect what content is shown or hidden in the user interface) to arbitrary DOM nodes via HTML content within a MediaWiki page. This occurs because jquery.makeCollapsible allows applying an event handler to any Cascading Style Sheets (CSS) selector. There is no known way to exploit this for cross-site scripting (XSS).	2020-04-03	not yet calculated	<a href="#">CVE-2020-10960</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
mitsubishi -- multiple_products	When MELSOFT transmission port (UDP/IP) of Mitsubishi Electric MELSEC iQ-R series (all versions), MELSEC iQ-F series (all versions), MELSEC Q series (all versions), MELSEC L series (all versions), and MELSEC F series (all versions) receives massive amount of data via unspecified vectors, resource consumption occurs and the port does not process the data properly. As a result, it may fall into a denial-of-service (DoS) condition. The vendor states this vulnerability only affects Ethernet communication functions.	2020-03-30	not yet calculated	<a href="#">CVE-2020-5527</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- multiple_products	NETGEAR has released fixes for a pre-authentication command injection in request_handler.php security vulnerability on the following product models: WC7500, running firmware versions prior to 6.5.3.5; WC7520, running firmware versions prior to 2.5.0.46; WC7600v1, running firmware versions prior to 6.5.3.5; WC7600v2, running firmware versions prior to 6.5.3.5; and WC9500, running firmware versions prior to 6.5.3.5.	2020-04-01	not yet calculated	<a href="#">CVE-2018-11106</a> <a href="#">CONFIRM</a>
parrot -- anafi_drone	Web server running on Parrot ANAFI can be crashed due to the SDK command "Common_CurrentDateTime" being sent to control_service with larger than expected date length.	2020-04-01	not yet calculated	<a href="#">CVE-2019-3945</a> <a href="#">MISC</a>
parrot -- anafi_drone	Parrot ANAFI is vulnerable to Wi-Fi deauthentication attack, allowing remote	2020-04-	not yet	<a href="#">CVE-2019-</a>

	and unauthenticated attackers to disconnect drone from controller during mid-flight.	01	calculated	<a href="#">3944</a> <a href="#">MISC</a>
pomelo-monitor -- pomelo-monitor	pomelo-monitor through 0.3.7 is vulnerable to Command Injection.It allows injection of arbitrary commands as part of 'pomelo-monitor' params.	2020-04-02	not yet calculated	<a href="#">CVE-2020-7620</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive_adserver -- revive_adserver	An Open Redirect vulnerability was discovered in Revive Adserver version < 5.0.5 and reported by HackerOne user hoangn144. A remote attacker could trick logged-in users to open a specifically crafted link and have them redirected to any destination.The CSRF protection of the "/www/admin/*-modify.php" could be skipped if no meaningful parameter was sent. No action was performed, but the user was still redirected to the target page, specified via the "returnurl" GET parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8143</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive_adserver -- revive_adserver	A security restriction bypass vulnerability has been discovered in Revive Adserver version < 5.0.5 by HackerOne user hoangn144. Revive Adserver, like many other applications, requires the logged in user to type the current password in order to change the e-mail address or the password. It was however possible for anyone with access to a Revive Adserver admin user interface to bypass such check and change e-email address or password of the currently logged in user by altering the form payload.The attack requires physical access to the user interface of a logged in user. If the POST payload was altered by turning the "pwold" parameter into an array, Revive Adserver would fetch and authorise the operation even if no password was provided.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8142</a> <a href="#">MISC</a> <a href="#">MISC</a>
slack -- nebula	Slack Nebula through 1.1.0 contains a relative path vulnerability that allows a low-privileged attacker to execute code in the context of the root user via tun_darwin.go or tun_windows.go. A user can also use Nebula to execute arbitrary code in the user's own context, e.g., for user-level persistence or to bypass security controls. NOTE: the vendor states that this "requires a high degree of access and other preconditions that are tough to achieve."	2020-04-02	not yet calculated	<a href="#">CVE-2020-11498</a> <a href="#">MISC</a> <a href="#">MISC</a>



sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager 3.x up to and including 3.21.2 has Incorrect Access Control.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11444</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
starface -- ucc_client	STARFACE UCC Client before 6.7.1.204 on WIndows allows binary planting to execute code with System rights, aka usd-2020-0006.	2020-04-02	not yet calculated	<a href="#">CVE-2020-10515</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
suse -- linux_enterprise_server	A Insufficient Verification of Data Authenticity vulnerability in autoyast2 of SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 15 allows remote attackers to MITM connections when deprecated and unused functionality of autoyast2 is used in autoyast2. This issue affects: SUSE Linux Enterprise Server 12 autoyast2 version 4.1.9-3.9.1 and prior versions. SUSE Linux Enterprise Server 15 autoyast2 version 4.0.70-3.20.1 and prior versions.	2020-04-03	not yet calculated	<a href="#">CVE-2019-18905</a> <a href="#">CONFIRM</a>
suse -- multiple_products	A Race Condition Enabling Link Following vulnerability in the packaging of texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users to corrupt files or potentially escalate privileges. This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filesystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filesystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filesystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filesystem versions prior to 2017.135-lp151.8.3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8016</a> <a href="#">CONFIRM</a>
	A Race Condition Enabling Link Following vulnerability in the cron job shipped with texlive-filesystem of SUSE Linux Enterprise Module for Desktop Applications 15-SP1, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local users in group mktex to delete arbitrary files on the			

suse -- multiple_products	system This issue affects: SUSE Linux Enterprise Module for Desktop Applications 15-SP1 texlive-filessystem versions prior to 2017.135-9.5.1. SUSE Linux Enterprise Software Development Kit 12-SP4 texlive-filessystem versions prior to 2013.74-16.5.1. SUSE Linux Enterprise Software Development Kit 12-SP5 texlive-filessystem versions prior to 2013.74-16.5.1. openSUSE Leap 15.1 texlive-filessystem versions prior to 2017.135-lp151.8.3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8017</a> <a href="#">CONFIRM</a>
suse -- multiple_products	A Uncontrolled Resource Consumption vulnerability in rmt of SUSE Linux Enterprise High Performance Computing 15-ESPOS, SUSE Linux Enterprise High Performance Computing 15-LTSS, SUSE Linux Enterprise Module for Public Cloud 15-SP1, SUSE Linux Enterprise Module for Server Applications 15, SUSE Linux Enterprise Module for Server Applications 15-SP1, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1 allows remote attackers to cause DoS against rmt by requesting migrations. This issue affects: SUSE Linux Enterprise High Performance Computing 15-ESPOS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise High Performance Computing 15-LTSS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Module for Public Cloud 15-SP1 rmt-server versions prior to 2.5.2-3.9.1. SUSE Linux Enterprise Module for Server Applications 15 rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Module for Server Applications 15-SP1 rmt-server versions prior to 2.5.2-3.9.1. SUSE Linux Enterprise Server 15-LTSS rmt-server versions prior to 2.5.2-3.26.1. SUSE Linux Enterprise Server for SAP 15 rmt-server versions prior to 2.5.2-3.26.1. openSUSE Leap 15.1 rmt-server versions prior to 2.5.2-lp151.2.9.1.	2020-04-03	not yet calculated	<a href="#">CVE-2019-18904</a> <a href="#">CONFIRM</a>
	A Least Privilege Violation vulnerability in crowbar of SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud 9, SUSE OpenStack Cloud Crowbar 8, SUSE OpenStack Cloud Crowbar 9 allows root users on any crowbar managed node to cause become			

suse -- openstack_cloud_and_	root on any other node. This issue affects: SUSE OpenStack Cloud 7 crowbar-core versions prior to 4.0+git.1578392992.fabfd186c-9.63.1, crowbar-. SUSE OpenStack Cloud 8 openstack_cloud_and_ versions prior to 8.0+git.1579279939.ee7da88-3.39.3, ardana-. SUSE OpenStack Cloud 9 ardana-ansible versions prior to 9.0+git.1581611758.f694f7d-3.16.1, ardana-. SUSE OpenStack Cloud Crowbar 8 crowbar-core versions prior to 5.0+git.1582968668.1a55c77c5-3.35.4, crowbar-. SUSE OpenStack Cloud Crowbar 9 crowbar-core versions prior to 6.0+git.1582892022.cbd70e833-3.19.3, crowbar-.	2020-04-03	not yet calculated	<a href="#">CVE-2018-17954</a> <a href="#">CONFIRM</a>
suse -- opensuse_factory	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of exim in openSUSE Factory allows local attackers to escalate from user mail to root. This issue affects: openSUSE Factory exim versions prior to 4.93.0.4-3.1.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8015</a> <a href="#">CONFIRM</a>
systemd -- systemd	A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.	2020-03-31	not yet calculated	<a href="#">CVE-2020-1712</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
testlink -- testlink	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in planUrgency.php via the urgency parameter.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8638</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
testlink -- testlink	An unrestricted file upload vulnerability in keywordsImport.php in TestLink 1.9.20 allows remote attackers to execute arbitrary code by uploading a file with an executable extension. This allows an authenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to a publicly accessible directory of the application.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8639</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
testlink -- testlink	A SQL injection vulnerability in TestLink 1.9.20 allows attackers to execute arbitrary SQL commands in dragdroptreenodes.php via the node_id	2020-04-03	not yet calculated	<a href="#">CVE-2020-8637</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	parameter.			
tp-link -- cloud_camera	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855.	2020-04-01	not yet calculated	<a href="#">CVE-2020-11445</a> <a href="#">MISC</a>
tp-link -- multiple_devices	TP-Link NC200 through 2.1.8_Build_171109, NC210 through 1.0.9_Build_171214, NC220 through 1.3.0_Build_180105, NC230 through 1.3.0_Build_171205, NC250 through 1.3.0_Build_171205, NC260 through 1.5.1_Build_190805, and NC450 through 1.5.0_Build_181022 devices allow a remote NULL Pointer Dereference.	2020-04-01	not yet calculated	<a href="#">CVE-2020-10231</a> <a href="#">MISC</a> <a href="#">MISC</a>
tp-link -- tl-wr841n_devices	A buffer overflow in the httpd daemon on TP-Link TL-WR841N V10 (firmware version 3.16.9) devices allows an authenticated remote attacker to execute arbitrary code via a GET request to the page for the configuration of the Wi-Fi network.	2020-04-02	not yet calculated	<a href="#">CVE-2020-8423</a> <a href="#">MISC</a> <a href="#">MISC</a>
utils-extend -- utils-extend	Flaw in input validation in npm package utils-extend version 1.0.8 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using utils-extend.	2020-04-03	not yet calculated	<a href="#">CVE-2020-8147</a> <a href="#">MISC</a>
viewvc -- viewvc	ViewVC before versions 1.1.28 and 1.2.1 has a XSS vulnerability in CVS show_subdir_lastmod support. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a CVS repository exposed by an otherwise trusted ViewVC instance that also has the `show_subdir_lastmod` feature enabled. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. This vulnerability is patched in versions 1.2.1 and 1.1.28.	2020-04-03	not yet calculated	<a href="#">CVE-2020-5283</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow a vulnerable ActiveX component to be exploited resulting in a buffer overflow, which may lead to a denial-of-service condition and execution of arbitrary code.	2020-04-03	not yet calculated	<a href="#">CVE-2020-10599</a> <a href="#">MISC</a>
	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may			



visam -- vbase_editor_and_vbase_web-remote_module	allow weak or insecure permissions on the VBASE directory resulting in elevation of privileges or malicious effects on the system the next time a privileged user runs the application.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7004 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow an unauthenticated attacker to discover the cryptographic key from the web server and gain information about the login and the encryption/decryption mechanism, which may be exploited to bypass authentication of the HTML5 HMI web interface.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7000 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module may allow an input passed in the URL that is not properly verified before use, which may allow an attacker to read arbitrary files from local resources.	2020-04-03	not yet calculated	<a href="#">CVE-2020-7008 MISC</a>
visam -- vbase_editor_and_vbase_web-remote_module	VISAM VBASE Editor version 11.5.0.2 and VBASE Web-Remote Module allow weak hashing algorithm and insecure permissions which may allow a local attacker to bypass the password-protected mechanism through brute-force attacks, cracking techniques, or overwriting the password hash.	2020-04-03	not yet calculated	<a href="#">CVE-2020-10601 MISC</a>
wordpress -- wordpress	includes/theme-functions.php in the OneTone theme through 3.0.6 for WordPress allows unauthenticated options changes.	2020-04-03	not yet calculated	<a href="#">CVE-2019-17230 MISC</a>
wordpress -- wordpress	includes/theme-functions.php in the OneTone theme through 3.0.6 for WordPress has multiple stored XSS issues.	2020-04-03	not yet calculated	<a href="#">CVE-2019-17231 MISC</a>
xampp -- xampp	An issue was discovered in XAMPP before 7.2.29, 7.3.x before 7.3.16 , and 7.4.x before 7.4.4 on Windows. An unprivileged user can change a .exe configuration in xampp-control.ini for all users (including admins) to enable arbitrary command execution.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11107 CONFIRM</a>
zevenet -- zen_load_balancer	Manage::Certificates in Zen Load Balancer 3.10.1 allows remote authenticated admins to execute arbitrary OS commands via shell metacharacters in the index.cgi cert_issuer, cert_division, cert_organization, cert_locality, cert_state, cert_country, or cert_email parameter.	2020-04-02	not yet calculated	<a href="#">CVE-2020-11490 MISC MISC</a>

zoho -- manageengine_ad_service_plus	Zoho ManageEngine ADSelfService Plus before 5.8.15 allows unauthenticated remote code execution.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11518</a> <a href="#">MISC</a>
zoho -- manageengine_op_manager	In Zoho ManageEngine OpManager before 12.4.181, an unauthenticated remote attacker can send a specially crafted URI to read arbitrary files.	2020-04-04	not yet calculated	<a href="#">CVE-2020-11527</a> <a href="#">MISC</a>
zoom -- client_for_meetings	Zoom Client for Meetings through 4.6.9 uses the ECB mode of AES for video and audio encryption. Within a meeting, all participants use a single 128-bit key.	2020-04-03	not yet calculated	<a href="#">CVE-2020-11500</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fgrgurina@sunnyvale.ca.gov](mailto:fgrgurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for March 30, 2020  
**Date:** Monday, March 30, 2020 5:04:25 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)



## **COVID-19 Watch: Los Angeles County Public Defenders, DAs, City Attorneys & Police Unions say courts are unsafe**

Right now, a lot of people don't appear to feel safe in most of Los Angeles County's courthouses. In a remarkable letter authored collectively by the Los Angeles County Public Defenders, LA District Attorneys, and Los Angeles City Attorneys, the three groups collectively called for "immediate closure" of the county's courts "due to unsafe conditions."

[Witness LA](#)

## **Justice amid a pandemic: court closures, rules vary from county to county**

In San Diego, state courthouses are closed to the public for three weeks and open only for a handful of emergency business through April 3. Placer County pared down many of its operations but authorities there last week said the Superior Court is open for "critical minimum functions," which include things like "matters involving civil liberties, restraining orders and similar emergency matters."

[San Diego Union-Tribune](#)

## **Lawyers press California judiciary for uniform operating standards amid pandemic**

California lawyers are pressing Chief Justice Tani Cantil-Sakauye for uniform operating standards as courts around the state take vastly different approaches to business in the wake of the COVID-19 outbreak. Alameda County District Attorney Nancy O'Malley, president of the California District Attorneys Association, sent a letter Saturday to judicial branch leaders, urging them to address "inequities in California's courthouses."

[Law.com](#)

## **Op-ed: Judicial inaction**

The state judiciary's imperviousness to the COVID-19 crisis is making things worse. The orders from both the California chief justice and the Los Angeles presiding judge lack clarity and action. They disregard all the science behind slowing down and defeating this pandemic. Meanwhile, they are giving the public the misconception that the judicial branch is on top of it - far from it.

[Antelope Valley Times](#)

## **A slew of federal and state courts suspend trials or close for coronavirus threat**

The number of federal and state courts taking steps to thwart transmission of the novel coronavirus continues to grow. More than 25 federal district courts are pausing jury trials, following a trend that is still gaining ground in state courts. The Administrative Office of U.S. Courts is keeping track of the orders in this chart. Several federal appellate and trial-level courts are also barring people who don't have



official court business from entering courthouses.

[ABA Journal](#)

### **U.S. Supreme Court lets states bar insanity defense**

The U.S. Supreme Court on Monday limited the rights of criminal defendants, declaring that states can bar them from using the so-called insanity defense in a ruling involving a Kansas man sentenced to death for killing four members of his family. The justices ruled 6-3 that a 1995 Kansas law eliminating the insanity defense - which bars holding criminally responsible mentally impaired defendants who do not know right from wrong - did not violate the U.S. Constitution.

[WHBL](#)

### **Panel ponders whether reversal is required based on ouster of juror**

Pending before the Ninth U.S. Circuit Court of Appeals is a case in which two appellants claim they were denied fair trials because the judge dismissed a juror during deliberations because two other panel members complained that she wasn't participating in the deliberations, one of them, the foreman, saying they could not reach a verdict unless the woman, a paralegal, were booted off.

[Metropolitan News-Enterprise](#)

### **Ninth Circuit tightens focus of abortion foe's look at lab researcher files**

Anti-abortion activist David Daleiden may see some unredacted public records on a group of employees and researchers affiliated with the University of Washington's Birth Defects Research Center but the identities of five employees are protected from disclosure, the Ninth Circuit ruled Wednesday.

[Courthouse News Service](#)

### **U.S. Supreme Court tosses ruling that revived comedian's racial bias suit against Comcast**

The U.S. Supreme Court on Monday threw out a lower court's ruling that had given the green light to comedian-turned-media entrepreneur Byron Allen's \$20 billion racial bias lawsuit against Comcast Corp CMCSA.O that accused the cable television operator of discriminating against black-owned channels.

[Reuters](#)

### **Appeals court sides with Redondo Beach in election date lawsuit**

California's Second District Court of Appeals has ruled in favor of the City of Redondo Beach in its lawsuit against Secretary of State Alex Padilla regarding election dates. The appellate court affirmed the Los Angeles Superior Court September 2018 ruling that the City of Redondo Beach, as a charter city, is not beholden to the effect of 2015's California Senate Bill 415. The appeal court's decision did not address whether or not the law is constitutional.

[EasyReaderNews](#)

### **Court won't review AV murder case**

The California Supreme Court refused Wednesday to review the case of a man convicted of murdering his girlfriend's ex-husband at a mobile home park. James Robert Carson was convicted of first-degree murder for the March 3, 2017, slaying of Joey Jojola, who was stabbed once in the heart and once in the back outside the trailer that the 50-year-old victim had bought for his ex-wife, her daughter and the daughter's baby.

[City News Service](#)

### **In phone hearing, panel takes up revoked White House press pass**

An attorney for a Playboy reporter warned the D.C. Circuit on Monday during unorthodox teleconference oral arguments that the White House revoking his client's press pass is particularly alarming during the Covid-19 outbreak. "Ensuring that the press can vigorously cover the president and the White House is more important now than ever," said Gibson Dunn attorney Theodore Boutrous Jr.

[Courthouse News Service](#)

### **Second Circuit won't rehear finding Trump can't block Twitter critics**

The Second Circuit refused to convene the full court on Monday to reconsider what the majority overwhelmingly called a straightforward application of First Amendment law: a ruling forbidding President Donald Trump from blocking his critics on Twitter. Only two members of the court argued for another hearing. Both are Trump appointees. U.S. Circuit Judge Barrington Parker, who was appointed by President George W. Bush, sounded off meanwhile on why the case is closed.

[Courthouse News Service](#)

### **Prosecutor whose father was victim of embezzlement, as was he, breached ethics in urging FBI probe**

It is unethical for a prosecutor who was personally victimized by criminal conduct to complain to a law enforcement office and prompt action, the Ninth U.S. Circuit Court of Appeals declared on Friday. A three-judge panel affirmed the conviction of James Miller on five counts of wire fraud and four counts of filing false tax returns but said, in an opinion by District Court Judge Jed S. Rakoff of the Southern District of New York, sitting by designation, that there was instructional error and misconduct by an assistant U.S. attorney.

[Metropolitan News-Enterprise](#)

### **Taxi companies strike out in bid to pursue 'predatory' pricing claims against Uber**

A California appeals court has joined a choir of federal courts who have ruled that Uber is a public utility service and entitled to certain

exemptions around below-cost sales. Taxi company plaintiffs had alleged Uber employs a predatory pricing model meant to undercut the competition. But California's First District Court of Appeal ruled Monday the state's Unfair Practices Act does not apply to Uber, whose rates are governed by the California Public Utilities Commission.

[Law.com](#)

### **Practice that made 5th Circuit an outlier snuffed out by SCOTUS**

The Supreme Court rapped the Fifth Circuit on Monday for its unusual practice of refusing to entertain any argument that was not raised at the lower court level. The case stems from a report of a suspicious car that prompted Dallas police to find meth and a gun on Charles Earl Davis in July 2016. Davis soon pleaded guilty to the resulting federal indictment but still had drug and gun charges pending at the state level from a 2015 arrest.

[Courthouse News Service](#)

### **High Court revives decades-old deportation dispute**

The Supreme Court on Monday held a federal appeals court may hear the claims of two men seeking to have their removal proceedings reopened decades after they were deported for committing drug crimes. The case concerned two men who were legal permanent residents but the federal government deported them after they were convicted of drug charges.

[Courthouse News Service](#)

### **Appeals court reverses murder conviction for well-known East Bay justice advocate DeAngelo Cortijo**

A California appeals court has reversed the second degree murder conviction against DeAngelo Cortijo, a criminal justice advocate from the East Bay, despite a rare dissenting view by one of the three judges on the panel. Cortijo, 26, was convicted in 2018 of killing 26-year-old Oakland resident Jamad Jerkins, who was fatally shot in October 2016. But in a decision issued March 6, the appeals court reversed that conviction, finding that a mistrial should have been declared during testimony of the prosecution's very first witness.

[Mercury News](#)

### **Judge overturns verdict against man who flipped off cop**

A Virginia man who claimed he was illegally searched after he gave the middle finger to a police officer scored a win in federal court where a judge overturned a jury verdict favoring the cop. Brian H. Clark was apparently no stranger to the Patrick County courthouse as he had previously been banned from entering the building except under certain circumstances.

[Courthouse News Service](#)

### **Ventura judge censured for years of 'sexist and unseemly' remarks**

A Ventura county judge accused of making crude and demeaning comments to lawyers and court employees has been censured under an agreement reached with state judicial disciplinarians. Judge Jeffrey Bennett of the Ventura County Superior Court acknowledged he acted inappropriately in 28 instances over eight years, according to a decision and order released Wednesday by the Commission on Judicial Performance.

[Law.com](#)

### **California Supreme Court sides against school districts in state mandates case**

In California School Boards Association v. State of California (CSBA), the California Supreme Court has allowed the Legislature to avoid appropriating new funding to cover the costs of state mandated programs. Instead, the Legislature is now able to point to existing, unrestricted state funding to satisfy the Constitutional requirement that it identify funding for such programs.

[Lozano Smith News](#)

## **Prosecutors/ Prosecutions**

### **Lacey headed for runoff with Gascon in DA's race**

Los Angeles County District Attorney Jackie Lacey is headed for a November runoff against former San Francisco D.A. George Gascon, according to the latest update from the March 3 primary election released Friday. Lacey has 48.71% of the vote, to 28.20% for Gascon. Former public defender Rachel Rossi was third with 23.09%. The incumbent needed to finish with more than 50% of the vote to avoid a runoff.

[City News Service](#)

### **Despicable: Feds shut down bogus virus vaccine website**

A scam website asking people for their credit card numbers by claiming it can sell free World Health Organization coronavirus vaccine kits for \$4.95 in shipping was taken down after the federal government filed a lawsuit to shutter it. An FBI agent visited coronavirusmedicalkit.com on Thursday and read: "Due to the recent outbreak for the Coronavirus (Covid-19) the World Health Organization is giving away vaccine kits. Just pay \$4.95 for shipping," the Justice Department said in a federal lawsuit filed Saturday in Austin.

[Courthouse News Service](#)

## **Policy/ Legal Issues**

### **LAPD Chief: Planning in case many more officers sickened by coronavirus**

Los Angeles Police Department Chief Michel Moore says he's optimistic the Department can prevent widespread coronavirus infections amongst officers by distancing when possible and using protective equipment.



"We've been fortunate to this point," the chief said. Still, Moore told NBCLA Thursday, he has spent the last few weeks making contingency plans in case a large group of officers is unable to work because of the virus.

[NBC4 Los Angeles](#)

### **Calif. police using drones to patrol during COVID-19 lockdown**

Some police departments in California plan on using drones to enforce a coronavirus lockdown and to, in part, monitor the homeless population, according to a report on Friday. The Chula Vista Police Department, located just south of San Diego near the California-Mexico border, recently purchased two \$11,000 drones - doubling its fleet - that will be outfitted with speakers and night vision cameras.

[Syracuse Media Group](#)

### **Coronavirus makes sex offenders scared of registering in person with cops: Lawsuit!**

A lawsuit has been filed against the city of Murrieta in Riverside County on behalf local sex offender registrants who are challenging requirements that they must register in person at police offices during the coronavirus pandemic, even though governments ask that residents stay home to prevent the virus' spread. The lawsuit was filed by the Alliance for Constitutional Sex Offense Laws, which also filed similar lawsuits this week in San Diego and Sacramento counties.

[My News LA](#)

### **Coronavirus has transformed policing in the US, as officers scramble to get tested, stay safe**

After a reserve police officer in San Jose, California, tested positive for coronavirus last week, 20 of his colleagues were quarantined. Another 10 full-time employees from the police department's family violence unit were also asked to stay home. "You can imagine. Just this one incident could create an issue with regards to investigations of those real high-profile domestic violence, child abuse cases," said Sgt. Paul Kelly, president of the San Jose Police Officers Association.

[USA Today](#)

### **Gov. Newsom halts intake of inmates into state prisons, citing coronavirus threat**

Gov. Gavin Newsom issued an executive order Tuesday evening suspending the intake of new prisoners into both state and juvenile facilities, citing the health and safety of current staff and inmates in state lockups. Newsom said counties should keep teenagers and adults in local facilities for at least the next 30 days. He also ordered all parole hearings to be conducted via video conference for the next 60 days, and instructed the state Board of Parole Hearings to create a system by April 13 to conduct those hearings.

[KQED](#)

## **Balancing justice, public safety: Virus brings changes to courts, jails, arrests**

What to do with a jury summons during a pandemic? That was the question Edward Lifson faced when he opened his mail and read that he was scheduled for jury duty in Los Angeles this week. Lifson believes it's an honor and a duty to serve on a jury, but, "to be honest, I would not do it right now," he says. "If they told me I had to come in I would say no." No worries for Lifson and other potential jurors, though.

[Valley Public Radio](#)

## **U.S. combats martial law conspiracy theories as the National Guard assists in coronavirus response**

The Defense Department's response to the coronavirus outbreak has expanded to include not only the expected deployment of tens of thousands of National Guardsmen, but also a growing effort to stamp out conspiracy theories that the United States will adopt martial law. Senior U.S. officials have addressed the issue in briefings, a Pentagon official rebutted speculative online posts and the government has created a new website titled "Coronavirus Rumor Control."

[Washington Post](#)

## **Los Angeles County/City**

### **L.A. County Sheriff cites retaliation after county leaders file urgency ordinance to remove him as Director of Emergency Operations**

Los Angeles County Sheriff Alex Villanueva told FOX 11 he believes he's the target of political retaliation after county leaders filed an urgency ordinance Wednesday afternoon that would remove him as Director of Emergency Operations during this coronavirus crisis if it's passed. "This is all about a power grab," Villanueva said. "It's a silent coup."

Villanueva believes the move came in response to comments he made to FOX 11 reporter Bill Melugin Monday night.

[Fox11 Los Angeles](#)

### **LA County releases 1,700 inmates to lessen jail population amid coronavirus pandemic**

The Los Angeles County Jail has released approximately 1,700 inmates to lessen the inmate population during the coronavirus pandemic, Sheriff Alex Villanueva said Tuesday. These releases lowered the county's jail population by about 10 percent, according to Villanueva. On Friday, L.A. District Attorney Jackie Lacey said that she instructed prosecutors to take steps to lower the number of people in local jails and area courthouses in an effort to slow the spread of COVID-19.

[CBS LA](#)

### **LA County Supervisors issue executive order in hope of protecting jails from COVID-19 catastrophe**

Late on Monday, March 23, Kathryn Barger, the Chair of Los Angeles

County Supervisors, issued an Executive Order that asks LA County's Health Officer, Muntu Davis, MD, MPH, to conduct an "immediate assessment" of the county's jails for the purpose of identifying any and all additional "necessary and appropriate measures" to prevent COVID-19 from spreading wildfire-like through the nation's largest jail system.

[Witness LA](#)

### **Staffer sues former LA City Councilman, says he was fired for speaking out**

A former aide to Los Angeles City Councilman Jose Huizar filed a lawsuit against his ex-boss and the city Tuesday, alleging he was fired in 2019 for speaking to authorities about alleged misconduct concerning the lawmaker. The retaliation- and whistleblower-based wrongful termination lawsuit was filed in Los Angeles Superior Court by Jesse Leon, who alleges that he is the third staffer that the council member has fired for speaking out about practices that he believed Huizar was engaged in that violated local, state and federal law.

[City News Service](#)

### **LAPD reserve officer saves veteran's life after suicide attempt**

At the Los Angeles Police Department Southwest station, he's known as "Doc," a volunteer reserve officer. At Cedars-Sinai, he is Paul Strauss, MD, an anesthesiologist at Cedars-Sinai since 1999. Either way, Strauss is a lifesaver. In January, he was among the officers dispatched after getting a call about a military veteran about to kill herself. When Strauss arrived on the scene, she was unresponsive and not breathing. Strauss told KCAL he acted immediately.

[PoliceOne](#)

### **City leaders in court over homeless lawsuit (Video)**

Mayor Eric Garcetti and LAPD Chief Michel Moore both were on hand to attend a court hearing to discuss what the city is doing to help the homeless community amid the coronavirus outbreak. Kandiss Crone reports.

[CBS LA](#)

### **More than 1,200 homeless people in California likely to die from coronavirus, report says**

More than 1,200 people experiencing homelessness in California will likely die due to the coronavirus, according to research released Wednesday. That number is a large chunk of the total of 3,400 homeless people expected to die from COVID-19 across the United States, said the study's authors, which included researchers from UCLA, Boston University and the University of Pennsylvania.

[NBC4 Los Angeles](#)

### **Drive-thru testing site for first-responders opens near Dodger Stadium**

A drive-thru coronavirus testing center for first-responders and essential

city employees was in operation Saturday morning at a fire department training facility near Dodger Stadium. Vehicles drove past signs that said "City Employees Only" and a pre-screening checkpoint at the entrance of the Frank Hotchkin Memorial Training Center on Stadium Way. The vehicles then drove through the parking lot and stopped next to a canopy, where persons in protective gear approached each driver.

[The Eastrider](#)

### **L.A. sues Venice landlord over 'illegal hotel.' Tenants say they face coronavirus risk**

Los Angeles is taking a longtime landlord to court, accusing him of illegally running a Venice apartment building as an unpermitted hotel outfitted with a reception desk, key cards and noisy shows for a revolving door of tourists. The Ellison has long been a focus for local activists and officials alarmed that apartment buildings have been illegally turned into hotels.

[Los Angeles Times](#)

### **Can you get a parking ticket during coronavirus moratorium in LA? We investigate**

Cities like Los Angeles are still issuing millions of dollars in parking citations, despite calling for "moratoriums" on most ticketing during the coronavirus pandemic. "I thought there was some sort of abatement on tickets. I thought that it was delayed or pushed off," Kayla said after her BMW was ticketed and towed Sunday near Lake Hollywood, costing her over \$300. Kayla was parked for two hours in a zone marked "5 Minute Limit Only."

[NBC4 Los Angeles](#)

## **Consumer**

### **COVID-19: Los Angeles City Attorney Mike Feuer warns against price-gouging**

Authorities locally are on the lookout for anyone who is price-gouging consumers. Los Angeles City Attorney Mike Feuer said in a public message that he has already located companies engaged in that practice online. "We recently purchased from third party sellers online on Amazon a half-gallon of bleach for more than \$100. We also bought a two-pack of one-liter hand sanitizer for \$149," he said.

[CBS LA](#)

### **LA County alerts public about increasing Covid-19 scams, warns of fraudulent websites, emails and donation requests**

As L.A. County continues to follow the "safer at home" public order in an effort to curb spread of the novel coronavirus, officials warned residents Tuesday of several fraud schemes designed to prey on the vulnerable in the midst of the public health crisis. "Malicious actors can prey upon those that are distracted by the COVID-19 pandemic, and use it to their advantage," Los Angeles County Chief Information Officer William Kehoe



said in a news release.

[KTLA](#)

### **In the coronavirus 'infodemic,' here's how to avoid bad information**

The same coronavirus post kept popping up on my Facebook feed last week. People in my network - a friend's mom, a college classmate and another "friend," who I'm not sure I've even met in person - had somehow obtained identical symptom and treatment guidance from Stanford University. There were details about an at-home testing technique involving breath holding, as well as something truly dubious about sipping water every 15 minutes.

[Wall Street Journal](#)

### **Attorney General Becerra issues consumer alert regarding false advertising related to coronavirus**

California Attorney General Xavier Becerra today issued a consumer alert about deceptive advertising related to novel coronavirus - or COVID-19 - in California. Attorney General Becerra reminds all Californians to be mindful of any products or services that falsely claim to treat, diagnose, prevent, or cure COVID-19.

[Attorney General Press Release](#)

## **Public Safety/Crime**

### **White supremacists encouraging their members to spread coronavirus to cops, Jews, FBI says**

Racist extremist groups, including neo-Nazis and other white supremacists, are encouraging members who contract novel coronavirus disease to spread the contagion to cops and Jews, according to intelligence gathered by the FBI. In an alert obtained by ABC News, the FBI's New York office reports that "members of extremist groups are encouraging one another to spread the virus, if contracted, through bodily fluids and personal interactions."

[ABC News](#)

### **FBI arrests man accused of seeking investments for a fake coronavirus miracle cure**

A man who claimed in a strange series of YouTube and Instagram videos that he had created a miracle cure for the novel coronavirus and needed financing to mass produce an unproven pill was arrested Wednesday by the FBI. Keith Lawrence Middlebrook, 53, was arrested Wednesday while delivering the pills to an undercover FBI agent posing as an investor, according to Thom Mrozek, director of media relations for the U.S. Attorney's Office.

[NBC4 Los Angeles](#)

### **Crime drops as LA stays home to combat coronavirus**

As people heed stay-at-home orders issued in an attempt to stop the

spread of the coronavirus, the number of crimes committed in Los Angeles County has declined, officials said Wednesday. "We took a pulse of the overall county crime numbers yesterday, and it was for violent crimes...a 10% drop and for overall crime throughout the county it was a 6% drop," Sheriff Alex Villanueva said Wednesday afternoon. The Los Angeles Police Department has also reported a decrease in crime.

[City News Service](#)

### **Is the coronavirus curbing crime?**

Schools are shuttered, restaurants are reduced to take out and Californians have now been ordered to stay home. As for crime? Early indications show that lawbreaking also seems to be on the wane, as life in Los Angeles retreats in order to slow the spread of COVID-19. Over the first 15 days of March, crime reports made to the Los Angeles Police Department saw a steady decline, as social distancing and restrictions put in place by authorities ramped up.

[Crosstown](#)

### **More L.A. County jail inmates released over fears of coronavirus outbreak**

Law enforcement officials speeded up efforts to release inmates from Los Angeles County jails over fears a coronavirus outbreak could afflict scores of individuals and strain the overburdened system. The Los Angeles County Sheriff's Department has reduced its inmate population by 6% in the last three weeks and Dist. Atty Jackie Lacey said her office will consider reducing bail for thousands of nonviolent offenders.

[Los Angeles Times](#)

### **Early release and other precautions taken at Southern California jails wary of coronavirus**

Southern California jails are releasing some low-level inmates early, checking new arrivals for fever and taking other precautions to prevent the novel coronavirus from taking hold behind bars. With thousands of inmates packed into close quarters, county jails seem an unlikely place to accomplish "social distancing," or staying six feet away from other people. But there is more breathing room in Los Angeles County jails, where the population has been reduced by 6 percent to 16,017, according to the Los Angeles Times.

[Orange County Register](#)

### **Gov. Newsom pardons 5 people, commutes sentences of 21 prison inmates**

California Gov. Gavin Newsom on Friday pardoned five people who already served their time and commuted the sentences of 21 state prison inmates, including more than a dozen convicted of murder or related crimes. The victims were children in two of the cases and a pregnant woman in a third. The clemency requests were being considered before the coronavirus crisis, "and, as resources permitted,

the governor decided to move forward with them," spokeswoman Vicky Waters said in an email.

[AP](#)

## California/National

### **Governor gives California Chief Justice 'unprecedented' authority to address pandemic**

Gov. Gavin Newsom late Friday issued an "unprecedented" executive order freeing Chief Justice Tani Cantil-Sakauye of statutory restrictions on her authority to issue statewide court orders addressing COVID-19. The three-page order, which cites the governor's wide-ranging powers under a state of emergency, also suspends laws that limit by-telephone depositions and the service of process by electronic means, two changes sought by the plaintiffs bar and defense counsel.

[Law.com](#)

### **President Trump: REAL ID deadline will be pushed back due to COVID-19 crisis**

President Donald Trump announced Monday that the federal government will push back the approaching deadline for REAL ID compliance due to the COVID-19 crisis. President Trump did not say what the new deadline was but said it will be announced: "very soon." The California DMV tweeted: "Due to COVID19 REALID enforcement date has been extended. Details to follow."

[Fox11 Los Angeles](#)

### **PG&E to plead guilty to 84 involuntary manslaughter counts in 2018 wildfire**

Pacific Gas & Electric will plead guilty to 84 counts of involuntary manslaughter for a swath of death and destruction left behind after its fraying electrical grid ignited a 2018 wildfire that decimated three Northern California towns and drove the nation's largest utility into bankruptcy. The plea agreement announced Monday resolves the charges facing PG&E as part of a previously sealed indictment in Butte County.

[NBC4 Los Angeles](#)

### **El Chapo's sons vs. "El Mencho": Mexico sees rising cartel bloodshed**

Another year, another homicide total unseen before in Mexico's modern history as the country struggles to check rising violence. Cartels and other criminal groups that hold sway over large swaths of territory are blamed for much of it, warring with each other and preying on local populations in places where the state, especially local authority, is weak or even in cahoots with the gangs.

[CBS News](#)

### **Virus attacks California ballot measures**

As the coronavirus pandemic was clobbering California - and the rest of the known world - this month, local government officials in Sacramento County enthusiastically decided to ask voters to approve a hefty sales tax increase for transportation improvements. Were members of the Sacramento Transportation Authority board smoking some of California's newly legalized marijuana? There must be some explanation for their flight of fiscal fantasy.

[CalMatters](#)

## Corrections

### **Coronavirus leads to some California inmates going free; more state prison workers infected**

Cramped, crowded conditions. Prolonged exposure to other people. Limited access to critical health care treatment. These conditions in state prisons and county jails nationwide have sparked urgent calls for the release of thousands of inmates across the country as corrections officials rush to avoid catastrophic outbreaks of coronavirus inside institutions that could infect inmates, correctional staffers and, ultimately, their families and communities at large.

[Sacramento Bee](#)

### **CDCR: First inmate tests positive for COVID-19**

The first inmate within the California state prison system has tested positive for COVID-19, according to the California Department of Corrections and Rehabilitation (CDCR) and California Correctional Health Care Services (CCHCS). The patient is an inmate at California State Prison, Los Angeles County (LAC). He is in stable condition and is being treated on-site. The patient has been in isolation since March 19 after he notified institution health care staff that he was not feeling well.

[Bakersfield Now](#)

### **California State Prison inmate in Lancaster tests positive for coronavirus, CDCR considering early release**

The California Department of Corrections and Rehabilitation was considering early release after an inmate in Lancaster tested positive for the novel coronavirus. "The patient is in stable condition and is being treated on-site," CDCR said in a statement released Sunday. The patient, an inmate at California State Prison in Lancaster, has been in isolation since March 19 when he reported not feeling well.

[CBS LA](#)

### **California state prison workers in San Bernardino County test positive for coronavirus**

Two employees at the California Institution for Men, a state prison in Chino, tested positive for the coronavirus, the California Department of Corrections and Rehabilitation reported on Sunday. "There are no confirmed cases of COVID-19 among the incarcerated population," CDCR



said in a statement about Chino. "If at any point it is determined there is a potential exposure to the incarcerated population, the agency will restrict movement at the institution while a contact investigation is underway and quarantine those deemed at-risk for an observation period."

[Palm Springs Desert Sun](#)

### **Harvey Weinstein quarantined after tested positive for COVID-19 while in N.Y. state prison**

The case was confirmed just a few days after the convicted film producer was moved from Rikers Island in N.Y. to the Wende Correctional Facility. The Deadline reported that Harvey is now in medical quarantine, as told by an official from the Empire State law enforcement. When asked for confirmation, a spokesperson for the New York State Department of Corrections said that they're not allowed to disclose information of an inmate's medical account as per policy.

[Who Knew! News](#)

## **Sentences/Convictions/Parole**

### **Former Waymo engineer pleads guilty to stealing company trade secrets**

Anthony Levandowski, a former engineer who worked on autonomous vehicles, pleaded guilty Thursday to theft of trade secrets, ending a trial that pitted two of the largest technology companies - Google and Uber - against each other. The guilty plea will put a punctuation mark on one of the most prominent trade secret cases in the modern era, as Silicon Valley continues to race each other to produce a self-driving car capable of maneuvering roadways as good, if not better than a human.

[Courthouse News Service](#)

### **Parole denied in 1997 stabbing death**

On March 13 at Centinela State Prison near El Centro, a California parole board issued a 7-year parole denial for Lucio Brito, 43, for the 1997 stabbing death of a 16-year-old Visalia man. At 1:32 a.m. on October 5, 1997, Visalia Police Department officers were called to Kaweah Delta Hospital regarding a stabbing. Contact was made with a witness who told officers the attack occurred in the parking lot of the Jack in the Box restaurant on Mooney Boulevard.

[The Porterville Recorder](#)

## **COVID-19**

### **California's stay-at-home order explained: What's allowed, what's not?**

California Gov. Gavin Newsom on Thursday ordered the state's 40 million residents to stay at home, restricting non-essential movements to control the spread of the coronavirus that threatens to overwhelm the state's medical system. Here are the highlights: All Californians must

stay at home except to get food, prescriptions and health care, care for a friend or relative, walking the dog and taking outdoor exercise such as walking, running or hiking.

[AP](#)

### **Dr. Anthony Fauci warns against following Trump's medical advice**

In a clash of gut instinct versus science, President Donald Trump and the government's top infectious disease expert, Dr. Anthony Fauci, are politely but publicly sparring over whether a malaria drug would work to treat people with coronavirus disease. Trump is clinging to his feeling that a malaria drug widely available could be the answer-in-waiting to an outbreak spreading around the nation, shutting down major parts of the economy, and posing the biggest challenge he has faced as president.

[AP](#)

### **COVID-19 and California's vulnerable populations**

To reduce community spread of COVID-19, California has instituted statewide guidance to shelter in place until further notice, and to practice social distancing when leaving home for approved activities such as grocery shopping or exercise. Because COVID-19 is novel, no vaccine is available and no one has preexisting immunity. However, individuals are not equally at risk, and there are several known sources of vulnerability.

[PPIC](#)

### **Browne George Ross attorneys file first lawsuit over Sen. Richard Burr's coronavirus-tied stock dumps**

A shareholder at one of the companies Sen. Richard Burr sold stock from in the weeks before the coronavirus pandemic rocked the U.S. is suing the senator, alleging the top Republican committed securities fraud by "exploiting material information unavailable to the public." The complaint, filed Monday evening in the U.S. District Court for the District of Columbia by attorneys with the litigation boutique Browne George Ross, alleges that Burr "has acted as a scofflaw in a time of national crisis."

[Law.com](#)

## **Articles of Interest**

### **Pressure builds to ban Congress members from trading stocks**

Records showing that U.S. lawmakers with early reports on the coronavirus pandemic dumped private stock holdings before markets posted recordbreaking losses has roiled the nation, but some experts say criminal fallout is unlikely. Courthouse News reached out to former federal prosecutors for their insights on the traditional avenues of accountability, from the difficulty in trying an inside-trading case to the toothlessness that tends to gum up congressional oversight.

[Courthouse News Service](#)

### **Walmart was almost charged criminally over opioids. Trump appointees killed the indictment.**

On a Tuesday just before Halloween in 2018, a group of federal prosecutors and agents from Texas arrived in Washington. For almost two years, they'd been investigating the opioid dispensing practices of Walmart, the largest company in the world. They had amassed what they viewed as highly damning evidence only to face a major obstacle: top Trump appointees at the Department of Justice.

[ProPublica](#)

## **Pensions**

### **CalPERS loses \$69 billion in biggest market losses since Great Recession**

The pot of invested money used to pay for hundreds of thousands of California public employee pensions has shrunk by \$69 billion as coronavirus has squeezed global markets. The California Public Employees' Retirement System's fund balance stood about \$335 billion Thursday, down from a record high of \$404 billion one month ago, according to CalPERS officials. The California State Teachers' Retirement System likely experienced similar losses, but the system doesn't publicly report its value as often as CalPERS does.

[Sacramento Bee](#)

### **California must act quickly to address the financial crisis**

The stock market dropped 33 percent in the past three weeks. This tremendous financial upheaval demands that California lawmakers take quick action to secure the state's finances. Consider that California's yearly tax revenues are extremely unbalanced. They rely too heavily on the 1 percent of the state's population that generates half of its personal income taxes, thanks mostly to capital gains. Well, those gains have now vanished.

[Orange County Register](#)

### **California teacher pension system secures \$992M for mixed-asset portfolio**

The California State Teachers' Retirement System (CalSTRS) has secured \$991.8 million in financing for a 17-property mixed-asset portfolio that spreads across seven states. The 10-year, fixed-rate loan was provided by New York Life Insurance Company, according to JLL, which announced the agreement and arranged the financing for CalSTRS. New York Life Insurance Company, CalSTRS and JLL did not immediately respond to requests for comment.

[Commercial Observer](#)

### **San Francisco pension fund asks S&P 500 firms for coronavirus action**

San Francisco City & County Employees' Retirement System is calling for companies to take action in the fight against the coronavirus pandemic and is specifically asking S&P 500 companies to provide reports on what actions they are taking. The \$25 billion pension fund is calling for companies to take actions including providing hotels and sporting venues as facilities for health-care professionals and patients, according to a Monday news release emailed by Executive Director Jay Huish.

[Pensions & Investments](#)

### **Riverside County could borrow \$727M via bonds to cut pension debt**

Riverside County could issue almost \$730 million in bonds to whittle down its \$3.5 billion pension debt, a move meant to save money while tackling a massive, growing and chronic expense that looms over county finances. The Board of Supervisors last week voted 3-2 to go to the bond market to pay 20% of the county's unfunded pension liability. The Tuesday, March 17, vote doesn't mean the county will sell bonds right away, but it sets the wheels in motion to get to that point.

[Riverside Press-Enterprise](#)

---

***For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).***

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)



From: [Homeland Security News Wire](#)  
To: [info@hcn.sunnyvale.ca.us](mailto:info@hcn.sunnyvale.ca.us)  
Subject: Week in Review  
Date: Saturday, March 14, 2020 6:53:31 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



## Week in Review

BIOMETRICS BORDER/IMMIG. BUSINESS CYBERSECURITY DETECTION DISASTERS GOVERNMENT INFRASTRUCTURE  
PUBLIC HEALTH PUBLIC SAFETY REGIONAL SCI-TECH SURVEILLANCE TERRORISM TRANSPORTATION WATER

Friday 13 March 2020 vol. 3 no. 49

### Epidemics

#### ECDC: COVID-19 Not Containable, Set to Overwhelm Hospitals

In a stark and urgent COVID-19 risk assessment update today, the European Centre for Disease Prevention and Control (ECDC) said that, in a few weeks or even days, other countries in the region may face huge surges that mirror those of China and Italy.

[Read more](#)

#### Testing and Isolation, Not Travel Bans, Are Best Tool Against Coronavirus, Experts Say

Travel bans may slow the outbreak somewhat, a growing body of research is showing that the best tool is one that is falling short in the United States: testing and isolating infected people.

[Read more](#)

#### What's the Difference Between Pandemic, Epidemic and Outbreak?

By Rebecca S. B. Fischer

The coronavirus is on everyone's minds. As an epidemiologist, I find it interesting to hear people using technical terms – like quarantine or super spreader or reproductive number – that my colleagues and I use in our work every day. But I'm also hearing newscasters and neighbors alike mixing up three important words: outbreak, epidemic and pandemic. Simply put, the difference between these three scenarios of disease spread is a matter of scale.

[Read more](#)

### Truth decay

#### Chinese and Russian State-Owned Media on the Coronavirus: United Against the West?

By Amber Frankland and Matt Schrader

Beginning in late January, when news emerged of a "novel coronavirus" spreading through China, Beijing's propaganda apparatus shifted into overdrive. The epidemic has also been heavily covered in externally directed Russian state-backed media outlets, offering an opportunity to compare and contrast the approaches of both countries' propaganda apparatuses.

[Read more](#)

#### Better Math to Help Stop Spread of False Rumors about COVID-19

Think of all the false rumors that went viral about COVID-19—it got so bad, the World Health Organization called it an "infodemic." Whether it is in hoaxes or a viral conspiracy theory, information travels fast these days. Just how fast and far information moves depends on who shares it, and where, from discussions on social media to conversations with fellow commuters on your way to work. So, how can our interactions and their infrastructures affect the spread of rumors and information? That's a question that researchers are beginning to answer with complex math models of social contagion, the concept that social behavior and

ideas spread like a pathogen.

[Read more](#)

#### **The Russia connection**

### **Facebook, Twitter Remove Russia-Linked Fake Accounts Targeting Americans**

Social-media giants Facebook and Twitter say they have removed a number of Russia-linked fake accounts that targeted U.S. users from their operations in Ghana and Nigeria. Facebook on 12 March said the accounts it removed were in the “early stages” of building an audience on behalf of individuals in Russia, posting on topics such as black history, celebrity gossip, and fashion.

[Read more](#)

#### **Extremism**

### **Extremists Use Coronavirus to Advance Racist, Conspiratorial Agendas**

As the number of confirmed cases of coronavirus surges globally, extremists continue to use the virus to advance their bigotry and anti-Semitism, while also promoting conspiracy theories and even boogaloo (the white supremacist term for civil war). As usual, extremists are relying primarily on fringe social media platforms to disseminate their views, but as the virus spreads, it has gotten easier to find xenophobia, anti-Semitism and conspiracy theories on mainstream social media platforms.

[Read more](#)

#### **China syndrome**

### **U.K.: Tory MPs Rebel against Government’s Huawei’s Plan**

The U.K. government has launched an all-hands-on-deck effort to contain a growing rebellion by Tory MPs who want to ban the use of Huawei’s equipment in the U.K. 5G telecoms network, arguing that allowing the Chinese company, with its close ties to China’s intelligence and military establishments, any access to the country’s communication infrastructure would be like inviting a fox to guard the hen house.

[Read more](#)

#### **Cybersecurity**

### **“Speed and Agility,” “Layered Cyber Deterrence” to Bolster American Cyber Defenses**

The Cyberspace Solarium Commission (CSC) the other day released its report on how to best protect the nation’s critical infrastructure from a cyberattack of significant consequence. In the report, the CSC lays out a comprehensive strategy to restore deterrence in cyberspace and provides extensive policy and legislative actions to enable this strategy. The report lays out more than 75 recommendations to improve the cybersecurity of U.S. critical infrastructure and recommends a strategy of “layered cyber deterrence” that seeks to shape behavior in cyberspace, deny benefits to adversaries who would seek to exploit cyberspace to their advantage, and impose costs against those who would nonetheless choose to target America in and through cyberspace.

[Read more](#)

### **Next Generation 911 Services Vulnerable to Cyberattacks**

Despite a previous warning by Ben-Gurion University of the Negev (BGU) researchers, who exposed vulnerabilities in 911 systems due to distributed denial of service attacks (DDoS), the next generation of 911 systems that now accommodate text, images and video still have the same or more severe issues.

[Read more](#)

### **Novel Cybersecurity Approach to Protect Army Systems**

Networked devices and infrastructure are becoming increasingly complex, making it nearly impossible to verify an entire system, and new attacks are continuously being developed. Researchers have identified an approach to network security that will enhance the

effectiveness and timeliness of protection against adversarial intrusion and evasion strategies.

[Read more](#)

#### Privacy

### **Mind Reading: New Software Agents Will Infer What Users Are Thinking**

Personal assistants today can figure out what you are saying, but what if they could infer what you were thinking based on your actions? A team of academic and industrial researchers is working to build artificially intelligent agents with this social skill.

[Read more](#)

#### Bomb disposal

### **Water Cannon Technology Disarms IEDs**

Improvised explosive devices (IEDs) are a constant and ever-changing threat to the security of our nation. Their extreme destructive potential demands innovative solutions. That's where the Reverse Velocity Jet Tamper (ReVJeT) comes in. ReVJeT breaks apart IEDs by targeting a stream of high-velocity liquid, such as water. It does not detonate the device, but rather disarms it from a distance and allows bomb technicians do their jobs faster, safer, and more effectively.

[Read more](#)

#### Drones

### **Identify, Track, Capture: Addressing UAS Threats**

Sandia National Laboratories robotics experts are working on a way to intercept enemy unmanned aircraft systems midflight. They successfully tested their concept indoors with a swarm of four unmanned aircraft systems that flew in unison, each carrying one corner of a net. Acting as a team, they intercepted the flying target, trapped it in air like an insect caught in a web and safely lowered it to the ground.

[Read more](#)

#### Bridges

### **A First: New Bridge Building Technology Successfully Used in Austrian Alps**

There are many different methods for erecting bridges, but the new technique -- the balanced lowering method -- is quite spectacular: the bridge is not built horizontally, as would normally be case, but erected in a vertical position and then rotated into the horizontal position. The new bridge construction technology has now been successfully used in the construction of the Fürstenfeld Motorway in the Austrian Alps.

[Read more](#)

#### Grid

### **The Modern Electric Grid Needs Smarter Modeling for Improving Resilience**

Today's smart grid involves components that talk to each other, sending signals over communication networks to keep power flowing smoothly and efficiently. But what happens when the "conversation" goes quiet? The growing interdependence of power systems and communication networks can affect the response and recovery times when problems occur.

[Read more](#)

#### Argument

### **Why the 2020 Election Will Be A Mess, Part II: Beyond Russian Disinformation**

In 2016, an effective Russian disinformation campaign helped Donald Trump win the presidential election. What would the next iteration of Russia's effort look like? Alex Finley, Asha Rangappa, and John Sipher write that an influence campaign "is only one piece of Russia's larger use of political warfare. Russia's full active-measures toolkit—one that goes back to the Soviet Union's KGB—includes subversion, espionage, sabotage, propaganda, deception, provocation, spreading of rumors and conspiracy, weaponization of social media, and even assassination and promotion of violence." The three authors write that a look at Russia's actions in Europe and past practice "suggests the United States should prepare for the worst."

[Read more](#)

**Perspective**

## **State Pushes to List White Supremacist Group as Terrorist Org**

The State Department is pushing to designate at least one violent white supremacist group as a foreign terrorist organization, an unprecedented move which national security experts say would be a big step toward fighting a growing threat on U.S. soil.

[Read more](#)

## **West Africa's Democratic Progress is Slipping Away, Even as Region's Significance Grows**

Rising authoritarianism is curtailing individual freedoms around the globe. Jon Temin and Isabel Linzer write that in an alarming development, however, the region that showed the fastest decline in political rights and civil liberties last year was West Africa, which had long been a driver of democratic gains. The warning signs have failed to spur corrective action.

[Read more](#)

**Our picks this week**

## **U.S. Flawed Coronavirus Test Strategy | A Resilient Cyber Future | Android Vulnerabilities, and more**

- [Flawed Coronavirus Test Strategy Contributed to U.S. Spread: Experts](#)
- [Iranian, Russian, Chinese Media Push COVID-19 'Bioweapon' Conspiracies](#)
- [Trump Is Peddling Dangerous Disinformation on Coronavirus](#)
- [Trump's European Novel Coronavirus Travel Ban Excludes Countries Where He Has Golf Courses](#)
- [Covid-19 Is Rapidly Spreading in America. The Country Does Not Look Ready](#)
- [Russian Intelligence-Backed Hackers Go after Armenian Embassy Website with New Code](#)
- [Analysis: Android has more vulnerabilities than Windows 10](#)
- [Surge of Virus Misinformation Stumps Facebook and Twitter](#)
- [Trump's Coronavirus Press Event Was Even Worse Than It Looked](#)
- [Cross-Whitehall Unit Set Up to Counter False Coronavirus Claims](#)
- [Facebook and Twitter Are Struggling to Get Coronavirus Disinformation Details from the Government](#)
- [How a Lack of Resources Has Made Russia's Military Even More Cunning](#)
- [The Big Iran Threat Is Nukes, Not Coronavirus](#)
- [The Internet Avoided a Minor Disaster Last Week](#)
- [Is Zero Hedge a Russian Trojan Horse?](#)
- [Monthlong Cyberattack Disrupts Operations at UKentucky Health](#)
- [Cyber Command Was Worried that WikiLeaks Dump Would Burn Operation Aurora Intel, Document Shows](#)
- [The U.S. Isn't Ready for What's About to Happen](#)
- [Trump's Visit to the CDC Shows Why There's Concern about His Coronavirus Response](#)
- [Building a Resilient Cyber Future](#)
- [Immigration Officers Say Asylum Deal with Guatemala Is Unlawful](#)
- [Watchdog: Poor Communication Left HHS Ill-Equipped to Handle Family Separation Policy](#)
- [Homeland Security Grades UM's Cybersecurity in Confidential Assessment](#)
- [Democrats Call on the State Department to List White Supremacist Groups As Foreign Terrorist Organizations](#)
- [Trump Tells Colombia: Spray Coca Fields with Alleged Carcinogen—or Else](#)

[Read more](#)

## **Also noted this week**



- European power grid organization says its IT network was hacked
- Supreme Court Justices Allow 'Remain in Mexico' Asylum Policy to Continue
- More Children Face US Immigration Judges Through Video Screens
- Building a nuclear plant? Go online
- AMD processors susceptible to security vulnerabilities, data leaks
- Facial recognition could stop terrorists before they act
- U.S. creates new envoy position to counter rising terrorism in Sahel
- Germany Protests: Thousands Demonstrate In Munich Against Rise Of Far-Right Terrorism
- Utilities on high alert as phishing attempts, cyber probing spike related to Coronavirus
- Secret document says WikiLeaks cable leaks disrupted tracking of nation-state hackers
- Greater cyber protections for healthcare providers urged
- Cyber Command preps force assessment
- DHS Launches Third Biometric Rally to Assess How the Tech Works on Crowds
- Super Tuesday gives feds and states a test run for securing November vote
- Justice Department Finalizes Rule Enabling DHS To Collect DNA From Detainees

[Read more](#)

---

BIOMETRICS | BORDER/IMMIG. | BUSINESS | CYBERSECURITY | DETECTION | DISASTERS | GOVERNMENT | INFRASTRUCTURE  
PUBLIC HEALTH | PUBLIC SAFETY | REGIONAL | SCI-TECH | SURVEILLANCE | TERRORISM | TRANSPORTATION | WATER

Homeland Security News Wire

[Home](#) | [About us](#) | [Subscribe](#) | [Advertise](#) | [Contact](#)



Advertising & Marketing [advertise@newswirepubs.com](mailto:advertise@newswirepubs.com)

Editorial [editor@newswirepubs.com](mailto:editor@newswirepubs.com)

General [info@newswirepubs.com](mailto:info@newswirepubs.com)

2010-2011 © News Wire Publications, LLC News Wire Publications, LLC

220 Old Country Road | Suite 200 | Mineola | New York | 11501

[Permissions and Policies](#)

Homeland Security News Wire, 220 Old Country Road, Suite 200, Mineola, NY 11501

SafeUnsubscribe™ [infotech@ci.sunnyvale.ca.us](mailto:infotech@ci.sunnyvale.ca.us)

[Forward email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [hsnewswire@newswirepubs.com](mailto:hsnewswire@newswirepubs.com)

[illegible]

[illegible]









		without being authentic called on the admin js or ads.			MISC
stack -- driftnet_devices		Immunity on D-Link DIR-615A10 devices has a stack-based buffer overflow via the omrWardSetup Wizard webpage parameter when L1nack_201 is malformed.	2020-03-02	6.5	CVE-2020-0655 MISC
stack -- driftnet_devices		Immunity on D-Link DIR-615A10 devices has a stack-based buffer overflow via the omrWardSetup webpage parameter when L1nack_201 is malformed.	2020-03-02	6.5	CVE-2020-0655 MISC
easyio -- easyio-30p_devices		EasyIO EasyIO-30P devices before 2.0.5.2.7 have their root Access Control, exposed to webuser.js.	2020-03-02	5	CVE-2019-18113 MISC
easyio -- easyio-30p_devices		EasyIO EasyIO-30P devices before 2.0.5.2.7 allow XSS via the dev.htm GCM parameter.	2020-03-02	4	CVE-2019-18113 MISC
easy -- easy_chat_server		An issue was discovered in EP3 Easy Chat Server 3.1. There is a buffer overflow via a long body/ping message parameter.	2020-03-05	6	CVE-2019-18559 MISC
emmy_p_ony -- emmy		CNCF Emmy through 1.13.0 may consume excessive amounts of memory when proxying HTTP/1.1 requests or responses with many small (i.e. 1 byte) chunks.	2020-03-0	6	CVE-2020-0669 MISC CONFIRM
emmy_p_ony -- emmy		CNCF Emmy through 1.13.0 may consume excessive amounts of memory when responding in email by a pipelined request.	2020-03-0	5	CVE-2020-0669 MISC CONFIRM
eset -- eset_nsf_secure		ESSET Cyber Security before 6.8.1.0 is vulnerable to a denial-of-service attack using any user to stop its ESSET processes. An attacker can abuse the bug to stop the process from ESSET and launch its attack.	2020-03-03	6	CVE-2019-17534 MISC
facebook -- htm		Insufficient boundary checks when decoding JSON in TryParse reads out of bounds memory, potentially leading to DOS. This issue affects HHVM 5.0.0, 5.0.1, 5.0.2, 5.0.3, 5.0.4, 5.0.5, 5.0.6, 5.0.7, 5.0.8, 5.0.9, 5.0.10, 5.0.11, 5.0.12, 5.0.13, 5.0.14, 5.0.15, 5.0.16, 5.0.17, 5.0.18, 5.0.19, 5.0.20, 5.0.21, 5.0.22, 5.0.23, 5.0.24, 5.0.25, 5.0.26, 5.0.27, 5.0.28, 5.0.29, 5.0.30, 5.0.31, 5.0.32, 5.0.33, 5.0.34, 5.0.35, 5.0.36, 5.0.37, 5.0.38, 5.0.39, 5.0.40, 5.0.41, 5.0.42, 5.0.43, 5.0.44, 5.0.45, 5.0.46, 5.0.47, 5.0.48, 5.0.49, 5.0.50, 5.0.51, 5.0.52, 5.0.53, 5.0.54, 5.0.55, 5.0.56, 5.0.57, 5.0.58, 5.0.59, 5.0.60, 5.0.61, 5.0.62, 5.0.63, 5.0.64, 5.0.65, 5.0.66, 5.0.67, 5.0.68, 5.0.69, 5.0.70, 5.0.71, 5.0.72, 5.0.73, 5.0.74, 5.0.75, 5.0.76, 5.0.77, 5.0.78, 5.0.79, 5.0.80, 5.0.81, 5.0.82, 5.0.83, 5.0.84, 5.0.85, 5.0.86, 5.0.87, 5.0.88, 5.0.89, 5.0.90, 5.0.91, 5.0.92, 5.0.93, 5.0.94, 5.0.95, 5.0.96, 5.0.97, 5.0.98, 5.0.99, 5.0.100, 5.0.101, 5.0.102, 5.0.103, 5.0.104, 5.0.105, 5.0.106, 5.0.107, 5.0.108, 5.0.109, 5.0.110, 5.0.111, 5.0.112, 5.0.113, 5.0.114, 5.0.115, 5.0.116, 5.0.117, 5.0.118, 5.0.119, 5.0.120, 5.0.121, 5.0.122, 5.0.123, 5.0.124, 5.0.125, 5.0.126, 5.0.127, 5.0.128, 5.0.129, 5.0.130, 5.0.131, 5.0.132, 5.0.133, 5.0.134, 5.0.135, 5.0.136, 5.0.137, 5.0.138, 5.0.139, 5.0.140, 5.0.141, 5.0.142, 5.0.143, 5.0.144, 5.0.145, 5.0.146, 5.0.147, 5.0.148, 5.0.149, 5.0.150, 5.0.151, 5.0.152, 5.0.153, 5.0.154, 5.0.155, 5.0.156, 5.0.157, 5.0.158, 5.0.159, 5.0.160, 5.0.161, 5.0.162, 5.0.163, 5.0.164, 5.0.165, 5.0.166, 5.0.167, 5.0.168, 5.0.169, 5.0.170, 5.0.171, 5.0.172, 5.0.173, 5.0.174, 5.0.175, 5.0.176, 5.0.177, 5.0.178, 5.0.179, 5.0.180, 5.0.181, 5.0.182, 5.0.183, 5.0.184, 5.0.185, 5.0.186, 5.0.187, 5.0.188, 5.0.189, 5.0.190, 5.0.191, 5.0.192, 5.0.193, 5.0.194, 5.0.195, 5.0.196, 5.0.197, 5.0.198, 5.0.199, 5.0.200, 5.0.201, 5.0.202, 5.0.203, 5.0.204, 5.0.205, 5.0.206, 5.0.207, 5.0.208, 5.0.209, 5.0.210, 5.0.211, 5.0.212, 5.0.213, 5.0.214, 5.0.215, 5.0.216, 5.0.217, 5.0.218, 5.0.219, 5.0.220, 5.0.221, 5.0.222, 5.0.223, 5.0.224, 5.0.225, 5.0.226, 5.0.227, 5.0.228, 5.0.229, 5.0.230, 5.0.231, 5.0.232, 5.0.233, 5.0.234, 5.0.235, 5.0.236, 5.0.237, 5.0.238, 5.0.239, 5.0.240, 5.0.241, 5.0.242, 5.0.243, 5.0.244, 5.0.245, 5.0.246, 5.0.247, 5.0.248, 5.0.249, 5.0.250, 5.0.251, 5.0.252, 5.0.253, 5.0.254, 5.0.255, 5.0.256, 5.0.257, 5.0.258, 5.0.259, 5.0.260, 5.0.261, 5.0.262, 5.0.263, 5.0.264, 5.0.265, 5.0.266, 5.0.267, 5.0.268, 5.0.269, 5.0.270, 5.0.271, 5.0.272, 5.0.273, 5.0.274, 5.0.275, 5.0.276, 5.0.277, 5.0.278, 5.0.279, 5.0.280, 5.0.281, 5.0.282, 5.0.283, 5.0.284, 5.0.285, 5.0.286, 5.0.287, 5.0.288, 5.0.289, 5.0.290, 5.0.291, 5.0.292, 5.0.293, 5.0.294, 5.0.295, 5.0.296, 5.0.297, 5.0.298, 5.0.299, 5.0.300, 5.0.301, 5.0.302, 5.0.303, 5.0.304, 5.0.305, 5.0.306, 5.0.307, 5.0.308, 5.0.309, 5.0.310, 5.0.311, 5.0.312, 5.0.313, 5.0.314, 5.0.315, 5.0.316, 5.0.317, 5.0.318, 5.0.319, 5.0.320, 5.0.321, 5.0.322, 5.0.323, 5.0.324, 5.0.325, 5.0.326, 5.0.327, 5.0.328, 5.0.329, 5.0.330, 5.0.331, 5.0.332, 5.0.333, 5.0.334, 5.0.335, 5.0.336, 5.0.337, 5.0.338, 5.0.339, 5.0.340, 5.0.341, 5.0.342, 5.0.343, 5.0.344, 5.0.345, 5.0.346, 5.0.347, 5.0.348, 5.0.349, 5.0.350, 5.0.351, 5.0.352, 5.0.353, 5.0.354, 5.0.355, 5.0.356, 5.0.357, 5.0.358, 5.0.359, 5.0.360, 5.0.361, 5.0.362, 5.0.363, 5.0.364, 5.0.365, 5.0.366, 5.0.367, 5.0.368, 5.0.369, 5.0.370, 5.0.371, 5.0.372, 5.0.373, 5.0.374, 5.0.375, 5.0.376, 5.0.377, 5.0.378, 5.0.379, 5.0.380, 5.0.381, 5.0.382, 5.0.383, 5.0.384, 5.0.385, 5.0.386, 5.0.387, 5.0.388, 5.0.389, 5.0.390, 5.0.391, 5.0.392, 5.0.393, 5.0.394, 5.0.395, 5.0.396, 5.0.397, 5.0.398, 5.0.399, 5.0.400, 5.0.401, 5.0.402, 5.0.403, 5.0.404, 5.0.405, 5.0.406, 5.0.407, 5.0.408, 5.0.409, 5.0.410, 5.0.411, 5.0.412, 5.0.413, 5.0.414, 5.0.415, 5.0.416, 5.0.417, 5.0.418, 5.0.419, 5.0.420, 5.0.421, 5.0.422, 5.0.423, 5.0.424, 5.0.425, 5.0.426, 5.0.427, 5.0.428, 5.0.429, 5.0.430, 5.0.431, 5.0.432, 5.0.433, 5.0.434, 5.0.435, 5.0.436, 5.0.437, 5.0.438, 5.0.439, 5.0.440, 5.0.441, 5.0.442, 5.0.443, 5.0.444, 5.0.445, 5.0.446, 5.0.447, 5.0.448, 5.0.449, 5.0.450, 5.0.451, 5.0.452, 5.0.453, 5.0.454, 5.0.455, 5.0.456, 5.0.457, 5.0.458, 5.0.459, 5.0.460, 5.0.461, 5.0.462, 5.0.463, 5.0.464, 5.0.465, 5.0.466, 5.0.467, 5.0.468, 5.0.469, 5.0.470, 5.0.471, 5.0.472, 5.0.473, 5.0.474, 5.0.475, 5.0.476, 5.0.477, 5.0.478, 5.0.479, 5.0.480, 5.0.481, 5.0.482, 5.0.483, 5.0.484, 5.0.485, 5.0.486, 5.0.487, 5.0.488, 5.0.489, 5.0.490, 5.0.491, 5.0.492, 5.0.493, 5.0.494, 5.0.495, 5.0.496, 5.0.497, 5.0.498, 5.0.499, 5.0.500, 5.0.501, 5.0.502, 5.0.503, 5.0.504, 5.0.505, 5.0.506, 5.0.507, 5.0.508, 5.0.509, 5.0.510, 5.0.511, 5.0.512, 5.0.513, 5.0.514, 5.0.515, 5.0.516, 5.0.517, 5.0.518, 5.0.519, 5.0.520, 5.0.521, 5.0.522, 5.0.523, 5.0.524, 5.0.525, 5.0.526, 5.0.527, 5.0.528, 5.0.529, 5.0.530, 5.0.531, 5.0.532, 5.0.533, 5.0.534, 5.0.535, 5.0.536, 5.0.537, 5.0.538, 5.0.539, 5.0.540, 5.0.541, 5.0.542, 5.0.543, 5.0.544, 5.0.545, 5.0.546, 5.0.547, 5.0.548, 5.0.549, 5.0.550, 5.0.551, 5.0.552, 5.0.553, 5.0.554, 5.0.555, 5.0.556, 5.0.557, 5.0.558, 5.0.559, 5.0.560, 5.0.561, 5.0.562, 5.0.563, 5.0.564, 5.0.565, 5.0.566, 5.0.567, 5.0.568, 5.0.569, 5.0.570, 5.0.571, 5.0.572, 5.0.573, 5.0.574, 5.0.575, 5.0.576, 5.0.577, 5.0.578, 5.0.579, 5.0.580, 5.0.581, 5.0.582, 5.0.583, 5.0.584, 5.0.585, 5.0.586, 5.0.587, 5.0.588, 5.0.589, 5.0.590, 5.0.591, 5.0.592, 5.0.593, 5.0.594, 5.0.595, 5.0.596, 5.0.597, 5.0.598, 5.0.599, 5.0.600, 5.0.601, 5.0.602, 5.0.603, 5.0.604, 5.0.605, 5.0.606, 5.0.607, 5.0.608, 5.0.609, 5.0.610, 5.0.611, 5.0.612, 5.0.613, 5.0.614, 5.0.615, 5.0.616, 5.0.617, 5.0.618, 5.0.619, 5.0.620, 5.0.621, 5.0.622, 5.0.623, 5.0.624, 5.0.625, 5.0.626, 5.0.627, 5.0.628, 5.0.629, 5.0.630, 5.0.631, 5.0.632, 5.0.633, 5.0.634, 5.0.635, 5.0.636, 5.0.637, 5.0.638, 5.0.639, 5.0.640, 5.0.641, 5.0.642, 5.0.643, 5.0.644, 5.0.645, 5.0.646, 5.0.647, 5.0.648, 5.0.649, 5.0.650, 5.0.651, 5.0.652, 5.0.653, 5.0.654, 5.0.655, 5.0.656, 5.0.657, 5.0.658, 5.0.659, 5.0.660, 5.0.661, 5.0.662, 5.0.663, 5.0.664, 5.0.665, 5.0.666, 5.0.667, 5.0.668, 5.0.669, 5.0.670, 5.0.671, 5.0.672, 5.0.673, 5.0.674, 5.0.675, 5.0.676, 5.0.677, 5.0.678, 5.0.679, 5.0.680, 5.0.681, 5.0.682, 5.0.683, 5.0.684, 5.0.685, 5.0.686, 5.0.687, 5.0.688, 5.0.689, 5.0.690, 5.0.691, 5.0.692, 5.0.693, 5.0.694, 5.0.695, 5.0.696, 5.0.697, 5.0.698, 5.0.699, 5.0.700, 5.0.701, 5.0.702, 5.0.703, 5.0.704, 5.0.705, 5.0.706, 5.0.707, 5.0.708, 5.0.709, 5.0.710, 5.0.711, 5.0.712, 5.0.713, 5.0.714, 5.0.715, 5.0.716, 5.0.717, 5.0.718, 5.0.719, 5.0.720, 5.0.721, 5.0.722, 5.0.723, 5.0.724, 5.0.725, 5.0.726, 5.0.727, 5.0.728, 5.0.729, 5.0.730, 5.0.731, 5.0.732, 5.0.733, 5.0.734, 5.0.735, 5.0.736, 5.0.737, 5.0.738, 5.0.739, 5.0.740, 5.0.741, 5.0.742, 5.0.743, 5.0.744, 5.0.745, 5.0.746, 5.0.747, 5.0.748, 5.0.749, 5.0.750, 5.0.751, 5.0.752, 5.0.753, 5.0.754, 5.0.755, 5.0.756, 5.0.757, 5.0.758, 5.0.759, 5.0.760, 5.0.761, 5.0.762, 5.0.763, 5.0.764, 5.0.765, 5.0.766, 5.0.767, 5.0.768, 5.0.769, 5.0.770, 5.0.771, 5.0.772, 5.0.773, 5.0.774, 5.0.775, 5.0.776, 5.0.777, 5.0.778, 5.0.779, 5.0.780, 5.0.781, 5.0.782, 5.0.783, 5.0.784, 5.0.785, 5.0.786, 5.0.787, 5.0.788, 5.0.789, 5.0.790, 5.0.791, 5.0.792, 5.0.793, 5.0.794, 5.0.795, 5.0.796, 5.0.797, 5.0.798, 5.0.799, 5.0.800, 5.0.801, 5.0.802, 5.0.803, 5.0.804, 5.0.805, 5.0.806, 5.0.807, 5.0.808, 5.0.809, 5.0.810, 5.0.811, 5.0.812, 5.0.813, 5.0.814, 5.0.815, 5.0.816, 5.0.817, 5.0.818, 5.0.819, 5.0.820, 5.0.821, 5.0.822, 5.0.823, 5.0.824, 5.0.825, 5.0.826, 5.0.827, 5.0.828, 5.0.829, 5.0.830, 5.0.831, 5.0.832, 5.0.833, 5.0.834, 5.0.835, 5.0.836, 5.0.837, 5.0.838, 5.0.839, 5.0.840, 5.0.841, 5.0.842, 5.0.843, 5.0.844, 5.0.845, 5.0.846, 5.0.847, 5.0.848, 5.0.849, 5.0.850, 5.0.851, 5.0.852, 5.0.853, 5.0.854, 5.0.855, 5.0.856, 5.0.857, 5.0.858, 5.0.859, 5.0.860, 5.0.861, 5.0.862, 5.0.863, 5.0.864, 5.0.865, 5.0.866, 5.0.867, 5.0.868, 5.0.869, 5.0.870, 5.0.871, 5.0.872, 5.0.873, 5.0.874, 5.0.875, 5.0.876, 5.0.877, 5.0.878, 5.0.879, 5.0.880, 5.0.881, 5.0.882, 5.0.883, 5.0.884, 5.0.885, 5.0.886, 5.0.887, 5.0.888, 5.0.889, 5.0.890, 5.0.891, 5.0.892, 5.0.893, 5.0.894, 5.0.895, 5.0.896, 5.0.897, 5.0.898, 5.0.899, 5.0.900, 5.0.901, 5.0.902, 5.0.903, 5.0.904, 5.0.905, 5.0.906, 5.0.907, 5.0.908, 5.0.909, 5.0.910, 5.0.911, 5.0.912, 5.0.913, 5.0.914, 5.0.915, 5.0.916, 5.0.917, 5.0.918, 5.0.919, 5.0.920, 5.0.921, 5.0.922, 5.0.923, 5.0.924, 5.0.925, 5.0.926, 5.0.927, 5.0.928, 5.0.929, 5.0.930, 5.0.931, 5.0.932, 5.0.933, 5.0.934, 5.0.935, 5.0.936, 5.0.937, 5.0.938, 5.0.939, 5.0.940, 5.0.941, 5.0.942, 5.0.943, 5.0.944, 5.0.945, 5.0.946, 5.0.947, 5.0.948, 5.0.949, 5.0.950, 5.0.951, 5.0.952, 5.0.953, 5.0.954, 5.0.955, 5.0.956, 5.0.957, 5.0.958, 5.0.959, 5.0.960, 5.0.961, 5.0.962, 5.0.963, 5.0.964, 5.0.965, 5.0.966, 5.0.967, 5.0.968, 5.0.969, 5.0.970, 5.0.971, 5.0.972, 5.0.973, 5.0.974, 5.0.975, 5.0.976, 5.0.977, 5.0.978, 5.0.979, 5.0.980, 5.0.981, 5.0.982, 5.0.983, 5.0.984, 5.0.985, 5.0.986, 5.0.987, 5.0.988, 5.0.989, 5.0.990, 5.0.991, 5.0.992, 5.0.993, 5.0.994, 5.0.995, 5.0.996, 5.0.997, 5.0.998, 5.0.999, 5.0.1000, 5.0.1001, 5.0.1002, 5.0.1003, 5.0.1004, 5.0.1005, 5.0.1006, 5.0.1007, 5.0.1008, 5.0.1009, 5.0.1010, 5.0.1011, 5.0.1012, 5.0.1013, 5.0.1014, 5.0.1015, 5.0.1016, 5.0.1017, 5.0.1018, 5.0.1019, 5.0.1020, 5.0.1021, 5.0.1022, 5.0.1023, 5.0.1024, 5.0.1025, 5.0.1026, 5.0.1027, 5.0.1028, 5.0.1029, 5.0.1030, 5.0.1031, 5.0.1032, 5.0.1033, 5.0.1034, 5.0.1035, 5.0.1036, 5.0.1037, 5.0.1038, 5.0.1039, 5.0.1040, 5.0.1041, 5.0.1042, 5.0.1043, 5.0.1044, 5.0.1045, 5.0.1046, 5.0.1047, 5.0.1048, 5.0.1049, 5.0.1050, 5.0.1051, 5.0.1052, 5.0.1053, 5.0.1054, 5.0.1055, 5.0.1056, 5.0.1057, 5.0.1058, 5.0.1059, 5.0.1060, 5.0.1061, 5.0.1062, 5.0.1063, 5.0.1064, 5.0.1065, 5.0.1066, 5.0.1067, 5.0.1068, 5.0.1069, 5.0.1070, 5.0.1071, 5.0.1072, 5.0.1073, 5.0.1074, 5.0.1075, 5.0.1076, 5.0.1077, 5.0.1078, 5.0.1079, 5.0.1080, 5.0.1081, 5.0.1082, 5.0.1083, 5.0.1084, 5.0.1085, 5.0.1086, 5.0.1087, 5.0.1088, 5.0.1089, 5.0.1090, 5.0.1091, 5.0.1092, 5.0.1093, 5.0.1094, 5.0.1095, 5.0.1096, 5.0.1097, 5.0.1098, 5.0.1099, 5.0.1100, 5.0.1101, 5.0.1102, 5.0.1103, 5.0.1104, 5.0.1105, 5.0.1106, 5.0.1107, 5.0.1108, 5.0.1109, 5.0.1110, 5.0.1111, 5.0.1112, 5.0.1113, 5.0.1114, 5.0.1115, 5.0.1116, 5.0.1117, 5.0.1118, 5.0.1119, 5.0.1120, 5.0.1121, 5.0.1122, 5.0.1123, 5.0.1124, 5.0.1125, 5.0.1126, 5.0.1127, 5.0.1128, 5.0.1129, 5.0.1130, 5.0.1131, 5.0.1132, 5.0.1133, 5.0.1134, 5.0.1135, 5.0.1136, 5.0.1137, 5.0.1138, 5.0.1139, 5.0.1140, 5.0.1141, 5.0.1142, 5.0.1143, 5.0.1144, 5.0.1145, 5.0.1146, 5.0.1147, 5.0.1148, 5.0.1149, 5.0.1150, 5.0.1151, 5.0.1152, 5.0.1153, 5.0.1154, 5.0.1155, 5.0.1156, 5.0.1157, 5.0.1158, 5.0.1159, 5.0.1160, 5.0.1161, 5.0.1162, 5.0.1163, 5.0.1164, 5.0.1165, 5.0.1166, 5.0.1167, 5.0.1168, 5.0.1169, 5.0.1170, 5.0.1171, 5.0.1172, 5.0.1173, 5.0.1174, 5.0.1175, 5.0.1176, 5.0.1177, 5.0.1178, 5.0.1179, 5.0.1180, 5.0.1181, 5.0.1182, 5.0.1183, 5.0.1184, 5.0.1185, 5.0.1186, 5.0.1187, 5.0.1188, 5.0.1189, 5.0.1190, 5.0.1191, 5.0.1192, 5.0.1193, 5.0.1194, 5.0.1195, 5.0.1196, 5.0.1197, 5.0.1198, 5.0.1199, 5.0.1200, 5.0.1201, 5.0.1202, 5.0.1203, 5.0.1204, 5.0.1205, 5.0.1206, 5.0.1207, 5.0.1208, 5.0.1209, 5.0.1210, 5.0.1211, 5.0.1212, 5.0.1213, 5.0.1214, 5.0.1215, 5.0.1216, 5.0.1217, 5.0.1218, 5.0.1219, 5.0.1220, 5.0.1221, 5.0.1222, 5.0.1223, 5.0.1224, 5.0.1225, 5.0.1226, 5.0.1227, 5.0.1228, 5.0.1229, 5.0.1230, 5.0.1231, 5.0.1232, 5.0.1233, 5.0.1234, 5.0.1235, 5.0.1236, 5.0.1237, 5.0.1238, 5.0.1239, 5.0.1240, 5.0.1241, 5.0.1242, 5.0.1243, 5.0.1244, 5.0.1245, 5.0.1246, 5.0.1247, 5.0.1248, 5.0.1249, 5.0.1250, 5.0.1251, 5.0.12			

item - security_informa	0.0.1, 0.0.2, 0.0.3, 0.0.4, 0.0.5, 0.0.6, 0.0.7, 0.0.8, 0.0.9, 0.0.10, 0.0.11, 0.0.12, 0.0.13, 0.0.14, 0.0.15, 0.0.16, 0.0.17, 0.0.18, 0.0.19, 0.0.20, 0.0.21, 0.0.22, 0.0.23, 0.0.24, 0.0.25, 0.0.26, 0.0.27, 0.0.28, 0.0.29, 0.0.30, 0.0.31, 0.0.32, 0.0.33, 0.0.34, 0.0.35, 0.0.36, 0.0.37, 0.0.38, 0.0.39, 0.0.40, 0.0.41, 0.0.42, 0.0.43, 0.0.44, 0.0.45, 0.0.46, 0.0.47, 0.0.48, 0.0.49, 0.0.50, 0.0.51, 0.0.52, 0.0.53, 0.0.54, 0.0.55, 0.0.56, 0.0.57, 0.0.58, 0.0.59, 0.0.60, 0.0.61, 0.0.62, 0.0.63, 0.0.64, 0.0.65, 0.0.66, 0.0.67, 0.0.68, 0.0.69, 0.0.70, 0.0.71, 0.0.72, 0.0.73, 0.0.74, 0.0.75, 0.0.76, 0.0.77, 0.0.78, 0.0.79, 0.0.80, 0.0.81, 0.0.82, 0.0.83, 0.0.84, 0.0.85, 0.0.86, 0.0.87, 0.0.88, 0.0.89, 0.0.90, 0.0.91, 0.0.92, 0.0.93, 0.0.94, 0.0.95, 0.0.96, 0.0.97, 0.0.98, 0.0.99, 0.0.100, 0.0.101, 0.0.102, 0.0.103, 0.0.104, 0.0.105, 0.0.106, 0.0.107, 0.0.108, 0.0.109, 0.0.110, 0.0.111, 0.0.112, 0.0.113, 0.0.114, 0.0.115, 0.0.116, 0.0.117, 0.0.118, 0.0.119, 0.0.120, 0.0.121, 0.0.122, 0.0.123, 0.0.124, 0.0.125, 0.0.126, 0.0.127, 0.0.128, 0.0.129, 0.0.130, 0.0.131, 0.0.132, 0.0.133, 0.0.134, 0.0.135, 0.0.136, 0.0.137, 0.0.138, 0.0.139, 0.0.140, 0.0.141, 0.0.142, 0.0.143, 0.0.144, 0.0.145, 0.0.146, 0.0.147, 0.0.148, 0.0.149, 0.0.150, 0.0.151, 0.0.152, 0.0.153, 0.0.154, 0.0.155, 0.0.156, 0.0.157, 0.0.158, 0.0.159, 0.0.160, 0.0.161, 0.0.162, 0.0.163, 0.0.164, 0.0.165, 0.0.166, 0.0.167, 0.0.168, 0.0.169, 0.0.170, 0.0.171, 0.0.172, 0.0.173, 0.0.174, 0.0.175, 0.0.176, 0.0.177, 0.0.178, 0.0.179, 0.0.180, 0.0.181, 0.0.182, 0.0.183, 0.0.184, 0.0.185, 0.0.186, 0.0.187, 0.0.188, 0.0.189, 0.0.190, 0.0.191, 0.0.192, 0.0.193, 0.0.194, 0.0.195, 0.0.196, 0.0.197, 0.0.198, 0.0.199, 0.0.200, 0.0.201, 0.0.202, 0.0.203, 0.0.204, 0.0.205, 0.0.206, 0.0.207, 0.0.208, 0.0.209, 0.0.210, 0.0.211, 0.0.212, 0.0.213, 0.0.214, 0.0.215, 0.0.216, 0.0.217, 0.0.218, 0.0.219, 0.0.220, 0.0.221, 0.0.222, 0.0.223, 0.0.224, 0.0.225, 0.0.226, 0.0.227, 0.0.228, 0.0.229, 0.0.230, 0.0.231, 0.0.232, 0.0.233, 0.0.234, 0.0.235, 0.0.236, 0.0.237, 0.0.238, 0.0.239, 0.0.240, 0.0.241, 0.0.242, 0.0.243, 0.0.244, 0.0.245, 0.0.246, 0.0.247, 0.0.248, 0.0.249, 0.0.250, 0.0.251, 0.0.252, 0.0.253, 0.0.254, 0.0.255, 0.0.256, 0.0.257, 0.0.258, 0.0.259, 0.0.260, 0.0.261, 0.0.262, 0.0.263, 0.0.264, 0.0.265, 0.0.266, 0.0.267, 0.0.268, 0.0.269, 0.0.270, 0.0.271, 0.0.272, 0.0.273, 0.0.274, 0.0.275, 0.0.276, 0.0.277, 0.0.278, 0.0.279, 0.0.280, 0.0.281, 0.0.282, 0.0.283, 0.0.284, 0.0.285, 0.0.286, 0.0.287, 0.0.288, 0.0.289, 0.0.290, 0.0.291, 0.0.292, 0.0.293, 0.0.294, 0.0.295, 0.0.296, 0.0.297, 0.0.298, 0.0.299, 0.0.300, 0.0.301, 0.0.302, 0.0.303, 0.0.304, 0.0.305, 0.0.306, 0.0.307, 0.0.308, 0.0.309, 0.0.310, 0.0.311, 0.0.312, 0.0.313, 0.0.314, 0.0.315, 0.0.316, 0.0.317, 0.0.318, 0.0.319, 0.0.320, 0.0.321, 0.0.322, 0.0.323, 0.0.324, 0.0.325, 0.0.326, 0.0.327, 0.0.328, 0.0.329, 0.0.330, 0.0.331, 0.0.332, 0.0.333, 0.0.334, 0.0.335, 0.0.336, 0.0.337, 0.0.338, 0.0.339, 0.0.340, 0.0.341, 0.0.342, 0.0.343, 0.0.344, 0.0.345, 0.0.346, 0.0.347, 0.0.348, 0.0.349, 0.0.350, 0.0.351, 0.0.352, 0.0.353, 0.0.354, 0.0.355, 0.0.356, 0.0.357, 0.0.358, 0.0.359, 0.0.360, 0.0.361, 0.0.362, 0.0.363, 0.0.364, 0.0.365, 0.0.366, 0.0.367, 0.0.368, 0.0.369, 0.0.370, 0.0.371, 0.0.372, 0.0.373, 0.0.374, 0.0.375, 0.0.376, 0.0.377, 0.0.378, 0.0.379, 0.0.380, 0.0.381, 0.0.382, 0.0.383, 0.0.384, 0.0.385, 0.0.386, 0.0.387, 0.0.388, 0.0.389, 0.0.390, 0.0.391, 0.0.392, 0.0.393, 0.0.394, 0.0.395, 0.0.396, 0.0.397, 0.0.398, 0.0.399, 0.0.400, 0.0.401, 0.0.402, 0.0.403, 0.0.404, 0.0.405, 0.0.406, 0.0.407, 0.0.408, 0.0.409, 0.0.410, 0.0.411, 0.0.412, 0.0.413, 0.0.414, 0.0.415, 0.0.416, 0.0.417, 0.0.418, 0.0.419, 0.0.420, 0.0.421, 0.0.422, 0.0.423, 0.0.424, 0.0.425, 0.0.426, 0.0.427, 0.0.428, 0.0.429, 0.0.430, 0.0.431, 0.0.432, 0.0.433, 0.0.434, 0.0.435, 0.0.436, 0.0.437, 0.0.438, 0.0.439, 0.0.440, 0.0.441, 0.0.442, 0.0.443, 0.0.444, 0.0.445, 0.0.446, 0.0.447, 0.0.448, 0.0.449, 0.0.450, 0.0.451, 0.0.452, 0.0.453, 0.0.454, 0.0.455, 0.0.456, 0.0.457, 0.0.458, 0.0.459, 0.0.460, 0.0.461, 0.0.462, 0.0.463, 0.0.464, 0.0.465
-------------------------	---







[Back to top](#)

[illegible]

[Back to top](#)







[illegible]

ATTN: Email s from an external source. Stop, Lock, and Think before opening attachments or links.



National Cyber Awareness System:

Vulnerability Summary for the Week of March 2, 2020

03/09/2020 05:07 AM EDT

Original release date: March 9, 2020

The CSA Weekly Vulnerability Summary Bulletin is created using information from the NIST NVD. In some cases, the vulnerability in the Bulletin may not yet have assigned CVE scores. Please visit NVD for updates on vulnerabilities, which include CVE scores once they are available.

High Vulnerabilities

Primary Vendor Product	Description	Published	CVE Score	Source & Patch Info
apple -- ios iphones, ipads	A denial of service issue was addressed with improved input validation.	2020-03-28	7.5 M.S.C. M.S.C. M.S.C. M.S.C. M.S.C.	CVE-2019-1171 M.S.C. M.S.C. M.S.C. M.S.C. M.S.C.
centreon -- centreon	An issue was discovered in Centreon before 2.8.30, 18.10.0, 19.0.0, and 19.10.2. SQL injection exists via the includeMonitoringStatus/Process/monitorInstance parameter.	2020-03-28	7.5	CVE-2019-1171 CONE RM CONE RM CONE RM CONE RM CONE RM
centreon -- centreon	Centreon 19.10 allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in the server_json field in JSON data in an api/v1/remote.php?object=centreon_config action request.	2020-03-28	9 L.B. M.S.C.	CVE-2020-1433 L.B. M.S.C.
cisco -- remote_pki_device	A vulnerability in Cisco FlexEdge PHY Device Software could allow an authenticated, local attacker to execute commands on the underlying Linux shell of an affected device with root privileges. The vulnerability exists because the affected software does not properly sanitize user-supplied input. An attacker can trigger user-supplied input to an affected device to exploit this vulnerability by supplying certain CLI commands with crafted arguments. A successful exploit could allow the attacker to run arbitrary commands as the root user, which could result in a complete system compromise.	2020-03-09	7.5	CVE-2020-1115 M.S.C.
cisco -- webex_network_k_recorder	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability is a buffer overflow in a file named elements within a Webex recording that is stored in a file named AdvancedRecordingPlayer. An attacker could exploit these vulnerabilities by sending a malicious ARP or WFF file to a user through a link or email at attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the logged user.	2020-03-09	8.3 M.S.C.	CVE-2020-1112 M.S.C.
cisco -- webex_network_k_recorder	Multiple vulnerabilities in Cisco Webex Network Recording Player for Microsoft Windows and Cisco Webex Player for Microsoft Windows could allow an attacker to execute arbitrary code on an affected system. The vulnerability is a buffer overflow in a file named elements within a Webex recording that is stored in a file named AdvancedRecordingPlayer. An attacker could exploit these vulnerabilities by sending a malicious ARP or WFF file to a user through a link or email at attachment and persuading the user to open the file on the local system. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the logged user.	2020-03-09	8.3 M.S.C.	CVE-2020-1112 M.S.C.
c-link -- dat-2800p_rtr	A Broken Access Control vulnerability in the Link DSL-2800 web administration interface (Firmware 1.10) allows an attacker to bypass the need for authentication to retrieve GET request without being authenticated on the admin interface.	2020-03-09	7.5	CVE-2019-1922 M.S.C. M.S.C. M.S.C.
c-link -- dat-2800ap_devices	Link DSL-2800AP 2.0.15 Rev A devices have an authentication bypass vulnerability via the Upgrade Firmware functionality in the Web interface, using shell metacharacters in the admin.cgi_sessionid parameter.	2020-03-05	7.5	CVE-2019-20001 M.S.C.
c-link -- dat-2800ap_devices	Link DSL-2800AP 2.0.15 Rev A devices have an authentication bypass vulnerability via the Session Configuration functionality in the Web interface, using shell metacharacters in the admin.cgi_sessionid parameter.	2020-03-05	7.5	CVE-2019-20002 M.S.C.
c-link -- dat-2800ap_devices	Link DSL-2800AP 2.0.15 Rev A devices have an authentication bypass vulnerability via the Session Configuration functionality in the Web interface, using shell metacharacters in the admin.cgi_sessionid parameter.	2020-03-05	7.5	CVE-2019-20003 M.S.C.
emgnet -- emgnet	Emgnet through 2.2.0 allows execution of arbitrary commands. The system argument is provided to the exec function without any sanitization.	2020-03-28	7.5	CVE-2019-19001 M.S.C. M.S.C.
emvay_p_01y -- emvay	CNCF Emvay through 1.13.0 has incorrect Access Control when using IDS with Combined Validation Control. Using the same set of (e.g., trusted CA) across many resources together with the combined validation control could lead to the state part of the validation control to be not applied, even though it was visible in the active configuration.	2020-03-09	7.5	CVE-2020-1113 M.S.C. CONE RM
emvay_p_01y -- emvay	CNCF Emvay through 1.13.0 TLS Inspector bypasses TLS Inspector could have been bypassed (not recognized as a TLS client) by a client using only TLS 1.1. Because TLS extensions (SNI, ALPN) were not inspected, those connections might have been misclassified as being legitimate, possibly bypassing some security checks in the process.	2020-03-09	7.5	CVE-2020-1114 M.S.C. CONE RM
eset -- cyber_security	A permission issue in ESET Cyber Security before 6.8.300.0 for macOS allows a local attacker to escalate privileges by appending data to root-owned files.	2020-03-05	7.5	CVE-2019-11134 M.S.C.
eset -- ios iphones, ipads	The ESET AV parsing engine allows via-decoy on bypass via a crafted ESET Checksum field in an archive. This affects versions before 120 of Smart Security Premium, Internet Security, NOD32, Antivirus, Cyber Security (macOS), Mobile Security for Android, Smart TV Security, and NOD32 Antivirus for Linux Desktop.	2020-03-05	7.5	CVE-2020-10033 M.S.C.
hynetohack -- netoweb	An issue was discovered in Hynetohack before 5.3.3. The netoweb web interface is a one-to-one injection, allowing an unauthorized attacker to perform various tasks such as authentication bypass via the user_id field in a cookie.	2020-03-28	7.5	CVE-2020-1434 M.S.C. M.S.C.
jackson -- jackson-databind	A flaw was discovered in FastXML Jackson-databind 2.10 versions before 2.10.11 and 2.8.7.3, where a would permit polymorphic deserialization of malicious objects using the java.lang.ClassName object when used in conjunction with polymorphic type handling methods such as readValueFromTree() or when @JsonTypeInfo() or @JsonTypeName() is used. An attacker could use this flaw to execute arbitrary code.	2020-03-02	7.5	CVE-2019-18080 CONE RM M.S.C.
jackson -- jackson-databind	A flaw was discovered in Jackson-databind 2.10 versions before 2.10.11 and 2.8.7.3, where a would permit polymorphic deserialization of a malicious object using common types on 1 and 2 JSON classes. An attacker could use this flaw to execute arbitrary code.	2020-03-02	7.5	CVE-2019-18081 CONE RM M.S.C.
huawei -- huawei_v10_smartphones	Huawei V10 smartphones with versions earlier than EMUI 10.0.0.156 (CODE19SP) and versions earlier than EMUI 10.0.0.160 (CPE 32E R1P) have an out-of-bounds write due to a vulnerability in the software buffer because of insufficient data on a certain parameter when initializing or launching a program. An attacker could trigger the user into triggering a malicious application, a successful exploit could cause the device to reboot.	2020-02-28	7.1	CVE-2020-1179 M.S.C.



[illegible]

[illegible]

[Back to top](#)

1





[illegible]

item - security_informa	0.0.1, 0.0.2, 0.0.3, 0.0.4, 0.0.5, 0.0.6, 0.0.7, 0.0.8, 0.0.9, 0.0.10, 0.0.11, 0.0.12, 0.0.13, 0.0.14, 0.0.15, 0.0.16, 0.0.17, 0.0.18, 0.0.19, 0.0.20, 0.0.21, 0.0.22, 0.0.23, 0.0.24, 0.0.25, 0.0.26, 0.0.27, 0.0.28, 0.0.29, 0.0.30, 0.0.31, 0.0.32, 0.0.33, 0.0.34, 0.0.35, 0.0.36, 0.0.37, 0.0.38, 0.0.39, 0.0.40, 0.0.41, 0.0.42, 0.0.43, 0.0.44, 0.0.45, 0.0.46, 0.0.47, 0.0.48, 0.0.49, 0.0.50, 0.0.51, 0.0.52, 0.0.53, 0.0.54, 0.0.55, 0.0.56, 0.0.57, 0.0.58, 0.0.59, 0.0.60, 0.0.61, 0.0.62, 0.0.63, 0.0.64, 0.0.65, 0.0.66, 0.0.67, 0.0.68, 0.0.69, 0.0.70, 0.0.71, 0.0.72, 0.0.73, 0.0.74, 0.0.75, 0.0.76, 0.0.77, 0.0.78, 0.0.79, 0.0.80, 0.0.81, 0.0.82, 0.0.83, 0.0.84, 0.0.85, 0.0.86, 0.0.87, 0.0.88, 0.0.89, 0.0.90, 0.0.91, 0.0.92, 0.0.93, 0.0.94, 0.0.95, 0.0.96, 0.0.97, 0.0.98, 0.0.99, 0.0.100, 0.0.101, 0.0.102, 0.0.103, 0.0.104, 0.0.105, 0.0.106, 0.0.107, 0.0.108, 0.0.109, 0.0.110, 0.0.111, 0.0.112, 0.0.113, 0.0.114, 0.0.115, 0.0.116, 0.0.117, 0.0.118, 0.0.119, 0.0.120, 0.0.121, 0.0.122, 0.0.123, 0.0.124, 0.0.125, 0.0.126, 0.0.127, 0.0.128, 0.0.129, 0.0.130, 0.0.131, 0.0.132, 0.0.133, 0.0.134, 0.0.135, 0.0.136, 0.0.137, 0.0.138, 0.0.139, 0.0.140, 0.0.141, 0.0.142, 0.0.143, 0.0.144, 0.0.145, 0.0.146, 0.0.147, 0.0.148, 0.0.149, 0.0.150, 0.0.151, 0.0.152, 0.0.153, 0.0.154, 0.0.155, 0.0.156, 0.0.157, 0.0.158, 0.0.159, 0.0.160, 0.0.161, 0.0.162, 0.0.163, 0.0.164, 0.0.165, 0.0.166, 0.0.167, 0.0.168, 0.0.169, 0.0.170, 0.0.171, 0.0.172, 0.0.173, 0.0.174, 0.0.175, 0.0.176, 0.0.177, 0.0.178, 0.0.179, 0.0.180, 0.0.181, 0.0.182, 0.0.183, 0.0.184, 0.0.185, 0.0.186, 0.0.187, 0.0.188, 0.0.189, 0.0.190, 0.0.191, 0.0.192, 0.0.193, 0.0.194, 0.0.195, 0.0.196, 0.0.197, 0.0.198, 0.0.199, 0.0.200, 0.0.201, 0.0.202, 0.0.203, 0.0.204, 0.0.205, 0.0.206, 0.0.207, 0.0.208, 0.0.209, 0.0.210, 0.0.211, 0.0.212, 0.0.213, 0.0.214, 0.0.215, 0.0.216, 0.0.217, 0.0.218, 0.0.219, 0.0.220, 0.0.221, 0.0.222, 0.0.223, 0.0.224, 0.0.225, 0.0.226, 0.0.227, 0.0.228, 0.0.229, 0.0.230, 0.0.231, 0.0.232, 0.0.233, 0.0.234, 0.0.235, 0.0.236, 0.0.237, 0.0.238, 0.0.239, 0.0.240, 0.0.241, 0.0.242, 0.0.243, 0.0.244, 0.0.245, 0.0.246, 0.0.247, 0.0.248, 0.0.249, 0.0.250, 0.0.251, 0.0.252, 0.0.253, 0.0.254, 0.0.255, 0.0.256, 0.0.257, 0.0.258, 0.0.259, 0.0.260, 0.0.261, 0.0.262, 0.0.263, 0.0.264, 0.0.265, 0.0.266, 0.0.267, 0.0.268, 0.0.269, 0.0.270, 0.0.271, 0.0.272, 0.0.273, 0.0.274, 0.0.275, 0.0.276, 0.0.277, 0.0.278, 0.0.279, 0.0.280, 0.0.281, 0.0.282, 0.0.283, 0.0.284, 0.0.285, 0.0.286, 0.0.287, 0.0.288, 0.0.289, 0.0.290, 0.0.291, 0.0.292, 0.0.293, 0.0.294, 0.0.295, 0.0.296, 0.0.297, 0.0.298, 0.0.299, 0.0.300, 0.0.301, 0.0.302, 0.0.303, 0.0.304, 0.0.305, 0.0.306, 0.0.307, 0.0.308, 0.0.309, 0.0.310, 0.0.311, 0.0.312, 0.0.313, 0.0.314, 0.0.315, 0.0.316, 0.0.317, 0.0.318, 0.0.319, 0.0.320, 0.0.321, 0.0.322, 0.0.323, 0.0.324, 0.0.325, 0.0.326, 0.0.327, 0.0.328, 0.0.329, 0.0.330, 0.0.331, 0.0.332, 0.0.333, 0.0.334, 0.0.335, 0.0.336, 0.0.337, 0.0.338, 0.0.339, 0.0.340, 0.0.341, 0.0.342, 0.0.343, 0.0.344, 0.0.345, 0.0.346, 0.0.347, 0.0.348, 0.0.349, 0.0.350, 0.0.351, 0.0.352, 0.0.353, 0.0.354, 0.0.355, 0.0.356, 0.0.357, 0.0.358, 0.0.359, 0.0.360, 0.0.361, 0.0.362, 0.0.363, 0.0.364, 0.0.365, 0.0.366, 0.0.367, 0.0.368, 0.0.369, 0.0.370, 0.0.371, 0.0.372, 0.0.373, 0.0.374, 0.0.375, 0.0.376, 0.0.377, 0.0.378, 0.0.379, 0.0.380, 0.0.381, 0.0.382, 0.0.383, 0.0.384, 0.0.385, 0.0.386, 0.0.387, 0.0.388, 0.0.389, 0.0.390, 0.0.391, 0.0.392, 0.0.393, 0.0.394, 0.0.395, 0.0.396, 0.0.397, 0.0.398, 0.0.399, 0.0.400, 0.0.401, 0.0.402, 0.0.403, 0.0.404, 0.0.405, 0.0.406, 0.0.407, 0.0.408, 0.0.409, 0.0.410, 0.0.411, 0.0.412, 0.0.413, 0.0.414, 0.0.415, 0.0.416, 0.0.417, 0.0.418, 0.0.419, 0.0.420, 0.0.421, 0.0.422, 0.0.423, 0.0.424, 0.0.425, 0.0.426, 0.0.427, 0.0.428, 0.0.429, 0.0.430, 0.0.431, 0.0.432, 0.0.433, 0.0.434, 0.0.435, 0.0.436, 0.0.437, 0.0.438, 0.0.439, 0.0.440, 0.0.441, 0.0.442, 0.0.443, 0.0.444, 0.0.445, 0.0.446, 0.0.447, 0.0.448, 0.0.449, 0.0.450, 0.0.451, 0.0.452, 0.0.453, 0.0.454, 0.0.455, 0.0.456, 0.0.457, 0.0.458, 0.0.459, 0.0.460, 0.0.461, 0.0.462, 0.0.463, 0.0.464, 0.0.465
-------------------------	---









[Back to top](#)



[illegible]



[illegible]

[Vulnerability Summary for the Week of March 2, 2020](#)  
03/09/2020 05:51 AM EDT

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

[illegible]







[illegible]













integrity –	6.0.3.9s WordPess's less remote authorized users (with minimal permissions) send sensitive data on behalf of the site via - id_rsa, my_service.php - sent_email, user_id	2020-03-06	CVE-2020-9355 CWE-352 MISC
integrity –	An issue was discovered in Zammad 3.9.2. The Webhooksec service receives messages in plaintext format sent from an attacker. The attacker can email, add attachments and parsing errors not handled. This is due to a crash of the service.	2020-03-05	CVE-2020-10101 MISC
zammad – zammad	An issue was discovered in Zammad 3.10.0. An exposed REST API endpoint sends messages that show internal app logs or infrastructure information. This is a result of a misconfiguration. A successful exploit is not possible.	2020-03-05	CVE-2020-10102
zammad – zammad	An issue was discovered in Zammad 3.10.0. It lets its source code and static resources when submitting an OPTIONS request, rather than returning an error. Disclosure of source code allows an attacker to modify or replace the code. Source code was disclosed or the file (/zammadapp/zammad) is exposed.	2020-03-05	CVE-2020-10103
zammad – zammad	An issue was discovered in Zammad 3.10.0. It allows for users to view their personal details and access specific features. However, the user can also send and receive messages controlled to limit the information. The user's company are able to access a local data and other companies. Due to the inherent nature of the app, access to user's can access local data and the organization to the mail at users or use the app to easily sensitive data of other companies.	2020-03-05	CVE-2020-10104
zammad – zammad	An issue was discovered in Zammad 3.10.0 through 3.2. An attacker can transmit sensitive information on the user's device. The user can access the app to gain unauthorized access. The affected passwords are related to the user when visiting a certain URL.	2020-03-05	CVE-2020-10105
zammad – zammad	An issue was discovered in Zammad 3.10.0 through 3.2. An attacker can access the user's data and obtain sensitive information. An attacker who's remotely compromised or obtains physical access to a user's work can can browse the browser's history and obtain sensitive user information on the app. The attacker does not need to be authenticated with the app icon or use the information, as it would be available via a browser.	2020-03-05	CVE-2020-10106

### Low Vulnerabilities

[illegible]







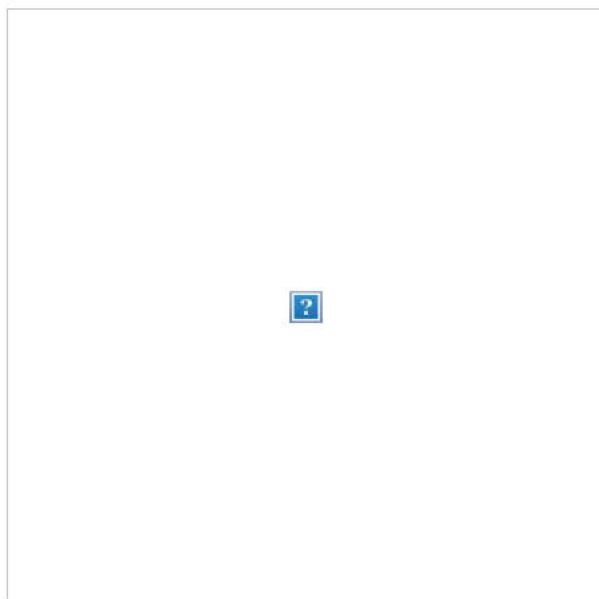
[illegible]

[illegible]

**From:** [IDG Insider Alert](#)  
**To:** [apham@sunnyvale.ca.gov](mailto:apham@sunnyvale.ca.gov)  
**Subject:** Boosting AI's smarts in the absence of training data  
**Date:** Monday, March 02, 2020 12:47:46 PM

---

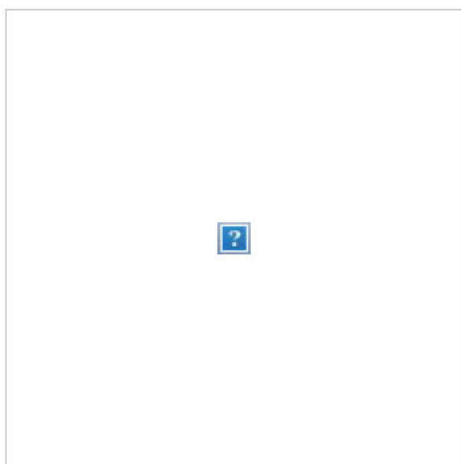
ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



---

## IDG Insider Alert

March 02, 2020



### Boosting AI's smarts in the absence of training data

Zero-shot learning repurposes knowledge through statistical or semantic approaches without needing huge amounts of fresh training data [Read more](#)



---

### Your Must-Read Stories

- [4 ways 5G will change your enterprise threat model](#)
- [Cloud outages show multicloud is essential](#)



- Posture management: Cloud security tools rise in wake of breaches
- Digital transformation innovators: FutureEdge Awards honor 50 companies
- 4 strategies for board presentation success
- Bank of America brings AI to equity capital markets
- 6 business concepts IT leaders should master
- Secrets of industry-hopping CSOs

eBook: Silver Peak Systems Inc

## 2020 Top SD-WAN Edge Trends

2020 will see SD-WAN edge become a critical integration point providing a uniform fabric across physical locations and multi-cloud instances. [Read more](#)



### 4 ways 5G will change your enterprise threat model

The benefits that fifth-generation cellular networks will enable come with security risks that organizations need to pay attention to right now. [Read more](#)



DEALPOST

### GoDaddy Websites + Marketing is perfect for new brands looking to get online.

GoDaddy Websites + Marketing is packed with tools to help your business' site succeed. [Read more](#)



### Cloud outages show multicloud is essential

Outages are inevitable and vendors are unreliable. You can't move fast enough unless you already have your service running on two or more clouds [Read more](#)



## Posture management: Cloud security tools rise in wake of breaches

Capital One's breach highlighted the pressing need for IT leaders to shore up misconfiguration errors. That's where cloud security posture management and other tools come into play, experts say. [Read more](#)

## Digital transformation innovators: FutureEdge Awards honor 50 companies

Top organizations harness AI, machine learning, RPA, cloud, data analytics, and mobile/smart devices to accelerate business and foster a culture of collaboration. [Read more](#)



## 4 strategies for board presentation success

Veteran execs share their best advice on understanding the mindset of the board. [Read more](#)



## Bank of America brings AI to equity capital markets

Machine learning and artificial intelligence is helping Bank of America's bankers more accurately identify investors for IPOs. [Read more](#)

## 6 business concepts IT leaders should



## master

CIOs who talk tech must also master critical business lingo when speaking to their leadership peers. Here are some essential terms. [Read more](#)



## Secrets of industry-hopping CSOs

Who says you can't change industries? Veteran security leaders Mark Weatherford and Cheri McGuire teach you how it's done. [Read more](#)

**Video/Webcast:** Gigamon

## Critical Network Security Trends of 2020

From Distributed Denial-of-Service to encryption hijacking, learn here's what IT teams and networking pros are focused on in their quest to keep their organizations safe. [Read more](#)



Email not displaying correctly? [View it in your browser](#)

You are currently subscribed to IDG Insider as [apham@sunnyvale.ca.gov](mailto:apham@sunnyvale.ca.gov).

[Unsubscribe from this newsletter](#) | [Manage your email preferences](#) | [Subscribe](#) | [Privacy Policy](#)

[Learn more about](#)



Please do not reply to this message.

To contact someone directly, send an email to [newsletters@idg.com](mailto:newsletters@idg.com).

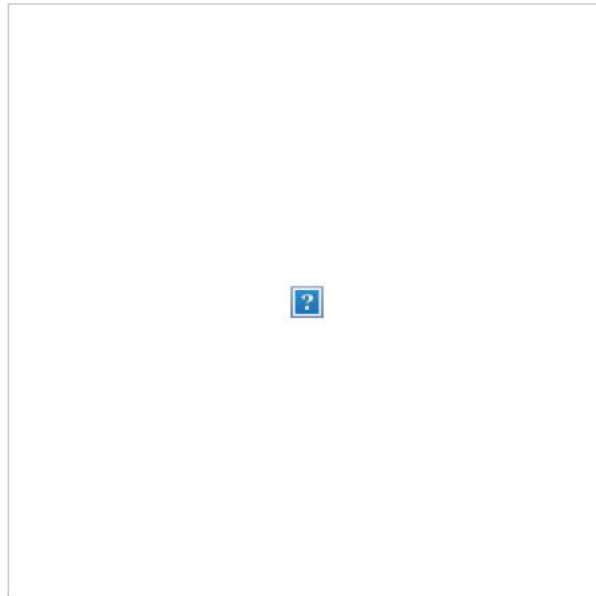




**From:** [IDG Insider Alert](#)  
**To:** [kbfooster@sunnyvale.ca.gov](mailto:kbfooster@sunnyvale.ca.gov)  
**Subject:** Boosting AI's smarts in the absence of training data  
**Date:** Monday, March 02, 2020 10:21:47 AM

---

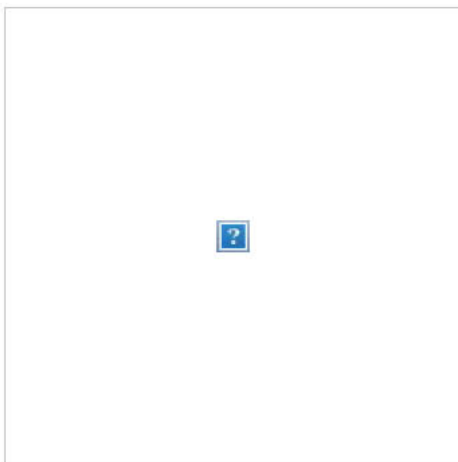
ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



---

## IDG Insider Alert

March 02, 2020



### Boosting AI's smarts in the absence of training data

Zero-shot learning repurposes knowledge through statistical or semantic approaches without needing huge amounts of fresh training data [Read more](#)



---

### Your Must-Read Stories

- [4 ways 5G will change your enterprise threat model](#)
- [Cloud outages show multicloud is essential](#)

- Posture management: Cloud security tools rise in wake of breaches
- Digital transformation innovators: FutureEdge Awards honor 50 companies
- 4 strategies for board presentation success
- Bank of America brings AI to equity capital markets
- 6 business concepts IT leaders should master
- Secrets of industry-hopping CSOs

eBook: Silver Peak Systems Inc

## 2020 Top SD-WAN Edge Trends

2020 will see SD-WAN edge become a critical integration point providing a uniform fabric across physical locations and multi-cloud instances. [Read more](#)



### 4 ways 5G will change your enterprise threat model

The benefits that fifth-generation cellular networks will enable come with security risks that organizations need to pay attention to right now. [Read more](#)



DEALPOST

### GoDaddy Websites + Marketing is perfect for new brands looking to get online.

GoDaddy Websites + Marketing is packed with tools to help your business' site succeed. [Read more](#)



### Cloud outages show multicloud is essential

Outages are inevitable and vendors are unreliable. You can't move fast enough unless you already have your service running on two or more clouds [Read more](#)



## Posture management: Cloud security tools rise in wake of breaches

Capital One's breach highlighted the pressing need for IT leaders to shore up misconfiguration errors. That's where cloud security posture management and other tools come into play, experts say. [Read more](#)

## Digital transformation innovators: FutureEdge Awards honor 50 companies

Top organizations harness AI, machine learning, RPA, cloud, data analytics, and mobile/smart devices to accelerate business and foster a culture of collaboration. [Read more](#)



## 4 strategies for board presentation success

Veteran execs share their best advice on understanding the mindset of the board. [Read more](#)



## Bank of America brings AI to equity capital markets

Machine learning and artificial intelligence is helping Bank of America's bankers more accurately identify investors for IPOs. [Read more](#)

## 6 business concepts IT leaders should



## master

CIOs who talk tech must also master critical business lingo when speaking to their leadership peers. Here are some essential terms. [Read more](#)



## Secrets of industry-hopping CSOs

Who says you can't change industries? Veteran security leaders Mark Weatherford and Cheri McGuire teach you how it's done. [Read more](#)

**Video/Webcast:** Gigamon

## Critical Network Security Trends of 2020

From Distributed Denial-of-Service to encryption hijacking, learn here's what IT teams and networking pros are focused on in their quest to keep their organizations safe. [Read more](#)



Email not displaying correctly? [View it in your browser](#)

You are currently subscribed to IDG Insider as kbfooster@sunnyvale.ca.gov.

[Unsubscribe from this newsletter](#) | [Manage your email preferences](#) | [Subscribe](#) | [Privacy Policy](#)

[Learn more about](#)



Please do not reply to this message.

To contact someone directly, send an email to [newsletters@idg.com](mailto:newsletters@idg.com).





**From:** US-CERT  
**To:** [edgewanna@sunmwale.ca.gov](mailto:edgewanna@sunmwale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of February 10, 2020  
**Date:** Monday, February 17, 2020 4:43:58 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

### Vulnerability Summary for the Week of February 10, 2020

02/17/2020 07:09 AM EST

Original release date: February 17, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	10	<a href="#">CVE-2020-3740</a> <a href="#">CONF RM</a>
ajaxplorer -- ajaxplorer	Ajaxplorer before 5.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) archive_name parameter to the Power FS module (plugins/action.powerfs/class PowerFSController.php), a (2) file name to the getTrustSizeOnFileSystem function in the File System (Standard) module (plugins/access.fs/class.fsAccessWrapper.php), or the (3) revision parameter to the Subversion Repository module (plugins/meta.svn/class.SvnManager.php)	2020-02-11	10	<a href="#">CVE-2013-4267</a> MISC MISC MISC
artica -- pandora_fms	functions_netflow.php in Artica Pandora FMS 7.0 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the index.php?operation/netflow/nf_live_view ip_dst, dst_port, or src_port parameter, a different vulnerability than CVE-2019-20224.	2020-02-12	9	<a href="#">CVE-2020-8947</a> MISC MISC MISC
atutor -- atutor	confirm.php in ATutor 2.2 and earlier allows remote attackers to bypass authentication and gain access as an existing user via the auto_login parameter.	2020-02-11	7.5	<a href="#">CVE-2014-9753</a> MISC MISC MISC MISC MISC
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	10	<a href="#">CVE-2013-3091</a> MISC MISC MISC
biscom -- secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1xxx before 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	7.5	<a href="#">CVE-2020-8796</a> MISC <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/175922">https://exchange.xforce.ibmcloud.com/vulnerabilities/175922</a>
bosch -- bvms_mobile_video_service	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	10	<a href="#">CVE-2020-6770</a> <a href="#">CONF RM</a>
canonical -- lxc	In LXC 2.0, many template scripts download code over cleartext HTTP, and omit a digital-signature check, before running it to bootstrap containers.	2020-02-10	9.3	<a href="#">CVE-2017-18641</a> MISC
corsair -- corsair_icue	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-	2020-02-		<a href="#">CVE-2020-8808</a>

	integrity level processes) to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.	07	7.2	MISC MISC
d-link -- multiple_products	Multiple SQL injection vulnerabilities in D-Link DSR-150 with firmware before 1.08B44; DSR-150N with firmware before 1.05B64; DSR-250 and DSR-250N with firmware before 1.08B44; and DSR-500, DSR-500N, DSR-1000, and DSR-1000N with firmware before 1.08B77 allow remote attackers to execute arbitrary SQL commands via the password to (1) the login.authenticate function in share/lua/5.1/teamf1lua/lib/login.lua or (2) captivePortal.lua.	2020-02-11	10	CVE-2013-5945 MISC MISC MISC MISC
dell -- multiple_products	An Authentication Bypass Vulnerability exists in DELL SonicWALL Analyzer 7.0, Global Management System (GMS) 4.1, 5.0, 5.1, 6 0, and 7.0; Universal Management Appliance (UMA) 5.1, 6 0, and 7 0 and ViewPoint 4.1, 5.0, 5.1, and 6.0 via the skipSessionCheck parameter to the UMA interface (/appliance/), which could let a remote malicious user obtain access to the root account.	2020-02-11	10	CVE-2013-1359 MISC MISC MISC MISC MISC MISC MISC
dell -- multiple_products	An Authentication Bypass vulnerability exists in DELL SonicWALL Global Management System (GMS) 4.1, 5.0, 5.1, 6.0, and 7 0, Analyzer 7.0, Universal Management Appliance (UMA) 5.1, 6 0, and 7 0 and ViewPoint 4.1, 5.0, 5.1, and 6.0 via a crafted request to the SGMS interface, which could let a remote malicious user obtain administrative access.	2020-02-11	10	CVE-2013-1360 MISC MISC MISC MISC MISC MISC
echoping_project -- echoping	echoping through 6.0 2 has buffer overflow vulnerabilities	2020-02-11	10	CVE-2013-4448 MISC MISC MISC
enorth -- enorth_webpublisher_cms	SQL injection vulnerability in pub/m_pending_news/delete_pending_news.jsp in Enorth Webpublisher CMS allows remote attackers to execute arbitrary SQL commands via the cbNewsId parameter.	2020-02-12	7.5	CVE-2015-5617 MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5 3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	9.3	CVE-2020-8655 MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5 3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php.	2020-02-07	7.5	CVE-2020-8656 MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5 3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	9	CVE-2020-8654 MISC MISC
golang -- go	The net/http library in net/http/transfer.go in Go before 1.4 3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains Content-Length and Transfer-Encoding header fields.	2020-02-08	7.5	CVE-2015-5741 MISC MISC MISC MISC MISC MISC MISC
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	9	CVE-2014-7224 MISC MISC MISC MISC
google -- chrome	Use after free in audio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	9.3	CVE-2020-6406 SUSE MISC

				MISC
hubot_scripts -- hubot_scripts	scripts/email coffee in the Hubot Scripts module before 2.4.4 for Node.js allows remote attackers to execute arbitrary commands.	2020-02-12	7.5	<a href="#">CVE-2013-7378</a> MISC MISC MISC MISC
ibm -- sterling_authentication	A Command Execution Vulnerability exists in IBM Sterling External Authentication Server 2.2.0, 2.3.01, 2.4.0, and 2.4.1 via an unspecified OS command, which could let a local malicious user execute arbitrary code.	2020-02-11	7.2	<a href="#">CVE-2013-0517</a> MISC MISC
libnotify -- libnotify	libnotify before 1.0.4 for Node.js allows remote attackers to execute arbitrary commands via unspecified characters in a call to libnotify.notify.	2020-02-12	7.5	<a href="#">CVE-2013-7381</a> MISC MISC CONF RM MISC
linux -- linux_kernel	Buffer overflow in the auerswald_probe function in the Auerswald Linux USB driver for the Linux kernel before 2.6.27 allows physically proximate attackers to execute arbitrary code, cause a denial of service via a crafted USB device, or take full control of the system.	2020-02-11	7.2	<a href="#">CVE-2009-4067</a> MISC MISC
Istio -- Istio	Istio 1.3 through 1.4.3 allows authentication bypass. The Authentication Policy exact-path matching logic can allow unauthorized access to HTTP paths even if they are configured to be only accessed after presenting a valid JWT token. For example, an attacker can add a ? or # character to a URI that would otherwise satisfy an exact-path match.	2020-02-12	7.5	<a href="#">CVE-2020-8595</a> REDHAT CONF RM MISC MISC MISC CONF RM
mediawiki -- mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	9.3	<a href="#">CVE-2012-4381</a> MISC MISC MISC MISC MISC MISC
microsoft -- multiple_internet_explorer_products	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0674</a> MISC
microsoft -- multiple_internet_explorer_products	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0673</a> MISC
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0711</a> MISC
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713.	2020-02-11	7.6	<a href="#">CVE-2020-0767</a> MISC
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0712</a> MISC
	A remote code execution vulnerability			



microsoft -- chakacore	exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0710 MISC</a>
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0713 MISC</a>
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	2020-02-11	9.3	<a href="#">CVE-2020-0759 MISC</a>
microsoft -- multiple_microsoft_exchange_server_products	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.	2020-02-11	9	<a href="#">CVE-2020-0688 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0720 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE D is unique from CVE-2020-0683.	2020-02-11	7.2	<a href="#">CVE-2020-0686 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE D is unique from CVE-2020-0734.	2020-02-11	7.6	<a href="#">CVE-2020-0681 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in Remote Desktop Services "rdp" formerly known as Terminal Services "ts" when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.	2020-02-11	8.5	<a href="#">CVE-2020-0655 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows improperly handles Secure Socket Shell remote commands, aka 'Windows SSH Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0757 MISC</a>
microsoft -- multiple_windows_products	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'.	2020-02-11	9.3	<a href="#">CVE-2020-0738 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.	2020-02-11	9	<a href="#">CVE-2020-0662 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows Error Reporting Manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0678 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726.	2020-02-11	7.2	<a href="#">CVE-2020-0731 MISC</a>
	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle			

microsoft -- multiple_windows_products	objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0725</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0671, CVE-2020-0672.	2020-02-11	7.2	<a href="#">CVE-2020-0670</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0726</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792.	2020-02-11	7.2	<a href="#">CVE-2020-0745</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681.	2020-02-11	9.3	<a href="#">CVE-2020-0734</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0723</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0719</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680.	2020-02-11	7.2	<a href="#">CVE-2020-0682</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0671.	2020-02-11	7.2	<a href="#">CVE-2020-0672</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686.	2020-02-11	7.2	<a href="#">CVE-2020-0683</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Wireless Network Manager improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Wireless Network Manager Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0704</a> <a href="#">MISC</a>
	An elevation of privilege vulnerability			

microsoft -- multiple_windows_products	exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0722 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0707 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0685 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0721 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0703 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0672.	2020-02-11	7.2	<a href="#">CVE-2020-0671 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0724 MISC</a>
microsoft -- office365_proplus_for_32-bit_and_64-bit_systems	An elevation of privilege vulnerability exists in Microsoft Office OLicenseHeartbeat task, where an attacker who successfully exploited this vulnerability could run this task as SYSTEM. To exploit the vulnerability, an authenticated attacker would need to place a specially crafted file in a specific location, thereby allowing arbitrary file corruption. The security update addresses the vulnerability by correcting how the process validates the log file., aka 'Microsoft Office Tampering Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0697 MISC</a>
microsoft -- windows_10_and_windows_server_2016	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0745.	2020-02-11	7.2	<a href="#">CVE-2020-0792 MISC</a>
microsoft -- windows_10_and_windows_server_2016	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0732.	2020-02-11	7.2	<a href="#">CVE-2020-0709 MISC</a>
microsoft -- windows_10_and_windows_server_2016	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0709.	2020-02-11	7.2	<a href="#">CVE-2020-0732 MISC</a>
	An issue was discovered in Microvirt MEmu all versions prior to 7.0.2. A guest			

microvirt -- memu	Android operating system inside the MEmu emulator contains a /system/bin/systemd binary that is run with root privileges on startup (this is unrelated to Red Hat's systemd init program, and is a closed-source proprietary tool that seems to be developed by Microvirt). This program opens TCP port 21509, presumably to receive installation-related commands from the host OS. Because everything after the installer:uninstall command is concatenated directly into a system() call, it is possible to execute arbitrary commands by supplying shell metacharacters.	2020-02-11	10	<a href="#">CVE-2019-14514</a> MISC
netgear -- ac1200_smart_wifi_router	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR AC1200 R6220 Firmware version 1.1 0.86 Smart WiFi Router. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of path strings. By inserting a null byte into the path, the user can skip most authentication checks. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-8616.	2020-02-10	7.5	<a href="#">CVE-2019-17137</a> MISC
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1 2.31805 and V2 2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracer diagnostic tool because of lack of user input sanitizing.	2020-02-07	8.5	<a href="#">CVE-2019-19356</a> MISC MISC
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	7.5	<a href="#">CVE-2019-15605</a> MISC FEDORA CONF RM CONF RM CONF RM
nodejs -- nodejs	Including trailing white space in HTTP header values in Node.js 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	7.5	<a href="#">CVE-2019-15606</a> MISC CONF RM CONF RM CONF RM
nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	7.5	<a href="#">CVE-2014-9530</a> CONF RM
omniauth-weibo-oauth2_gem_for_ruby - omniauth-weibo-oauth2_gem_for_ruby	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	7.5	<a href="#">CVE-2019-17268</a> MISC CONF RM
openpne -- opopensocialplugin	opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple XML External Entity Injection Vulnerabilities	2020-02-07	7.5	<a href="#">CVE-2013-4335</a> MISC MISC MISC
openpne -- opwebapiplugin	opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	7.5	<a href="#">CVE-2013-4334</a> MISC MISC
phxeventmanager -- phxeventmanager	SQL injection vulnerability in search.php in phxEventManager 2.0 beta 5 allows remote attackers to execute arbitrary SQL commands via the search_terms parameter.	2020-02-11	7.5	<a href="#">CVE-2012-1124</a> MISC MISC MISC MISC
polarbear -- polarbear_cms	A PHP File Upload Vulnerability exists in PolarBear CMS 2.5 via upload.php, which could let a malicious user execute arbitrary code.	2020-02-11	7.5	<a href="#">CVE-2013-0803</a> MISC MISC MISC
polycomm -- web_management_interface_g3/hdx_800_hd	An issue was discovered in Polycom Web Management Interface G3/HDX 8000 HD with Durango 2.6.0 4740 software and embedded Polycom Linux Development	2020-02-	10	<a href="#">CVE-2012-6611</a>



	Platform 2.14.g3. It has a blank administrative password by default, and can be successfully used without setting this password.	10		<a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	The virtqueue_map_sg function in hw/virtio/virtio.c in QEMU before 1.7.2 allows remote attackers to execute arbitrary files via a crafted savevm image, related to virtio-block or virtio-serial read.	2020-02-11	<a href="#">7.2</a>	<a href="#">CVE-2013-4535</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open close in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14044</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14002</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14088</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14046</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	Stage-2 fault will occur while writing to an ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14049</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14055</a> <a href="#">CONF RM</a>

qualcomm -- multiple_snapdragon_p	Uninitialized stack data gets used If memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14060</a> CONF RM
qualcomm -- multiple_snapdragon_p	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> CONF RM
qualcomm -- multiple_snapdragon_p	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> CONF RM
qualcomm -- multiple_snapdragon_p	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	2020-02-07	9.4	<a href="#">CVE-2019-14057</a> CONF RM

	SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	Out of bound access due to Invalid inputs to dpm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14063</a> <a href="#">CONF RM</a>
qualcomm -- snapdragon_industrial_iot	Subsequent additions performed during Module loading while allocating the memory would lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	7.2	<a href="#">CVE-2019-14061</a> <a href="#">CONF RM</a>
ruby_pdfkit_gem_for_ruby_on_rails - ruby_pdfkit_gem_for_ruby_on_rails	Ruby PDFKit gem prior to 0.5.3 has a Code Execution Vulnerability	2020-02-11	7.5	<a href="#">CVE-2013-1607</a> <a href="#">MISC</a> <a href="#">MISC</a>
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, contains a vulnerability of Pre-auth SQL Injection, allowing attackers to inject a specific SQL command.	2020-02-11	7.5	<a href="#">CVE-2020-3934</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
siemens -- multiple_scalance_products	A vulnerability has been identified in SCALANCE S602 (All versions >= V3.0), SCALANCE S612 (All versions >= V3.0), SCALANCE S623 (All versions >= V3.0), SCALANCE S627-2M (All versions >= V3.0). Specially crafted packets sent to port 443/tcp of affected devices could cause a Denial-of-Service condition of the web server. A cold reboot is required to restore the functionality of the device.	2020-02-11	7.8	<a href="#">CVE-2019-13926</a> <a href="#">MISC</a>
simplejobscrip -- simplejobscrip	An issue was discovered in Simplejobscrip.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	7.5	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
sphider -- sphider_pro_and_sphider_plus	A Command Execution vulnerability exists in Sphider Pro, and Sphider Plus 3 2 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5086 pertains to instances of fwrite in Sphider Pro and Sphider Plus only, but don't exist in Sphider.	2020-02-10	7.5	<a href="#">CVE-2014-5086</a> <a href="#">MISC</a>
sphider -- sphider_search_engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 due to exec calls in admin/spiderfuncs.php, which could let a remote malicious user execute arbitrary code.	2020-02-07	7.5	<a href="#">CVE-2014-5087</a> <a href="#">MISC</a> <a href="#">MISC</a>
status2k -- server_monitoring_software	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multiplies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	10	<a href="#">CVE-2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ui -- edgswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	7.2	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress W3 Total Cache Plugin 0.9.2.8 has a Remote PHP Code Execution Vulnerability	2020-02-12	7.5	<a href="#">CVE-2013-2010</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	NextGEN Gallery plugin before 1.9.13 for WordPress: nggallery.php file upload	2020-02-11	10	<a href="#">CVE-2013-3684</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress --	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for	2020-02-		<a href="#">CVE-2014-8739</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

wordpress	WordPress and before 2 0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	08	<a href="#">7.5</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
yabb -- yabb	YaBB through 2.5.2: 'guestlanguage' Cookie Parameter Local File Include Vulnerability	2020-02-11	<a href="#">7.5</a>	<a href="#">CVE-2013-2057</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zend_framework -- zend_framework	Zend Framework, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	2020-02-11	<a href="#">7.5</a>	<a href="#">CVE-2014-2052</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3733</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3731</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3721</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3739</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3738</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3728</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3736</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3735</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3734</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3732</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3737</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3730</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3729</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3727</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3726</a> <a href="#">CONF RM</a>



adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3725</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3724</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3723</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3722</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3720</a> <a href="#">CONF RM</a>
apple -- ios_and_os_x	LibTIFF prior to 4.0.4, as used in Apple iOS before 8.4 and OS X before 10.10.4 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted TIFF image.	2020-02-12	4.3	<a href="#">CVE-2014-8128</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira_server_and_data_center	The VerifyPopServerConnection!add jsps component in Atlassian Jira Server and Data Center before version 8.7.0 is vulnerable to cross-site request forgery (CSRF). An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	6.8	<a href="#">CVE-2019-20099</a> <a href="#">N/A</a> <a href="#">N/A</a>
atlassian -- jira_server_and_data_center	The VerifySmtpServerConnection!add jsps component in Atlassian Jira Server and Data Center before version 8.7.0 is vulnerable to cross-site request forgery (CSRF). An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	6.8	<a href="#">CVE-2019-20098</a> <a href="#">N/A</a> <a href="#">N/A</a>
blackberry -- playbook	BlackBerry PlayBook before 2.1 has an Information Disclosure Vulnerability via a Web browser component error	2020-02-10	4.3	<a href="#">CVE-2012-5828</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	4	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>
bosch -- multiple_products	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR P 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-07	5	<a href="#">CVE-2020-6768</a> <a href="#">CONF RM</a>
bosch -- video_streaming_gateway_and_divar_ip	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This	2020-02-07	6.4	<a href="#">CVE-2020-6769</a> <a href="#">CONF RM</a>

	affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR P all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR P 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.			
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	4.6	<a href="#">CVE-2019-11484</a> MISC MISC
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	6.1	<a href="#">CVE-2019-11481</a> MISC MISC
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	6.8	<a href="#">CVE-2020-1700</a> SUSE CONF RM
chamilo -- chamilo_lms	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	4.3	<a href="#">CVE-2012-4029</a> MISC MISC MISC
cisco -- application_control_engine	Cisco ACE A2(3.6) allows log retention DOS.	2020-02-07	5	<a href="#">CVE-2013-1202</a> MISC
clearcanvas -- clearcanvas	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	4.3	<a href="#">CVE-2020-8788</a> MISC
cypress -- psoc_4_devices	The Bluetooth Low Energy (BLE) stack implementation on Cypress PSoC 4 through 3.62 devices does not properly restrict the BLE Link Layer header and executes certain memory contents upon receiving a packet with a Link Layer D (LLID) equal to zero. This allows attackers within radio range to cause deadlocks, cause anomalous behavior in the BLE state machine, or trigger a buffer overflow via a crafted BLE Link Layer frame.	2020-02-10	6.1	<a href="#">CVE-2019-17061</a> MISC MISC
d-link -- dir865l_devices	D-Link DIR865L v1 03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	4.3	<a href="#">CVE-2013-3096</a> MISC MISC MISC
daum_communications -- potplayer	Potplayer prior to 1 5.39659: DLL Loading Arbitrary Code Execution Vulnerability	2020-02-11	6.8	<a href="#">CVE-2013-3942</a> MISC MISC
dialog -- da14580/1/2/3_devices	The Bluetooth Low Energy implementation on Dialog Semiconductor SDK through 5.0.4 for DA14580/1/2/3 devices does not properly restrict the L2CAP payload length, allowing attackers in radio range to cause a buffer overflow via a crafted Link Layer packet.	2020-02-10	6.1	<a href="#">CVE-2019-17517</a> MISC MISC
dialog -- da1468x_devices	The Bluetooth Low Energy implementation on Dialog Semiconductor SDK through 1.0.14.1081 for DA1468x devices responds to link layer packets with a payload length larger than expected, allowing attackers in radio range to cause a buffer overflow via a crafted packet. This affects, for example, August Smart Lock.	2020-02-10	6.1	<a href="#">CVE-2019-17518</a> MISC MISC
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container Ds.	2020-02-07	4.3	<a href="#">CVE-2014-5278</a> MISC MISC MISC

drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access_basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	4	<a href="#">CVE-2012-5570</a> MISC MISC MISC CONFIRM
filemaker -- filemaker_pro_and_filemaker_pro_advanced	An Authentication Bypass vulnerability exists in the MatchPasswordData function in DBEngine.dll in Filemaker Pro 13.03 and Filemaker Pro Advanced 12.04, which could let a malicious user obtain elevated privileges.	2020-02-11	4.6	<a href="#">CVE-2014-8347</a> MISC MISC MISC MISC
flowplayer -- flowplayer_flash	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	6.8	<a href="#">CVE-2011-3642</a> MISC MISC MISC MISC MISC MISC MISC MISC
fork -- fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	4.3	<a href="#">CVE-2014-9470</a> MISC MISC MISC MISC MISC
fortiguard -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctsched process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	6.6	<a href="#">CVE-2019-16155</a> MISC CONFIRM
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	6.8	<a href="#">CVE-2019-13333</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	6.8	<a href="#">CVE-2019-13334</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	6.8	<a href="#">CVE-2019-17135</a> MISC

foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	6.8	<a href="#">CVE-2019-17136</a> MISC
gizmo5 -- gizmo5	The S P implementation on the Gizmo5 software phone provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "S P Digest Leak" issue.	2020-02-12	4.3	<a href="#">CVE-2009-5139</a> MISC MISC
google -- chrome	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6414</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2020-02-11	4.3	<a href="#">CVE-2020-6392</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6393</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6415</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass HTML validators via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6413</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in navigation in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to confuse the user via a crafted domain name.	2020-02-11	6.8	<a href="#">CVE-2020-6410</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker who convinced the user to enter a URI to bypass navigation restrictions via a crafted domain name.	2020-02-11	6.8	<a href="#">CVE-2020-6409</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2020-02-11	6.8	<a href="#">CVE-2020-6402</a> SUSE MISC MISC
google -- chrome	Use after free in V8 in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6379</a> MISC MISC
google -- chrome	Type confusion in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6382</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in storage in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass site isolation via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6385</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.130 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted Chrome Extension.	2020-02-11	6.8	<a href="#">CVE-2020-6380</a> MISC MISC
	Integer overflow in JavaScript in Google			<a href="#">CVE-2020-</a>



google -- chrome	Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6381</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use of uninitialized data in PDFium in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2020-02-11	6.8	<a href="#">CVE-2020-6398</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6390</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.	2020-02-11	6.8	<a href="#">CVE-2020-6389</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds access in WebAudio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6388</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.	2020-02-11	6.8	<a href="#">CVE-2020-6387</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	5.8	<a href="#">CVE-2020-6412</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use after free in speech in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6378</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient data validation in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6416</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	5.8	<a href="#">CVE-2020-6411</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in installer in Google Chrome prior to 80.0.3987.87 allowed a local attacker to execute arbitrary code via a crafted registry entry.	2020-02-11	4.6	<a href="#">CVE-2020-6417</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to potentially exploit heap corruption via crafted clipboard content.	2020-02-11	4.6	<a href="#">CVE-2020-6404</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2020-02-11	5.8	<a href="#">CVE-2020-6394</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient validation of untrusted input in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to bypass content security policy via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6391</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds read in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6395</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in Skia in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6396</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in sharing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6397</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in CORS in Google Chrome prior to 80.0.3987.87	2020-02-		<a href="#">CVE-2020-6400</a>

	allowed a remote attacker to leak cross-origin data via a crafted HTML page.	11	4.3	<a href="#">SUSE MISC MISC</a>
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	4.3	<a href="#">CVE-2020-6401 SUSE MISC MISC</a>
google -- chrome	Incorrect implementation in Omnibox in Google Chrome on iOS prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6403 SUSE MISC MISC</a>
google -- chrome	Out of bounds read in SQLite in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6405 SUSE MISC MISC</a>
google -- chrome	Insufficient policy enforcement in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6399 SUSE MISC MISC</a>
hp -- system_event_utility	A potential security vulnerability has been identified with certain versions of HP System Event Utility prior to version 1.4.33. This vulnerability may allow a local attacker to execute arbitrary code via an HP System Event Utility system service.	2020-02-13	4.6	<a href="#">CVE-2019-18915 FULLDISC MISC</a>
htmlunit -- htmlunit	HtmlUnit prior to 2.37.0 contains code execution vulnerabilities. HtmlUnit initializes Rhino engine improperly, hence a malicious JavaScript code can execute arbitrary Java code on the application. Moreover, when embedded in Android application, Android-specific initialization of Rhino engine is done in an improper way, hence a malicious JavaScript code can execute arbitrary Java code on the application.	2020-02-11	6.8	<a href="#">CVE-2020-5529 CONF RM JVN</a>
ibm -- cloud_cli	IBM Cloud CLI 0.6.0 through 0.16.1 windows installers are signed using SHA1 certificate. An attacker might be able to exploit the weak algorithm to generate a installer with malicious software inside. IBM X-Force ID: 162773.	2020-02-12	5	<a href="#">CVE-2019-4427 XE CONF RM</a>
ibm -- content_navigator	IBM Content Navigator 3.0CD is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 172815.	2020-02-12	5	<a href="#">CVE-2019-4741 XE CONF RM</a>
ibm -- infosphere_guardium	InfoSphere Guardium aix_ktap module: DoS	2020-02-10	4.9	<a href="#">CVE-2012-2204 MISC</a>
ispconfig -- ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	6.5	<a href="#">CVE-2013-3629 MISC MISC MISC MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2020-02-12	4	<a href="#">CVE-2020-2118 MLIST CONF RM</a>
jenkins -- jenkins	Jenkins NUnit Plugin 0.25 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks.	2020-02-12	6.5	<a href="#">CVE-2020-2115 MLIST CONF RM</a>
jenkins -- jenkins	Jenkins ECX Copy Data Management Plugin 1.9 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2128 MLIST CONF RM</a>
jenkins -- jenkins	Jenkins FitNesse Plugin 1.30 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks.	2020-02-12	6.5	<a href="#">CVE-2020-2120 MLIST CONF RM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers	2020-02-		<a href="#">CVE-2020-2116</a>

	to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	12	6.8	<a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2020-02-12	4	<a href="#">CVE-2020-2117</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Debian Package Builder Plugin 1.6.11 and earlier stores a GPG passphrase unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2125</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Google Kubernetes Engine Plugin 0.8.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	2020-02-12	6.5	<a href="#">CVE-2020-2121</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins DigitalOcean Plugin 1.1 and earlier stores a token unencrypted in the global config.xml file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2126</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins BMC Release Package and Deployment Plugin 1.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2127</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Applatix Plugin 1.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2133</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Eagle Tester Plugin 1.0.9 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2129</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Sandbox protection in Jenkins Script Security Plugin 1.69 and earlier could be circumvented during the script compilation phase by applying AST transforming annotations to imports or by using them inside of other annotations.	2020-02-12	6.5	<a href="#">CVE-2020-2110</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Sandbox protection in Jenkins Pipeline: Groovy Plugin 2.78 and earlier can be circumvented through default parameter expressions in CPS-transformed methods.	2020-02-12	6.5	<a href="#">CVE-2020-2109</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2130</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores passwords unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2131</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins S3 publisher Plugin 0.11.4 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	2020-02-12	5	<a href="#">CVE-2020-2114</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Azure AD Plugin 1.1.2 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	2020-02-12	5	<a href="#">CVE-2020-2119</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Parasoft Environment Manager Plugin 2.14 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2132</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can	2020-02-12	4	<a href="#">CVE-2020-2124</a> <a href="#">MLIST</a>

	be viewed by users with Extended Read permission, or access to the master file system.			<a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins RadarGun Plugin 1.7 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	2020-02-12	<a href="#">6.5</a>	<a href="#">CVE-2020-2123</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
kemp_technologies -- loadmaster	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	<a href="#">6.8</a>	<a href="#">CVE-2014-5288</a> <a href="#">MISC</a> <a href="#">MISC</a>
konqueror -- konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	<a href="#">6.8</a>	<a href="#">CVE-2012-4512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgd -- libgd	gdImageClone in gd.c in libgd 2.1.0-rc2 through 2.2.5 has a NULL pointer dereference allowing attackers to crash an application via a specific function call sequence. Only affects PHP when linked with an external libgd (not bundled).	2020-02-11	<a href="#">5</a>	<a href="#">CVE-2018-14553</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys -- spa2102_devices	The S P implementation on the Linksys SPA2102 phone adapter provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "S P Digest Leak" issue.	2020-02-12	<a href="#">4.3</a>	<a href="#">CVE-2009-5140</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	The int3 handler in the Linux kernel before 3.3 relies on a per-CPU debug stack, which allows local users to cause a denial of service (stack corruption and panic) via a crafted application that triggers certain lock contention.	2020-02-12	<a href="#">4.9</a>	<a href="#">CVE-2012-0810</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
linuxmint -- linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	<a href="#">5</a>	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint -- linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	<a href="#">5</a>	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Upload Center Forms Component of Web File Manager in Rumpus FTP 8.2.9.1. This could allow an attacker to delete, create, and update the upload forms via RAPR/TriggerServerFunction.html.	2020-02-10	<a href="#">5.8</a>	<a href="#">CVE-2019-19669</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Block Clients component of Web File Manager in Rumpus FTP 8.2.9.1 that could allow an attacker to whitelist or block any IP address via RAPR/BlockedClients.html.	2020-02-10	<a href="#">5.8</a>	<a href="#">CVE-2019-19667</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the File Types component of Web File Manager in Rumpus FTP 8.2.9.1 that allows an attacker to add or delete the file types that are used on the server via RAPR/TriggerServerFunction.html.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19668</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the FTP Settings of Web File Manager in Rumpus FTP 8.2.9.1. Exploitation of this vulnerability can result in manipulation of Server FTP settings at RAPR/FTPSettingsSet.html.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19665</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A Cookie based reflected XSS exists in the Web File Manager of Rumpus FTP Server 8.2.9.1, related to RumpusLoginUserName and snp.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19661</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Folder Sets Settings of Web File Manager in Rumpus FTP 8.2.9.1. This allows an attacker to Create/Delete Folders after exploiting it at RAPR/FolderSetsSet.html.	2020-02-10	<a href="#">5.8</a>	<a href="#">CVE-2019-19663</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Event Notices Settings of Web File Manager in Rumpus FTP 8.2.9.1. An attacker can create/update event notices via	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19666</a> <a href="#">MISC</a> <a href="#">MISC</a>



	RAPR/EventNoticesSet.html.			
maxum_development corporation - rumpus_ftp	A CSRF vulnerability exists in the Web File Manager's Network Setting functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can manipulate the SMTP setting and other network settings via RAPR/NetworkSettingsSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19660</a> MISC MISC
maxum_development corporation - rumpus_ftp	A HTTP Response Splitting vulnerability was identified in the Web Settings Component of Web File Manager in Rumpus FTP Server 8.2.9.1. A successful exploit can result in stored XSS, website defacement, etc. via ExtraHTTPHeader to RAPR/WebSettingsGeneralSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19670</a> MISC MISC
maxum_development corporation - rumpus_ftp_server	A CSRF vulnerability exists in the Web File Manager's Edit Accounts functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can take over a user account by changing the password, update users' details, and escalate privileges via RAPR/DefineUsersSet.html.	2020-02-10	6.8	<a href="#">CVE-2019-19659</a> MISC MISC
mfscripts -- yetishare	MFScripts YetiShare v3 5 2 through v4 5 4 might allow an attacker to reset a password by using a leaked hash (the hash never expires until used).	2020-02-10	5	<a href="#">CVE-2019-20062</a> MISC MISC MISC
mfscripts -- yetishare	MFScripts YetiShare v3 5 2 through v4 5 4 places sensitive information in the Referer header. If this leaks, then third parties may discover password-reset hashes, file-delete links, or other sensitive information.	2020-02-10	5	<a href="#">CVE-2019-20060</a> MISC MISC MISC
mfscripts -- yetishare	The user-introduction email in MFScripts YetiShare v3 5 2 through v4 5 4 may leak the (system-picked) password if this email is sent in cleartext. In other words, the user is not allowed to choose their own initial password.	2020-02-10	5	<a href="#">CVE-2019-20061</a> MISC MISC MISC
mfscripts -- yetishare	payment_manage.ajax.php and various *_manage.ajax.php in MFScripts YetiShare 3 5 2 through 4 5 4 directly insert values from the sSortDir_0 parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection. NOTE: this issue exists because of an incomplete fix for CVE-2019-19732.	2020-02-10	6.8	<a href="#">CVE-2019-20059</a> MISC MISC MISC MISC
microchip_technology -- atsamb11_devices	The Bluetooth Low Energy implementation on Microchip Technology BluSDK Smart through 6.2 for ATSAMB11 devices does not properly restrict link-layer data length on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.	2020-02-10	6.1	<a href="#">CVE-2019-19195</a> MISC MISC
microsoft -- edge	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'.	2020-02-11	4	<a href="#">CVE-2020-0663</a> MISC
microsoft -- exchange_server_2013, and 2016 and 2019	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0692</a> MISC
microsoft -- internet_explorer_10_and_11	An information disclosure vulnerability exists in the way that affected Microsoft Internet Explorer handles cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'.	2020-02-11	4.3	<a href="#">CVE-2020-0706</a> MISC
microsoft -- malicious_software_removal_tool	An elevation of privilege vulnerability exists when the Windows Malicious Software Removal Tool (MSRT) improperly handles junctions. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Malicious Software Removal Tool Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0733</a> MISC
microsoft --	A security feature bypass vulnerability exists in Microsoft Outlook software when			<a href="#">CVE-2020-</a>

multiple_products	it improperly handles the parsing of URI formats, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'.	2020-02-11	4.3	<a href="#">0696 MISC</a>
microsoft -- multiple_windows_products	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0689 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682.	2020-02-11	4.6	<a href="#">CVE-2020-0680 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0735 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.	2020-02-11	4.6	<a href="#">CVE-2020-0669 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Client License Service (ClipSVC) handles objects in memory, aka 'Windows Client License Service Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0701 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0740 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739.	2020-02-11	4.6	<a href="#">CVE-2020-0737 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749.	2020-02-11	4.6	<a href="#">CVE-2020-0750 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0737.	2020-02-11	4.6	<a href="#">CVE-2020-0739 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.	2020-02-11	4.6	<a href="#">CVE-2020-0668 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0741 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-	2020-02-11	4.6	<a href="#">CVE-2020-0742 MISC</a>

	2020-0743, CVE-2020-0749, CVE-2020-0750.			
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0743</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0659.	2020-02-11	4.6	<a href="#">CVE-2020-0747</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0749</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735.	2020-02-11	4.6	<a href="#">CVE-2020-0752</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682.	2020-02-11	4.6	<a href="#">CVE-2020-0679</a> MISC
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'.	2020-02-11	5	<a href="#">CVE-2020-0746</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0665</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754.	2020-02-11	4.6	<a href="#">CVE-2020-0753</a> MISC
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0729</a> MISC
microsoft -- multiple_windows_products	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	2020-02-11	5	<a href="#">CVE-2020-0660</a> MISC
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751.	2020-02-11	5.5	<a href="#">CVE-2020-0661</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0657</a> MISC

microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0747.	2020-02-11	4.6	<a href="#">CVE-2020-0659</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0666</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0667</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753.	2020-02-11	4.6	<a href="#">CVE-2020-0754</a> MISC
microsoft -- sql_server_2012_and_2014_and_2016	A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests, aka 'Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability'.	2020-02-11	6.5	<a href="#">CVE-2020-0618</a> MISC
microsoft -- surface_hub	A security feature bypass vulnerability exists in Surface Hub when prompting for credentials, aka 'Surface Hub Security Feature Bypass Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0702</a> MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It mishandled time skew (between the machine hosting the web server and the machine hosting the database) when trying to block a brute-force series of invalid requests.	2020-02-12	4.3	<a href="#">CVE-2020-8890</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It did not canonicalize usernames when trying to block a brute-force series of invalid requests.	2020-02-12	4.3	<a href="#">CVE-2020-8891</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It did not consider the HTTP PUT method when trying to block a brute-force series of invalid requests.	2020-02-12	6.8	<a href="#">CVE-2020-8892</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. The Galaxy view contained an incorrectly sanitized search string in app/View/Galaxies/view.ctp.	2020-02-12	5	<a href="#">CVE-2020-8893</a> MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. ACLs for discussion threads were mishandled in app/Controller/ThreadsController.php and app/Model/Thread.php.	2020-02-12	6.4	<a href="#">CVE-2020-8894</a> MISC MISC
netcracker -- netcracker_resource_management_system	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h, (3) %2427, (3) h, (4) %2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	6.5	<a href="#">CVE-2015-3423</a> MISC MISC
netsurf -- libnsbmp	Heap-based buffer overflow in the bmp_decode_rle function in libnsbmp.c in Libnsbmp 0.1.2 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the last row of RLE data in a crafted BMP file.	2020-02-12	6.8	<a href="#">CVE-2015-7508</a> MISC MISC
node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	5	<a href="#">CVE-2019-15604</a> MISC CONF RM CONF RM CONF RM



nxp -- kw41z_devices	The Bluetooth Low Energy (BLE) stack implementation on the NXP KW41Z (based on the MCUXpresso SDK with Bluetooth Low Energy Driver 2.1 and earlier) does not properly restrict the BLE Link Layer header and executes certain memory contents upon receiving a packet with a Link Layer D (LL D) equal to zero. This allows attackers within radio range to cause deadlocks, cause anomalous behavior in the BLE state machine, or trigger a buffer overflow via a crafted BLE Link Layer frame.	2020-02-10	6.1	<a href="#">CVE-2019-17060</a> MISC MISC
oberhumer -- libzo2_and_lzo-2	Integer overflow in the LZO algorithm variant in Oberhumer libzo2 and lzo-2 before 2.07 on 32-bit platforms might allow remote attackers to execute arbitrary code via a crafted Literal Run.	2020-02-12	6.8	<a href="#">CVE-2014-4607</a> MISC CONF RM
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	4	<a href="#">CVE-2014-9127</a> MISC
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the YII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	4.3	<a href="#">CVE-2014-9126</a> MISC
openfiler -- openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	4.3	<a href="#">CVE-2011-1086</a> MISC MISC MISC
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	5.5	<a href="#">CVE-2020-1768</a> CONF RM
perforce_software -- p4web	Perforce P4web 2011.1 and 2012.1 has multiple XSS vulnerabilities	2020-02-12	4.3	<a href="#">CVE-2013-1410</a> MISC MISC
phonerlite -- phonerlite	The PhonerLite phone before 2.15 provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "SIP Digest Leak" issue.	2020-02-12	4.3	<a href="#">CVE-2014-2560</a> MISC
php -- php	When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbf_ffi_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.	2020-02-10	6.4	<a href="#">CVE-2020-7060</a> MISC
php -- php	When using fgets() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash.	2020-02-10	6.4	<a href="#">CVE-2020-7059</a> MISC
pragmamx -- pragmamx	Multiple cross-site scripting (XSS) vulnerabilities in pragmaMx 1.x before 1.12.2 allow remote attackers to inject arbitrary web script or HTML via the (1) name parameter to modules.php or (2) img_url to includes/wysiwyg/spaw/editor/plugins/imgpopup/img_popup.php.	2020-02-11	4.3	<a href="#">CVE-2012-2452</a> MISC MISC MISC
prestashop -- prestashop	Cross-site scripting (XSS) vulnerability in PrestaShop before 1.4.9 allows remote attackers to inject arbitrary web script or HTML via the index of the product[] parameter to ajax.php.	2020-02-11	4.3	<a href="#">CVE-2012-2517</a> MISC MISC
	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon			

qualcomm -- multiple_snapdragon_products	Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> CONF RM
qualcomm -- multiple_snapdragon_products	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> CONF RM
railo_technologies -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	6.8	<a href="#">CVE-2014-5468</a> MISC MISC MISC MISC
red_hat -- openshift_entrpise	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-app.	2020-02-07	4.4	<a href="#">CVE-2020-1708</a> CONF RM
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, stores users' information by cleartext in the cookie, which divulges password to attackers.	2020-02-11	5	<a href="#">CVE-2020-3935</a> MISC MISC MISC
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, allows attackers to enumerate and exam user account in the system.	2020-02-11	5	<a href="#">CVE-2020-3933</a> MISC MISC MISC
siemens -- multiple_scalance_devices	A vulnerability has been identified in SCALANCE S602 (All versions >= V3.0), SCALANCE S612 (All versions >= V3.0), SCALANCE S623 (All versions >= V3.0), SCALANCE S627-2M (All versions >= V3.0). Specially crafted packets sent to port 443/tcp of affected devices could cause a Denial-of-Service condition of the web server.	2020-02-11	5	<a href="#">CVE-2019-13925</a> MISC
siemens -- multiple_scalance_switches	A vulnerability has been identified in SCALANCE X-200 switch family (incl. SIPLUS NET variants) (all versions < 5.2.4), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All versions), SCALANCE X-300 switch family (incl. X408 and S PLUS NET variants) (all versions < 4.1.3). The device does not send the X-Frame-Option Header in the administrative web interface, which makes it vulnerable to Clickjacking attacks. The security vulnerability could be exploited by an attacker that is able to trick an administrative user with a valid session on the target device into clicking on a website controlled by the attacker. The	2020-02-11	4.3	<a href="#">CVE-2019-13924</a> MISC

	vulnerability could allow an attacker to perform administrative actions via the web interface. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- multiple_simatic_devices	A vulnerability has been identified in SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.1), SIMATIC S7-300 PN/DP CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions). Affected devices contain a vulnerability that could cause a Denial-of-Service condition of the web server by sending specially crafted HTTP requests to ports 80/tcp and 443/tcp. The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device's web server. Beyond the web service, no other functions or interfaces are affected by the Denial-of-Service condition.	2020-02-11	5	<a href="#">CVE-2019-13940</a> <a href="#">MISC</a> <a href="#">MISC</a>
siemens -- ozw672_and_772_web_servers	A vulnerability has been identified in OZW672 (All versions < V10.00), OZW772 (All versions < V10.00). Vulnerable versions of OZW Web Server use predictable path names for project files that legitimately authenticated users have created by using the application's export function. By accessing a specific uniform resource locator on the web servers a remote attacker could be able to download a project file without prior authentication. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected system. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises the confidentiality of the targeted system.	2020-02-11	5	<a href="#">CVE-2019-13941</a> <a href="#">MISC</a>
simple_machines -- simple_machines_forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: Forum admin can read files such as the database config.	2020-02-07	4	<a href="#">CVE-2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
smoothwall - smoothwall_express_3	A cross-site scripting (XSS) vulnerability in Smoothwall Express 3.	2020-02-07	4.3	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall -- smoothwall_express_3	CSRF vulnerability in Smoothwall Express 3.	2020-02-07	6.8	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
socialengine -- socialengine	Multiple cross-site request forgery (CSRF) vulnerabilities in the (1) Forum, (2) Event, and (3) Classifieds plugins in SocialEngine before 4.2.4.	2020-02-11	6.8	<a href="#">CVE-2012-6721</a> <a href="#">MISC</a>
socialengine -- socialengine	Multiple cross-site scripting (XSS) vulnerabilities in SocialEngine before 4.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) title parameter to music/create, (2) location parameter to events/create, or (3) search parameter to widget/index/content_id/*.	2020-02-11	4.3	<a href="#">CVE-2012-6720</a> <a href="#">MISC</a>
sockjs -- sockjs	htmlfile in lib/transport/htmlfile.js in SockJS before 3.0 is vulnerable to Reflected XSS via the /htmlfile c (aka callback) parameter.	2020-02-10	4.3	<a href="#">CVE-2020-8823</a> <a href="#">MISC</a> <a href="#">MISC</a>
sphider -- sphider	A Command Execution vulnerability exists in Sphider before 1.3.6 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5083 pertains to instances of fwrite in Sphider.	2020-02-10	6.5	<a href="#">CVE-2014-5083</a> <a href="#">MISC</a>
sphider -- sphider_plus	A Command Execution vulnerability exists in Sphider Plus 3.2 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5085 pertains to instances of fwrite in Sphider Plus, but do not exist in either Sphider or Sphider Pro.	2020-02-10	6.5	<a href="#">CVE-2014-5085</a> <a href="#">MISC</a>

sphider -- sphider_pro	A Command Execution vulnerability exists in Sphider Pro 3.2 due to insufficient sanitization of fwrite, which could let a remote malicious user execute arbitrary code. CVE-2014-5084 pertains to instances of fwrite in Sphider Pro only, but do not exist in either Sphider or Sphider Plus.	2020-02-10	6.5	<a href="#">CVE-2014-5084</a> MISC
statusnet -- statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	5	<a href="#">CVE-2010-4658</a> MISC MISC
suse -- opensuse_wicked	An ni_dhcp4_fsm_process_dhcp4_packet memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets with a different client-id.	2020-02-11	5	<a href="#">CVE-2020-7217</a> SUSE MISC MISC MISCm
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5820</a> MISC
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5822</a> MISC
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a DLL injection vulnerability, which is a type of issue whereby an individual attempts to execute their own code in place of legitimate code as a means to perform an exploit.	2020-02-11	4.6	<a href="#">CVE-2020-5821</a> MISC
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5823</a> MISC
teamviewer -- teamviewer_desktop	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9 x , this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.	2020-02-07	4.4	<a href="#">CVE-2019-18988</a> MISC MISC MISC MISC
testlink -- testlink	An issue was discovered in TestLink 1.9.19. The relation_type parameter of	2020-02-		<a href="#">CVE-2020-8841</a>



	the lib/requirements/reqSearch.php endpoint is vulnerable to authenticated SQL Injection.	10	<a href="#">6.5</a>	<a href="#">MISC</a> <a href="#">MISC</a>
texas_instruments -- cc2640r2_devices	The Bluetooth Low Energy implementation on Texas Instruments SDK through 3.30.00.20 for CC2640R2 devices does not properly restrict the SM Public Key packet on reception, allowing attackers in radio range to cause a denial of service (crash) via crafted packets.	2020-02-10	<a href="#">6.1</a>	<a href="#">CVE-2019-17520</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
texas_instruments -- multiple_devices	The Bluetooth Low Energy peripheral implementation on Texas Instruments SIMPLELINK-CC2640R2-SDK through 3.30.00.20 and BLE-STACK through 1.5.0 before Q4 2019 for CC2640R2 and CC2540/1 devices does not properly restrict the advertisement connection request packet on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.	2020-02-10	<a href="#">6.1</a>	<a href="#">CVE-2019-19193</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_bug_genie -- the_bug_genie	The Bug Genie before 3.2.6 has Multiple XSS and HTML Injection Vulnerabilities	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2013-1760</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ubiquiti_networks -- unifi_controller	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4) authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the UniFi Controller name via a request to api/set/setting/identity.	2020-02-08	<a href="#">6.8</a>	<a href="#">CVE-2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>
vbseo -- vbseo	vbSeo before 3.6.0PL2 allows XSS via the member.php u parameter.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2012-6666</a> <a href="#">MISC</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	<a href="#">6.5</a>	<a href="#">CVE-2013-3591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
watchguard -- firewire_xtm	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	<a href="#">4.3</a>	<a href="#">CVE-2014-6413</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	<a href="#">6.5</a>	<a href="#">CVE-2015-2062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	A Cross-site Scripting (XSS) vulnerability exists in the All in One SEO Pack plugin before 2.0.3.1 for WordPress via the Search parameter.	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2013-5988</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	<a href="#">6.8</a>	<a href="#">CVE-2013-2009</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	<a href="#">4.3</a>	<a href="#">CVE-2013-2008</a> <a href="#">MISC</a> <a href="#">MISC</a>

				<a href="#">MISC</a>
xiaomi -- mi6_devices	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Xiaomi Browser Prior to 10.4.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the miui.share application. The issue results from the lack of proper validation of user-supplied data, which can result in an arbitrary application download. An attacker can leverage this vulnerability to execute code in the context of the user. Was ZDI-CAN-7483.	2020-02-10	<a href="#">6.8</a>	<a href="#">CVE-2019-13322</a> <a href="#">MISC</a>
xiaomi -- mi6_devices	This vulnerability allows network adjacent attackers to execute arbitrary code on affected installations of Xiaomi Browser Prior to 10.4.0. User interaction is required to exploit this vulnerability in that the target must connect to a malicious access point. The specific flaw exists within the handling of HTTP responses to the Captive Portal. A crafted HTML response can cause the Captive Portal to open a browser to a specified location without user interaction. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7467.	2020-02-10	<a href="#">5.4</a>	<a href="#">CVE-2019-13321</a> <a href="#">MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	<a href="#">6.5</a>	<a href="#">CVE-2013-3628</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Zenphoto before 1.4.3.4 admin-news-articles.php date parameter XSS.	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2012-4519</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - applications_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	<a href="#">5</a>	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apport -- apport	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	<a href="#">1.9</a>	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a> <a href="#">MISC</a>
apport -- apport	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	<a href="#">2.1</a>	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a> <a href="#">MISC</a>
apport -- apport	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	<a href="#">2.1</a>	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a> <a href="#">MISC</a>
bludit -- bludit	<b>** DISPUTED **</b> Bludit 3.10.0 allows Editor or Author roles to insert malicious JavaScript on the WYSIWYG editor. NOTE: the vendor's perspective is that this is "not a bug."	2020-02-07	<a href="#">3.5</a>	<a href="#">CVE-2020-8812</a> <a href="#">MISC</a>
cpanel -- cpanel_and_whm	The clientconf.html and detailbw.html pages in x3 in cPanel & WHM 11.34.0 (build 8) have a XSS vulnerability.	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2012-6449</a> <a href="#">MISC</a>
digi_transport -- multiple_devices	Digi TransPort WR21 5.2.2 3, WR44 5.1 6.4, and WR44v2 5.1.6.9 devices	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2020-8822</a>

	allow stored XSS in the web application.			<a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in CORS in Google Chrome prior to 80.0 3987.87 allowed a local attacker to obtain potentially sensitive information via a crafted HTML page.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-6408</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- hp_systems_insight_manager	HP Systems Insight Manager before 7.0 allows a remote user on adjacent network to access information	2020-02-10	<a href="#">2.7</a>	<a href="#">CVE-2012-1994</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- rational_publishing_engine	IBM Rational Publishing Engine 6 0.6 and 6.0 6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 162888.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2019-4431</a> <a href="#">XE</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Brakeman Plugin 0.12 and earlier did not escape values received from parsed JSON files when rendering them, resulting in a stored cross-site scripting vulnerability exploitable by users able to control the Brakeman post-build step input data.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2122</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Subversion Plugin 2.13.0 and earlier does not escape the error message for the Project Repository Base URL field form validation, resulting in a stored cross-site scripting vulnerability.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2111</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the parameter name shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2112</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the default value shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2113</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
keycloak -- keycloak	It was found in all keycloak versions before 9.0.0 that links to external applications (Application Links) in the admin console are not validated properly and could allow Stored XSS attacks. An authed malicious user could create URLs to trick users in other realms, and possibly conduct further attacks.	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2020-1697</a> <a href="#">CONF RM</a>
linksys -- wrt310nv2ne	Linksys WRT310Nv2 2.0 0.1 is vulnerable to XSS.	2020-02-07	<a href="#">3.5</a>	<a href="#">CVE-2013-3067</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'.	2020-02-11	<a href="#">3.6</a>	<a href="#">CVE-2020-0730</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-0658</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-0755</a> <a href="#">MISC</a>
	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to			

microsoft -- multiple_windows_products	properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0675 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0748 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0744 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755.	2020-02-11	2.1	<a href="#">CVE-2020-0756 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0716.	2020-02-11	2.1	<a href="#">CVE-2020-0717 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0717.	2020-02-11	2.1	<a href="#">CVE-2020-0716 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0705 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0698 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation	2020-02-11	2.1	<a href="#">CVE-2020-0677 MISC</a>



	Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.			
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0676</a> MISC
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows kernel does not properly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0736</a> MISC
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0693.	2020-02-11	3.5	<a href="#">CVE-2020-0694</a> MISC
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0694.	2020-02-11	3.5	<a href="#">CVE-2020-0693</a> MISC
microsoft -- windows_10_and_windows_server_products	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, could run a specially crafted application. The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE D is unique from CVE-2020-0661.	2020-02-11	2.1	<a href="#">CVE-2020-0751</a> MISC
moodle -- moodle	Persistent XSS in /course/modedit.php of Moodle through 3.7.2 allows authenticated users (Teacher and above) to inject JavaScript into the session of another user (e.g., enrolled student or site administrator) via the introeditor[text] parameter. NOTE: the discoverer and vendor disagree on whether Moodle customers have a reasonable expectation that anyone authenticated as a Teacher can be trusted with the ability to add arbitrary JavaScript (this ability is not documented on Moodle's Teacher_role page). Because the vendor has this expectation, they have stated "this report has been closed as a false positive, and not a bug."	2020-02-11	3.5	<a href="#">CVE-2019-18210</a> MISC MISC
mybulletinboard -- mybulletinboard	Cross-site scripting (XSS) vulnerability in MyBB before 1.6.13 allows remote authenticated users to inject arbitrary web script or HTML via the name parameter in the edit action of the config-profile_fields module.	2020-02-11	3.5	<a href="#">CVE-2014-3826</a> MISC
mybulletinboard -- mybulletinboard	Multiple cross-site scripting (XSS) vulnerabilities in the MyBB (aka MyBulletinBoard) before 1.8.4 allow remote authenticated users to inject arbitrary web script or HTML via the title parameter in the (1) edit or (2) add action in the user-users module or the (3) finduser action or the name parameter in an (4) edit action in the user-user module or the (5) editprofile action to modcp.php.	2020-02-11	3.5	<a href="#">CVE-2014-3827</a> CONF RM MISC
netapp --	NetApp Snap Creator Framework before			<a href="#">CVE-2016-</a>

snap_creator_framework	4.3P1 allows remote authenticated users to conduct clickjacking attacks via unspecified vectors.	2020-02-11	3.5	<a href="#">CVE-2020-5710</a> <a href="#">MISC</a>
netcracker -- netcracker_resource_manager	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the (1) ctrl, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8) xname, or (9) mpTransactionId parameter.	2020-02-08	3.5	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>
orange_hrm -- orange_hrm	Orange HRM 2.7.1 allows XSS via the vacancy name.	2020-02-10	3.5	<a href="#">CVE-2013-1353</a> <a href="#">MISC</a>
piwigo -- piwigo	Piwigo 2.10.1 is affected by stored XSS via the Group Name Field to the group_list page.	2020-02-10	3.5	<a href="#">CVE-2020-8089</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0.8.8 has stored XSS	2020-02-07	3.5	<a href="#">CVE-2013-3635</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	3.5	<a href="#">CVE-2013-3636</a> <a href="#">MISC</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	3.5	<a href="#">CVE-2013-3637</a> <a href="#">MISC</a>
rakuten -- viber_for_android	An exploitable information disclosure vulnerability exists in the 'Secret Chats' functionality of Rakuten Viber on Android 9.3 0.6. The 'Secret Chats' functionality allows a user to delete all traces of a chat either by using a time trigger or by direct request. There is a bug in this functionality which leaves behind photos taken and shared on the secret chats, even after the chats are deleted. These photos will be stored in the device and accessible to all applications installed on the Android device.	2020-02-13	2.1	<a href="#">CVE-2018-3987</a> <a href="#">MISC</a>
samsung -- knox	This vulnerability allows local attackers to disclose sensitive information on affected installations of Samsung Knox 1.2.02.39 on Samsung Galaxy S9 build G9600ZHS3ARL1 Secure Folder. An attacker must first obtain physical access to the device in order to exploit this vulnerability. The specific flaws exists within the the handling of the lock screen for Secure Folder. The issue results from the lack of proper validation that a user has correctly authenticated. An attacker can leverage this vulnerability to disclose the contents of the secure container. Was ZDI-CAN-7381.	2020-02-10	2.1	<a href="#">CVE-2019-6744</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a denial of service vulnerability, which is a type of issue whereby a threat actor attempts to tie up the resources of a resident application, thereby making certain functions unavailable.	2020-02-11	2.1	<a href="#">CVE-2020-5824</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5826</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an arbitrary file write vulnerability, which is a type of issue whereby an attacker is able to overwrite existing files on the resident system without proper privileges.	2020-02-11	3.6	<a href="#">CVE-2020-5825</a> <a href="#">MISC</a>
	Symantec Endpoint Protection Manager			

symantec -- endpoint_protection_manager	(SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5827</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5829</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5830</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5831</a> MISC
symantec -- symantec_endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5828</a> MISC
syska -- smart_bulb_devices	Syska Smart Bulb devices through 2017-08-06 receive RGB parameters over cleartext Bluetooth Low Energy (BLE), leading to sniffing, reverse engineering, and replay attacks.	2020-02-10	3.3	<a href="#">CVE-2017-18642</a> MISC
vanilla_forum -- vanilla	index.php? p=/dashboard/settings/branding in Vanilla 2.6 3 allows stored XSS.	2020-02-10	3.5	<a href="#">CVE-2020-8825</a> MISC MISC
wordpress -- wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	3.5	<a href="#">CVE-2015-1394</a> MISC MISC MISC MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll PNG pngread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted PNG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2020-6068</a> MISC
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll JPEG SOFx parser of the Accusoft ImageGear 19.5.0 library. A specially crafted JPEG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6066</a> MISC
	An exploitable out-of-bounds write vulnerability exists in the TIFreadstripdata function of the igcore19d.dll library of Accusoft ImageGear 19 5 0. A specially			<a href="#">CVE-2019-</a>

accusoft -- imagegear	crafted T FF file file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2020-5187</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the uncompress_scan_line function of the igcore19d.dll library of Accusoft ImageGear, version 19.5 0. A specially crafted PCX file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6063</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the bmp_parsing function of the igcore19d.dll library of Accusoft ImageGear, version 19.5.0. A specially crafted BMP file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6065</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the uncompress_scan_line function of the igcore19d.dll library of Accusoft ImageGear, version 19.5 0. A specially crafted PCX file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6064</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d dll JPEG jpegread precision parser of the Accusoft ImageGear 19 5 0 library. A specially crafted JPEG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6069</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d dll TIFF tifread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted T FF file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6067</a> <a href="#">MISC</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to arbitrary file system write.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3762</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3748</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to arbitrary file system write.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3763</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions, 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3742</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2017.011.30156 and earlier, and	2020-02-	not yet calculated	<a href="#">CVE-2020-3743</a>



	2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	13	calculated	<a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3744</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3745</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3746</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3747</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3749</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3750</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to memory leak .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3753</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3754</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3755</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to memory leak .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3756</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code	2020-02-13	not yet calculated	<a href="#">CVE-2020-3751</a> <a href="#">CONFIRM</a>

	execution .			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3752</a> <a href="#">CONFIRM</a>
adobe -- digital_editions	Adobe Digital Editions versions 4.5.10 and below have a buffer errors vulnerability. Successful exploitation could lead to information disclosure.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3759</a> <a href="#">CONFIRM</a>
adobe -- digital_editions	Adobe Digital Editions versions 4.5.10 and below have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3760</a> <a href="#">CONFIRM</a>
adobe -- experience_manager	Adobe Experience Manager versions 6.5, and 6.4 have an uncontrolled resource consumption vulnerability. Successful exploitation could lead to denial-of-service.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3741</a> <a href="#">CONFIRM</a>
adobe -- flash_player	Adobe Flash Player versions 32.0.0.321 and earlier, 32.0.0.314 and earlier, 32.0.0.321 and earlier, and 32.0.0.255 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3757</a> <a href="#">CONFIRM</a>
ai -- risknet_acquirer	RiskNet Acquirer before hotfix 6.0 b7+ADHOC-443 ApplicationServiceBean contains a service information disclosure.	2020-02-14	not yet calculated	<a href="#">CVE-2013-5687</a> <a href="#">X</a>
amazon -- aws-js-s3-explorer	explorer.js in Amazon AWS JavaScript S3 Explorer (aka aws-js-s3-explorer) v2 alpha before 2019-08-02 allows XSS in certain circumstances.	2020-02-13	not yet calculated	<a href="#">CVE-2019-14652</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
amd -- raadeon_amd_user_exp	The AUEPLauncher service in Radeon AMD User Experience Program Launcher through 1.0.0.1 on Windows allows elevation of privilege by placing a crafted file in %PROGRAMDATA%\AMD\PPC\upload and then creating a symbolic link in %PROGRAMDATA%\AMD\PPC\temp that points to an arbitrary folder with an arbitrary file name.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8950</a> <a href="#">MISC</a> <a href="#">MISC</a>
ammy -- ammy_admin	Ammy Admin 3.2 and earlier stores the client ID at a fixed memory location, which might make it easier for user-assisted remote attackers to bypass authentication by running a local program that extracts a field from the AA_v3.2.exe file.	2020-02-11	not yet calculated	<a href="#">CVE-2013-5582</a> <a href="#">MISC</a>
apache -- nifi	In Apache NiFi 0.0.1 to 1.11.0, the flow fingerprint factory generated flow fingerprints which included sensitive property descriptor values. In the event a node attempted to join a cluster and the cluster flow was not inheritable, the flow fingerprint of both the cluster and local flow was printed, potentially containing sensitive values in plaintext.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1942</a> <a href="#">MISC</a>
ariadne -- ariadne	Multiple cross-site scripting (XSS) vulnerabilities in Ariadne 2.7.6 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO parameter to (1) index.php and (2) loader.php.	2020-02-11	not yet calculated	<a href="#">CVE-2011-4938</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
aruba_networks -- intelligent_edge_switch	A remotely exploitable information disclosure vulnerability is present in Aruba Intelligent Edge Switch models 5400, 3810, 2920, 2930, 2530 with GigT port, 2530 10/100 port, or 2540. The vulnerability impacts firmware 16.08.* before 16.08.0009, 16.09.* before 16.09.0007 and 16.10.* before 16.10.0003. The vulnerability allows an attacker to retrieve sensitive system information. This attack can be carried out without user authentication under very specific conditions.	2020-02-13	not yet calculated	<a href="#">CVE-2019-5322</a> <a href="#">MISC</a>
askey -- ap400w_devices	An issue was discovered on Askey AP4000W TDC_V1 01.003 devices. An attacker can perform Remote Code Execution (RCE) by sending a specially crafted network packer to the bd_srv service listening on TCP port 54188.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8614</a> <a href="#">MISC</a>

askpop3d -- askpop3d	A Denial of Service vulnerability exists in askpop3d 0.7.7 in free (psQuery),	2020-02-13	not yet calculated	<a href="#">CVE-2014-3208</a> <a href="#">MISC</a>
atlassian -- jira_and_greenhopper	Stored XSS vulnerability in UpdateFieldJson.jspa in JIRA 4.4.3 and GreenHopper before 5.9.8 allows an attacker to inject arbitrary script code.	2020-02-13	not yet calculated	<a href="#">CVE-2012-1500</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
atlassian -- jira_server_and_data_center	The Atlassian Application Links plugin is vulnerable to cross-site request forgery (CSRF). The following versions are affected: all versions prior to 5.4.21, from version 6.0.0 before version 6.0.12, from version 6.1.0 before version 6.1.2, from version 7.0.0 before version 7.0.2, and from version 7.1.0 before version 7.1.3. The vulnerable plugin is used by Atlassian Jira Server and Data Center before version 8.7.0. An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	not yet calculated	<a href="#">CVE-2019-20100</a> <a href="#">N/A</a> <a href="#">N/A</a> <a href="#">N/A</a>
avira -- antivir_engine	A Denial of Service (infinite loop) vulnerability exists in Avira AntiVir Engine before 8.2.12.58 via an unspecified function in the PDF Scanner Engine.	2020-02-12	not yet calculated	<a href="#">CVE-2013-4602</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
barracuda -- web_application_firewall	Barracuda Web Application Firewall (WAF) 7.8.1.013 allows remote attackers to bypass authentication by leveraging a permanent authentication token obtained from a query string.	2020-02-12	not yet calculated	<a href="#">CVE-2014-2595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bearftp -- bearftp	Improper connection handling in the base connection handler in IKTeam BearFTP before v0.3.1 allows a remote attacker to achieve denial of service via a Slowloris approach by sending a large volume of small packets.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
belkin -- n750_routers	Belkin n750 routers have a buffer overflow.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7173</a> <a href="#">MISC</a> <a href="#">MISC</a>
boat_browser -- boat_browser_for_android	The WebView class and use of the WebView.addJavascriptInterface method in the Boat Browser application 8.0 and 8.0.1 for Android allow remote attackers to execute arbitrary code via a crafted web site, a related issue to CVE-2012-6636.	2020-02-12	not yet calculated	<a href="#">CVE-2014-4968</a> <a href="#">MISC</a>
bss -- bs-client_private_client	A Two-Factor Authentication Bypass Vulnerability exists in BS-Client Private Client 2.4 and 2.5 via an XML request that neglects the use of ADPsw D and AD parameters, which could let a malicious user access privileged function.	2020-02-13	not yet calculated	<a href="#">CVE-2014-4198</a> <a href="#">MISC</a>
chiyu_technology -- bf-430_devices	Stored XSS was discovered on CHIYU BF-430 232/485 TCP/ P Converter devices before 1.16.00, as demonstrated by the /if cgi TF_submask field.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8839</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- internetwork_operating_systems	A memory leak vulnerability exists in Cisco IOS before 15.2(1)T due to a memory leak in the HTTP PROXY Server process (aka CSCu52820), when configured with Cisco ISR Web Security with Cisco ScanSafe and User Authentication NTLM configured.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4661</a> <a href="#">MISC</a>
cloud_foundry -- credhub	Cloud Foundry CredHub, versions prior to 2.5.10, connects to a MySQL database without TLS even when configured to use TLS. A malicious user with access to the network between CredHub and its MySQL database may eavesdrop on database connections and thereby gain unauthorized access to CredHub and other components.	2020-02-12	not yet calculated	<a href="#">CVE-2020-5399</a> <a href="#">CONF RM</a>
	Codologic CodoForum through 4.8.4 allows a DOM-based XSS. While creating			

codologic -- codofurm	a new topic as a normal user, it is possible to add a poll that is automatically loaded in the DOM once the thread/topic is opened. Because session cookies lack the HttpOnly flag, it is possible to steal authentication cookies and take over accounts.	2020-02-15	not yet calculated	<a href="#">CVE-2020-7050</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
codologic -- codofurm	Codologic Codoforum through 4.8.4 allows stored XSS in the login area. This is relevant in conjunction with CVE-2020-5842 because session cookies lack the HttpOnly flag. The impact is account takeover.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7051</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	In iTop through 2.6.0, an XSS payload can be delivered in certain fields (such as icon) of the XML file used to build the dashboard. This is similar to CVE-2015-6544 (which is only about the dashboard title).	2020-02-14	not yet calculated	<a href="#">CVE-2019-13966</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	iTop 2.2.0 through 2.6.0 allows remote attackers to cause a denial of service (application outage) via many requests to launch a compile operation. The requests use the pages/exec.php?exec_env=production&exec_module=itop-hub-connector&exec_page=ajax.php&operation=compile URI. This only affects the community version.	2020-02-14	not yet calculated	<a href="#">CVE-2019-13967</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	Because of a lack of sanitization around error messages, multiple Reflective XSS issues exist in iTop through 2.6.0 via the param_file parameter to webservices/export.php, webservices/cron.php, or env-production/itop-backup/backup.php. By default, any XSS sent to the administrator can be transformed to remote command execution because of CVE-2018-10642 (still working through 2.6.0) The Reflective XSS can also become a stored XSS within the same account because of another vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2019-13965</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	In Combodo iTop 2.2.0 through 2.6.0, if the configuration file is writable, then execution of arbitrary code can be accomplished by calling ajax.dataloader with a maliciously crafted payload. Many conditions can place the configuration file into a writable state: during installation; during upgrade; in certain cases, an error during modification of the file from the web interface leaves the file writable (can be triggered with XSS); a race condition can be triggered by the hub-connector module (community version only from 2.4.1 to 2.6.0); or editing the file in a CLI.	2020-02-14	not yet calculated	<a href="#">CVE-2019-11215</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
cypress -- psoc_4_devices	The Bluetooth Low Energy implementation in Cypress PSoC 4 BLE component 3.61 and earlier processes data channel frames with a payload length larger than the configured link layer maximum RX payload size, which allows attackers (in radio range) to cause a denial of service (crash) via a crafted BLE Link Layer frame.	2020-02-12	not yet calculated	<a href="#">CVE-2019-16336</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-842_rev_c_devices	A stack-based buffer overflow was found on the D-Link DIR-842 REVC with firmware v3.13B09 HOTFIX due to the use of strcpy for LOGINPASSWORD when handling a POST request to the /MTFWU endpoint.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8962</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
digi_international -- connectport_lts_32_mei	Digi International ConnectPort LTS 32 MEI, Firmware Version 1.4.3 (82002228_K 08/09/2018), bios Version 1.2. Successful exploitation of this vulnerability could allow an attacker to upload a malicious file to the application.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6975</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
digi_international -- connectport_lts_32_mei	Digi International ConnectPort LTS 32 MEI, Firmware Version 1.4.3 (82002228_K 08/09/2018), bios Version 1.2. Multiple cross-site scripting vulnerabilities exist that could allow an attacker to cause a denial-of-service condition.	2020-02-13	not yet calculated	<a href="#">CVE-2020-6973</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
dojo -- dojox	dojox is vulnerable to Cross-site Scripting in all versions before version 1.16.1, 1.15.2, 1.14.5, 1.13.6, 1.12.7 and 1.11.9. This is due to dojox xmpp util.xmlEncode	2020-02-13	not yet calculated	<a href="#">CVE-2019-10785</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>



	only encoding the first occurrence of each character, not all of them.			<a href="#">MISC</a>
dovecot -- dovecot	The IMAP and LMTP components in Dovecot 2.3.9 before 2.3.9.3 mishandle snippet generation when many characters must be read to compute the snippet and a trailing > character exists. This causes a denial of service in which the recipient cannot read all of their messages.	2020-02-12	not yet calculated	<a href="#">CVE-2020-7957</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
dovecot -- dovecot	lib-smtp in submission-login and lmtp in Dovecot 2.3.9 before 2.3.9.3 mishandles truncated UTF-8 data in command parameters, as demonstrated by the unauthenticated triggering of a submission-login infinite loop.	2020-02-12	not yet calculated	<a href="#">CVE-2020-7046</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
drupal -- drupal	The RESTful Web Services (restws) module 7.x-1.x before 7.x-1.4 and 7.x-2.x before 7.x-2.1 for Drupal does not properly restrict access to entity write operations, which makes it easier for remote authenticated users with the "access resource node" and "create page content" permissions (or equivalents) to conduct cross-site scripting (XSS) or execute arbitrary PHP code via a crafted text field.	2020-02-11	not yet calculated	<a href="#">CVE-2013-4225</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
easyxdm -- easyxdm	Cross-site Scripting (XSS) in EasyXDM before 2.4.18 allows remote attackers to inject arbitrary web script or HTML via the easyxdm.swf file.	2020-02-14	not yet calculated	<a href="#">CVE-2013-5212</a> <a href="#">MISC</a> <a href="#">XF</a>
etherpad -- etherpad	Directory traversal vulnerability in node/Utils/Minify.js in Etherpad 1.1.2 through 1.5.4 allows remote attackers to read arbitrary files with permissions of the user running the service via a .. (dot dot) in the path parameter of HTTP API requests. NOTE: This vulnerability is due to an incomplete fix to CVE-2015-3297.	2020-02-13	not yet calculated	<a href="#">CVE-2015-3309</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
extrun -- ilbo	ilbo App (ilbo App for Android prior to version 1.1.8 and ilbo App for iOS prior to version 1.2.01) allows an attacker on the same network segment to bypass authentication and to view the images which were recorded by the other ilbo user's device via unspecified vectors.	2020-02-14	not yet calculated	<a href="#">CVE-2020-5532</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.	2020-02-10	not yet calculated	<a href="#">CVE-2020-8840</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of text field objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9400.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8846</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.2947. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the fxhtml2pdf.exe module. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9560.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8855</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of watermarks in AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this	2020-02-14	not yet calculated	<a href="#">CVE-2020-8845</a> <a href="#">MISC</a> <a href="#">MISC</a>

	vulnerability to execute code in the context of the current process. Was ZDI-CAN-9358.			
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7 0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9591.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8853</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7 0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of JPEG files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9606.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8854</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6 0.25608. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of watermarks. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9640.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8856</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.7 0.29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9416.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8852</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of form Annotation objects within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9862.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8857</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this	2020-02-14	not yet calculated	<a href="#">CVE-2020-8847</a> <a href="#">MISC</a> <a href="#">MISC</a>

	vulnerability to execute code in the context of the current process. Was ZDI-CAN-9414.			
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9406.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8851</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9407.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8848</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9415.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8850</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9413.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8849</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.6.0 25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG files within CovertToPDF. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9102.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8844</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
free_reprintables -- articlefr	A Privilege Escalation Vulnerability exists in Free Reprintables ArticleFR 11.06 2014 due to insufficient access restrictions in the data.php script, which could let a remote malicious user obtain access or modify or delete database information.	2020-02-13	not yet calculated	<a href="#">CVE-2014-4170</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
freebsd -- bsd_libc	regcomp in the BSD implementation of libc is vulnerable to denial of service due to stack exhaustion.	2020-02-12	not yet calculated	<a href="#">CVE-2011-3336</a> <a href="#">FULLDISC</a> <a href="#">END</a> <a href="#">MISC</a>

				<a href="#">BUGTRAQ</a>
fujitsu -- multiple_products	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions, Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3, Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.	2020-02-07	not yet calculated	<a href="#">CVE-2019-13163</a> <a href="#">CONFIRM</a>
git -- git	Git before 1 8.5.6, 1.9.x before 1.9.5, 2.0 x before 2.0.5, 2.1 x before 2.1.4, and 2.2 x before 2.2.1 on Windows and OS X; Mercurial before 3.2.3 on Windows and OS X; Apple Xcode before 6.2 beta 3; mine; libgit2; Egit; and JGit allow remote Git servers to execute arbitrary commands via a tree containing a crafted .git/config file with (1) an ignorable Unicode codepoint, (2) a git~1/config representation, or (3) mixed case that is improperly handled on a case-insensitive filesystem.	2020-02-12	not yet calculated	<a href="#">CVE-2014-9390</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab 12.2.2 and below contains a security vulnerability that allows a guest user in a private project to see the merge request ID associated to an issue via the activity timeline.	2020-02-14	not yet calculated	<a href="#">CVE-2019-15592</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab 11.8 and later contains a security vulnerability that allows a user to obtain details of restricted pipelines via the merge request endpoint.	2020-02-14	not yet calculated	<a href="#">CVE-2019-15594</a> <a href="#">MISC</a> <a href="#">MISC</a>
global_payments -- php-sdk	Gateways/Gateway.php in Heartland & Global Payments PHP SDK before 2.0.0 does not enforce SSL certificate validations.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20455</a> <a href="#">MISC</a> <a href="#">MISC</a>
gocloud -- multiple_devices	Gocloud S2A_WL 4.2.7.16471, S2A 4.2.7.17278, S2A 4.3 0.15815, S2A 4.3 0.17193, S3A K2P MTK 4.2.7.16528, S3A 4.3 0.16572, and ISP3000 4.3 0.17190 devices allows remote attackers to execute arbitrary OS commands via shell metacharacters in a ping operation, as demonstrated by the cgi-bin/webui/admin/tools/app_ping/diag_ping/substring.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8949</a> <a href="#">MISC</a>
google -- android	In notifyNetworkTested and related functions of NetworkMonitor.java, there is a possible bypass of private DNS settings. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-9 Android ID: A-122652057	2020-02-13	not yet calculated	<a href="#">CVE-2020-0028</a> <a href="#">MISC</a>
google -- android	In btm_read_remote_ext_features_complete of btm_acl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0 Android-8.1 Android-9 Android-10 Android D: A-141552859	2020-02-13	not yet calculated	<a href="#">CVE-2020-0005</a> <a href="#">MISC</a>
google -- android	It is possible for a malicious application to construct a TYPE_TOAST window manually and make that window clickable. This could lead to a local escalation of privilege with no additional execution privileges needed. User action is needed	2020-02-13	not yet calculated	<a href="#">CVE-2020-0014</a> <a href="#">MISC</a>



	for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-128674520			
google -- android	In binder_thread_release of binder.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android kernelAndroid ID: A-145286050References: Upstream kernel	2020-02-13	not yet calculated	<a href="#">CVE-2020-0030</a> MISC
google -- android	The Bluetooth stack in Android before 2.3.6 allows a physically proximate attacker to obtain contact information via an AT phonebook transfer.	2020-02-12	not yet calculated	<a href="#">CVE-2011-2343</a> CONFIRMED MISC
google -- android	In updatePermissions of PermissionManagerService.java, it may be possible for a malicious app to obtain a custom permission from another app due to a permission bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-10Android D: A-67319274	2020-02-13	not yet calculated	<a href="#">CVE-2019-2200</a> MISC
google -- android	In onCreate of CertInstaller.java, there is a possible way to overlay the Certificate Installation dialog by a malicious application. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-139017101	2020-02-13	not yet calculated	<a href="#">CVE-2020-0015</a> MISC
google -- android	In Parcel::continueWrite of Parcel.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-140419401	2020-02-13	not yet calculated	<a href="#">CVE-2020-0026</a> MISC
google -- android	In multiple places, it was possible for the primary user's dictionary to be visible to and modifiable by secondary users. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-123232892	2020-02-13	not yet calculated	<a href="#">CVE-2020-0017</a> MISC
google -- android	In MotionEvent::appendDescription of InputDispatcher.cpp, there is a possible log information disclosure. This could lead to local disclosure of user input with System execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-139945049	2020-02-13	not yet calculated	<a href="#">CVE-2020-0018</a> MISC
google -- android	In HidRawSensor::batch of HidRawSensor.cpp, there is a possible out of bounds write due to an unexpected switch fallthrough. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-144040966	2020-02-13	not yet calculated	<a href="#">CVE-2020-0027</a> MISC
google -- android	In getAttributeRange of ExifInterface.java, there is a possible failure to redact location information from media files due to an incorrect bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-10Android D: A-143118731	2020-02-13	not yet calculated	<a href="#">CVE-2020-0020</a> MISC
google -- android	In removeUnusedPackagesLPw of PackageManagerService.java, there is a possible permanent denial-of-service due to a missing package dependency test. This could lead to remote denial of service with User execution privileges needed. User interaction is not needed for	2020-02-13	not yet calculated	<a href="#">CVE-2020-0021</a> MISC

	exploitation Product: AndroidVersions: Android-10Android D: A-141413692			
google -- android	In reassemble_and_dispatch of packet_fragmenter.cc, there is possible out of bounds write due to an incorrect bounds calculation. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-143894715	2020-02-13	not yet calculated	<a href="#">CVE-2020-0022</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
google -- android	In setPhonebookAccessPermission of AdapterService.java, there is a possible disclosure of user contacts over bluetooth due to a missing permission check. This could lead to local information disclosure if a malicious app enables contacts over a bluetooth connection, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145130871	2020-02-13	not yet calculated	<a href="#">CVE-2020-0023</a> <a href="#">MISC</a>
hashicorp -- sentinel	HashiCorp Sentinel up to 0.10.1 incorrectly parsed negation in certain policy expressions. Fixed in 0.10.2.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19879</a> <a href="#">MISC</a>
hcl -- appscan_standard_edition	HCL AppScan Standard Edition 9 0.3.13 and earlier uses hard-coded credentials which can be exploited by attackers to get unauthorized access to the system.	2020-02-14	not yet calculated	<a href="#">CVE-2019-4392</a> <a href="#">MISC</a>
hitachi -- command_suite_and_automation_director	A vulnerability in Hitachi Command Suite prior to 8.7.1-00 and Hitachi Automation Director prior to 8.5.0-00 allow authenticated remote users to expose technical information through error messages. Hitachi Command Suite includes Hitachi Device Manager and Hitachi Compute Systems Manager.	2020-02-14	not yet calculated	<a href="#">CVE-2018-21032</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
hitachi -- multiple_products	A vulnerability in Hitachi Command Suite prior to 8 6.2-00, Hitachi Automation Director prior to 8.6.2-00 and Hitachi Infrastructure Analytics Advisor prior to 4.2 0-00 allow authenticated remote users to load an arbitrary Cascading Style Sheets (CSS) token sequence. Hitachi Command Suite includes Hitachi Device Manager, Hitachi Tiered Storage Manager, Hitachi Replication Manager, Hitachi Tuning Manager, Hitachi Global Link Manager and Hitachi Compute Systems Manager.	2020-02-14	not yet calculated	<a href="#">CVE-2018-21033</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
hp -- linuxki	LinuxKI v6.0-1 and earlier is vulnerable to an XSS which is resolved in release 6.0-2.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7208</a> <a href="#">MISC</a>
hp -- linuxki	LinuxKI v6.0-1 and earlier is vulnerable to a remote code execution which is resolved in release 6 0-2.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7209</a> <a href="#">MISC</a>
ibm -- tivoli_monitoring_service	IBM Tivoli Monitoring Service 6.3.0.7.3 through 6.3 0.7.10 could allow an unauthorized user to access and modify operation aspects of the ITM monitoring server possibly leading to an effective denial of service or disabling of the monitoring server. BM X-Force ID: 167647.	2020-02-13	not yet calculated	<a href="#">CVE-2019-4592</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
ibm -- urbandcode_deploy_and_build	IBM UrbanCode Deploy (UCD) 7.0.3 and IBM UrbanCode Build 6.1.5 could allow a local user to obtain sensitive information by unmasking certain secure values in documents. IBM X-Force D: 171248.	2020-02-13	not yet calculated	<a href="#">CVE-2019-4666</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
intel -- converged_security_and_management_engine	Improper Authentication in subsystem in Intel(R) CSME versions 12.0 through 12.0.48 (IOT only: 12 0.56), versions 13.0 through 13.0.20, versions 14.0 through 14.0.10 may allow a privileged user to potentially enable escalation of privilege, denial of service or information disclosure via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2019-14598</a> <a href="#">MISC</a>
intel -- e1000e/82574l_network_processing_state_when_parsing_32_hex_33_hex_or_34_hex_byte_values_at_the_0x47f_offset.	A denial of service vulnerability exists in some motherboard implementations of Intel e1000e/82574L network controller devices through 2013-02-06 where the device can be brought into a non-processing state when parsing 32 hex, 33 hex, or 34 hex byte values at the 0x47f offset. NOTE: A followup statement from Intel suggests that the root cause of this issue was an incorrectly configured	2020-02-13	not yet calculated	<a href="#">CVE-2013-1634</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">SECTRAK</a> <a href="#">XF</a>

	EEPROM image.			
intel -- manycore_platform_sof	Improper permissions in the installer for Intel(R) MPSS before version 3.8.6 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0563</a> MISC
intel -- renesas_electronics_usb	Improper permissions in the installer for the Intel(R) Renesas Electronics(R) USB 3.0 Driver, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0560</a> MISC
intel -- sgx_software_development	Improper initialization in the Intel(R) SGX SDK before v2.6.100.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0561</a> MISC
intel -- raid_web_console_2	Improper permissions in the installer for Intel(R) RWC2, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0562</a> MISC
intel -- raid_web_console_3_for_windows	Improper permissions in the installer for Intel(R) RWC3 for Windows before version 7.010.009.000 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0564</a> MISC
invision_power_services -- invision_power_board	Invision Power Board (PB) through 3.x allows admin account takeover leading to code execution.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3725</a> MISC
istio -- istio	An issue was discovered in Istio 1.3 through 1.3.6. Under certain circumstances, it is possible to bypass a specifically configured Mixer policy. Istio-proxy accepts the x-istio-attributes header at ingress that can be used to affect policy decisions when Mixer policy selectively applies to a source equal to ingress. To exploit this vulnerability, someone has to encode a source.uid in this header. This feature is disabled by default in Istio 1.3 and 1.4.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8843</a> MISC MISC CONF RM
joomla! -- joomla!	Tiny browser in TinyMCE 3.0 editor in Joomla! before 1.5.13 allows file upload and arbitrary PHP code execution.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4906</a> CONF RM EXPLOIT-DB MISC
joomla! -- joomla!	TinyBrowser plugin for Joomla! before 1.5.13 allows arbitrary file upload via upload.php.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4908</a> MISC EXPLOIT-DB MLIST
jsreport -- jsreport	An unintended require and server-side request forgery vulnerabilities in jsreport version 2.5.0 and earlier allow attackers to execute arbitrary code.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8128</a> MISC
jsreport -- script-manager	An unintended require vulnerability in script-manager npm package version 0.8.6 and earlier may allow attackers to execute arbitrary code.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8129</a> MISC
juniper -- junos_os	Multiple vulnerabilities exist in Juniper Junos J-Web error handling that may lead to cross site scripting (XSS) issues or crash the J-Web service (DoS). This affects Juniper Junos OS 12.1X44 before 12.1X44-D45, 12.1X46 before 12.1X46-D30, 12.1X47 before 12.1X47-D20, 12.3 before 12.3R8, 12.3X48 before 12.3X48-D10, 13.1 before 13.1R5, 13.2 before 13.2R6, 13.3 before 13.3R4, 14.1 before 14.1R3, 14.1X53 before 14.1X53-D10, 14.2 before 14.2R1, and 15.1 before 15.1R1.	2020-02-11	not yet calculated	<a href="#">CVE-2014-6447</a> CONF RM MISC
kaseya -- virtual_system_administrator	Directory traversal vulnerability in Kaseya Virtual System Administrator (VSA) 7.0.0.0 before 7.0.0.33, 8.0.0.0 before 8.0.0.23, 9.0.0.0 before 9.0.0.19, and 9.1.0.0 before 9.1.0.9 allows remote authenticated users to write to and execute arbitrary files due to insufficient restrictions in file paths to json.ashx.	2020-02-13	not yet calculated	<a href="#">CVE-2015-6589</a> MISC MISC MISC MISC
kde -- paste_applet	The %{password(...)} macro in pastemacroexpander.cpp in the KDE Paste Applet before 4.10.5 in kdeplasma-addons does not properly generate passwords, which allows context-dependent attackers to bypass	2020-02-11	not yet calculated	<a href="#">CVE-2013-2120</a> MISC MISC MISC MISC

	authentication via a brute-force attack.			MISC
kde -- paste_applet	The KRandom::random function in KDE Paste Applet after 4.10.5 in kdeplasma-addons uses the GNU C Library rand function's linear congruential generator, which makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms by predicting the generator output.	2020-02-11	not yet calculated	<a href="#">CVE-2013-2213</a> MISC MISC MISC
kinetica -- kinetica	The Admin web application in Kinetica 7.0 9.2.20191118151947 does not properly sanitise the input for the function getLogs. This lack of sanitisation could be exploited to allow an authenticated attacker to run remote code on the underlying operating system. The logFile parameter in the getLogs function was used as a variable in a command to read log files; however, due to poor input sanitisation, it was possible to bypass a replacement and break out of the command.	2020-02-11	not yet calculated	<a href="#">CVE-2020-8429</a> MISC MISC
lenovo -- ez_media_&_backup_center	A vulnerability in the web interface of Lenovo EZ Media & Backup Center, ix2 & ix2-dl version 4.1.406.34763 and prior could allow an unauthenticated, remote attacker to redirect a user to an untrusted web page.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19758</a> CONF RM
lenovo -- multiple_devices	Lenovo was notified of a potential denial of service vulnerability, affecting various versions of BIOS for Lenovo Desktop, Desktop - All in One, and ThinkStation, that could cause PCRs to be cleared intermittently after resuming from sleep (S3) on systems with Intel TXT enabled.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6190</a> CONF RM
lenovo -- xclarity_administrator	An internal product security audit of Lenovo XClarity Administrator (LXCA) discovered a Document Object Model (DOM) based cross-site scripting vulnerability in versions prior to 2.6.6 that could allow JavaScript code to be executed in the user's web browser if a specially crafted link is visited. The JavaScript code is executed on the user's system, not executed on LXCA itself.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19757</a> CONF RM
lenovo -- xclarity_administrator	An XML External Entity (XXE) processing vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.6.6 that could allow information disclosure.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6194</a> CONF RM
lenovo -- xclarity_administrator	An information disclosure vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.6.6 that could allow unauthenticated access to some configuration files which may contain usernames, license keys, IP addresses, and encrypted password hashes.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6193</a> CONF RM
lenovo -- xclarity_controller	An authorization bypass exists in Lenovo XClarity Controller (XCC) versions prior to 3.08 CDI340V, 3.01 TEI392O, 1.71 PSI328N where a valid authenticated user with lesser privileges may be granted read-only access to higher-privileged information if 1) "LDAP Authentication Only with Local Authorization" mode is configured and used by XCC, and 2) a lesser privileged user logs into XCC within 1 minute of a higher privileged user logging out. The authorization bypass does not exist when "Local Authentication and Authorization" or "LDAP Authentication and Authorization" modes are configured and used by XCC.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6195</a> CONF RM
lexmark -- multiple_devices	Lexmark printer MS812 and multiple older generation Lexmark devices have a stored XSS vulnerability in the embedded web server. The vulnerability can be exploited to expose session credentials and other information via the users web browser.	2020-02-13	not yet calculated	<a href="#">CVE-2019-18791</a> MISC CONF RM
libuv -- libuv	The uv_rwlock_t fallback implementation for Windows XP and Server 2003 in libuv before 1.7.4 does not properly prevent threads from releasing the locks of other threads, which allows attackers to cause a denial of service (deadlock) or possibly have unspecified other impact by	2020-02-11	not yet calculated	<a href="#">CVE-2014-9748</a> MISC MISC MISC MISC



	leveraging a race condition.			<a href="#">MISC</a>
linux -- linux_kernel	ext4_protect_reserved_inode in fs/ext4/block_validity.c in the Linux kernel through 5.5.3 allows attackers to cause a denial of service (soft lockup) via a crafted journal size.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8992</a> <a href="#">MISC</a>
lvm2 -- lvm2	vg_lookup in daemons/lvmetad/lvmetad-core.c in LVM2 2.02 mismanages memory, leading to an lvmetad memory leak, as demonstrated by running pvs.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8991</a> <a href="#">MISC</a>
magento -- magento	Zend_XmlRpc Class in Magento before 1.7.0.2 contains an information disclosure vulnerability.	2020-02-13	not yet calculated	<a href="#">CVE-2012-6091</a> <a href="#">MLIST</a> <a href="#">BID</a> <a href="#">XF</a>
mailu -- mailu	In Mailu before version 1.7, an authenticated user can exploit a vulnerability in Mailu fetchmail script and gain full access to a Mailu instance. Mailu servers that have open registration or untrusted users are most impacted. The master and 1.7 branches are patched on our git repository. All Docker images published on docker.io/mailu for tags 1.5, 1.6, 1.7 and master are patched. For detailed instructions about patching and securing the server afterwards, see <a href="https://github.com/Mailu/Mailu/issues/1354">https://github.com/Mailu/Mailu/issues/1354</a>	2020-02-13	not yet calculated	<a href="#">CVE-2020-5239</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
mambo -- mambo_cms	Mambo CMS through 4.6.5 has multiple XSS.	2020-02-12	not yet calculated	<a href="#">CVE-2011-2499</a> <a href="#">MLIST</a>
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability was discovered in the Source Integration plugin before 1.6.2 and 2.x before 2.3.1 for MantisBT. The repo_delete.php Delete Repository page allows execution of arbitrary code via a repo name (if CSP settings permit it). This is related to CVE-2018-16362.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8981</a> <a href="#">MISC</a> <a href="#">MISC</a>
matestack-ui-core_gem_for_ruby_on_rails -- matestack-ui-core_gem_for_ruby_on_rails	matestack-ui-core (RubyGem) before 0.7.14 is vulnerable to XSS/Script injection. This vulnerability is patched in version 0.7.14.	2020-02-13	not yet calculated	<a href="#">CVE-2020-5241</a> <a href="#">CONF RM</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Web Settings of Web File Manager in Rumpus FTP 8.2.9.1. Exploitation of this vulnerability can result in manipulation of Server Web settings at RAPR/WebSettingsGeneralSet.html.	2020-02-10	not yet calculated	<a href="#">CVE-2019-19664</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp_server	A CSRF vulnerability exists in the Web File Manager's Create/Delete Accounts functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can Create and Delete accounts via RAPR/TriggerServerFunction.html.	2020-02-10	not yet calculated	<a href="#">CVE-2019-19662</a> <a href="#">MISC</a> <a href="#">MISC</a>
mcafee -- endpoint_security	Improper access control vulnerability in Configuration Tool in McAfee McAfee Endpoint Security (ENS) Prior to 10.6.1 February 2020 Update allows local users to disable security features via unauthorised use of the configuration tool from older versions of ENS.	2020-02-14	not yet calculated	<a href="#">CVE-2020-7251</a> <a href="#">CONF RM</a>
microsoft -- multiple_windows_products	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0728</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0714</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0745, CVE-2020-0792.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0715</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0727</a> <a href="#">MISC</a>
	A remote code execution vulnerability exists when the Windows Imaging Library			

microsoft -- multiple_windows_products	improperly handles memory.To exploit this vulnerability, an attacker would first have to coerce a victim to open a specially crafted file.The security update addresses the vulnerability by correcting how the Windows Imaging Library handles memory., aka 'Windows Imaging Library Remote Code Execution Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0708</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0691</a> MISC
microsoft -- office_online_server	A spoofing vulnerability exists when Office Online Server does not validate origin in cross-origin communications correctly, aka 'Microsoft Office Online Server Spoofing Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0695</a> MISC
microsys -- promotic	Microsys PROMOTIC 8.2.13 contains an ActiveX Control Start Buffer Overflow vulnerability which can lead to denial of service.	2020-02-13	not yet calculated	<a href="#">CVE-2014-1617</a> MISC MISC
mobileiron -- vsp_and_sentry	MobileIron VSP < 5.9.1 and Sentry < 5.0 has an insecure encryption scheme.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7287</a> MISC MISC
mobileiron -- vsp_and_sentry	MobileIron VSP < 5.9.1 and Sentry < 5.0 has a weak password obfuscation algorithm	2020-02-12	not yet calculated	<a href="#">CVE-2013-7286</a> MISC MISC
moxa -- mgate_5105-mb-eip_devices	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Moxa MGate 5105-MB-EIP firmware version 4.1. Authentication is required to exploit this vulnerability. The specific flaw exists within the DestIP parameter within MainPing.asp. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9552.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8858</a> MISC MISC
netgear -- cg3100_devices	A vulnerability exists in Netgear CG3100 devices before 3.9.2421.13.mp3 V0027 via an embed malicious script in an unspecified page, which could let a malicious user obtain sensitive information.	2020-02-13	not yet calculated	<a href="#">CVE-2014-3919</a> MISC
netis -- wf2471_devices	Netis WF2471 v1.2.30142 devices allow an authenticated attacker to execute arbitrary OS commands via shell metacharacters in the /cgi-bin-igdd/sys_log_clean cgi log_3g_type parameter.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8946</a> MISC
nvidia -- graphics_drivers	A Memory Corruption Vulnerability exists in NVIDIA Graphics Drivers 29549 due to an unknown function in the file proc/driver/nvidia/registry.	2020-02-12	not yet calculated	<a href="#">CVE-2012-0951</a> MISC MISC
nxp -- kw41z_devices	The Bluetooth Low Energy implementation on NXP SDK through 2.2.1 for KW41Z devices does not properly restrict the Link Layer payload length, allowing attackers in radio range to cause a buffer overflow via a crafted packet.	2020-02-12	not yet calculated	<a href="#">CVE-2019-17519</a> MISC
openconnect_project - - openconnect_vpn_client	OpenConnect VPN client with GnuTLS before 5.02 contains a heap overflow if MTU is increased on reconnection.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7098</a> CONF RM
openvpn -- access_server	OpenVPN Access Server 2.8.x before 2.8.1 allows LDAP authentication bypass (except when a user is enrolled in two-factor authentication).	2020-02-13	not yet calculated	<a href="#">CVE-2020-8953</a> CONF RM
openx -- openx_ad_server	A Code Execution Vulnerability exists in OpenX Ad Server 2.8.10 due to a backdoor in flowplayer-3.1.1.min.js library, which could let a remote malicious user execute arbitrary PHP code	2020-02-14	not yet calculated	<a href="#">CVE-2013-4211</a> MISC MISC MISC MISC
	A Cross-Site Scripting (XSS) Vulnerability			<a href="#">CVE-2013-</a>

otrs -- itsm_and_faq	exists in OTRS ITSM prior to 3.2.4, 3.1.8, and 3.0.7 and FAQ prior to 2.1.4 and 2.0.8 via changes, workorder items, and FAQ articles, which could let a remote malicious user execute arbitrary code.	2020-02-12	not yet calculated	2637 <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
palo_alto_networks -- expedition_migration_tool	Insufficient Cross-Site Request Forgery (XSRF) protection on Expedition Migration Tool allows remote unauthenticated attackers to hijack the authentication of administrators and to perform actions on the Expedition Migration Tool. This issue affects Expedition Migration Tool 1.1.51 and earlier versions.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1977</a> <a href="#">CONF RM</a>
palo_alto_networks -- globalprotect	A denial-of-service (DoS) vulnerability in Palo Alto Networks GlobalProtect software running on Mac OS allows authenticated local users to cause the Mac OS kernel to hang or crash. This issue affects GlobalProtect 5.0.5 and earlier versions of GlobalProtect 5.0 on Mac OS.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1976</a> <a href="#">CONF RM</a>
palo_alto_networks -- pan-os	Missing XML validation vulnerability in the PAN-OS web interface on Palo Alto Networks PAN-OS software allows authenticated users to inject arbitrary XML that results in privilege escalation. This issue affects PAN-OS 8.1 versions earlier than PAN-OS 8.1.12 and PAN-OS 9.0 versions earlier than PAN-OS 9.0.6. This issue does not affect PAN-OS 7.1, PAN-OS 8.0, or PAN-OS 9.1 or later versions.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1975</a> <a href="#">CONF RM</a>
pcr -- pcre2 -- pcre2_jit_compile	An out-of-bounds read was discovered in PCRE before 10.34 when the pattern JIT compiled and used to match specially crafted subjects in non-UTF mode. Applications that use PCRE to parse untrusted input may be vulnerable to this flaw, which would allow an attacker to crash the application. The flaw occurs in do_extuni_no_utf in pcre2_jit_compile.c.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20454</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
podman -- podman	A flaw was discovered in Podman where it incorrectly allows containers when created to overwrite existing files in volumes, even if they are mounted as read-only. When a user runs a malicious container or a container based on a malicious image with an attached volume that is used for the first time, it is possible to trigger the flaw and overwrite files in the volume. This issue was introduced in version 1.6.0.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1726</a> <a href="#">CONF RM</a>
prestashop -- prestashop	PrestaShop before 1.4.11 allows logout CSRF.	2020-02-14	not yet calculated	<a href="#">CVE-2013-4792</a> <a href="#">MISC</a>
prestashop -- prestashop	PrestaShop before 1.4.11 allows Logistician, translators and other low level profiles/accounts to inject a persistent XSS vector on TinyMCE.	2020-02-14	not yet calculated	<a href="#">CVE-2013-4791</a> <a href="#">MISC</a>
prismview -- prismview_system_and_prismview_player	The HTTP API in Prismview System 9.11.10.17.00 and Prismview Player 11.13.09.1100 allows remote code execution by uploading RebootSystem.Ink and requesting /REBOOTSYSTEM or /RESTARTVNC. (Authentication is required but an XML file containing credentials can be downloaded.)	2020-02-10	not yet calculated	<a href="#">CVE-2019-20451</a> <a href="#">MISC</a>
proglottis -- gpgme	The proglottis Go wrapper before 0.1.1 for the GPGME library has a use-after-free, as demonstrated by use for container image pulls by Docker or CRI-O. This leads to a crash or potential code execution during GPG signature verification.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8945</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
progress -- moveit_transfer	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, multiple SQL Injection vulnerabilities have been found in the REST API that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database via the REST API. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or	2020-02-14	not yet calculated	<a href="#">CVE-2020-8611</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>

	destroy database elements.			
progress -- moveit_transfer	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, a REST API endpoint failed to adequately sanitize malicious input, which could allow an authenticated attacker to execute arbitrary code in a victim's browser, aka XSS.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8612</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
python-mode -- python-mode	A Code Execution vulnerability exists in select.py when using python-mode 2012-12-19.	2020-02-12	not yet calculated	<a href="#">CVE-2013-5106</a> <a href="#">MISC</a>
qemu -- qemu	An out-of-bounds heap buffer access flaw was found in the way the iSCSI Block driver in QEMU versions 2.12.0 before 4.2.1 handled a response coming from an iSCSI server while checking the status of a Logical Address Block (LBA) in an iscsi_co_block_status() routine. A remote user could use this flaw to crash the QEMU process, resulting in a denial of service or potential execution of arbitrary code with privileges of the QEMU process on the host.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1711</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a>
qnas -- viocard-300_devices	QNAP VioCard 300 has hardcoded RSA private keys.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6277</a> <a href="#">MISC</a> <a href="#">MISC</a>
realtek -- ndis_driver_rt64x64.sys	Realtek NDIS driver rt64x64.sys, file version 10.1.505.2015, fails to do any size checking on an input buffer from user space, which the driver assumes has a size greater than zero bytes. To exploit this vulnerability, an attacker must send an RP with a system buffer size of 0.	2020-02-12	not yet calculated	<a href="#">CVE-2019-11867</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openshift_enterprise	The default configuration of broker.conf in Red Hat OpenShift Enterprise 2.x before 2.1 has a password of "mo00" for a Mongo account, which allows remote attackers to hijack the broker by providing this password, related to the openshift.sh script in Openshift Extras before 20130920. NOTE: this may overlap CVE-2013-4253 and CVE-2013-4281.	2020-02-12	not yet calculated	<a href="#">CVE-2014-0234</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
runc -- runc	runc through 1.0.0-rc9 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. (This vulnerability does not affect Docker due to an implementation detail that happens to block the attack.)	2020-02-12	not yet calculated	<a href="#">CVE-2019-19921</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.10 allows SQL Injection via the SOAP API, the EmailUIAjax interface, or the MailMerge module.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8804</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows Directory Traversal to include arbitrary .php files within the webroot via add_to_prospect_list.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8803</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 has Incorrect Access Control via action_saveHTMLField Bean Manipulation.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8802</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows PHAR Deserialization.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8801</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows EmailsControllerActionGetFromFields PHP Object Injection.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung -- s6_edge_smartphone	Multiple buffer overflows in the esa_write function in /dev/seirenin the Exynos Seiren Audio driver, as used in Samsung S6 Edge, allow local users to cause a denial of service (memory corruption) via a large (1) buffer or (2) size parameter.	2020-02-12	not yet calculated	<a href="#">CVE-2015-7890</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap --	Certain settings page(s) in SAP Business Objects Business Intelligence Platform (CMC), version 4.2, generates error	2020-02-	not yet	<a href="#">CVE-2020-6189</a>



business_objects_intelligence_platform	messages that can give enterprise private-network related information which would otherwise be restricted leading to Information Disclosure.	12	calculator	<a href="#">CVE-2020-6183</a> <a href="#">MISC</a>
sap -- enterprise_resource_planning_and_s4hana	VAT Pro-Rata reports in SAP ERP (SAP_APPL versions 600, 602, 603, 604, 605, 606, 616 and SAP_FIN versions 617, 618, 700, 720, 730) and SAP S/4HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user leading to Missing Authorization Check.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6188</a> <a href="#">MISC</a>
sap -- host_agent	SAP Host Agent, version 7.21, allows an unprivileged user to read the shared memory or write to the shared memory by sending request to the main SAPOSCOL process and receive responses that may contain data read with user root privileges e.g. size of any directory, system hardware and OS details, leading to Missing Authorization Check vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6183</a> <a href="#">MISC</a>
sap -- host_agent	SAP Host Agent, version 7.21, allows an attacker to cause a slowdown in processing of username/password-based authentication requests of the SAP Host Agent, leading to Denial of Service.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6186</a> <a href="#">MISC</a>
sap -- landscape_management	SAP Landscape Management, version 3.0, allows an attacker with admin privileges to execute malicious commands with root privileges in SAP Host Agent via SAP Landscape Management.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6192</a> <a href="#">MISC</a>
sap -- landscape_management	SAP Landscape Management, version 3.0, allows an attacker with admin privileges to execute malicious executables with root privileges in SAP Host Agent via SAP Landscape Management due to Missing Input Validation.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6191</a> <a href="#">MISC</a>
sap -- mobile_platform	SAP Mobile Platform, version 3.0, does not sufficiently validate an XML document accepted from an untrusted source which could lead to partial denial of service. Since SAP Mobile Platform does not allow External-Entity resolving, there is no issue of leaking content of files on the server.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6177</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver (Guided Procedures), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently validate an XML document input from a compromised admin, leading to Denial of Service.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6187</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver (Knowledge Management ICE Service), versions 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to execute malicious scripts leading to Reflected Cross-Site Scripting (XSS) vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6193</a> <a href="#">MISC</a>
sap -- netweaver_and_abap_platform	Under some circumstances the SAML SSO implementation in the SAP NetWeaver (SAP_BASIS versions 702, 730, 731, 740 and SAP ABAP Platform (SAP_BASIS versions 750, 751, 752, 753, 754), allows an attacker to include invalidated data in the HTTP response header sent to a Web user, leading to HTTP Response Splitting vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6181</a> <a href="#">MISC</a>
sap -- netweaver_and_s4hana	Under certain conditions, ABAP Online Community in SAP NetWeaver (SAP_BASIS version 7.40) and SAP S/4HANA (SAP_BASIS versions 7.50, 7.51, 7.52, 7.53, 7.54), does not sufficiently encode user-controlled inputs, resulting in Reflected Cross-Site Scripting (XSS) vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6184</a> <a href="#">MISC</a>
sap -- netweaver_and_s4hana	Under certain conditions ABAP Online Community in SAP NetWeaver (SAP_BASIS version 7.40) and SAP S/4HANA (SAP_BASIS versions 7.50, 7.51, 7.52, 7.53, 7.54), allows an authenticated attacker to store a malicious payload which results in Stored Cross Site Scripting vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6185</a> <a href="#">MISC</a>
sap -- netweaver_as_java	Certain vulnerable endpoints in SAP NetWeaver AS Java (Heap Dump Application), versions 7.30, 7.31, 7.40, 7.50, provide valuable information about	2020-02-	not yet	<a href="#">CVE-2020-6190</a>

	the system like hostname, server node and installation path that could be misused by an attacker leading to Information Disclosure.	12	calculator	<a href="#">MISC</a> <a href="#">MISC</a>
shaman -- shaman	Shaman 1.0 9: Users can add the line askforpwd=false to his shaman.conf file, without entering the root password in shaman. The next time shaman is run, root privileges are granted despite the fact that the user never entered the root password.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4338</a> <a href="#">MISC</a> <a href="#">MISC</a>
siemens -- multiple_devices	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All Versions < V4.5), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All Versions < V4.6), PROFINET Driver for Controller (All Versions < V2.1), RUGGEDCOM RM1224 (All versions < V4 3), SCALANCE M-800 / S615 (All versions < V4.3), SCALANCE W700 IEEE 802.11n (All versions <= V6 0.1), SCALANCE X-200 switch family (incl. SIPLUS NET variants) (All versions), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All Versions < V5 3), SCALANCE X-300 switch family (incl. X408 and S PLUS NET variants) (All versions), SCALANCE XB-200, XC-200, XP-200, XF-200BA and XR-300WG (All Versions < V3.0), SCALANCE XM-400 switch family (All Versions < V6.0), SCALANCE XR-500 switch family (All Versions < V6.0), SIMATIC CP 1616 and CP 1604 (All Versions < V2.8), S MATIC CP 343-1 (incl. SIPLUS NET variants) (All versions), SIMATIC CP 343-1 Advanced (incl. SIPLUS NET variants) (All versions), SIMATIC CP 343-1 ERPC (All versions), SIMATIC CP 343-1 LEAN (incl. SIPLUS NET variants) (All versions), SIMATIC CP 443-1 (incl. SIPLUS NET variants) (All versions), SIMATIC CP 443-1 Advanced (incl. S PLUS NET variants) (All versions), S MATIC CP 443-1 OPC UA (All versions), SIMATIC ET200AL M 157-1 PN (All versions), SIMATIC ET200M IM153-4 PN IO HF (incl. SIPLUS variants) (All versions), SIMATIC ET200M IM153-4 PN IO ST (incl. SIPLUS variants) (All versions), S MATIC ET200MP IM155-5 PN HF (incl. S PLUS variants) (All Versions < V4.2.0), SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants) (All Versions < V4.1.0), SIMATIC ET200S (incl. SIPLUS variants) (All versions), SIMATIC ET200SP IM155-6 PN Basic (incl. SIPLUS variants) (All versions), SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants) (All Versions < V3.3.1), SIMATIC ET200SP IM155-6 PN ST (incl. SIPLUS variants) (All Versions < V4.1 0), SIMATIC ET200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0) (All versions), S MATIC ET200pro, IM 154-3 PN HF (All versions), SIMATIC ET200pro, IM 154-4 PN HF (All versions), SIMATIC IPC Support, Package for VxWorks (All versions), SIMATIC MV400 family (All versions), S MATIC PN/PN Coupler 6ES7158-3AD01-0XA0 (incl. SIPLUS NET variant) (All Versions), SIMATIC RF180C (All versions), SIMATIC RF182C (All versions), SIMATIC RF600 family (All versions < V3), SINAMICS DCP (All Versions < V1 3). Profinet-IO (PNIO) stack versions prior V06.00 do not properly limit internal resource allocation when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface. This could lead to a denial of service condition due to lack of memory for devices that include a vulnerable version of the stack. The security vulnerability could be exploited by an attacker with network access to an affected device. Successful	2020-02-11	not yet calculated	<a href="#">CVE-2019-13946</a> <a href="#">MISC</a>

	exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device.			
simple_machines -- simple_machines_forum	Simple Machines Forum (SMF) through 2.0.5 has XSS	2020-02-12	not yet calculated	<a href="#">CVE-2013-4395</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplisafe -- ss3_devices	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to modify the Wi-Fi network the base station connects to.	2020-02-13	not yet calculated	<a href="#">CVE-2019-3998</a> <a href="#">MISC</a>
skril -- skril	Commerce Skril (Formerly Moneybookers) has an Access bypass vulnerability in all versions prior to 7.x-1.2	2020-02-12	not yet calculated	<a href="#">CVE-2013-1924</a> <a href="#">MISC</a> <a href="#">MISC</a>
sprite_software -- spritebud_and_backup	A Privilege Escalation Vulnerability exists in Sprite Software Spritebud 1.3.24 and 1.3.28 and Backup 2.5.4105 and 2.5.4108 on LG Android smartphones due to a race condition in the spritebud daemon, which could let a local malicious user obtain root privileges.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3685</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sqlite -- android_sqlite	Android SQLite Journal before 4.0.1 has an information disclosure vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2011-3901</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
squirrelmail -- squirrelmail	Squirrelmail 4.0 uses the outdated MD5 hash algorithm for passwords.	2020-02-13	not yet calculated	<a href="#">CVE-2012-5623</a> <a href="#">MISC</a>
stem_innovation -- izon_ip_camera	IZON P 2 0.2: hard-coded password vulnerability	2020-02-12	not yet calculated	<a href="#">CVE-2013-6236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
stmicroelectronics -- stm32wb5x_series_devices	The Bluetooth Low Energy implementation on STMicroelectronics BLE Stack through 1.3.1 for STM32WB5x devices does not properly handle consecutive Attribute Protocol (ATT) requests on reception, allowing attackers in radio range to cause an event deadlock or crash via crafted packets.	2020-02-12	not yet calculated	<a href="#">CVE-2019-19192</a> <a href="#">MISC</a>
synergy_systems_&_solutions -- husky_rtu_devices	The Synergy Systems & Solutions PLC & RTU system has a vulnerability in HUSKY RTU 6049-E70 firmware versions 5.0 and prior. Specially crafted malicious packets could cause disconnection of active authentic connections or reboot of device. This is a different issue than CVE-2019-16879 and CVE-2019-20046.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20045</a> <a href="#">MISC</a>
synergy_systems_&_solutions -- husky_rtu_devices	The Synergy Systems & Solutions PLC & RTU system has a vulnerability in HUSKY RTU 6049-E70 firmware versions 5.0 and prior. The affected product does not require adequate authentication, which may allow an attacker to read sensitive information or execute arbitrary code. This is a different issue than CVE-2019-16879 and CVE-2019-20045.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20046</a> <a href="#">MISC</a>
telink -- tslr8x5_and_tslr823x_and_tslr826x_devices	The Bluetooth Low Energy Secure Manager Protocol (SMP) implementation on Telink Semiconductor BLE SDK versions before November 2019 for TSLR8x5x through 3.4.0, TSLR823x through 1.3.0, and TSLR826x through 3.3 devices accepts a pairing request with a key size greater than 16 bytes, allowing an attacker in radio range to cause a buffer overflow and denial of service (crash) via crafted packets.	2020-02-12	not yet calculated	<a href="#">CVE-2019-19196</a> <a href="#">MISC</a> <a href="#">MISC</a>
telink -- tslr8x5_and_tslr823x_and_tslr826x_devices	The Bluetooth Low Energy Secure Manager Protocol (SMP) implementation on Telink Semiconductor BLE SDK versions before November 2019 for TSLR8x5x through 3.4.0, TSLR823x through 1.3.0, and TSLR826x through 3.3 devices installs a zero long term key (LTK) if an out-of-order link-layer encryption request is received during Secure Connections pairing. An attacker in radio range can have arbitrary read/write access to protected GATT service data, cause a device crash, or possibly control a device's function by	2020-02-12	not yet calculated	<a href="#">CVE-2019-19194</a> <a href="#">MISC</a> <a href="#">MISC</a>

	establishing an encrypted session with the zero LTK.			
telligent_systems -- telligent_community	XSS in Telligent Community 5.6 583.20496 via a flash file and related to the allowScriptAccess parameter.	2020-02-13	not yet calculated	<a href="#">CVE-2012-1903</a> MISC
tiki_wiki -- cms_groupware	A Cross-Site Scripting (XSS) vulnerability exists in Tiki Wiki CMG Groupware 11.0 via the id paraZeroClipboard swf, which could let a remote malicious user execute arbitrary code.	2020-02-12	not yet calculated	<a href="#">CVE-2013-6022</a> MISC
timetools -- multiple_deivces	TimeTools SC7105 1 0.007, SC9205 1.0 007, SC9705 1.0.007, SR7110 1.0 007, SR9210 1.0.007, SR9750 1.0 007, SR9850 1.0.007, T100 1.0.003, T300 1.0 003, and T550 1.0.003 devices allow remote attackers to bypass authentication by placing t3axs=TiMEtOOlsj7G3xMm52wB in a t3.cgi request, aka a "hardcoded cookie."	2020-02-13	not yet calculated	<a href="#">CVE-2020-8964</a> MISC
timetools -- multiple_deivces	TimeTools SC7105 1 0.007, SC9205 1.0 007, SC9705 1.0.007, SR7110 1.0 007, SR9210 1.0.007, SR9750 1.0 007, SR9850 1.0.007, T100 1.0.003, T300 1.0 003, and T550 1.0.003 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the t3.cgi srmodel or srtime parameter.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8963</a> MISC
trendnet -- ts- s402_devices	TRENDnet TS-S402 has a backdoor to enable TELNET.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6360</a> MISC
tri-plc -- internet_trilogi_server	Internet TRILOGI Server (unknown versions) could allow a local user to bypass security and create a local user account.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6927</a> MISC
umplayer -- umplayer	A Code Execution Vulnerability exists in UMPlayer 0 98 in wintab32 dll due to insufficient path restrictions when loading external libraries. which could let a malicious user execute arbitrary code.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3494</a> MISC
varnish_software -- varnish_http_cache	Varnish HTTP cache before 3.0.4: ACL bug	2020-02-12	not yet calculated	<a href="#">CVE-2013-4090</a> MISC
visual_it -- tube_map_live_underground	Tube Map Live Underground for Android before 0.2.2 has an Information Disclosure Vulnerability	2020-02-12	not yet calculated	<a href="#">CVE-2013-6681</a> MISC
voatz -- voatz_for_android	The Voatz application 2020-01-01 for Android allows only 100 million different PINs, which makes it easier for attackers (after using root access to make a copy of the local database) to discover login credentials and voting history via an offline brute-force approach.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8988</a> MISC
voatz -- voatz_for_android	In the Voatz application 2020-01-01 for Android, the amount of data transmitted during a single voter's vote depends on the different lengths of the metadata across the available voting choices, which makes it easier for remote attackers to discover this voter's choice by sniffing the network. For example, a small amount of sniffed data may indicate that a vote was cast for the candidate with the least metadata. An active man-in-the-middle attacker can leverage this behavior to disrupt voters' abilities to vote for a candidate opposed by the attacker.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8989</a> MISC
weechat - weechat	irc_mode_channel_update in plugins/irc-mode.c in WeeChat through 2.7 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a malformed IRC message 324 (channel mode).	2020-02-12	not yet calculated	<a href="#">CVE-2020-8955</a> MISC
wordpress -- wordpress	participants-database.php in the Participants Database plugin 1 9.5.5 and previous versions for WordPress has a time-based SQL injection vulnerability via the ascdesc, list_filter_count, or sortBy parameters. It is possible to exfiltrate data and potentially execute code (if certain conditions are met).	2020-02-11	not yet calculated	<a href="#">CVE-2020-8596</a> MISC
wordpress --	The Ninja Forms plugin 3.4.22 for WordPress has Multiple Stored XSS vulnerabilities via	2020-02-	not yet	<a href="#">CVE-2020-8594</a>



wordpress	ninja_forms[recaptcha_site_key], ninja_forms[recaptcha_secret_key], ninja_forms[recaptcha_lang], or ninja_forms[date_format].	14	calculator	<a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	Multiple SQL injection vulnerabilities in CWPPoll.js in WordPress Poll Plugin 34.5 for WordPress allow attackers to execute arbitrary SQL commands via the pollid or poll_id parameter in a viewPollResults or userlogs action.	2020-02-13	not yet calculator	<a href="#">CVE-2013-1400</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">BUGTRAQ</a>
wordpress -- wordpress	Multiple security bypass vulnerabilities in the editAnswer, deleteAnswer, addAnswer, and deletePoll functions in WordPress Poll Plugin 34.5 for WordPress allow a remote attacker to add, edit, and delete an answer and delete a poll.	2020-02-13	not yet calculator	<a href="#">CVE-2013-1401</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">BUGTRAQ</a>
wordpress -- wordpress	WordPress WP Cleanfix Plugin 2.4.4 has CSRF	2020-02-10	not yet calculator	<a href="#">CVE-2013-2108</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress plugin wp-cleanfix has Remote Code Execution	2020-02-10	not yet calculator	<a href="#">CVE-2013-2109</a> <a href="#">MISC</a> <a href="#">MISC</a>
xerox -- colorcube_and_workcenter	Xerox ColorCube and WorkCenter devices in 2013 had hardcoded FTP and shell user accounts.	2020-02-13	not yet calculator	<a href="#">CVE-2013-6362</a> <a href="#">MISC</a> <a href="#">MISC</a>
xilisoft -- video_converter_ultimate	Xilisoft Video Converter Ultimate 7.8.1 build-20140505 has a DLL Hijacking vulnerability	2020-02-12	not yet calculator	<a href="#">CVE-2014-3860</a> <a href="#">MISC</a>
zenoss -- zenoss_core	Multiple format string vulnerabilities in the python module in RRDtool, as used in Zenoss Core before 4.2.5 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted third argument to the rrdtool.graph function, aka ZEN-15415, a related issue to CVE-2013-2131.	2020-02-12	not yet calculator	<a href="#">CVE-2014-6262</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zimbra -- zimbra_collaboration	Zimbra 2013 has XSS in aspell php	2020-02-12	not yet calculator	<a href="#">CVE-2013-1938</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zpanel_project -- zpanel	ZPanel through 10.1.0 has Remote Command Execution	2020-02-12	not yet calculator	<a href="#">CVE-2013-2097</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



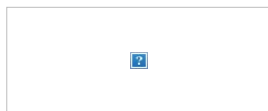
#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20508 · (888) 282-0870



**From:** US-CERT  
**To:** [wsu@artec.com](mailto:wsu@artec.com)  
**Subject:** Vulnerability Summary for the Week of February 10, 2020  
**Date:** Monday, February 17, 2020 4:33:48 PM



National Cyber Awareness System:

## Vulnerability Summary for the Week of February 10, 2020

02/17/2020 07:09 AM EST

Original release date: February 17, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	10	<a href="#">CVE-2020-3740</a> CONF RM
ajaxplorer -- ajaxplorer	Ajaxplorer before 5.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) archive_name parameter to the Power FS module (plugins/action.powerfs/class PowerFSController.php), a (2) file name to the getTrustSizeOnFileSystem function in the File System (Standard) module (plugins/access.fs/class.fsAccessWrapper.php), or the (3) revision parameter to the Subversion Repository module (plugins/meta.svn/class.SvnManager.php).	2020-02-11	10	<a href="#">CVE-2013-4267</a> MISC MISC MISC
artica -- pandora_fms	functions_netflow.php in Artica Pandora FMS 7.0 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the index.php?operation/netflow/nf_live_view ip_dst, dst_port, or src_port parameter, a different vulnerability than CVE-2019-20224.	2020-02-12	9	<a href="#">CVE-2020-8947</a> MISC MISC MISC
atutor -- atutor	confirm.php in ATutor 2.2 and earlier allows remote attackers to bypass authentication and gain access as an existing user via the auto_login parameter.	2020-02-11	7.5	<a href="#">CVE-2014-9753</a> MISC MISC MISC MISC
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	10	<a href="#">CVE-2013-3091</a> MISC MISC MISC
biscom -- secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6 0.1xxx before 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	7.5	<a href="#">CVE-2020-8796</a> MISC <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/175922">https://exchange.xforce.ibmcloud.com/vulnerabilities/175922</a>
bosch -- bvms_mobile_video_service	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0 0.827, 8.0 <= 8.0 0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	10	<a href="#">CVE-2020-6770</a> CONF RM
canonical -- lxc	In LXC 2.0, many template scripts download code over cleartext HTTP, and omit a digital-signature check, before running it to bootstrap containers.	2020-02-10	9.3	<a href="#">CVE-2017-18641</a> MISC
corsair -- corsair_icue	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to read and write to arbitrary physical memory locations, and consequently gain NT	2020-02-07	7.2	<a href="#">CVE-2020-8808</a> MISC MISC

	AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.			
d-link -- multiple_products	Multiple SQL injection vulnerabilities in D-Link DSR-150 with firmware before 1.08B44; DSR-150N with firmware before 1.05B64; DSR-250 and DSR-250N with firmware before 1.08B44; and DSR-500, DSR-500N, DSR-1000, and DSR-1000N with firmware before 1.08B77 allow remote attackers to execute arbitrary SQL commands via the password to (1) the login.authenticate function in share/luas/5.1/teamf1lua/lib/login.lua or (2) captivePortal.lua.	2020-02-11	10	<a href="#">CVE-2013-5945</a> MISC MISC MISC MISC MISC
dell -- multiple_products	An Authentication Bypass Vulnerability exists in DELL SonicWALL Analyzer 7.0, Global Management System (GMS) 4.1, 5.0, 5.1, 6.0, and 7.0; Universal Management Appliance (UMA) 5.1, 6.0, and 7.0 and ViewPoint 4.1, 5.0, 5.1, and 6.0 via the skipSessionCheck parameter to the UMA interface (/appliance/), which could let a remote malicious user obtain access to the root account.	2020-02-11	10	<a href="#">CVE-2013-1359</a> MISC MISC MISC MISC MISC MISC MISC
dell -- multiple_products	An Authentication Bypass vulnerability exists in DELL SonicWALL Global Management System (GMS) 4.1, 5.0, 5.1, 6.0, and 7.0, Analyzer 7.0, Universal Management Appliance (UMA) 5.1, 6.0, and 7.0 and ViewPoint 4.1, 5.0, and 6.0 via a crafted request to the SGMS interface, which could let a remote malicious user obtain administrative access.	2020-02-11	10	<a href="#">CVE-2013-1360</a> MISC MISC MISC MISC MISC MISC
echoping_project -- echoping	echoping through 6.0.2 has buffer overflow vulnerabilities	2020-02-11	10	<a href="#">CVE-2013-4448</a> MISC MISC MISC
enorth -- enorth_webpublisher_cms	SQL injection vulnerability in pub/m_pending_news/delete_pending_news.jsp in Enorth Webpublisher CMS allows remote attackers to execute arbitrary SQL commands via the cbNewsId parameter.	2020-02-12	7.5	<a href="#">CVE-2015-5617</a> MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	9.3	<a href="#">CVE-2020-8655</a> MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php.	2020-02-07	7.5	<a href="#">CVE-2020-8656</a> MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	9	<a href="#">CVE-2020-8654</a> MISC MISC
golang -- go	The net/http library in net/http/transfer.go in Go before 1.4.3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains Content-Length and Transfer-Encoding header fields.	2020-02-08	7.5	<a href="#">CVE-2015-5741</a> MISC MISC MISC MISC MISC MISC MISC
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	9	<a href="#">CVE-2014-7224</a> MISC MISC MISC MISC
google -- chrome	Use after free in audio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	9.3	<a href="#">CVE-2020-6406</a> SUSE MISC MISC
	scripts/email coffee in the Hubot Scripts			<a href="#">CVE-2013-7378</a>

hubot_scripts -- hubot_scripts	module before 2.4.4 for Node.js allows remote attackers to execute arbitrary commands.	2020-02-12	7.5	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- sterling_authentication	A Command Execution Vulnerability exists in IBM Sterling External Authentication Server 2.2.0, 2.3.01, 2.4.0, and 2.4.1 via an unspecified OS command, which could let a local malicious user execute arbitrary code.	2020-02-11	7.2	<a href="#">CVE-2013-0517</a> <a href="#">MISC</a> <a href="#">MISC</a>
libnotify -- libnotify	libnotify before 1.0.4 for Node.js allows remote attackers to execute arbitrary commands via unspecified characters in a call to libnotify.notify.	2020-02-12	7.5	<a href="#">CVE-2013-7381</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
linux -- linux_kernel	Buffer overflow in the auerswald_probe function in the Auerswald Linux USB driver for the Linux kernel before 2.6.27 allows physically proximate attackers to execute arbitrary code, cause a denial of service via a crafted USB device, or take full control of the system.	2020-02-11	7.2	<a href="#">CVE-2009-4067</a> <a href="#">MISC</a> <a href="#">MISC</a>
Istio -- Istio	Istio 1.3 through 1.4.3 allows authentication bypass. The Authentication Policy exact-path matching logic can allow unauthorized access to HTTP paths even if they are configured to be only accessed after presenting a valid JWT token. For example, an attacker can add a ? or # character to a URI that would otherwise satisfy an exact-path match.	2020-02-12	7.5	<a href="#">CVE-2020-8595</a> <a href="#">REDHAT</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
mediawiki -- mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	9.3	<a href="#">CVE-2012-4381</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_internet_explorer_products	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0674</a> <a href="#">MISC</a>
microsoft -- multiple_internet_explorer_products	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0673</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0711</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713.	2020-02-11	7.6	<a href="#">CVE-2020-0767</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0712</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory	2020-02-	7.6	<a href="#">CVE-2020-0710</a>



	Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	11		MISC
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0713</a> MISC
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	2020-02-11	9.3	<a href="#">CVE-2020-0759</a> MISC
microsoft -- multiple_microsoft_exchange_server_products	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.	2020-02-11	9	<a href="#">CVE-2020-0688</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0720</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE D is unique from CVE-2020-0683.	2020-02-11	7.2	<a href="#">CVE-2020-0686</a> MISC
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE D is unique from CVE-2020-0734.	2020-02-11	7.6	<a href="#">CVE-2020-0681</a> MISC
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in Remote Desktop Services "rdp" formerly known as Terminal Services "ts" when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.	2020-02-11	8.5	<a href="#">CVE-2020-0655</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows improperly handles Secure Socket Shell remote commands, aka 'Windows SSH Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0757</a> MISC
microsoft -- multiple_windows_products	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'.	2020-02-11	9.3	<a href="#">CVE-2020-0738</a> MISC
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.	2020-02-11	9	<a href="#">CVE-2020-0662</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows Error Reporting Manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0678</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726.	2020-02-11	7.2	<a href="#">CVE-2020-0731</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-	2020-02-11	7.2	<a href="#">CVE-2020-0725</a>

	0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731.			<a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0671, CVE-2020-0672.	2020-02-11	7.2	<a href="#">CVE-2020-0670</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0726</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792.	2020-02-11	7.2	<a href="#">CVE-2020-0745</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681.	2020-02-11	9.3	<a href="#">CVE-2020-0734</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0723</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0719</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680.	2020-02-11	7.2	<a href="#">CVE-2020-0682</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0671.	2020-02-11	7.2	<a href="#">CVE-2020-0672</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686.	2020-02-11	7.2	<a href="#">CVE-2020-0683</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Wireless Network Manager improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Wireless Network Manager Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0704</a> <a href="#">MISC</a>
	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation			

microsoft -- multiple_windows_products	of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0722</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0707</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0685</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0721</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0703</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0672.	2020-02-11	7.2	<a href="#">CVE-2020-0671</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0724</a> MISC
microsoft -- office365_proplus_for_32-bit_and_64-bit_systems	An elevation of privilege vulnerability exists in Microsoft Office OLicenseHeartbeat task, where an attacker who successfully exploited this vulnerability could run this task as SYSTEM. To exploit the vulnerability, an authenticated attacker would need to place a specially crafted file in a specific location, thereby allowing arbitrary file corruption. The security update addresses the vulnerability by correcting how the process validates the log file., aka 'Microsoft Office Tampering Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0697</a> MISC
microsoft -- windows_10_and_windows_server	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0745.	2020-02-11	7.2	<a href="#">CVE-2020-0792</a> MISC
microsoft -- windows_10_and_windows_server	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0732.	2020-02-11	7.2	<a href="#">CVE-2020-0709</a> MISC
microsoft -- windows_10_and_windows_server	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0709.	2020-02-11	7.2	<a href="#">CVE-2020-0732</a> MISC
	An issue was discovered in Microvirt MEmu all versions prior to 7.0.2. A guest Android operating system inside the MEmu emulator contains a /system/bin/systemd binary that is run			

microvirt -- memu	with root privileges on startup (this is unrelated to Red Hat's systemd init program, and is a closed-source proprietary tool that seems to be developed by Microvirt). This program opens TCP port 21509, presumably to receive installation-related commands from the host OS. Because everything after the installer.uninstall command is concatenated directly into a system() call, it is possible to execute arbitrary commands by supplying shell metacharacters.	2020-02-11	10	<a href="#">CVE-2019-14514</a> MISC
netgear -- ac1200_smart_wifi_router	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR AC1200 R6220 Firmware version 1.1 0.86 Smart WiFi Router. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of path strings. By inserting a null byte into the path, the user can skip most authentication checks. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-8616.	2020-02-10	7.5	<a href="#">CVE-2019-17137</a> MISC
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1.2.31805 and V2.2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracert diagnostic tool because of lack of user input sanitizing.	2020-02-07	8.5	<a href="#">CVE-2019-19356</a> MISC MISC
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	7.5	<a href="#">CVE-2019-15605</a> MISC FEDORA CONF RM CONF RM CONF RM
node.js -- nodejs	Including trailing white space in HTTP header values in Node.js 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	7.5	<a href="#">CVE-2019-15606</a> MISC CONF RM CONF RM CONF RM
nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	7.5	<a href="#">CVE-2014-9530</a> CONF RM
omniauth-weibo-oauth2_gem_for_ruby - omniauth-weibo-oauth2_gem_for_ruby	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	7.5	<a href="#">CVE-2019-17268</a> MISC CONF RM
openpne -- opopensocialplugin	opOpenSocialPlugin 0.8.2.1, > 0.9.2, 0.9.13, 1.2.6: Multiple XML External Entity Injection Vulnerabilities	2020-02-07	7.5	<a href="#">CVE-2013-4335</a> MISC MISC MISC
openpne -- opwebapiplugin	opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	7.5	<a href="#">CVE-2013-4334</a> MISC MISC
phxeventmanager -- phxeventmanager	SQL injection vulnerability in search.php in phxEventManager 2.0 beta 5 allows remote attackers to execute arbitrary SQL commands via the search_terms parameter.	2020-02-11	7.5	<a href="#">CVE-2012-1124</a> MISC MISC MISC MISC
polarbear -- polarbear_cms	A PHP File Upload Vulnerability exists in PolarBear CMS 2.5 via upload.php, which could let a malicious user execute arbitrary code.	2020-02-11	7.5	<a href="#">CVE-2013-0803</a> MISC MISC MISC
polycomm -- web_management_interface_g3/hdx_8000_hd	An issue was discovered in Polycom Web Management Interface G3/HDX 8000 HD with Durango 2.6.0 4740 software and embedded Polycom Linux Development Platform 2.14.g3. It has a blank administrative password by default, and can be successfully used without setting	2020-02-10	10	<a href="#">CVE-2012-6611</a> MISC MISC



	this password.			
qemu -- qemu	The virtqueue_map_sg function in hw/virtio/virtio.c in QEMU before 1.7.2 allows remote attackers to execute arbitrary files via a crafted savevm image, related to virtio-block or virtio-serial read.	2020-02-11	7.2	<a href="#">CVE-2013-4535</a> MISC MISC MISC MISC MISC
qualcomm -- multiple_snapdragon_products	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open close in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	7.2	<a href="#">CVE-2019-14044</a> CONF RM
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14002</a> CONF RM
qualcomm -- multiple_snapdragon_products	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14088</a> CONF RM MISC
qualcomm -- multiple_snapdragon_products	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	7.2	<a href="#">CVE-2019-14046</a> CONF RM
qualcomm -- multiple_snapdragon_products	Stage-2 fault will occur while writing to an ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14049</a> CONF RM
qualcomm -- multiple_snapdragon_products	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14055</a> CONF RM
	Uninitialized stack data gets used if memory is not allocated for blob or if the			

qualcomm -- multiple_snapdragon_p	allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14060</a> CONF RM
qualcomm -- multiple_snapdragon_p	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> CONF RM
qualcomm -- multiple_snapdragon_p	Out of bound access while parsing dtb atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> CONF RM
qualcomm -- multiple_snapdragon_p	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14057</a> CONF RM

qualcomm -- multiple_snapdragon_products	Out of bound access due to Invalid inputs to dpm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon IoT & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Renell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14063</a> CONFIRM
qualcomm -- snapdragon_industrial_products	Subsequent additions performed during Module loading while allocating the memory would lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	7.2	<a href="#">CVE-2019-14051</a> CONFIRM
ruby_pdfkit_gem_for_ruby_on_rails - ruby_pdfkit_gem_for_ruby_on_rails	Ruby PDFKit gem prior to 0.5.3 has a Code Execution Vulnerability	2020-02-11	7.5	<a href="#">CVE-2013-1607</a> MISC MISC
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, contains a vulnerability of Pre-auth SQL Injection, allowing attackers to inject a specific SQL command.	2020-02-11	7.5	<a href="#">CVE-2020-3934</a> MISC MISC MISC
siemens -- multiple_scalance_products	A vulnerability has been identified in SCALANCE S602 (All versions >= V3.0), SCALANCE S612 (All versions >= V3.0), SCALANCE S623 (All versions >= V3.0), SCALANCE S627-2M (All versions >= V3.0). Specially crafted packets sent to port 443/tcp of affected devices could cause a Denial-of-Service condition of the web server. A cold reboot is required to restore the functionality of the device.	2020-02-11	7.8	<a href="#">CVE-2019-13926</a> MISC
simplejobscript -- simplejobscript	An issue was discovered in Simplejobscript.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	7.5	<a href="#">CVE-2020-8645</a> MISC
sphider -- sphider_pro_and_sphider_plus	A Command Execution vulnerability exists in Sphider Pro, and Sphider Plus 3.2 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5086 pertains to instances of fwrite in Sphider Pro and Sphider Plus only, but don't exist in Sphider.	2020-02-10	7.5	<a href="#">CVE-2014-5086</a> MISC
sphider -- sphider_search_engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 due to exec calls in admin/spiderfuncs.php, which could let a remote malicious user execute arbitrary code.	2020-02-07	7.5	<a href="#">CVE-2014-5087</a> MISC MISC
status2k -- server_monitoring_software	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	10	<a href="#">CVE-2014-5091</a> MISC MISC MISC MISC
ui -- edgswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	7.2	<a href="#">CVE-2020-8126</a> MISC
wordpress -- wordpress	WordPress W3 Total Cache Plugin 0.9.2.8 has a Remote PHP Code Execution Vulnerability	2020-02-12	7.5	<a href="#">CVE-2013-2010</a> MISC MISC MISC MISC
wordpress -- wordpress	NextGEN Gallery plugin before 1.9.13 for WordPress: ngggallery.php file upload	2020-02-11	10	<a href="#">CVE-2013-3684</a> MISC MISC
wordpress -- wordpress	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for WordPress and before 2.0.1 for Joomla!, allows remote attackers to execute	2020-02-08	7.5	<a href="#">CVE-2014-8739</a> MISC MISC MISC MISC MISC

	arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.			MISC MISC MISC
yabb -- yabb	YaBB through 2.5.2: 'guestlanguage' Cookie Parameter Local File Include Vulnerability	2020-02-11	7.5	CVE-2013-2057 MISC MISC MISC
zend_framework -- zend_framework	Zend Framework, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	2020-02-11	7.5	CVE-2014-2052 MISC CONF RM MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3733 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3731 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3721 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3739 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3738 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3728 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3736 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3735 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3734 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3732 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3737 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3730 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3729 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3727 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	CVE-2020-3726 CONF RM
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write	2020-02-	6.8	CVE-2020-3725



	vulnerability. Successful exploitation could lead to arbitrary code execution.	13		<a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3724</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3723</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3722</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3720</a> <a href="#">CONF RM</a>
apple -- ios_and_os_x	LibTIFF prior to 4.0.4, as used in Apple iOS before 8.4 and OS X before 10.10.4 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted TIFF image.	2020-02-12	<a href="#">4.3</a>	<a href="#">CVE-2014-8128</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira_server_and_data_center	The VerifyPopServerConnection!add jspsa component in Atlassian Jira Server and Data Center before version 8.7.0 is vulnerable to cross-site request forgery (CSRF). An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	<a href="#">6.8</a>	<a href="#">CVE-2019-20099</a> <a href="#">N/A</a> <a href="#">N/A</a>
atlassian -- jira_server_and_data_center	The VerifySmtpServerConnection!add jspsa component in Atlassian Jira Server and Data Center before version 8.7.0 is vulnerable to cross-site request forgery (CSRF). An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	<a href="#">6.8</a>	<a href="#">CVE-2019-20098</a> <a href="#">N/A</a> <a href="#">N/A</a>
blackberry -- playbook	BlackBerry PlayBook before 2.1 has an Information Disclosure Vulnerability via a Web browser component error	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2012-5828</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	<a href="#">4</a>	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>
bosch -- multiple_products	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR P 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-07	<a href="#">5</a>	<a href="#">CVE-2020-6768</a> <a href="#">CONF RM</a>
bosch -- video_streaming_gateway_and_divar_ip	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR P all-in-one 5000 if a	2020-02-07	<a href="#">6.4</a>	<a href="#">CVE-2020-6769</a> <a href="#">CONF RM</a>

	vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR P 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.			
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	4.6	<a href="#">CVE-2019-11484</a> MISC MISC
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	6.1	<a href="#">CVE-2019-11481</a> MISC MISC
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	6.8	<a href="#">CVE-2020-1700</a> SUSE CONF RM
chamilo -- chamilo_lms	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	4.3	<a href="#">CVE-2012-4029</a> MISC MISC MISC
cisco -- application_control_engine	Cisco ACE A2(3.6) allows log retention DOS.	2020-02-07	5	<a href="#">CVE-2013-1202</a> MISC
clearcanvas -- clearcanvas	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	4.3	<a href="#">CVE-2020-8788</a> MISC
cypress -- psoc_4_devices	The Bluetooth Low Energy (BLE) stack implementation on Cypress PSoC 4 through 3.62 devices does not properly restrict the BLE Link Layer header and executes certain memory contents upon receiving a packet with a Link Layer D (LLID) equal to zero. This allows attackers within radio range to cause deadlocks, cause anomalous behavior in the BLE state machine, or trigger a buffer overflow via a crafted BLE Link Layer frame.	2020-02-10	6.1	<a href="#">CVE-2019-17061</a> MISC MISC
d-link -- dir865l_devices	D-Link DIR865L v1 03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	4.3	<a href="#">CVE-2013-3096</a> MISC MISC MISC
daum_communications -- potplayer	Potplayer prior to 1.5.39659: DLL Loading Arbitrary Code Execution Vulnerability	2020-02-11	6.8	<a href="#">CVE-2013-3942</a> MISC MISC
dialog -- da14580/1/2/3_devices	The Bluetooth Low Energy implementation on Dialog Semiconductor SDK through 5.0.4 for DA14580/1/2/3 devices does not properly restrict the L2CAP payload length, allowing attackers in radio range to cause a buffer overflow via a crafted Link Layer packet.	2020-02-10	6.1	<a href="#">CVE-2019-17517</a> MISC MISC
dialog -- da1468x_devices	The Bluetooth Low Energy implementation on Dialog Semiconductor SDK through 1.0.14.1081 for DA1468x devices responds to link layer packets with a payload length larger than expected, allowing attackers in radio range to cause a buffer overflow via a crafted packet. This affects, for example, August Smart Lock.	2020-02-10	6.1	<a href="#">CVE-2019-17518</a> MISC MISC
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container Ds.	2020-02-07	4.3	<a href="#">CVE-2014-5278</a> MISC MISC MISC
	The Basic webmail module 6 x-1.x before			<a href="#">CVE-2012-5570</a>

drupal -- drupal	6.x-1.2 for Drupal allows remote authenticated users with the "access_basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	4	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
filemaker -- filemaker_pro_and_filemaker_advanced	An Authentication Bypass vulnerability exists in the MatchPasswordData function in DBEngine.dll in Filemaker Pro 13.03 and Filemaker Pro Advanced 12.04, which could let a malicious user obtain elevated privileges.	2020-02-11	4.6	<a href="#">CVE-2014-8347</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
flowplayer -- flowplayer_flash	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	6.8	<a href="#">CVE-2011-3642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fork -- fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	4.3	<a href="#">CVE-2014-9470</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fortiguard -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctsched process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	6.6	<a href="#">CVE-2019-16155</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	6.8	<a href="#">CVE-2019-13333</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	6.8	<a href="#">CVE-2019-13334</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	6.8	<a href="#">CVE-2019-17135</a> <a href="#">MISC</a>
	This vulnerability allows remote attackers to execute arbitrary code on affected			

foxit -- phantompdf	installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	6.8	<a href="#">CVE-2019-17136</a> MISC
gizmo5 -- gizmo5	The S P implementation on the Gizmo5 software phone provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "S P Digest Leak" issue.	2020-02-12	4.3	<a href="#">CVE-2009-5139</a> MISC
google -- chrome	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6414</a> SUSE MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2020-02-11	4.3	<a href="#">CVE-2020-6392</a> SUSE MISC
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6393</a> SUSE MISC
google -- chrome	Inappropriate implementation in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6415</a> SUSE MISC
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass HTML validators via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6413</a> SUSE MISC
google -- chrome	Insufficient policy enforcement in navigation in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to confuse the user via a crafted domain name.	2020-02-11	6.8	<a href="#">CVE-2020-6410</a> SUSE MISC
google -- chrome	Inappropriate implementation in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker who convinced the user to enter a URI to bypass navigation restrictions via a crafted domain name.	2020-02-11	6.8	<a href="#">CVE-2020-6409</a> SUSE MISC
google -- chrome	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2020-02-11	6.8	<a href="#">CVE-2020-6402</a> SUSE MISC
google -- chrome	Use after free in V8 in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6379</a> MISC
google -- chrome	Type confusion in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6382</a> SUSE MISC
google -- chrome	Insufficient policy enforcement in storage in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass site isolation via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6385</a> SUSE MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.130 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted Chrome Extension.	2020-02-11	6.8	<a href="#">CVE-2020-6380</a> MISC
google -- chrome	Integer overflow in JavaScript in Google Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote	2020-02-11	6.8	<a href="#">CVE-2020-6381</a> SUSE



	attacker to potentially exploit heap corruption via a crafted HTML page.			MISC MISC
google -- chrome	Use of uninitialized data in PDFium in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2020-02-11	6.8	<a href="#">CVE-2020-6398</a> SUSE MISC MISC
google -- chrome	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6390</a> SUSE MISC MISC
google -- chrome	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.	2020-02-11	6.8	<a href="#">CVE-2020-6389</a> SUSE MISC MISC
google -- chrome	Out of bounds access in WebAudio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6388</a> SUSE MISC MISC
google -- chrome	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.	2020-02-11	6.8	<a href="#">CVE-2020-6387</a> SUSE MISC MISC
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	5.8	<a href="#">CVE-2020-6412</a> SUSE MISC MISC
google -- chrome	Use after free in speech in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6378</a> MISC MISC
google -- chrome	Insufficient data validation in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6416</a> SUSE MISC MISC
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	5.8	<a href="#">CVE-2020-6411</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in installer in Google Chrome prior to 80.0.3987.87 allowed a local attacker to execute arbitrary code via a crafted registry entry.	2020-02-11	4.6	<a href="#">CVE-2020-6417</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to potentially exploit heap corruption via crafted clipboard content.	2020-02-11	4.6	<a href="#">CVE-2020-6404</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2020-02-11	5.8	<a href="#">CVE-2020-6394</a> SUSE MISC MISC
google -- chrome	Insufficient validation of untrusted input in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to bypass content security policy via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6391</a> SUSE MISC MISC
google -- chrome	Out of bounds read in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6395</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in Skia in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6396</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in sharing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6397</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in CORS in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6400</a> SUSE MISC

				MISC
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	4.3	<a href="#">CVE-2020-6401</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Incorrect implementation in Omnibox in Google Chrome on iOS prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6403</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds read in SQLite in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6405</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6399</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- system_event_utility	A potential security vulnerability has been identified with certain versions of HP System Event Utility prior to version 1.4.33. This vulnerability may allow a local attacker to execute arbitrary code via an HP System Event Utility system service.	2020-02-13	4.6	<a href="#">CVE-2019-18915</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
htmlunit -- htmlunit	HtmlUnit prior to 2.37.0 contains code execution vulnerabilities. HtmlUnit initializes Rhino engine improperly, hence a malicious JavaScript code can execute arbitrary Java code on the application. Moreover, when embedded in Android application, Android-specific initialization of Rhino engine is done in an improper way, hence a malicious JavaScript code can execute arbitrary Java code on the application.	2020-02-11	6.8	<a href="#">CVE-2020-5529</a> <a href="#">CONF RM</a> <a href="#">JVN</a>
ibm -- cloud_cli	IBM Cloud CLI 0.6.0 through 0.16.1 windows installers are signed using SHA1 certificate. An attacker might be able to exploit the weak algorithm to generate a installer with malicious software inside. IBM X-Force D: 162773.	2020-02-12	5	<a href="#">CVE-2019-4427</a> <a href="#">XE</a> <a href="#">CONF RM</a>
ibm -- content_navigator	IBM Content Navigator 3.0CD is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force D: 172815.	2020-02-12	5	<a href="#">CVE-2019-4741</a> <a href="#">XE</a> <a href="#">CONF RM</a>
ibm -- infosphere_guardium	InfoSphere Guardium aix_ktap module: DoS	2020-02-10	4.9	<a href="#">CVE-2012-2204</a> <a href="#">MISC</a>
ispconfig -- ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	6.5	<a href="#">CVE-2013-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2020-02-12	4	<a href="#">CVE-2020-2118</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins NUnit Plugin 0.25 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks.	2020-02-12	6.5	<a href="#">CVE-2020-2115</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins ECX Copy Data Management Plugin 1.9 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2128</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins FitNesse Plugin 1.30 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks.	2020-02-12	6.5	<a href="#">CVE-2020-2120</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs	2020-02-12	6.8	<a href="#">CVE-2020-2116</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>

	obtained through another method, capturing credentials stored in Jenkins.			
jenkins -- jenkins	A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2020-02-12	4	<a href="#">CVE-2020-2117</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Debian Package Builder Plugin 1.6.11 and earlier stores a GPG passphrase unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2125</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Google Kubernetes Engine Plugin 0.8.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	2020-02-12	6.5	<a href="#">CVE-2020-2121</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins DigitalOcean Plugin 1.1 and earlier stores a token unencrypted in the global config.xml file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2126</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins BMC Release Package and Deployment Plugin 1.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2127</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Applatix Plugin 1.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2133</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Eagle Tester Plugin 1.0.9 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2129</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Sandbox protection in Jenkins Script Security Plugin 1.69 and earlier could be circumvented during the script compilation phase by applying AST transforming annotations to imports or by using them inside of other annotations.	2020-02-12	6.5	<a href="#">CVE-2020-2110</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Sandbox protection in Jenkins Pipeline: Groovy Plugin 2.78 and earlier can be circumvented through default parameter expressions in CPS-transformed methods.	2020-02-12	6.5	<a href="#">CVE-2020-2109</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2130</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores passwords unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2131</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins S3 publisher Plugin 0.11.4 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	2020-02-12	5	<a href="#">CVE-2020-2114</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Azure AD Plugin 1.1.2 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	2020-02-12	5	<a href="#">CVE-2020-2119</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Parasoft Environment Manager Plugin 2.14 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	<a href="#">CVE-2020-2132</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file	2020-02-12	4	<a href="#">CVE-2020-2124</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>

	system.			
jenkins -- jenkins	Jenkins RadarGun Plugin 1.7 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	2020-02-12	6.5	<a href="#">CVE-2020-2123</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
kemp_technologies -- loadmaster	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	6.8	<a href="#">CVE-2014-5288</a> <a href="#">MISC</a> <a href="#">MISC</a>
konqueror -- konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	6.8	<a href="#">CVE-2012-4512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgd -- libgd	gdImageClone in gd.c in libgd 2.1.0-rc2 through 2.2.5 has a NULL pointer dereference allowing attackers to crash an application via a specific function call sequence. Only affects PHP when linked with an external libgd (not bundled).	2020-02-11	5	<a href="#">CVE-2018-14553</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys -- spa2102_devices	The S P implementation on the Linksys SPA2102 phone adapter provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "S P Digest Leak" issue.	2020-02-12	4.3	<a href="#">CVE-2009-5140</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	The int3 handler in the Linux kernel before 3.3 relies on a per-CPU debug stack, which allows local users to cause a denial of service (stack corruption and panic) via a crafted application that triggers certain lock contention.	2020-02-12	4.9	<a href="#">CVE-2012-0810</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
linuxmint -- linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	5	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint -- linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	5	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Upload Center Forms Component of Web File Manager in Rumpus FTP 8.2.9.1. This could allow an attacker to delete, create, and update the upload forms via RAPR/TriggerServerFunction.html.	2020-02-10	5.8	<a href="#">CVE-2019-19669</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Block Clients component of Web File Manager in Rumpus FTP 8.2.9.1 that could allow an attacker to whitelist or block any IP address via RAPR/BlockedClients.html.	2020-02-10	5.8	<a href="#">CVE-2019-19667</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the File Types component of Web File Manager in Rumpus FTP 8.2.9.1 that allows an attacker to add or delete the file types that are used on the server via RAPR/TriggerServerFunction.html.	2020-02-10	4.3	<a href="#">CVE-2019-19668</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the FTP Settings of Web File Manager in Rumpus FTP 8.2.9.1. Exploitation of this vulnerability can result in manipulation of Server FTP settings at RAPR/FTPSettingsSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19665</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A Cookie based reflected XSS exists in the Web File Manager of Rumpus FTP Server 8.2.9.1, related to RumpusLoginUserName and snp.	2020-02-10	4.3	<a href="#">CVE-2019-19661</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Folder Sets Settings of Web File Manager in Rumpus FTP 8.2.9.1. This allows an attacker to Create/Delete Folders after exploiting it at RAPR/FolderSetsSet.html.	2020-02-10	5.8	<a href="#">CVE-2019-19663</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Event Notices Settings of Web File Manager in Rumpus FTP 8.2.9.1. An attacker can create/update event notices via RAPR/EventNoticesSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19666</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A CSRF vulnerability exists in the Web			



maxum_development - rumpus_ftp	File Manager's Network Setting functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can manipulate the SMTP setting and other network settings via RAPR/NetworkSettingsSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19660</a> MISC MISC
maxum_development - rumpus_ftp	A HTTP Response Splitting vulnerability was identified in the Web Settings Component of Web File Manager in Rumpus FTP Server 8.2.9.1. A successful exploit can result in stored XSS, website defacement, etc. via ExtraHTTPHeader to RAPR/WebSettingsGeneralSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19670</a> MISC MISC
maxum_development - rumpus_ftp_server	A CSRF vulnerability exists in the Web File Manager's Edit Accounts functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can take over a user account by changing the password, update users' details, and escalate privileges via RAPR/DefineUsersSet.html.	2020-02-10	6.8	<a href="#">CVE-2019-19659</a> MISC MISC
mfscripts -- yetishare	MFScripts YetiShare v3 5 2 through v4 5 4 might allow an attacker to reset a password by using a leaked hash (the hash never expires until used).	2020-02-10	5	<a href="#">CVE-2019-20062</a> MISC MISC MISC
mfscripts -- yetishare	MFScripts YetiShare v3 5 2 through v4 5 4 places sensitive information in the Referer header. If this leaks, then third parties may discover password-reset hashes, file-delete links, or other sensitive information.	2020-02-10	5	<a href="#">CVE-2019-20060</a> MISC MISC MISC
mfscripts -- yetishare	The user-introduction email in MFScripts YetiShare v3 5 2 through v4 5 4 may leak the (system-picked) password if this email is sent in cleartext. In other words, the user is not allowed to choose their own initial password.	2020-02-10	5	<a href="#">CVE-2019-20061</a> MISC MISC MISC
mfscripts -- yetishare	payment_manage.ajax.php and various *_manage.ajax.php in MFScripts YetiShare 3 5 2 through 4 5 4 directly insert values from the sSortDir_0 parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection. NOTE: this issue exists because of an incomplete fix for CVE-2019-19732.	2020-02-10	6.8	<a href="#">CVE-2019-20059</a> MISC MISC MISC MISC
microchip_technology -- atsamb11_devices	The Bluetooth Low Energy implementation on Microchip Technology BluSDK Smart through 6.2 for ATSAMB11 devices does not properly restrict link-layer data length on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.	2020-02-10	6.1	<a href="#">CVE-2019-19195</a> MISC MISC
microsoft -- edge	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'.	2020-02-11	4	<a href="#">CVE-2020-0663</a> MISC
microsoft -- exchange_server_2013_and_2016_and_2019	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0692</a> MISC
microsoft -- internet_explorer_10_and_11	An information disclosure vulnerability exists in the way that affected Microsoft Internet Explorer handles cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'.	2020-02-11	4.3	<a href="#">CVE-2020-0706</a> MISC
microsoft -- malicious_software_removal_tool	An elevation of privilege vulnerability exists when the Windows Malicious Software Removal Tool (MSRT) improperly handles junctions. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Malicious Software Removal Tool Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0733</a> MISC
microsoft -- multiple_products	A security feature bypass vulnerability exists in Microsoft Outlook software when it improperly handles the parsing of URI formats, aka 'Microsoft Outlook Security	2020-02-11	4.3	<a href="#">CVE-2020-0696</a> MISC

	Feature Bypass Vulnerability'.			
microsoft -- multiple_windows_products	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0689</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682.	2020-02-11	4.6	<a href="#">CVE-2020-0680</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0735</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.	2020-02-11	4.6	<a href="#">CVE-2020-0669</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Client License Service (ClipSVC) handles objects in memory, aka 'Windows Client License Service Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0701</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0740</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739.	2020-02-11	4.6	<a href="#">CVE-2020-0737</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749.	2020-02-11	4.6	<a href="#">CVE-2020-0750</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0737.	2020-02-11	4.6	<a href="#">CVE-2020-0739</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.	2020-02-11	4.6	<a href="#">CVE-2020-0668</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0741</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0742</a> MISC

microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0743</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0659.	2020-02-11	4.6	<a href="#">CVE-2020-0747</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0749</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735.	2020-02-11	4.6	<a href="#">CVE-2020-0752</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682.	2020-02-11	4.6	<a href="#">CVE-2020-0679</a> MISC
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'.	2020-02-11	5	<a href="#">CVE-2020-0746</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0665</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754.	2020-02-11	4.6	<a href="#">CVE-2020-0753</a> MISC
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0729</a> MISC
microsoft -- multiple_windows_products	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	2020-02-11	5	<a href="#">CVE-2020-0660</a> MISC
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751.	2020-02-11	5.5	<a href="#">CVE-2020-0661</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0657</a> MISC
	An elevation of privilege vulnerability exists when the Windows Data Sharing			

microsoft -- multiple_windows_products	Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0747.	2020-02-11	4.6	<a href="#">CVE-2020-0659</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0666</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0667</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753.	2020-02-11	4.6	<a href="#">CVE-2020-0754</a> MISC
microsoft -- sql_server_2012_and_2014_and_2016	A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests, aka 'Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability'.	2020-02-11	6.5	<a href="#">CVE-2020-0618</a> MISC
microsoft -- surface_hub	A security feature bypass vulnerability exists in Surface Hub when prompting for credentials, aka 'Surface Hub Security Feature Bypass Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0702</a> MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It mishandled time skew (between the machine hosting the web server and the machine hosting the database) when trying to block a brute-force series of invalid requests.	2020-02-12	4.3	<a href="#">CVE-2020-8890</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It did not canonicalize usernames when trying to block a brute-force series of invalid requests.	2020-02-12	4.3	<a href="#">CVE-2020-8891</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It did not consider the HTTP PUT method when trying to block a brute-force series of invalid requests.	2020-02-12	6.8	<a href="#">CVE-2020-8892</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. The Galaxy view contained an incorrectly sanitized search string in app/View/Galaxies/view.ctp.	2020-02-12	5	<a href="#">CVE-2020-8893</a> MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. ACLs for discussion threads were mishandled in app/Controller/ThreadsController.php and app/Model/Thread.php.	2020-02-12	6.4	<a href="#">CVE-2020-8894</a> MISC MISC
netcracker -- netcracker_resource_management	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h_____%2427, (3) h_____%2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	6.5	<a href="#">CVE-2015-3423</a> MISC MISC
netsurf -- libnsbmp	Heap-based buffer overflow in the bmp_decode_rle function in libnsbmp.c in Libnsbmp 0.1.2 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the last row of RLE data in a crafted BMP file.	2020-02-12	6.8	<a href="#">CVE-2015-7508</a> MISC MISC
node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	5	<a href="#">CVE-2019-15604</a> MISC CONF RM CONF RM CONF RM
	The Bluetooth Low Energy (BLE) stack			



nxp -- kw41z_devices	implementation on the NXP KW41Z (based on the MCUXpresso SDK with Bluetooth Low Energy Driver 2.2.1 and earlier) does not properly restrict the BLE Link Layer header and executes certain memory contents upon receiving a packet with a Link Layer D (LL D) equal to zero. This allows attackers within radio range to cause deadlocks, cause anomalous behavior in the BLE state machine, or trigger a buffer overflow via a crafted BLE Link Layer frame.	2020-02-10	6.1	<a href="#">CVE-2019-17060</a> MISC MISC
oberhumer -- libzo2_and_lzo-2	Integer overflow in the LZO algorithm variant in Oberhumer libzo2 and lzo-2 before 2.07 on 32-bit platforms might allow remote attackers to execute arbitrary code via a crafted Literal Run.	2020-02-12	6.8	<a href="#">CVE-2014-4607</a> MISC CONF RM
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	4	<a href="#">CVE-2014-9127</a> MISC
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the Yii_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	4.3	<a href="#">CVE-2014-9126</a> MISC
openfiler -- openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	4.3	<a href="#">CVE-2011-1086</a> MISC MISC MISC
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	5.5	<a href="#">CVE-2020-1768</a> CONF RM
perforce_software -- p4web	Perforce P4web 2011.1 and 2012.1 has multiple XSS vulnerabilities	2020-02-12	4.3	<a href="#">CVE-2013-1410</a> MISC MISC
phonerlite -- phonerlite	The PhonerLite phone before 2.15 provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "SIP Digest Leak" issue.	2020-02-12	4.3	<a href="#">CVE-2014-2560</a> MISC
php -- php	When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbfl_filt_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.	2020-02-10	6.4	<a href="#">CVE-2020-7060</a> MISC
php -- php	When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash.	2020-02-10	6.4	<a href="#">CVE-2020-7059</a> MISC
pragmamx -- pragmamx	Multiple cross-site scripting (XSS) vulnerabilities in pragmaMx 1.x before 1.12.2 allow remote attackers to inject arbitrary web script or HTML via the (1) name parameter to modules.php or (2) img_url to includes/wysiwyg/spaw/editor/plugins/imgpopup/img_popup.php.	2020-02-11	4.3	<a href="#">CVE-2012-2452</a> MISC MISC MISC MISC
prestashop -- prestashop	Cross-site scripting (XSS) vulnerability in PrestaShop before 1.4.9 allows remote attackers to inject arbitrary web script or HTML via the index of the product[] parameter to ajax.php.	2020-02-11	4.3	<a href="#">CVE-2012-2517</a> MISC MISC
	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial			

qualcomm -- multiple_snapdragon_products	IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> CONF RM
qualcomm -- multiple_snapdragon_products	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> CONF RM
railo_technologies -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	6.8	<a href="#">CVE-2014-5468</a> MISC MISC MISC MISC
red_hat -- openshift_enterprise	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb.	2020-02-07	4.4	<a href="#">CVE-2020-1708</a> CONF RM
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, stores users' information by cleartext in the cookie, which divulges password to attackers.	2020-02-11	5	<a href="#">CVE-2020-3935</a> MISC MISC MISC
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, allows attackers to enumerate and exam user account in the system.	2020-02-11	5	<a href="#">CVE-2020-3933</a> MISC MISC MISC
siemens -- multiple_scalance_devices	A vulnerability has been identified in SCALANCE S602 (All versions >= V3.0), SCALANCE S612 (All versions >= V3.0), SCALANCE S623 (All versions >= V3.0), SCALANCE S627-2M (All versions >= V3.0). Specially crafted packets sent to port 443/top of affected devices could cause a Denial-of-Service condition of the web server.	2020-02-11	5	<a href="#">CVE-2019-13925</a> MISC
siemens -- multiple_scalance_switches	A vulnerability has been identified in SCALANCE X-200 switch family (incl. SIPLUS NET variants) (all versions < 5.2.4), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All versions), SCALANCE X-300 switch family (incl. X408 and S PLUS NET variants) (all versions < 4.1.3). The device does not send the X-Frame-Option Header in the administrative web interface, which makes it vulnerable to Clickjacking attacks. The security vulnerability could be exploited by an attacker that is able to trick an administrative user with a valid session on the target device into clicking on a website controlled by the attacker. The vulnerability could allow an attacker to	2020-02-11	4.3	<a href="#">CVE-2019-13924</a> MISC

	perform administrative actions via the web interface. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- multiple_simatic_devices	A vulnerability has been identified in SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.1), SIMATIC S7-300 PN/DP CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions). Affected devices contain a vulnerability that could cause a Denial-of-Service condition of the web server by sending specially crafted HTTP requests to ports 80/tcp and 443/tcp. The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device's web server. Beyond the web service, no other functions or interfaces are affected by the Denial-of-Service condition.	2020-02-11	5	<a href="#">CVE-2019-13940</a> MISC MISC
siemens -- ozw672_and_772_web_servers	A vulnerability has been identified in OZW672 (All versions < V10.00), OZW772 (All versions < V10.00). Vulnerable versions of OZW Web Server use predictable path names for project files that legitimately authenticated users have created by using the application's export function. By accessing a specific uniform resource locator on the web servers a remote attacker could be able to download a project file without prior authentication. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected system. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises the confidentiality of the targeted system.	2020-02-11	5	<a href="#">CVE-2019-13941</a> MISC
simple_machines -- simple_machines_forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: Forum admin can read files such as the database config.	2020-02-07	4	<a href="#">CVE-2013-0192</a> MISC MISC MISC
smoothwall - smoothwall_express_3	A cross-site scripting (XSS) vulnerability in Smoothwall Express 3.	2020-02-07	4.3	<a href="#">CVE-2011-1084</a> MISC
smoothwall -- smoothwall_express_3	CSRF vulnerability in Smoothwall Express 3.	2020-02-07	6.8	<a href="#">CVE-2011-1085</a> MISC
socialengine -- socialengine	Multiple cross-site request forgery (CSRF) vulnerabilities in the (1) Forum, (2) Event, and (3) Classifieds plugins in SocialEngine before 4.2.4.	2020-02-11	6.8	<a href="#">CVE-2012-6721</a> MISC
socialengine -- socialengine	Multiple cross-site scripting (XSS) vulnerabilities in SocialEngine before 4.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) title parameter to music/create, (2) location parameter to events/create, or (3) search parameter to widget/index/content_id/*.	2020-02-11	4.3	<a href="#">CVE-2012-6720</a> MISC
sockjs -- sockjs	htmlfile in lib/transport/htmlfile.js in SockJS before 3.0 is vulnerable to Reflected XSS via the /htmlfile c (aka callback) parameter.	2020-02-10	4.3	<a href="#">CVE-2020-8823</a> MISC MISC
sphider -- sphider	A Command Execution vulnerability exists in Sphider before 1.3.6 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5083 pertains to instances of fwrite in Sphider.	2020-02-10	6.5	<a href="#">CVE-2014-5083</a> MISC
sphider -- sphider_plus	A Command Execution vulnerability exists in Sphider Plus 3.2 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5085 pertains to instances of fwrite in Sphider Plus, but do not exist in either Sphider or Sphider Pro.	2020-02-10	6.5	<a href="#">CVE-2014-5085</a> MISC

sphider -- sphider_pro	A Command Execution vulnerability exists in Sphider Pro 3.2 due to insufficient sanitization of fwrite, which could let a remote malicious user execute arbitrary code. CVE-2014-5084 pertains to instances of fwrite in Sphider Pro only, but do not exist in either Sphider or Sphider Plus.	2020-02-10	6.5	<a href="#">CVE-2014-5084</a> MISC
statusnet -- statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	5	<a href="#">CVE-2010-4658</a> MISC MISC
suse -- opensuse_wicked	An ni_dhcp4_fsm_process_dhcp4_packet memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets with a different client-id.	2020-02-11	5	<a href="#">CVE-2020-7217</a> SUSE MISC MISC MISCm
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5820</a> MISC
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5822</a> MISC
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a DLL injection vulnerability, which is a type of issue whereby an individual attempts to execute their own code in place of legitimate code as a means to perform an exploit.	2020-02-11	4.6	<a href="#">CVE-2020-5821</a> MISC
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5823</a> MISC
teamviewer -- teamviewer_desktop	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9.x, this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.	2020-02-07	4.4	<a href="#">CVE-2019-18988</a> MISC MISC MISC MISC
testlink -- testlink	An issue was discovered in TestLink 1.9.19. The relation_type parameter of	2020-02-		<a href="#">CVE-2020-8841</a>



	the lib/requirements/reqSearch.php endpoint is vulnerable to authenticated SQL Injection.	10	<a href="#">6.5</a>	<a href="#">MISC</a> <a href="#">MISC</a>
texas_instruments -- cc2640r2_devices	The Bluetooth Low Energy implementation on Texas Instruments SDK through 3.30.00.20 for CC2640R2 devices does not properly restrict the SM Public Key packet on reception, allowing attackers in radio range to cause a denial of service (crash) via crafted packets.	2020-02-10	<a href="#">6.1</a>	<a href="#">CVE-2019-17520</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
texas_instruments -- multiple_devices	The Bluetooth Low Energy peripheral implementation on Texas Instruments SIMPLELINK-CC2640R2-SDK through 3.30.00.20 and BLE-STACK through 1.5.0 before Q4 2019 for CC2640R2 and CC2540/1 devices does not properly restrict the advertisement connection request packet on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.	2020-02-10	<a href="#">6.1</a>	<a href="#">CVE-2019-19193</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_bug_genie -- the_bug_genie	The Bug Genie before 3.2.6 has Multiple XSS and HTML Injection Vulnerabilities	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2013-1760</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ubiquiti_networks -- unifi_controller	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4) authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the UniFi Controller name via a request to api/set/setting/identity.	2020-02-08	<a href="#">6.8</a>	<a href="#">CVE-2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>
vbseo -- vbseo	vbSeo before 3.6.0PL2 allows XSS via the member.php u parameter.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2012-6666</a> <a href="#">MISC</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	<a href="#">6.5</a>	<a href="#">CVE-2013-3591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
watchguard -- firewire_xtm	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	<a href="#">4.3</a>	<a href="#">CVE-2014-6413</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	<a href="#">6.5</a>	<a href="#">CVE-2015-2062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	A Cross-site Scripting (XSS) vulnerability exists in the All in One SEO Pack plugin before 2.0.3.1 for WordPress via the Search parameter.	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2013-5988</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	<a href="#">6.8</a>	<a href="#">CVE-2013-2009</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	<a href="#">4.3</a>	<a href="#">CVE-2013-2008</a> <a href="#">MISC</a> <a href="#">MISC</a>

				<a href="#">MISC</a>
xiaomi -- mi6_devices	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Xiaomi Browser Prior to 10.4.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the miui.share application. The issue results from the lack of proper validation of user-supplied data, which can result in an arbitrary application download. An attacker can leverage this vulnerability to execute code in the context of the user. Was ZDI-CAN-7483.	2020-02-10	<a href="#">6.8</a>	<a href="#">CVE-2019-13322</a> <a href="#">MISC</a>
xiaomi -- mi6_devices	This vulnerability allows network adjacent attackers to execute arbitrary code on affected installations of Xiaomi Browser Prior to 10.4.0. User interaction is required to exploit this vulnerability in that the target must connect to a malicious access point. The specific flaw exists within the handling of HTTP responses to the Captive Portal. A crafted HTML response can cause the Captive Portal to open a browser to a specified location without user interaction. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7467.	2020-02-10	<a href="#">5.4</a>	<a href="#">CVE-2019-13321</a> <a href="#">MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	<a href="#">6.5</a>	<a href="#">CVE-2013-3628</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Zenphoto before 1.4.3.4 admin-news-articles.php date parameter XSS.	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2012-4519</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - applications_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	<a href="#">5</a>	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apport -- apport	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	<a href="#">1.9</a>	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a> <a href="#">MISC</a>
apport -- apport	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	<a href="#">2.1</a>	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a> <a href="#">MISC</a>
apport -- apport	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	<a href="#">2.1</a>	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a> <a href="#">MISC</a>
bludit -- bludit	<b>** DISPUTED **</b> Bludit 3.10.0 allows Editor or Author roles to insert malicious JavaScript on the WYSIWYG editor. NOTE: the vendor's perspective is that this is "not a bug."	2020-02-07	<a href="#">3.5</a>	<a href="#">CVE-2020-8812</a> <a href="#">MISC</a>
cpanel -- cpanel_and_whm	The clientconf.html and detailbw.html pages in x3 in cPanel & WHM 11.34.0 (build 8) have a XSS vulnerability.	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2012-6449</a> <a href="#">MISC</a>
digi_transport -- multiple_devices	Digi TransPort WR21 5.2.2 3, WR44 5.1 6.4, and WR44v2 5.1.6.9 devices	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2020-8822</a>

	allow stored XSS in the web application.			<a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in CORS in Google Chrome prior to 80.0 3987.87 allowed a local attacker to obtain potentially sensitive information via a crafted HTML page.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-6408</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- hp_systems_insight_manager	HP Systems Insight Manager before 7.0 allows a remote user on adjacent network to access information	2020-02-10	<a href="#">2.7</a>	<a href="#">CVE-2012-1994</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- rational_publishing_engine	IBM Rational Publishing Engine 6 0.6 and 6.0 6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 162888.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2019-4431</a> <a href="#">XE</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Brakeman Plugin 0.12 and earlier did not escape values received from parsed JSON files when rendering them, resulting in a stored cross-site scripting vulnerability exploitable by users able to control the Brakeman post-build step input data.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2122</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Subversion Plugin 2.13.0 and earlier does not escape the error message for the Project Repository Base URL field form validation, resulting in a stored cross-site scripting vulnerability.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2111</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the parameter name shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2112</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the default value shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2113</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
keycloak -- keycloak	It was found in all keycloak versions before 9.0.0 that links to external applications (Application Links) in the admin console are not validated properly and could allow Stored XSS attacks. An authed malicious user could create URLs to trick users in other realms, and possibly conduct further attacks.	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2020-1697</a> <a href="#">CONF RM</a>
linksys -- wrt310nv2ne	Linksys WRT310Nv2 2.0 0.1 is vulnerable to XSS.	2020-02-07	<a href="#">3.5</a>	<a href="#">CVE-2013-3067</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'.	2020-02-11	<a href="#">3.6</a>	<a href="#">CVE-2020-0730</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-0658</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-0755</a> <a href="#">MISC</a>
	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to			

microsoft -- multiple_windows_products	properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0675</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0748</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0744</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755.	2020-02-11	2.1	<a href="#">CVE-2020-0756</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0716.	2020-02-11	2.1	<a href="#">CVE-2020-0717</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0717.	2020-02-11	2.1	<a href="#">CVE-2020-0716</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0705</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0698</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation	2020-02-11	2.1	<a href="#">CVE-2020-0677</a> <a href="#">MISC</a>



	Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.			
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0676</a> MISC
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows kernel does not properly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0736</a> MISC
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0693.	2020-02-11	3.5	<a href="#">CVE-2020-0694</a> MISC
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0694.	2020-02-11	3.5	<a href="#">CVE-2020-0693</a> MISC
microsoft -- windows_10_and_windows_server_products	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, could run a specially crafted application. The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE D is unique from CVE-2020-0661.	2020-02-11	2.1	<a href="#">CVE-2020-0751</a> MISC
moodle -- moodle	Persistent XSS in /course/modedit.php of Moodle through 3.7.2 allows authenticated users (Teacher and above) to inject JavaScript into the session of another user (e.g., enrolled student or site administrator) via the introeditor[text] parameter. NOTE: the discoverer and vendor disagree on whether Moodle customers have a reasonable expectation that anyone authenticated as a Teacher can be trusted with the ability to add arbitrary JavaScript (this ability is not documented on Moodle's Teacher_role page). Because the vendor has this expectation, they have stated "this report has been closed as a false positive, and not a bug."	2020-02-11	3.5	<a href="#">CVE-2019-18210</a> MISC
mybulletinboard -- mybulletinboard	Cross-site scripting (XSS) vulnerability in MyBB before 1.6.13 allows remote authenticated users to inject arbitrary web script or HTML via the name parameter in the edit action of the config-profile_fields module.	2020-02-11	3.5	<a href="#">CVE-2014-3826</a> MISC
mybulletinboard -- mybulletinboard	Multiple cross-site scripting (XSS) vulnerabilities in the MyBB (aka MyBulletinBoard) before 1.8.4 allow remote authenticated users to inject arbitrary web script or HTML via the title parameter in the (1) edit or (2) add action in the user-users module or the (3) finduser action or the name parameter in an (4) edit action in the user-user module or the (5) editprofile action to modcp.php.	2020-02-11	3.5	<a href="#">CVE-2014-3827</a> CONF RM MISC
netapp --	NetApp Snap Creator Framework before			<a href="#">CVE-2016-</a>

snap_creator_framework	4.3P1 allows remote authenticated users to conduct clickjacking attacks via unspecified vectors.	2020-02-11	3.5	<a href="#">CVE-2020-5710</a> <a href="#">MISC</a>
netcracker -- netcracker_resource_manager	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary HTML via the (1) ctrl, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8) xname, or (9) mpTransactionId parameter.	2020-02-08	3.5	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>
orange_hrm -- orange_hrm	Orange HRM 2.7.1 allows XSS via the vacancy name.	2020-02-10	3.5	<a href="#">CVE-2013-1353</a> <a href="#">MISC</a>
piwigo -- piwigo	Piwigo 2.10.1 is affected by stored XSS via the Group Name Field to the group_list page.	2020-02-10	3.5	<a href="#">CVE-2020-8089</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0.8.8 has stored XSS	2020-02-07	3.5	<a href="#">CVE-2013-3635</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	3.5	<a href="#">CVE-2013-3636</a> <a href="#">MISC</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	3.5	<a href="#">CVE-2013-3637</a> <a href="#">MISC</a>
rakuten -- viber_for_android	An exploitable information disclosure vulnerability exists in the 'Secret Chats' functionality of Rakuten Viber on Android 9.3 0.6. The 'Secret Chats' functionality allows a user to delete all traces of a chat either by using a time trigger or by direct request. There is a bug in this functionality which leaves behind photos taken and shared on the secret chats, even after the chats are deleted. These photos will be stored in the device and accessible to all applications installed on the Android device.	2020-02-13	2.1	<a href="#">CVE-2018-3987</a> <a href="#">MISC</a>
samsung -- knox	This vulnerability allows local attackers to disclose sensitive information on affected installations of Samsung Knox 1.2.02.39 on Samsung Galaxy S9 build G9600ZHS3ARL1 Secure Folder. An attacker must first obtain physical access to the device in order to exploit this vulnerability. The specific flaws exists within the the handling of the lock screen for Secure Folder. The issue results from the lack of proper validation that a user has correctly authenticated. An attacker can leverage this vulnerability to disclose the contents of the secure container. Was ZDI-CAN-7381.	2020-02-10	2.1	<a href="#">CVE-2019-6744</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a denial of service vulnerability, which is a type of issue whereby a threat actor attempts to tie up the resources of a resident application, thereby making certain functions unavailable.	2020-02-11	2.1	<a href="#">CVE-2020-5824</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5826</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an arbitrary file write vulnerability, which is a type of issue whereby an attacker is able to overwrite existing files on the resident system without proper privileges.	2020-02-11	3.6	<a href="#">CVE-2020-5825</a> <a href="#">MISC</a>
	Symantec Endpoint Protection Manager			

symantec -- endpoint_protection_manager	(SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5827</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5829</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5830</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5831</a> MISC
symantec -- symantec_endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5828</a> MISC
syska -- smart_bulb_devices	Syska Smart Bulb devices through 2017-08-06 receive RGB parameters over cleartext Bluetooth Low Energy (BLE), leading to sniffing, reverse engineering, and replay attacks.	2020-02-10	3.3	<a href="#">CVE-2017-18642</a> MISC
vanilla_forum -- vanilla	index.php? p=/dashboard/settings/branding in Vanilla 2.6 3 allows stored XSS.	2020-02-10	3.5	<a href="#">CVE-2020-8825</a> MISC MISC
wordpress -- wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	3.5	<a href="#">CVE-2015-1394</a> MISC MISC MISC MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll PNG pngread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted PNG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2020-6068</a> MISC
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll JPEG SOFx parser of the Accusoft ImageGear 19.5.0 library. A specially crafted JPEG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6066</a> MISC
	An exploitable out-of-bounds write vulnerability exists in the TIFreadstripdata function of the igcore19d.dll library of Accusoft ImageGear 19 5 0. A specially			<a href="#">CVE-2019-</a>

accusoft -- imagegear	crafted T FF file file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2020-5187</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the uncompress_scan_line function of the igcore19d.dll library of Accusoft ImageGear, version 19.5 0. A specially crafted PCX file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6063</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the bmp_parsing function of the igcore19d.dll library of Accusoft ImageGear, version 19.5.0. A specially crafted BMP file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6065</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the uncompress_scan_line function of the igcore19d.dll library of Accusoft ImageGear, version 19.5 0. A specially crafted PCX file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6064</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d dll JPEG jpegread precision parser of the Accusoft ImageGear 19 5 0 library. A specially crafted JPEG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6069</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d dll TIFF tifread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted T FF file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6067</a> <a href="#">MISC</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to arbitrary file system write.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3762</a> <a href="#">CONF RM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3748</a> <a href="#">CONF RM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to arbitrary file system write.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3763</a> <a href="#">CONF RM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions, 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3742</a> <a href="#">CONF RM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2017.011.30156 and earlier, and	2020-02-	not yet calculated	<a href="#">CVE-2020-3743</a>



	2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	13	calculated	<a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3744</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3745</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3746</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3747</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3749</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3750</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to memory leak .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3753</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3754</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3755</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to memory leak .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3756</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code	2020-02-13	not yet calculated	<a href="#">CVE-2020-3751</a> <a href="#">CONFIRM</a>

	execution .			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3752</a> <a href="#">CONFIRM</a>
adobe -- digital_editions	Adobe Digital Editions versions 4.5.10 and below have a buffer errors vulnerability. Successful exploitation could lead to information disclosure.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3759</a> <a href="#">CONFIRM</a>
adobe -- digital_editions	Adobe Digital Editions versions 4.5.10 and below have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3760</a> <a href="#">CONFIRM</a>
adobe -- experience_manager	Adobe Experience Manager versions 6.5, and 6.4 have an uncontrolled resource consumption vulnerability. Successful exploitation could lead to denial-of-service.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3741</a> <a href="#">CONFIRM</a>
adobe -- flash_player	Adobe Flash Player versions 32.0.0.321 and earlier, 32.0.0.314 and earlier, 32.0.0.321 and earlier, and 32.0.0.255 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3757</a> <a href="#">CONFIRM</a>
ai -- risknet_acquirer	RiskNet Acquirer before hotfix 6.0 b7+ADHOC-443 ApplicationServiceBean contains a service information disclosure.	2020-02-14	not yet calculated	<a href="#">CVE-2013-5687</a> <a href="#">X</a>
amazon -- aws-js-s3-explorer	explorer.js in Amazon AWS JavaScript S3 Explorer (aka aws-js-s3-explorer) v2 alpha before 2019-08-02 allows XSS in certain circumstances.	2020-02-13	not yet calculated	<a href="#">CVE-2019-14652</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
amd -- raadeon_amd_user_exp	The AUEPLauncher service in Radeon AMD User Experience Program Launcher through 1.0.0.1 on Windows allows elevation of privilege by placing a crafted file in %PROGRAMDATA%\AMD\PPC\upload and then creating a symbolic link in %PROGRAMDATA%\AMD\PPC\temp that points to an arbitrary folder with an arbitrary file name.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8950</a> <a href="#">MISC</a> <a href="#">MISC</a>
ammy -- ammy_admin	Ammy Admin 3.2 and earlier stores the client ID at a fixed memory location, which might make it easier for user-assisted remote attackers to bypass authentication by running a local program that extracts a field from the AA_v3.2.exe file.	2020-02-11	not yet calculated	<a href="#">CVE-2013-5582</a> <a href="#">MISC</a>
apache -- nifi	In Apache NiFi 0.0.1 to 1.11.0, the flow fingerprint factory generated flow fingerprints which included sensitive property descriptor values. In the event a node attempted to join a cluster and the cluster flow was not inheritable, the flow fingerprint of both the cluster and local flow was printed, potentially containing sensitive values in plaintext.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1942</a> <a href="#">MISC</a>
ariadne -- ariadne	Multiple cross-site scripting (XSS) vulnerabilities in Ariadne 2.7.6 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO parameter to (1) index.php and (2) loader.php.	2020-02-11	not yet calculated	<a href="#">CVE-2011-4938</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
aruba_networks -- intelligent_edge_switch	A remotely exploitable information disclosure vulnerability is present in Aruba Intelligent Edge Switch models 5400, 3810, 2920, 2930, 2530 with GigT port, 2530 10/100 port, or 2540. The vulnerability impacts firmware 16.08.* before 16.08.0009, 16.09.* before 16.09.0007 and 16.10.* before 16.10.0003. The vulnerability allows an attacker to retrieve sensitive system information. This attack can be carried out without user authentication under very specific conditions.	2020-02-13	not yet calculated	<a href="#">CVE-2019-5322</a> <a href="#">MISC</a>
askey -- ap400w_devices	An issue was discovered on Askey AP4000W TDC_V1 01.003 devices. An attacker can perform Remote Code Execution (RCE) by sending a specially crafted network packer to the bd_srv service listening on TCP port 54188.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8614</a> <a href="#">MISC</a>

askpop3d -- askpop3d	A Denial of Service vulnerability exists in askpop3d 0.7.7 in free (psQuery),	2020-02-13	not yet calculated	<a href="#">CVE-2014-3208</a> <a href="#">MISC</a>
atlassian -- jira_and_greenhopper	Stored XSS vulnerability in UpdateFieldJson.jspa in JIRA 4.4.3 and GreenHopper before 5.9.8 allows an attacker to inject arbitrary script code.	2020-02-13	not yet calculated	<a href="#">CVE-2012-1500</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
atlassian -- jira_server_and_data_center	The Atlassian Application Links plugin is vulnerable to cross-site request forgery (CSRF). The following versions are affected: all versions prior to 5.4.21, from version 6.0.0 before version 6.0.12, from version 6.1.0 before version 6.1.2, from version 7.0.0 before version 7.0.2, and from version 7.1.0 before version 7.1.3. The vulnerable plugin is used by Atlassian Jira Server and Data Center before version 8.7.0. An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	not yet calculated	<a href="#">CVE-2019-20100</a> <a href="#">N/A</a> <a href="#">N/A</a> <a href="#">N/A</a>
avira -- antivir_engine	A Denial of Service (infinite loop) vulnerability exists in Avira AntiVir Engine before 8.2.12.58 via an unspecified function in the PDF Scanner Engine.	2020-02-12	not yet calculated	<a href="#">CVE-2013-4602</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
barracuda -- web_application_firewall	Barracuda Web Application Firewall (WAF) 7.8.1.013 allows remote attackers to bypass authentication by leveraging a permanent authentication token obtained from a query string.	2020-02-12	not yet calculated	<a href="#">CVE-2014-2595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bearftp -- bearftp	Improper connection handling in the base connection handler in IKTeam BearFTP before v0.3.1 allows a remote attacker to achieve denial of service via a Slowloris approach by sending a large volume of small packets.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
belkin -- n750_routers	Belkin n750 routers have a buffer overflow.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7173</a> <a href="#">MISC</a> <a href="#">MISC</a>
boat_browser -- boat_browser_for_android	The WebView class and use of the WebView.addJavascriptInterface method in the Boat Browser application 8.0 and 8.0.1 for Android allow remote attackers to execute arbitrary code via a crafted web site, a related issue to CVE-2012-6636.	2020-02-12	not yet calculated	<a href="#">CVE-2014-4968</a> <a href="#">MISC</a>
bss -- bs-client_private_client	A Two-Factor Authentication Bypass Vulnerability exists in BS-Client Private Client 2.4 and 2.5 via an XML request that neglects the use of ADPsw D and AD parameters, which could let a malicious user access privileged function.	2020-02-13	not yet calculated	<a href="#">CVE-2014-4198</a> <a href="#">MISC</a>
chiyu_technology -- bf-430_devices	Stored XSS was discovered on CHIYU BF-430 232/485 TCP/ P Converter devices before 1.16.00, as demonstrated by the /if cgi TF_submask field.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8839</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- internetwork_operating_systems	A memory leak vulnerability exists in Cisco IOS before 15.2(1)T due to a memory leak in the HTTP PROXY Server process (aka CSCu52820), when configured with Cisco ISR Web Security with Cisco ScanSafe and User Authentication NTLM configured.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4661</a> <a href="#">MISC</a>
cloud_foundry -- credhub	Cloud Foundry CredHub, versions prior to 2.5.10, connects to a MySQL database without TLS even when configured to use TLS. A malicious user with access to the network between CredHub and its MySQL database may eavesdrop on database connections and thereby gain unauthorized access to CredHub and other components.	2020-02-12	not yet calculated	<a href="#">CVE-2020-5399</a> <a href="#">CONF RM</a>
	Codologic CodoForum through 4.8.4 allows a DOM-based XSS. While creating			

codologic -- codofurm	a new topic as a normal user, it is possible to add a poll that is automatically loaded in the DOM once the thread/topic is opened. Because session cookies lack the HttpOnly flag, it is possible to steal authentication cookies and take over accounts.	2020-02-15	not yet calculated	<a href="#">CVE-2020-7050</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
codologic -- codofurm	Codologic Codoforum through 4.8.4 allows stored XSS in the login area. This is relevant in conjunction with CVE-2020-5842 because session cookies lack the HttpOnly flag. The impact is account takeover.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7051</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	In iTop through 2.6.0, an XSS payload can be delivered in certain fields (such as icon) of the XML file used to build the dashboard. This is similar to CVE-2015-6544 (which is only about the dashboard title).	2020-02-14	not yet calculated	<a href="#">CVE-2019-13966</a> <a href="#">MISC</a>
combodo -- itop	iTop 2.2.0 through 2.6.0 allows remote attackers to cause a denial of service (application outage) via many requests to launch a compile operation. The requests use the pages/exec.php?exec_env=production&exec_module=itop-hub-connector&exec_page=ajax.php&operation=compile URI. This only affects the community version.	2020-02-14	not yet calculated	<a href="#">CVE-2019-13967</a> <a href="#">MISC</a>
combodo -- itop	Because of a lack of sanitization around error messages, multiple Reflective XSS issues exist in iTop through 2.6.0 via the param_file parameter to webservices/export.php, webservices/cron.php, or env-production/itop-backup/backup.php. By default, any XSS sent to the administrator can be transformed to remote command execution because of CVE-2018-10642 (still working through 2.6.0) The Reflective XSS can also become a stored XSS within the same account because of another vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2019-13965</a> <a href="#">MISC</a>
combodo -- itop	In Combodo iTop 2.2.0 through 2.6.0, if the configuration file is writable, then execution of arbitrary code can be accomplished by calling ajax.dataloader with a maliciously crafted payload. Many conditions can place the configuration file into a writable state: during installation; during upgrade; in certain cases, an error during modification of the file from the web interface leaves the file writable (can be triggered with XSS); a race condition can be triggered by the hub-connector module (community version only from 2.4.1 to 2.6.0); or editing the file in a CLI.	2020-02-14	not yet calculated	<a href="#">CVE-2019-11215</a> <a href="#">MISC</a>
cypress -- psoc_4_devices	The Bluetooth Low Energy implementation in Cypress PSoC 4 BLE component 3.61 and earlier processes data channel frames with a payload length larger than the configured link layer maximum RX payload size, which allows attackers (in radio range) to cause a denial of service (crash) via a crafted BLE Link Layer frame.	2020-02-12	not yet calculated	<a href="#">CVE-2019-16336</a> <a href="#">MISC</a>
d-link -- dir-842_rev_c_devices	A stack-based buffer overflow was found on the D-Link DIR-842 REVC with firmware v3.13B09 HOTFIX due to the use of strcpy for LOGINPASSWORD when handling a POST request to the /MTFWU endpoint.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8962</a> <a href="#">MISC</a>
digi_international -- connectport_lts_32_mei	Digi International ConnectPort LTS 32 MEI, Firmware Version 1.4.3 (82002228_K 08/09/2018), bios Version 1.2. Successful exploitation of this vulnerability could allow an attacker to upload a malicious file to the application.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6975</a> <a href="#">MISC</a>
digi_international -- connectport_lts_32_mei	Digi International ConnectPort LTS 32 MEI, Firmware Version 1.4.3 (82002228_K 08/09/2018), bios Version 1.2. Multiple cross-site scripting vulnerabilities exist that could allow an attacker to cause a denial-of-service condition.	2020-02-13	not yet calculated	<a href="#">CVE-2020-6973</a> <a href="#">MISC</a>
dojo -- dojox	dojox is vulnerable to Cross-site Scripting in all versions before version 1.16.1, 1.15.2, 1.14.5, 1.13.6, 1.12.7 and 1.11.9. This is due to dojox xmpp util.xmlEncode	2020-02-13	not yet calculated	<a href="#">CVE-2019-10785</a> <a href="#">MISC</a>



	only encoding the first occurrence of each character, not all of them.			<a href="#">MISC</a>
dovecot -- dovecot	The IMAP and LMTP components in Dovecot 2.3.9 before 2.3.9.3 mishandle snippet generation when many characters must be read to compute the snippet and a trailing > character exists. This causes a denial of service in which the recipient cannot read all of their messages.	2020-02-12	not yet calculated	<a href="#">CVE-2020-7957</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
dovecot -- dovecot	lib-smtp in submission-login and lmtp in Dovecot 2.3.9 before 2.3.9.3 mishandles truncated UTF-8 data in command parameters, as demonstrated by the unauthenticated triggering of a submission-login infinite loop.	2020-02-12	not yet calculated	<a href="#">CVE-2020-7046</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
drupal -- drupal	The RESTful Web Services (restws) module 7.x-1.x before 7.x-1.4 and 7.x-2.x before 7.x-2.1 for Drupal does not properly restrict access to entity write operations, which makes it easier for remote authenticated users with the "access resource node" and "create page content" permissions (or equivalents) to conduct cross-site scripting (XSS) or execute arbitrary PHP code via a crafted text field.	2020-02-11	not yet calculated	<a href="#">CVE-2013-4225</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
easyxdm -- easyxdm	Cross-site Scripting (XSS) in EasyXDM before 2.4.18 allows remote attackers to inject arbitrary web script or HTML via the easyxdm.swf file.	2020-02-14	not yet calculated	<a href="#">CVE-2013-5212</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
etherpad -- etherpad	Directory traversal vulnerability in node/Utils/Minify.js in Etherpad 1.1.2 through 1.5.4 allows remote attackers to read arbitrary files with permissions of the user running the service via a .. (dot dot) in the path parameter of HTTP API requests. NOTE: This vulnerability is due to an incomplete fix to CVE-2015-3297.	2020-02-13	not yet calculated	<a href="#">CVE-2015-3309</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
extrun -- ilbo	ilbo App (ilbo App for Android prior to version 1.1.8 and ilbo App for iOS prior to version 1.2.01) allows an attacker on the same network segment to bypass authentication and to view the images which were recorded by the other ilbo user's device via unspecified vectors.	2020-02-14	not yet calculated	<a href="#">CVE-2020-5532</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.	2020-02-10	not yet calculated	<a href="#">CVE-2020-8840</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of text field objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9400.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8846</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.2947. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the fxhtml2pdf.exe module. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9560.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8855</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of watermarks in AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this	2020-02-14	not yet calculated	<a href="#">CVE-2020-8845</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	vulnerability to execute code in the context of the current process. Was ZDI-CAN-9358.			
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7 0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9591.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8853</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7 0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of JPEG files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9606.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8854</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6 0.25608. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of watermarks. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9640.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8856</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.7 0.29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9416.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8852</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of form Annotation objects within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9862.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8857</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this	2020-02-14	not yet calculated	<a href="#">CVE-2020-8847</a> <a href="#">MISC</a> <a href="#">MISC</a>

	vulnerability to execute code in the context of the current process. Was ZDI-CAN-9414.			
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9406.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8851</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9407.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8848</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9415.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8850</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9413.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8849</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.6.0 25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG files within CovertToPDF. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9102.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8844</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
free_reprintables -- articlefr	A Privilege Escalation Vulnerability exists in Free Reprintables ArticleFR 11.06 2014 due to insufficient access restrictions in the data.php script, which could let a remote malicious user obtain access or modify or delete database information.	2020-02-13	not yet calculated	<a href="#">CVE-2014-4170</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
freebsd -- bsd_libc	regcomp in the BSD implementation of libc is vulnerable to denial of service due to stack exhaustion.	2020-02-12	not yet calculated	<a href="#">CVE-2011-3336</a> <a href="#">FULLDISC</a> <a href="#">END</a> <a href="#">MISC</a>

				BUGTRAQ
fujitsu -- multiple_products	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions, Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3, Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.	2020-02-07	not yet calculated	<a href="#">CVE-2019-13163</a> CONF RM
git -- git	Git before 1 8.5.6, 1.9.x before 1.9.5, 2.0 x before 2.0.5, 2.1 x before 2.1.4, and 2.2 x before 2.2.1 on Windows and OS X; Mercurial before 3.2.3 on Windows and OS X; Apple Xcode before 6.2 beta 3; mine; libgit2; Egit; and JGit allow remote Git servers to execute arbitrary commands via a tree containing a crafted .git/config file with (1) an ignorable Unicode codepoint, (2) a git~1/config representation, or (3) mixed case that is improperly handled on a case-insensitive filesystem.	2020-02-12	not yet calculated	<a href="#">CVE-2014-9390</a> MISC MISC MISC MISC MISC MISC
gitlab -- gitlab	GitLab 12.2.2 and below contains a security vulnerability that allows a guest user in a private project to see the merge request D associated to an issue via the activity timeline.	2020-02-14	not yet calculated	<a href="#">CVE-2019-15592</a> MISC MISC
gitlab -- gitlab	GitLab 11.8 and later contains a security vulnerability that allows a user to obtain details of restricted pipelines via the merge request endpoint.	2020-02-14	not yet calculated	<a href="#">CVE-2019-15594</a> MISC MISC
global_payments -- php-sdk	Gateways/Gateway.php in Heartland & Global Payments PHP SDK before 2.0.0 does not enforce SSL certificate validations.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20455</a> MISC MISC
gocloud -- multiple_devices	Gocloud S2A_WL 4.2.7.16471, S2A 4.2.7.17278, S2A 4.3 0.15815, S2A 4.3 0.17193, S3A K2P MTK 4.2.7.16528, S3A 4.3 0.16572, and ISP3000 4.3 0.17190 devices allows remote attackers to execute arbitrary OS commands via shell metacharacters in a ping operation, as demonstrated by the cgi-bin/webui/admin/tools/app_ping/diag_ping/substring.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8949</a> MISC
google -- android	In notifyNetworkTested and related functions of NetworkMonitor.java, there is a possible bypass of private DNS settings. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-9Android ID: A-122652057	2020-02-13	not yet calculated	<a href="#">CVE-2020-0028</a> MISC
google -- android	In btm_read_remote_ext_features_complete of btm_acl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-141552859	2020-02-13	not yet calculated	<a href="#">CVE-2020-0005</a> MISC
google -- android	It is possible for a malicious application to construct a TYPE_TOAST window manually and make that window clickable. This could lead to a local escalation of privilege with no additional execution privileges needed. User action is needed	2020-02-13	not yet calculated	<a href="#">CVE-2020-0014</a> MISC



	for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-128674520			
google -- android	In binder_thread_release of binder.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android kernelAndroid ID: A-145286050References: Upstream kernel	2020-02-13	not yet calculated	<a href="#">CVE-2020-0030</a> MISC
google -- android	The Bluetooth stack in Android before 2.3.6 allows a physically proximate attacker to obtain contact information via an AT phonebook transfer.	2020-02-12	not yet calculated	<a href="#">CVE-2011-2343</a> CONFIRMED MISC
google -- android	In updatePermissions of PermissionManagerService.java, it may be possible for a malicious app to obtain a custom permission from another app due to a permission bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-10Android D: A-67319274	2020-02-13	not yet calculated	<a href="#">CVE-2019-2200</a> MISC
google -- android	In onCreate of CertInstaller.java, there is a possible way to overlay the Certificate Installation dialog by a malicious application. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-139017101	2020-02-13	not yet calculated	<a href="#">CVE-2020-0015</a> MISC
google -- android	In Parcel::continueWrite of Parcel.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-140419401	2020-02-13	not yet calculated	<a href="#">CVE-2020-0026</a> MISC
google -- android	In multiple places, it was possible for the primary user's dictionary to be visible to and modifiable by secondary users. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-123232892	2020-02-13	not yet calculated	<a href="#">CVE-2020-0017</a> MISC
google -- android	In MotionEvent::appendDescription of InputDispatcher.cpp, there is a possible log information disclosure. This could lead to local disclosure of user input with System execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-139945049	2020-02-13	not yet calculated	<a href="#">CVE-2020-0018</a> MISC
google -- android	In HidRawSensor::batch of HidRawSensor.cpp, there is a possible out of bounds write due to an unexpected switch fallthrough. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-144040966	2020-02-13	not yet calculated	<a href="#">CVE-2020-0027</a> MISC
google -- android	In getAttributeRange of ExifInterface.java, there is a possible failure to redact location information from media files due to an incorrect bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-10Android D: A-143118731	2020-02-13	not yet calculated	<a href="#">CVE-2020-0020</a> MISC
google -- android	In removeUnusedPackagesLPw of PackageManagerService.java, there is a possible permanent denial-of-service due to a missing package dependency test. This could lead to remote denial of service with User execution privileges needed. User interaction is not needed for	2020-02-13	not yet calculated	<a href="#">CVE-2020-0021</a> MISC

	exploitation Product: AndroidVersions: Android-10Android D: A-141413692			
google -- android	In reassemble_and_dispatch of packet_fragmenter.cc, there is possible out of bounds write due to an incorrect bounds calculation. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-143894715	2020-02-13	not yet calculated	<a href="#">CVE-2020-0022</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
google -- android	In setPhonebookAccessPermission of AdapterService.java, there is a possible disclosure of user contacts over bluetooth due to a missing permission check. This could lead to local information disclosure if a malicious app enables contacts over a bluetooth connection, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145130871	2020-02-13	not yet calculated	<a href="#">CVE-2020-0023</a> <a href="#">MISC</a>
hashicorp -- sentinel	HashiCorp Sentinel up to 0.10.1 incorrectly parsed negation in certain policy expressions. Fixed in 0.10.2.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19879</a> <a href="#">MISC</a>
hcl -- appscan_standard_edition	HCL AppScan Standard Edition 9 0.3.13 and earlier uses hard-coded credentials which can be exploited by attackers to get unauthorized access to the system.	2020-02-14	not yet calculated	<a href="#">CVE-2019-4392</a> <a href="#">MISC</a>
hitachi -- command_suite_and_automation_director	A vulnerability in Hitachi Command Suite prior to 8.7.1-00 and Hitachi Automation Director prior to 8.5.0-00 allow authenticated remote users to expose technical information through error messages. Hitachi Command Suite includes Hitachi Device Manager and Hitachi Compute Systems Manager.	2020-02-14	not yet calculated	<a href="#">CVE-2018-21032</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
hitachi -- multiple_products	A vulnerability in Hitachi Command Suite prior to 8 6.2-00, Hitachi Automation Director prior to 8.6.2-00 and Hitachi Infrastructure Analytics Advisor prior to 4.2 0-00 allow authenticated remote users to load an arbitrary Cascading Style Sheets (CSS) token sequence. Hitachi Command Suite includes Hitachi Device Manager, Hitachi Tiered Storage Manager, Hitachi Replication Manager, Hitachi Tuning Manager, Hitachi Global Link Manager and Hitachi Compute Systems Manager.	2020-02-14	not yet calculated	<a href="#">CVE-2018-21033</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
hp -- linuxki	LinuxKI v6.0-1 and earlier is vulnerable to an XSS which is resolved in release 6.0-2.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7208</a> <a href="#">MISC</a>
hp -- linuxki	LinuxKI v6.0-1 and earlier is vulnerable to a remote code execution which is resolved in release 6 0-2.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7209</a> <a href="#">MISC</a>
ibm -- tivoli_monitoring_service	IBM Tivoli Monitoring Service 6.3.0.7.3 through 6.3 0.7.10 could allow an unauthorized user to access and modify operation aspects of the ITM monitoring server possibly leading to an effective denial of service or disabling of the monitoring server. BM X-Force ID: 167647.	2020-02-13	not yet calculated	<a href="#">CVE-2019-4592</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
ibm -- urbandeploy_and_urbancode_build	IBM UrbanCode Deploy (UCD) 7.0.3 and IBM UrbanCode Build 6.1.5 could allow a local user to obtain sensitive information by unmasking certain secure values in documents. IBM X-Force D: 171248.	2020-02-13	not yet calculated	<a href="#">CVE-2019-4666</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
intel -- converged_security_and_management_engine	Improper Authentication in subsystem in Intel(R) CSME versions 12.0 through 12.0.48 (IOT only: 12 0.56), versions 13.0 through 13.0.20, versions 14.0 through 14.0.10 may allow a privileged user to potentially enable escalation of privilege, denial of service or information disclosure via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2019-14598</a> <a href="#">MISC</a>
intel -- e1000e/82574l_network_processing_state_when_parsing_32_hex_33_hex_or_34_hex_byte_values_at_the_0x47f_offset.	A denial of service vulnerability exists in some motherboard implementations of Intel e1000e/82574L network controller devices through 2013-02-06 where the device can be brought into a non-processing state when parsing 32 hex, 33 hex, or 34 hex byte values at the 0x47f offset. NOTE: A followup statement from Intel suggests that the root cause of this issue was an incorrectly configured	2020-02-13	not yet calculated	<a href="#">CVE-2013-1634</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">SECTRAK</a> <a href="#">XF</a>

	EEPROM image.			
intel -- manycore_platform_so	Improper permissions in the installer for Intel(R) MPSS before version 3.8.6 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0563</a> MISC
intel -- renesas_electronics_us	Improper permissions in the installer for the Intel(R) Renesas Electronics(R) USB 3.0 Driver, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0560</a> MISC
intel -- sgx_software_developm	Improper initialization in the Intel(R) SGX SDK before v2.6.100.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0561</a> MISC
intel -- raid_web_console_2	Improper permissions in the installer for Intel(R) RWC2, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0562</a> MISC
intel -- raid_web_console_3_for	Improper permissions in the installer for Intel(R) RWC3 for Windows before version 7.010.009.000 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0564</a> MISC
invision_power_services -- invision_power_board	Invision Power Board (PB) through 3.x allows admin account takeover leading to code execution.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3725</a> MISC
istio -- istio	An issue was discovered in Istio 1.3 through 1.3.6. Under certain circumstances, it is possible to bypass a specifically configured Mixer policy. Istio-proxy accepts the x-istio-attributes header at ingress that can be used to affect policy decisions when Mixer policy selectively applies to a source equal to ingress. To exploit this vulnerability, someone has to encode a source.uid in this header. This feature is disabled by default in Istio 1.3 and 1.4.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8843</a> MISC MISC CONF RM
joomla! -- joomla!	Tiny browser in TinyMCE 3.0 editor in Joomla! before 1.5.13 allows file upload and arbitrary PHP code execution.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4906</a> CONF RM EXPLOIT-DB MISC
joomla! -- joomla!	TinyBrowser plugin for Joomla! before 1.5.13 allows arbitrary file upload via upload.php.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4908</a> MISC EXPLOIT-DB MLIST
jsreport -- jsreport	An unintended require and server-side request forgery vulnerabilities in jsreport version 2.5.0 and earlier allow attackers to execute arbitrary code.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8128</a> MISC
jsreport -- script- manager	An unintended require vulnerability in script-manager npm package version 0.8.6 and earlier may allow attackers to execute arbitrary code.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8129</a> MISC
juniper -- junos_os	Multiple vulnerabilities exist in Juniper Junos J-Web error handling that may lead to cross site scripting (XSS) issues or crash the J-Web service (DoS). This affects Juniper Junos OS 12.1X44 before 12.1X44-D45, 12.1X46 before 12.1X46-D30, 12.1X47 before 12.1X47-D20, 12.3 before 12.3R8, 12.3X48 before 12.3X48-D10, 13.1 before 13.1R5, 13.2 before 13.2R6, 13.3 before 13.3R4, 14.1 before 14.1R3, 14.1X53 before 14.1X53-D10, 14.2 before 14.2R1, and 15.1 before 15.1R1.	2020-02-11	not yet calculated	<a href="#">CVE-2014-6447</a> CONF RM MISC
kaseya -- virtual_system_adminis	Directory traversal vulnerability in Kaseya Virtual System Administrator (VSA) 7.0.0.0 before 7.0.0.33, 8.0.0.0 before 8.0.0.23, 9.0.0.0 before 9.0.0.19, and 9.1.0.0 before 9.1.0.9 allows remote authenticated users to write to and execute arbitrary files due to insufficient restrictions in file paths to json.ashx.	2020-02-13	not yet calculated	<a href="#">CVE-2015-6589</a> MISC MISC MISC MISC
kde -- paste_applet	The %{password(...)} macro in pastemacroexpander.cpp in the KDE Paste Applet before 4.10.5 in kdeplasma-addons does not properly generate passwords, which allows context-dependent attackers to bypass	2020-02-11	not yet calculated	<a href="#">CVE-2013-2120</a> MISC MISC MISC MISC

	authentication via a brute-force attack.			MISC
kde -- paste_applet	The KRandom::random function in KDE Paste Applet after 4.10.5 in kdeplasma-addons uses the GNU C Library rand function's linear congruential generator, which makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms by predicting the generator output.	2020-02-11	not yet calculated	<a href="#">CVE-2013-2213</a> MISC MISC MISC
kinetica -- kinetica	The Admin web application in Kinetica 7.0 9.2.20191118151947 does not properly sanitise the input for the function getLogs. This lack of sanitisation could be exploited to allow an authenticated attacker to run remote code on the underlying operating system. The logFile parameter in the getLogs function was used as a variable in a command to read log files; however, due to poor input sanitisation, it was possible to bypass a replacement and break out of the command.	2020-02-11	not yet calculated	<a href="#">CVE-2020-8429</a> MISC MISC
lenovo -- ez_media_&_backup_center	A vulnerability in the web interface of Lenovo EZ Media & Backup Center, ix2 & ix2-dl version 4.1.406.34763 and prior could allow an unauthenticated, remote attacker to redirect a user to an untrusted web page.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19758</a> CONF RM
lenovo -- multiple_devices	Lenovo was notified of a potential denial of service vulnerability, affecting various versions of BIOS for Lenovo Desktop, Desktop - All in One, and ThinkStation, that could cause PCRs to be cleared intermittently after resuming from sleep (S3) on systems with Intel TXT enabled.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6190</a> CONF RM
lenovo -- xclarity_administrator	An internal product security audit of Lenovo XClarity Administrator (LXCA) discovered a Document Object Model (DOM) based cross-site scripting vulnerability in versions prior to 2.6.6 that could allow JavaScript code to be executed in the user's web browser if a specially crafted link is visited. The JavaScript code is executed on the user's system, not executed on LXCA itself.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19757</a> CONF RM
lenovo -- xclarity_administrator	An XML External Entity (XXE) processing vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.6.6 that could allow information disclosure.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6194</a> CONF RM
lenovo -- xclarity_administrator	An information disclosure vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.6.6 that could allow unauthenticated access to some configuration files which may contain usernames, license keys, IP addresses, and encrypted password hashes.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6193</a> CONF RM
lenovo -- xclarity_controller	An authorization bypass exists in Lenovo XClarity Controller (XCC) versions prior to 3.08 CDI340V, 3.01 TEI392O, 1.71 PSI328N where a valid authenticated user with lesser privileges may be granted read-only access to higher-privileged information if 1) "LDAP Authentication Only with Local Authorization" mode is configured and used by XCC, and 2) a lesser privileged user logs into XCC within 1 minute of a higher privileged user logging out. The authorization bypass does not exist when "Local Authentication and Authorization" or "LDAP Authentication and Authorization" modes are configured and used by XCC.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6195</a> CONF RM
lexmark -- multiple_devices	Lexmark printer MS812 and multiple older generation Lexmark devices have a stored XSS vulnerability in the embedded web server. The vulnerability can be exploited to expose session credentials and other information via the users web browser.	2020-02-13	not yet calculated	<a href="#">CVE-2019-18791</a> MISC CONF RM
libuv -- libuv	The uv_rwlock_t fallback implementation for Windows XP and Server 2003 in libuv before 1.7.4 does not properly prevent threads from releasing the locks of other threads, which allows attackers to cause a denial of service (deadlock) or possibly have unspecified other impact by	2020-02-11	not yet calculated	<a href="#">CVE-2014-9748</a> MISC MISC MISC MISC



	leveraging a race condition.			<a href="#">MISC</a>
linux -- linux_kernel	ext4_protect_reserved_inode in fs/ext4/block_validity.c in the Linux kernel through 5.5.3 allows attackers to cause a denial of service (soft lockup) via a crafted journal size.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8992</a> <a href="#">MISC</a>
lvm2 -- lvm2	vg_lookup in daemons/lvmetad/lvmetad-core.c in LVM2 2.02 mismanages memory, leading to an lvmetad memory leak, as demonstrated by running pvs.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8991</a> <a href="#">MISC</a>
magento -- magento	Zend_XmlRpc Class in Magento before 1.7.0.2 contains an information disclosure vulnerability.	2020-02-13	not yet calculated	<a href="#">CVE-2012-6091</a> <a href="#">MLIST</a> <a href="#">BID</a> <a href="#">XF</a>
mailu -- mailu	In Mailu before version 1.7, an authenticated user can exploit a vulnerability in Mailu fetchmail script and gain full access to a Mailu instance. Mailu servers that have open registration or untrusted users are most impacted. The master and 1.7 branches are patched on our git repository. All Docker images published on docker.io/mailu for tags 1.5, 1.6, 1.7 and master are patched. For detailed instructions about patching and securing the server afterwards, see <a href="https://github.com/Mailu/Mailu/issues/1354">https://github.com/Mailu/Mailu/issues/1354</a>	2020-02-13	not yet calculated	<a href="#">CVE-2020-5239</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
mambo -- mambo_cms	Mambo CMS through 4.6.5 has multiple XSS.	2020-02-12	not yet calculated	<a href="#">CVE-2011-2499</a> <a href="#">MLIST</a>
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability was discovered in the Source Integration plugin before 1.6.2 and 2.x before 2.3.1 for MantisBT. The repo_delete.php Delete Repository page allows execution of arbitrary code via a repo name (if CSP settings permit it). This is related to CVE-2018-16362.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8981</a> <a href="#">MISC</a> <a href="#">MISC</a>
matestack-ui-core_gem_for_ruby_on_rails -- matestack-ui-core_gem_for_ruby_on_rails	matestack-ui-core (RubyGem) before 0.7.14 is vulnerable to XSS/Script injection. This vulnerability is patched in version 0.7.14.	2020-02-13	not yet calculated	<a href="#">CVE-2020-5241</a> <a href="#">CONF RM</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Web Settings of Web File Manager in Rumpus FTP 8.2.9.1. Exploitation of this vulnerability can result in manipulation of Server Web settings at RAPR/WebSettingsGeneralSet.html.	2020-02-10	not yet calculated	<a href="#">CVE-2019-19664</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp_server	A CSRF vulnerability exists in the Web File Manager's Create/Delete Accounts functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can Create and Delete accounts via RAPR/TriggerServerFunction.html.	2020-02-10	not yet calculated	<a href="#">CVE-2019-19662</a> <a href="#">MISC</a> <a href="#">MISC</a>
mcafee -- endpoint_security	Improper access control vulnerability in Configuration Tool in McAfee McAfee Endpoint Security (ENS) Prior to 10.6.1 February 2020 Update allows local users to disable security features via unauthorised use of the configuration tool from older versions of ENS.	2020-02-14	not yet calculated	<a href="#">CVE-2020-7251</a> <a href="#">CONF RM</a>
microsoft -- multiple_windows_products	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0728</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0714</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0745, CVE-2020-0792.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0715</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0727</a> <a href="#">MISC</a>
	A remote code execution vulnerability exists when the Windows Imaging Library			

microsoft -- multiple_windows_products	improperly handles memory.To exploit this vulnerability, an attacker would first have to coerce a victim to open a specially crafted file.The security update addresses the vulnerability by correcting how the Windows Imaging Library handles memory., aka 'Windows Imaging Library Remote Code Execution Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0708</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0691</a> MISC
microsoft -- office_online_server	A spoofing vulnerability exists when Office Online Server does not validate origin in cross-origin communications correctly, aka 'Microsoft Office Online Server Spoofing Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0695</a> MISC
microsys -- promotic	Microsys PROMOTIC 8.2.13 contains an ActiveX Control Start Buffer Overflow vulnerability which can lead to denial of service.	2020-02-13	not yet calculated	<a href="#">CVE-2014-1617</a> MISC MISC
mobileiron -- vsp_and_sentry	MobileIron VSP < 5.9.1 and Sentry < 5.0 has an insecure encryption scheme.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7287</a> MISC MISC
mobileiron -- vsp_and_sentry	MobileIron VSP < 5.9.1 and Sentry < 5.0 has a weak password obfuscation algorithm	2020-02-12	not yet calculated	<a href="#">CVE-2013-7286</a> MISC MISC
moxa -- mgate_5105-mb-eip_devices	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Moxa MGate 5105-MB-EIP firmware version 4.1. Authentication is required to exploit this vulnerability. The specific flaw exists within the DestIP parameter within MainPing.asp. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9552.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8858</a> MISC MISC
netgear -- cg3100_devices	A vulnerability exists in Netgear CG3100 devices before 3.9.2421.13.mp3 V0027 via an embed malicious script in an unspecified page, which could let a malicious user obtain sensitive information.	2020-02-13	not yet calculated	<a href="#">CVE-2014-3919</a> MISC
netis -- wf2471_devices	Netis WF2471 v1.2.30142 devices allow an authenticated attacker to execute arbitrary OS commands via shell metacharacters in the /cgi-bin-igdd/sys_log_clean cgi log_3g_type parameter.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8946</a> MISC
nvidia -- graphics_drivers	A Memory Corruption Vulnerability exists in NVIDIA Graphics Drivers 29549 due to an unknown function in the file proc/driver/nvidia/registry.	2020-02-12	not yet calculated	<a href="#">CVE-2012-0951</a> MISC MISC
nxp -- kw41z_devices	The Bluetooth Low Energy implementation on NXP SDK through 2.2.1 for KW41Z devices does not properly restrict the Link Layer payload length, allowing attackers in radio range to cause a buffer overflow via a crafted packet.	2020-02-12	not yet calculated	<a href="#">CVE-2019-17519</a> MISC
openconnect_project - openconnect_vpn_client	OpenConnect VPN client with GnuTLS before 5.02 contains a heap overflow if MTU is increased on reconnection.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7098</a> CONF RM
openvpn -- access_server	OpenVPN Access Server 2.8.x before 2.8.1 allows LDAP authentication bypass (except when a user is enrolled in two-factor authentication).	2020-02-13	not yet calculated	<a href="#">CVE-2020-8953</a> CONF RM
openx -- openx_ad_server	A Code Execution Vulnerability exists in OpenX Ad Server 2.8.10 due to a backdoor in flowplayer-3.1.1.min.js library, which could let a remote malicious user execute arbitrary PHP code	2020-02-14	not yet calculated	<a href="#">CVE-2013-4211</a> MISC MISC MISC MISC
	A Cross-Site Scripting (XSS) Vulnerability			<a href="#">CVE-2013-</a>

otrs -- itsm_and_faq	exists in OTRS ITSM prior to 3.2.4, 3.1.8, and 3.0.7 and FAQ prior to 2.1.4 and 2.0.8 via changes, workorder items, and FAQ articles, which could let a remote malicious user execute arbitrary code.	2020-02-12	not yet calculated	2637 <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
palo_alto_networks -- expedition_migration_tool	Insufficient Cross-Site Request Forgery (XSRF) protection on Expedition Migration Tool allows remote unauthenticated attackers to hijack the authentication of administrators and to perform actions on the Expedition Migration Tool. This issue affects Expedition Migration Tool 1.1.51 and earlier versions.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1977</a> <a href="#">CONF RM</a>
palo_alto_networks -- globalprotect	A denial-of-service (DoS) vulnerability in Palo Alto Networks GlobalProtect software running on Mac OS allows authenticated local users to cause the Mac OS kernel to hang or crash. This issue affects GlobalProtect 5.0.5 and earlier versions of GlobalProtect 5.0 on Mac OS.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1976</a> <a href="#">CONF RM</a>
palo_alto_networks -- pan-os	Missing XML validation vulnerability in the PAN-OS web interface on Palo Alto Networks PAN-OS software allows authenticated users to inject arbitrary XML that results in privilege escalation. This issue affects PAN-OS 8.1 versions earlier than PAN-OS 8.1.12 and PAN-OS 9.0 versions earlier than PAN-OS 9.0.6. This issue does not affect PAN-OS 7.1, PAN-OS 8.0, or PAN-OS 9.1 or later versions.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1975</a> <a href="#">CONF RM</a>
pcr -- pcre2 -- pcre2_jit_compile	An out-of-bounds read was discovered in PCRE before 10.34 when the pattern JIT compiled and used to match specially crafted subjects in non-UTF mode. Applications that use PCRE to parse untrusted input may be vulnerable to this flaw, which would allow an attacker to crash the application. The flaw occurs in do_extuni_no_utf in pcre2_jit_compile.c.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20454</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
podman -- podman	A flaw was discovered in Podman where it incorrectly allows containers when created to overwrite existing files in volumes, even if they are mounted as read-only. When a user runs a malicious container or a container based on a malicious image with an attached volume that is used for the first time, it is possible to trigger the flaw and overwrite files in the volume. This issue was introduced in version 1.6.0.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1726</a> <a href="#">CONF RM</a>
prestashop -- prestashop	PrestaShop before 1.4.11 allows logout CSRF.	2020-02-14	not yet calculated	<a href="#">CVE-2013-4792</a> <a href="#">MISC</a>
prestashop -- prestashop	PrestaShop before 1.4.11 allows Logistician, translators and other low level profiles/accounts to inject a persistent XSS vector on TinyMCE.	2020-02-14	not yet calculated	<a href="#">CVE-2013-4791</a> <a href="#">MISC</a>
prismview -- prismview_system_and_prismview_player	The HTTP API in Prismview System 9.11.10.17.00 and Prismview Player 11.13.09.1100 allows remote code execution by uploading RebootSystem.Ink and requesting /REBOOTSYSTEM or /RESTARTVNC. (Authentication is required but an XML file containing credentials can be downloaded.)	2020-02-10	not yet calculated	<a href="#">CVE-2019-20451</a> <a href="#">MISC</a>
proglottis -- gpgme	The proglottis Go wrapper before 0.1.1 for the GPGME library has a use-after-free, as demonstrated by use for container image pulls by Docker or CRI-O. This leads to a crash or potential code execution during GPG signature verification.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8945</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
progress -- moveit_transfer	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, multiple SQL Injection vulnerabilities have been found in the REST API that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database via the REST API. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or	2020-02-14	not yet calculated	<a href="#">CVE-2020-8611</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>

	destroy database elements.			
progress -- moveit_transfer	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, a REST API endpoint failed to adequately sanitize malicious input, which could allow an authenticated attacker to execute arbitrary code in a victim's browser, aka XSS.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8612</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
python-mode -- python-mode	A Code Execution vulnerability exists in select.py when using python-mode 2012-12-19.	2020-02-12	not yet calculated	<a href="#">CVE-2013-5106</a> <a href="#">MISC</a>
qemu -- qemu	An out-of-bounds heap buffer access flaw was found in the way the iSCSI Block driver in QEMU versions 2.12.0 before 4.2.1 handled a response coming from an iSCSI server while checking the status of a Logical Address Block (LBA) in an iscsi_co_block_status() routine. A remote user could use this flaw to crash the QEMU process, resulting in a denial of service or potential execution of arbitrary code with privileges of the QEMU process on the host.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1711</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a>
qnep -- viocard-300_devices	QNAP VioCard 300 has hardcoded RSA private keys.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6277</a> <a href="#">MISC</a> <a href="#">MISC</a>
realtek -- ndis_driver_rt64x64.sys	Realtek NDIS driver rt640x64.sys, file version 10.1.505.2015, fails to do any size checking on an input buffer from user space, which the driver assumes has a size greater than zero bytes. To exploit this vulnerability, an attacker must send an RP with a system buffer size of 0.	2020-02-12	not yet calculated	<a href="#">CVE-2019-11867</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openshift_enterprise	The default configuration of broker.conf in Red Hat OpenShift Enterprise 2.x before 2.1 has a password of "mo00" for a Mongo account, which allows remote attackers to hijack the broker by providing this password, related to the openshift.sh script in Openshift Extras before 20130920. NOTE: this may overlap CVE-2013-4253 and CVE-2013-4281.	2020-02-12	not yet calculated	<a href="#">CVE-2014-0234</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
runc -- runc	runc through 1.0.0-rc9 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. (This vulnerability does not affect Docker due to an implementation detail that happens to block the attack.)	2020-02-12	not yet calculated	<a href="#">CVE-2019-19921</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.10 allows SQL Injection via the SOAP API, the EmailUIAjax interface, or the MailMerge module.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8804</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows Directory Traversal to include arbitrary .php files within the webroot via add_to_prospect_list.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8803</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 has Incorrect Access Control via action_saveHTMLField Bean Manipulation.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8802</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows PHAR Deserialization.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8801</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows EmailsControllerActionGetFromFields PHP Object Injection.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung -- s6_edge_smartphone	Multiple buffer overflows in the esa_write function in /dev/seirenin the Exynos Seiren Audio driver, as used in Samsung S6 Edge, allow local users to cause a denial of service (memory corruption) via a large (1) buffer or (2) size parameter.	2020-02-12	not yet calculated	<a href="#">CVE-2015-7890</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap --	Certain settings page(s) in SAP Business Objects Business Intelligence Platform (CMC), version 4.2, generates error	2020-02-	not yet	<a href="#">CVE-2020-6189</a>



business_objects_intelligence_platform	messages that can give enterprise private-network related information which would otherwise be restricted leading to Information Disclosure.	12	calculator	<a href="#">CVE-2020-6183</a> <a href="#">MISC</a>
sap -- enterprise_resource_planning_and_s4hana	VAT Pro-Rata reports in SAP ERP (SAP_APPL versions 600, 602, 603, 604, 605, 606, 616 and SAP_FIN versions 617, 618, 700, 720, 730) and SAP S/4HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user leading to Missing Authorization Check.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6188</a> <a href="#">MISC</a>
sap -- host_agent	SAP Host Agent, version 7.21, allows an unprivileged user to read the shared memory or write to the shared memory by sending request to the main SAPOSCOL process and receive responses that may contain data read with user root privileges e.g. size of any directory, system hardware and OS details, leading to Missing Authorization Check vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6183</a> <a href="#">MISC</a>
sap -- host_agent	SAP Host Agent, version 7.21, allows an attacker to cause a slowdown in processing of username/password-based authentication requests of the SAP Host Agent, leading to Denial of Service.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6186</a> <a href="#">MISC</a>
sap -- landscape_management	SAP Landscape Management, version 3.0, allows an attacker with admin privileges to execute malicious commands with root privileges in SAP Host Agent via SAP Landscape Management.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6192</a> <a href="#">MISC</a>
sap -- landscape_management	SAP Landscape Management, version 3.0, allows an attacker with admin privileges to execute malicious executables with root privileges in SAP Host Agent via SAP Landscape Management due to Missing Input Validation.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6191</a> <a href="#">MISC</a>
sap -- mobile_platform	SAP Mobile Platform, version 3.0, does not sufficiently validate an XML document accepted from an untrusted source which could lead to partial denial of service. Since SAP Mobile Platform does not allow External-Entity resolving, there is no issue of leaking content of files on the server.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6177</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver (Guided Procedures), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently validate an XML document input from a compromised admin, leading to Denial of Service.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6187</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver (Knowledge Management ICE Service), versions 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to execute malicious scripts leading to Reflected Cross-Site Scripting (XSS) vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6193</a> <a href="#">MISC</a>
sap -- netweaver_and_abap_platform	Under some circumstances the SAML SSO implementation in the SAP NetWeaver (SAP_BASIS versions 702, 730, 731, 740 and SAP ABAP Platform (SAP_BASIS versions 750, 751, 752, 753, 754), allows an attacker to include invalidated data in the HTTP response header sent to a Web user, leading to HTTP Response Splitting vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6181</a> <a href="#">MISC</a>
sap -- netweaver_and_s4hana	Under certain conditions, ABAP Online Community in SAP NetWeaver (SAP_BASIS version 7.40) and SAP S/4HANA (SAP_BASIS versions 7.50, 7.51, 7.52, 7.53, 7.54), does not sufficiently encode user-controlled inputs, resulting in Reflected Cross-Site Scripting (XSS) vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6184</a> <a href="#">MISC</a>
sap -- netweaver_and_s4hana	Under certain conditions ABAP Online Community in SAP NetWeaver (SAP_BASIS version 7.40) and SAP S/4HANA (SAP_BASIS versions 7.50, 7.51, 7.52, 7.53, 7.54), allows an authenticated attacker to store a malicious payload which results in Stored Cross Site Scripting vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6185</a> <a href="#">MISC</a>
sap -- netweaver_as_java	Certain vulnerable endpoints in SAP NetWeaver AS Java (Heap Dump Application), versions 7.30, 7.31, 7.40, 7.50, provide valuable information about	2020-02-	not yet	<a href="#">CVE-2020-6190</a>

	the system like hostname, server node and installation path that could be misused by an attacker leading to Information Disclosure.	12	calculator	<a href="#">MISC</a> <a href="#">MISC</a>
shaman -- shaman	Shaman 1.0 9: Users can add the line askforpwd=false to his shaman.conf file, without entering the root password in shaman. The next time shaman is run, root privileges are granted despite the fact that the user never entered the root password.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4338</a> <a href="#">MISC</a> <a href="#">MISC</a>
siemens -- multiple_devices	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All Versions < V4.5), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All Versions < V4.6), PROFINET Driver for Controller (All Versions < V2.1), RUGGEDCOM RM1224 (All versions < V4 3), SCALANCE M-800 / S615 (All versions < V4.3), SCALANCE W700 IEEE 802.11n (All versions <= V6 0.1), SCALANCE X-200 switch family (incl. SIPLUS NET variants) (All versions), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All Versions < V5 3), SCALANCE X-300 switch family (incl. X408 and S PLUS NET variants) (All versions), SCALANCE XB-200, XC-200, XP-200, XF-200BA and XR-300WG (All Versions < V3.0), SCALANCE XM-400 switch family (All Versions < V6.0), SCALANCE XR-500 switch family (All Versions < V6.0), SIMATIC CP 1616 and CP 1604 (All Versions < V2.8), S MATIC CP 343-1 (incl. SIPLUS NET variants) (All versions), SIMATIC CP 343-1 Advanced (incl. SIPLUS NET variants) (All versions), SIMATIC CP 343-1 ERPC (All versions), SIMATIC CP 343-1 LEAN (incl. SIPLUS NET variants) (All versions), SIMATIC CP 443-1 (incl. SIPLUS NET variants) (All versions), SIMATIC CP 443-1 Advanced (incl. S PLUS NET variants) (All versions), S MATIC CP 443-1 OPC UA (All versions), SIMATIC ET200AL M 157-1 PN (All versions), SIMATIC ET200M IM153-4 PN IO HF (incl. SIPLUS variants) (All versions), SIMATIC ET200M IM153-4 PN IO ST (incl. SIPLUS variants) (All versions), S MATIC ET200MP IM155-5 PN HF (incl. S PLUS variants) (All Versions < V4.2.0), SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants) (All Versions < V4.1.0), SIMATIC ET200S (incl. SIPLUS variants) (All versions), SIMATIC ET200SP IM155-6 PN Basic (incl. SIPLUS variants) (All versions), SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants) (All Versions < V3.3.1), SIMATIC ET200SP IM155-6 PN ST (incl. SIPLUS variants) (All Versions < V4.1 0), SIMATIC ET200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0) (All versions), S MATIC ET200pro, IM 154-3 PN HF (All versions), SIMATIC ET200pro, IM 154-4 PN HF (All versions), SIMATIC IPC Support, Package for VxWorks (All versions), SIMATIC MV400 family (All versions), S MATIC PN/PN Coupler 6ES7158-3AD01-0XA0 (incl. SIPLUS NET variant) (All Versions), SIMATIC RF180C (All versions), SIMATIC RF182C (All versions), SIMATIC RF600 family (All versions < V3), SINAMICS DCP (All Versions < V1 3). Profinet-IO (PNIO) stack versions prior V06.00 do not properly limit internal resource allocation when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface. This could lead to a denial of service condition due to lack of memory for devices that include a vulnerable version of the stack. The security vulnerability could be exploited by an attacker with network access to an affected device. Successful	2020-02-11	not yet calculated	<a href="#">CVE-2019-13946</a> <a href="#">MISC</a>

	exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device.			
simple_machines -- simple_machines_forum	Simple Machines Forum (SMF) through 2.0.5 has XSS	2020-02-12	not yet calculated	<a href="#">CVE-2013-4395</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplisafe -- ss3_devices	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to modify the Wi-Fi network the base station connects to.	2020-02-13	not yet calculated	<a href="#">CVE-2019-3998</a> <a href="#">MISC</a>
skril -- skril	Commerce Skril (Formerly Moneybookers) has an Access bypass vulnerability in all versions prior to 7.x-1.2	2020-02-12	not yet calculated	<a href="#">CVE-2013-1924</a> <a href="#">MISC</a> <a href="#">MISC</a>
sprite_software -- spritebud_and_backup	A Privilege Escalation Vulnerability exists in Sprite Software Spritebud 1.3.24 and 1.3.28 and Backup 2.5.4105 and 2.5.4108 on LG Android smartphones due to a race condition in the spritebud daemon, which could let a local malicious user obtain root privileges.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3685</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sqlite -- android_sqlite	Android SQLite Journal before 4.0.1 has an information disclosure vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2011-3901</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
squirrelmail -- squirrelmail	Squirrelmail 4.0 uses the outdated MD5 hash algorithm for passwords.	2020-02-13	not yet calculated	<a href="#">CVE-2012-5623</a> <a href="#">MISC</a> <a href="#">MISC</a>
stem_innovation -- izon_ip_camera	IZON P 2 0.2: hard-coded password vulnerability	2020-02-12	not yet calculated	<a href="#">CVE-2013-6236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
stmicroelectronics -- stm32wb5x_series_devices	The Bluetooth Low Energy implementation on STMicroelectronics BLE Stack through 1.3.1 for STM32WB5x devices does not properly handle consecutive Attribute Protocol (ATT) requests on reception, allowing attackers in radio range to cause an event deadlock or crash via crafted packets.	2020-02-12	not yet calculated	<a href="#">CVE-2019-19192</a> <a href="#">MISC</a>
synergy_systems_&_solutions -- husky_rtu_devices	The Synergy Systems & Solutions PLC & RTU system has a vulnerability in HUSKY RTU 6049-E70 firmware versions 5.0 and prior. Specially crafted malicious packets could cause disconnection of active authentic connections or reboot of device. This is a different issue than CVE-2019-16879 and CVE-2019-20046.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20045</a> <a href="#">MISC</a>
synergy_systems_&_solutions -- husky_rtu_devices	The Synergy Systems & Solutions PLC & RTU system has a vulnerability in HUSKY RTU 6049-E70 firmware versions 5.0 and prior. The affected product does not require adequate authentication, which may allow an attacker to read sensitive information or execute arbitrary code. This is a different issue than CVE-2019-16879 and CVE-2019-20046.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20046</a> <a href="#">MISC</a>
telink -- tslr8x5_and_tslr823x_and_tslr826x_devices	The Bluetooth Low Energy Secure Manager Protocol (SMP) implementation on Telink Semiconductor BLE SDK versions before November 2019 for TSLR8x5x through 3.4.0, TSLR823x through 1.3.0, and TSLR826x through 3.3 devices accepts a pairing request with a key size greater than 16 bytes, allowing an attacker in radio range to cause a buffer overflow and denial of service (crash) via crafted packets.	2020-02-12	not yet calculated	<a href="#">CVE-2019-19196</a> <a href="#">MISC</a> <a href="#">MISC</a>
telink -- tslr8x5_and_tslr823x_and_tslr826x_devices	The Bluetooth Low Energy Secure Manager Protocol (SMP) implementation on Telink Semiconductor BLE SDK versions before November 2019 for TSLR8x5x through 3.4.0, TSLR823x through 1.3.0, and TSLR826x through 3.3 devices installs a zero long term key (LTK) if an out-of-order link-layer encryption request is received during Secure Connections pairing. An attacker in radio range can have arbitrary read/write access to protected GATT service data, cause a device crash, or possibly control a device's function by	2020-02-12	not yet calculated	<a href="#">CVE-2019-19194</a> <a href="#">MISC</a> <a href="#">MISC</a>

	establishing an encrypted session with the zero LTK.			
telligent_systems -- telligent_community	XSS in Telligent Community 5.6 583.20496 via a flash file and related to the allowScriptAccess parameter.	2020-02-13	not yet calculated	<a href="#">CVE-2012-1903</a> MISC
tiki_wiki -- cms_groupware	A Cross-Site Scripting (XSS) vulnerability exists in Tiki Wiki CMG Groupware 11.0 via the id paraZeroClipboard swf, which could let a remote malicious user execute arbitrary code.	2020-02-12	not yet calculated	<a href="#">CVE-2013-6022</a> MISC
timetools -- multiple_deivces	TimeTools SC7105 1 0.007, SC9205 1.0 007, SC9705 1.0.007, SR7110 1.0 007, SR9210 1.0.007, SR9750 1.0 007, SR9850 1.0.007, T100 1.0.003, T300 1.0 003, and T550 1.0.003 devices allow remote attackers to bypass authentication by placing t3axs=TiMEtOOlsj7G3xMm52wB in a t3.cgi request, aka a "hardcoded cookie."	2020-02-13	not yet calculated	<a href="#">CVE-2020-8964</a> MISC
timetools -- multiple_deivces	TimeTools SC7105 1 0.007, SC9205 1.0 007, SC9705 1.0.007, SR7110 1.0 007, SR9210 1.0.007, SR9750 1.0 007, SR9850 1.0.007, T100 1.0.003, T300 1.0 003, and T550 1.0.003 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the t3.cgi srmodel or srtime parameter.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8963</a> MISC
trendnet -- ts- s402_devices	TRENDnet TS-S402 has a backdoor to enable TELNET.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6360</a> MISC
tri-plc -- internet_trilogi_server	Internet TRILOGI Server (unknown versions) could allow a local user to bypass security and create a local user account.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6927</a> MISC
umplayer -- umplayer	A Code Execution Vulnerability exists in UMPlayer 0 98 in wintab32 dll due to insufficient path restrictions when loading external libraries. which could let a malicious user execute arbitrary code.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3494</a> MISC
varnish_software -- varnish_http_cache	Varnish HTTP cache before 3.0.4: ACL bug	2020-02-12	not yet calculated	<a href="#">CVE-2013-4090</a> MISC
visual_it -- tube_map_live_underground	Tube Map Live Underground for Android before 0.22 has an Information Disclosure Vulnerability	2020-02-12	not yet calculated	<a href="#">CVE-2013-6681</a> MISC
voatz -- voatz_for_android	The Voatz application 2020-01-01 for Android allows only 100 million different PINs, which makes it easier for attackers (after using root access to make a copy of the local database) to discover login credentials and voting history via an offline brute-force approach.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8988</a> MISC
voatz -- voatz_for_android	In the Voatz application 2020-01-01 for Android, the amount of data transmitted during a single voter's vote depends on the different lengths of the metadata across the available voting choices, which makes it easier for remote attackers to discover this voter's choice by sniffing the network. For example, a small amount of sniffed data may indicate that a vote was cast for the candidate with the least metadata. An active man-in-the-middle attacker can leverage this behavior to disrupt voters' abilities to vote for a candidate opposed by the attacker.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8989</a> MISC
weechat - weechat	irc_mode_channel_update in plugins/irc-mode.c in WeeChat through 2.7 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a malformed IRC message 324 (channel mode).	2020-02-12	not yet calculated	<a href="#">CVE-2020-8955</a> MISC
wordpress -- wordpress	participants-database.php in the Participants Database plugin 1 9.5.5 and previous versions for WordPress has a time-based SQL injection vulnerability via the ascdesc, list_filter_count, or sortBy parameters. It is possible to exfiltrate data and potentially execute code (if certain conditions are met).	2020-02-11	not yet calculated	<a href="#">CVE-2020-8596</a> MISC
wordpress --	The Ninja Forms plugin 3.4.22 for WordPress has Multiple Stored XSS vulnerabilities via	2020-02-	not yet	<a href="#">CVE-2020-8594</a>



wordpress	ninja_forms[recaptcha_site_key], ninja_forms[recaptcha_secret_key], ninja_forms[recaptcha_lang], or ninja_forms[date_format].	14	calculator	<a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	Multiple SQL injection vulnerabilities in CWPPoll.js in WordPress Poll Plugin 34.5 for WordPress allow attackers to execute arbitrary SQL commands via the pollid or poll_id parameter in a viewPollResults or userlogs action.	2020-02-13	not yet calculator	<a href="#">CVE-2013-1400</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">BUGTRAQ</a>
wordpress -- wordpress	Multiple security bypass vulnerabilities in the editAnswer, deleteAnswer, addAnswer, and deletePoll functions in WordPress Poll Plugin 34.5 for WordPress allow a remote attacker to add, edit, and delete an answer and delete a poll.	2020-02-13	not yet calculator	<a href="#">CVE-2013-1401</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">BUGTRAQ</a>
wordpress -- wordpress	WordPress WP Cleanfix Plugin 2.4.4 has CSRF	2020-02-10	not yet calculator	<a href="#">CVE-2013-2108</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress plugin wp-cleanfix has Remote Code Execution	2020-02-10	not yet calculator	<a href="#">CVE-2013-2109</a> <a href="#">MISC</a> <a href="#">MISC</a>
xerox -- colorcube_and_workcenter	Xerox ColorCube and WorkCenter devices in 2013 had hardcoded FTP and shell user accounts.	2020-02-13	not yet calculator	<a href="#">CVE-2013-6362</a> <a href="#">MISC</a> <a href="#">MISC</a>
xilisoft -- video_converter_ultimate	Xilisoft Video Converter Ultimate 7.8.1 build-20140505 has a DLL Hijacking vulnerability	2020-02-12	not yet calculator	<a href="#">CVE-2014-3860</a> <a href="#">MISC</a>
zenoss -- zenoss_core	Multiple format string vulnerabilities in the python module in RRDtool, as used in Zenoss Core before 4.2.5 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted third argument to the rrdtool.graph function, aka ZEN-15415, a related issue to CVE-2013-2131.	2020-02-12	not yet calculator	<a href="#">CVE-2014-6262</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zimbra -- zimbra_collaboration	Zimbra 2013 has XSS in aspell php	2020-02-12	not yet calculator	<a href="#">CVE-2013-1938</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zpanel_project -- zpanel	ZPanel through 10.1.0 has Remote Command Execution	2020-02-12	not yet calculator	<a href="#">CVE-2013-2097</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [wgutarte@ci.sunnyvale.ca.us](mailto:wgutarte@ci.sunnyvale.ca.us) using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20508 · (888) 282-0870



**From:** US-CERT  
**To:** [incnms@sunwyale.ca.gov](mailto:incnms@sunwyale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of February 10, 2020  
**Date:** Monday, February 17, 2020 4:28:34 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

### Vulnerability Summary for the Week of February 10, 2020

02/17/2020 07:09 AM EST

Original release date: February 17, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	10	<a href="#">CVE-2020-3740</a> <a href="#">CONF RM</a>
ajaxexplorer -- ajaxexplorer	Ajaxexplorer before 5.0.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) archive_name parameter to the Power FS module (plugins/action.powerfs/class PowerFSController.php), a (2) file name to the getTrustSizeOnFileSystem function in the File System (Standard) module (plugins/access.fs/class.fsAccessWrapper.php), or the (3) revision parameter to the Subversion Repository module (plugins/meta.svn/class.SvnManager.php).	2020-02-11	10	<a href="#">CVE-2013-4267</a> MISC MISC MISC
artica -- pandora_fms	functions_netflow.php in Artica Pandora FMS 7.0 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the index.php?operation/netflow/nf_live_view ip_dst, dst_port, or src_port parameter, a different vulnerability than CVE-2019-20224.	2020-02-12	9	<a href="#">CVE-2020-8947</a> MISC MISC MISC
atutor -- atutor	confirm.php in ATutor 2.2 and earlier allows remote attackers to bypass authentication and gain access as an existing user via the auto_login parameter.	2020-02-11	7.5	<a href="#">CVE-2014-9753</a> MISC MISC MISC MISC
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	10	<a href="#">CVE-2013-3091</a> MISC MISC MISC
biscom -- secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1xxx before 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	7.5	<a href="#">CVE-2020-8796</a> MISC <a href="https://exchange.xforce.ibmcloud.com/vulnerabilities/175922">https://exchange.xforce.ibmcloud.com/vulnerabilities/175922</a>
bosch -- bvms_mobile_video_service	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	10	<a href="#">CVE-2020-6770</a> <a href="#">CONF RM</a>
canonical -- lxc	In LXC 2.0, many template scripts download code over cleartext HTTP, and omit a digital-signature check, before running it to bootstrap containers.	2020-02-10	9.3	<a href="#">CVE-2017-18641</a> MISC
corsair -- corsair_icue	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-	2020-02-		<a href="#">CVE-2020-8808</a>

	integrity level processes) to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.	07	7.2	MISC MISC
d-link -- multiple_products	Multiple SQL injection vulnerabilities in D-Link DSR-150 with firmware before 1.08B44; DSR-150N with firmware before 1.05B64; DSR-250 and DSR-250N with firmware before 1.08B44; and DSR-500, DSR-500N, DSR-1000, and DSR-1000N with firmware before 1.08B77 allow remote attackers to execute arbitrary SQL commands via the password to (1) the login.authenticate function in share/lua/5.1/teamf1lua/lib/login.lua or (2) captivePortal.lua.	2020-02-11	10	CVE-2013-5945 MISC MISC MISC MISC
dell -- multiple_products	An Authentication Bypass Vulnerability exists in DELL SonicWALL Analyzer 7.0, Global Management System (GMS) 4.1, 5.0, 5.1, 6 0, and 7.0; Universal Management Appliance (UMA) 5.1, 6 0, and 7 0 and ViewPoint 4.1, 5.0, 5.1, and 6.0 via the skipSessionCheck parameter to the UMA interface (/appliance/), which could let a remote malicious user obtain access to the root account.	2020-02-11	10	CVE-2013-1359 MISC MISC MISC MISC MISC MISC MISC
dell -- multiple_products	An Authentication Bypass vulnerability exists in DELL SonicWALL Global Management System (GMS) 4.1, 5.0, 5.1, 6.0, and 7 0, Analyzer 7.0, Universal Management Appliance (UMA) 5.1, 6 0, and 7 0 and ViewPoint 4.1, 5.0, 5.1, and 6.0 via a crafted request to the SGMS interface, which could let a remote malicious user obtain administrative access.	2020-02-11	10	CVE-2013-1360 MISC MISC MISC MISC MISC MISC
echoping_project -- echoping	echoping through 6.0 2 has buffer overflow vulnerabilities	2020-02-11	10	CVE-2013-4448 MISC MISC MISC
enorth -- enorth_webpublisher_cms	SQL injection vulnerability in pub/m_pending_news/delete_pending_news.jsp in Enorth Webpublisher CMS allows remote attackers to execute arbitrary SQL commands via the cbNewsId parameter.	2020-02-12	7.5	CVE-2015-5617 MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5 3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	9.3	CVE-2020-8655 MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5 3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php.	2020-02-07	7.5	CVE-2020-8656 MISC MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5 3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	9	CVE-2020-8654 MISC MISC
golang -- go	The net/http library in net/http/transfer.go in Go before 1.4 3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains Content-Length and Transfer-Encoding header fields.	2020-02-08	7.5	CVE-2015-5741 MISC MISC MISC MISC MISC MISC MISC
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	9	CVE-2014-7224 MISC MISC MISC MISC
google -- chrome	Use after free in audio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	9.3	CVE-2020-6406 SUSE MISC

				MISC
hubot_scripts -- hubot_scripts	scripts/email coffee in the Hubot Scripts module before 2.4.4 for Node.js allows remote attackers to execute arbitrary commands.	2020-02-12	7.5	<a href="#">CVE-2013-7378</a> MISC MISC MISC MISC
ibm -- sterling_authentication	A Command Execution Vulnerability exists in IBM Sterling External Authentication Server 2.2.0, 2.3.01, 2.4.0, and 2.4.1 via an unspecified OS command, which could let a local malicious user execute arbitrary code.	2020-02-11	7.2	<a href="#">CVE-2013-0517</a> MISC MISC
libnotify -- libnotify	libnotify before 1.0.4 for Node.js allows remote attackers to execute arbitrary commands via unspecified characters in a call to libnotify.notify.	2020-02-12	7.5	<a href="#">CVE-2013-7381</a> MISC MISC CONF RM MISC
linux -- linux_kernel	Buffer overflow in the auerswald_probe function in the Auerswald Linux USB driver for the Linux kernel before 2.6.27 allows physically proximate attackers to execute arbitrary code, cause a denial of service via a crafted USB device, or take full control of the system.	2020-02-11	7.2	<a href="#">CVE-2009-4067</a> MISC MISC
Istio -- Istio	Istio 1.3 through 1.4.3 allows authentication bypass. The Authentication Policy exact-path matching logic can allow unauthorized access to HTTP paths even if they are configured to be only accessed after presenting a valid JWT token. For example, an attacker can add a ? or # character to a URI that would otherwise satisfy an exact-path match.	2020-02-12	7.5	<a href="#">CVE-2020-8595</a> REDHAT CONF RM MISC MISC MISC CONF RM
mediawiki -- mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	9.3	<a href="#">CVE-2012-4381</a> MISC MISC MISC MISC MISC MISC
microsoft -- multiple_internet_explorer_products	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0674</a> MISC
microsoft -- multiple_internet_explorer_products	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0673</a> MISC
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0711</a> MISC
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713.	2020-02-11	7.6	<a href="#">CVE-2020-0767</a> MISC
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0712</a> MISC
	A remote code execution vulnerability			



microsoft -- chakacore	exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0711, CVE-2020-0712, CVE-2020-0713, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0710 MISC</a>
microsoft -- chakacore	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE D is unique from CVE-2020-0673, CVE-2020-0674, CVE-2020-0710, CVE-2020-0711, CVE-2020-0712, CVE-2020-0767.	2020-02-11	7.6	<a href="#">CVE-2020-0713 MISC</a>
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'.	2020-02-11	9.3	<a href="#">CVE-2020-0759 MISC</a>
microsoft -- multiple_microsoft_exchange_server_products	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.	2020-02-11	9	<a href="#">CVE-2020-0688 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0720 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE D is unique from CVE-2020-0683.	2020-02-11	7.2	<a href="#">CVE-2020-0686 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE D is unique from CVE-2020-0734.	2020-02-11	7.6	<a href="#">CVE-2020-0681 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in Remote Desktop Services "formerly known as Terminal Services" when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.	2020-02-11	8.5	<a href="#">CVE-2020-0655 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows improperly handles Secure Socket Shell remote commands, aka 'Windows SSH Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0757 MISC</a>
microsoft -- multiple_windows_products	A memory corruption vulnerability exists when Windows Media Foundation improperly handles objects in memory, aka 'Media Foundation Memory Corruption Vulnerability'.	2020-02-11	9.3	<a href="#">CVE-2020-0738 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the way that Windows handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'.	2020-02-11	9	<a href="#">CVE-2020-0662 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows Error Reporting Manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0678 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726.	2020-02-11	7.2	<a href="#">CVE-2020-0731 MISC</a>
	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle			

microsoft -- multiple_windows_products	objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0725</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0671, CVE-2020-0672.	2020-02-11	7.2	<a href="#">CVE-2020-0670</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0726</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0792.	2020-02-11	7.2	<a href="#">CVE-2020-0745</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-0681.	2020-02-11	9.3	<a href="#">CVE-2020-0734</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0723</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0719</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0680.	2020-02-11	7.2	<a href="#">CVE-2020-0682</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0671.	2020-02-11	7.2	<a href="#">CVE-2020-0672</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the Windows Installer when MSI packages process symbolic links, aka 'Windows Installer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0686.	2020-02-11	7.2	<a href="#">CVE-2020-0683</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Wireless Network Manager improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Wireless Network Manager Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0704</a> <a href="#">MISC</a>
	An elevation of privilege vulnerability			

microsoft -- multiple_windows_products	exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0722</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows IME improperly handles memory. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows IME Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0707</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows improperly handles COM object creation, aka 'Windows COM Server Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0685</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0721</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Backup Service improperly handles file operations. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Backup Service Elevation of Privilege Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0703</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0669, CVE-2020-0670, CVE-2020-0672.	2020-02-11	7.2	<a href="#">CVE-2020-0671</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0691, CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	7.2	<a href="#">CVE-2020-0724</a> MISC
microsoft -- office365_proplus_for_32-bit_and_64-bit_systems	An elevation of privilege vulnerability exists in Microsoft Office OLicenseHeartbeat task, where an attacker who successfully exploited this vulnerability could run this task as SYSTEM. To exploit the vulnerability, an authenticated attacker would need to place a specially crafted file in a specific location, thereby allowing arbitrary file corruption. The security update addresses the vulnerability by correcting how the process validates the log file., aka 'Microsoft Office Tampering Vulnerability'.	2020-02-11	7.2	<a href="#">CVE-2020-0697</a> MISC
microsoft -- windows_10_and_windows_server_2016	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0715, CVE-2020-0745.	2020-02-11	7.2	<a href="#">CVE-2020-0792</a> MISC
microsoft -- windows_10_and_windows_server_2016	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0732.	2020-02-11	7.2	<a href="#">CVE-2020-0709</a> MISC
microsoft -- windows_10_and_windows_server_2016	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0709.	2020-02-11	7.2	<a href="#">CVE-2020-0732</a> MISC
	An issue was discovered in Microvirt MEmu all versions prior to 7.0.2. A guest			

microvirt -- memu	Android operating system inside the MEmu emulator contains a /system/bin/systemd binary that is run with root privileges on startup (this is unrelated to Red Hat's systemd init program, and is a closed-source proprietary tool that seems to be developed by Microvirt). This program opens TCP port 21509, presumably to receive installation-related commands from the host OS. Because everything after the installer:uninstall command is concatenated directly into a system() call, it is possible to execute arbitrary commands by supplying shell metacharacters.	2020-02-11	10	<a href="#">CVE-2019-14514</a> MISC
netgear -- ac1200_smart_wifi_router	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR AC1200 R6220 Firmware version 1.1 0.86 Smart WiFi Router. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of path strings. By inserting a null byte into the path, the user can skip most authentication checks. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-8616.	2020-02-10	7.5	<a href="#">CVE-2019-17137</a> MISC
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1 2.31805 and V2 2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracer diagnostic tool because of lack of user input sanitizing.	2020-02-07	8.5	<a href="#">CVE-2019-19356</a> MISC MISC
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	7.5	<a href="#">CVE-2019-15605</a> MISC FEDORA CONF RM CONF RM CONF RM
nodejs -- nodejs	Including trailing white space in HTTP header values in Node.js 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	7.5	<a href="#">CVE-2019-15606</a> MISC CONF RM CONF RM CONF RM
nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	7.5	<a href="#">CVE-2014-9530</a> CONF RM
omniauth-weibo-oauth2_gem_for_ruby - omniauth-weibo-oauth2_gem_for_ruby	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	7.5	<a href="#">CVE-2019-17268</a> MISC CONF RM
openpne -- opopensocialplugin	opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple XML External Entity Injection Vulnerabilities	2020-02-07	7.5	<a href="#">CVE-2013-4335</a> MISC MISC MISC
openpne -- opwebapiplugin	opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	7.5	<a href="#">CVE-2013-4334</a> MISC MISC
phxeventmanager -- phxeventmanager	SQL injection vulnerability in search.php in phxEventManager 2.0 beta 5 allows remote attackers to execute arbitrary SQL commands via the search_terms parameter.	2020-02-11	7.5	<a href="#">CVE-2012-1124</a> MISC MISC MISC MISC
polarbear -- polarbear_cms	A PHP File Upload Vulnerability exists in PolarBear CMS 2.5 via upload.php, which could let a malicious user execute arbitrary code.	2020-02-11	7.5	<a href="#">CVE-2013-0803</a> MISC MISC MISC
polycomm -- web_management_interface_g3/hdx_800_hd	An issue was discovered in Polycom Web Management Interface G3/HDX 8000 HD with Durango 2.6.0 4740 software and embedded Polycom Linux Development	2020-02-	10	<a href="#">CVE-2012-6611</a>



	Platform 2.14.g3. It has a blank administrative password by default, and can be successfully used without setting this password.	10		<a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	The virtqueue_map_sg function in hw/virtio/virtio.c in QEMU before 1.7.2 allows remote attackers to execute arbitrary files via a crafted savevm image, related to virtio-block or virtio-serial read.	2020-02-11	<a href="#">7.2</a>	<a href="#">CVE-2013-4535</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open close in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14044</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14002</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14088</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14046</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	Stage-2 fault will occur while writing to an ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14049</a> <a href="#">CONF RM</a>
qualcomm -- multiple_snapdragon_products	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14055</a> <a href="#">CONF RM</a>

qualcomm -- multiple_snapdragon_p	Uninitialized stack data gets used If memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14060</a> CONF RM
qualcomm -- multiple_snapdragon_p	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> CONF RM
qualcomm -- multiple_snapdragon_p	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> CONF RM
qualcomm -- multiple_snapdragon_p	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	2020-02-07	9.4	<a href="#">CVE-2019-14057</a> CONF RM

	SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	Out of bound access due to Invalid inputs to dpm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon IoT & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14063</a> <a href="#">CONF RM</a>
qualcomm -- snapdragon_industrial_products	Subsequent additions performed during Module loading while allocating the memory would lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	7.2	<a href="#">CVE-2019-14061</a> <a href="#">CONF RM</a>
ruby_pdfkit_gem_for_ruby_on_rails -- ruby_pdfkit_gem_for_ruby_on_rails	Ruby PDFKit gem prior to 0.5.3 has a Code Execution Vulnerability	2020-02-11	7.5	<a href="#">CVE-2013-1607</a> <a href="#">MISC</a> <a href="#">MISC</a>
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, contains a vulnerability of Pre-auth SQL Injection, allowing attackers to inject a specific SQL command.	2020-02-11	7.5	<a href="#">CVE-2020-3934</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
siemens -- multiple_scalance_products	A vulnerability has been identified in SCALANCE S602 (All versions >= V3.0), SCALANCE S612 (All versions >= V3.0), SCALANCE S623 (All versions >= V3.0), SCALANCE S627-2M (All versions >= V3.0). Specially crafted packets sent to port 443/tcp of affected devices could cause a Denial-of-Service condition of the web server. A cold reboot is required to restore the functionality of the device.	2020-02-11	7.8	<a href="#">CVE-2019-13926</a> <a href="#">MISC</a>
simplejobscrip -- simplejobscrip	An issue was discovered in Simplejobscrip.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	7.5	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
sphider -- sphider_pro_and_sphider_plus	A Command Execution vulnerability exists in Sphider Pro, and Sphider Plus 3 2 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5086 pertains to instances of fwrite in Sphider Pro and Sphider Plus only, but don't exist in Sphider.	2020-02-10	7.5	<a href="#">CVE-2014-5086</a> <a href="#">MISC</a>
sphider -- sphider_search_engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 due to exec calls in admin/spiderfuncs.php, which could let a remote malicious user execute arbitrary code.	2020-02-07	7.5	<a href="#">CVE-2014-5087</a> <a href="#">MISC</a> <a href="#">MISC</a>
status2k -- server_monitoring_software	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multiplies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	10	<a href="#">CVE-2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ui -- edgswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	7.2	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress W3 Total Cache Plugin 0.9 2.8 has a Remote PHP Code Execution Vulnerability	2020-02-12	7.5	<a href="#">CVE-2013-2010</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	NextGEN Gallery plugin before 1.9.13 for WordPress: nggallery.php file upload	2020-02-11	10	<a href="#">CVE-2013-3684</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress --	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0 0 for	2020-02-		<a href="#">CVE-2014-8739</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

wordpress	WordPress and before 2 0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	08	<a href="#">7.5</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
yabb -- yabb	YaBB through 2.5.2: 'guestlanguage' Cookie Parameter Local File Include Vulnerability	2020-02-11	<a href="#">7.5</a>	<a href="#">CVE-2013-2057</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zend_framework -- zend_framework	Zend Framework, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	2020-02-11	<a href="#">7.5</a>	<a href="#">CVE-2014-2052</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3733</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3731</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3721</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3739</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3738</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3728</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3736</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3735</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3734</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3732</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3737</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3730</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3729</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3727</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	<a href="#">6.8</a>	<a href="#">CVE-2020-3726</a> <a href="#">CONF RM</a>



adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3725</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3724</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3723</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3722</a> <a href="#">CONF RM</a>
adobe -- framemaker	Adobe Framemaker versions 2019 0.4 and below have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	6.8	<a href="#">CVE-2020-3720</a> <a href="#">CONF RM</a>
apple -- ios_and_os_x	LibTIFF prior to 4.0.4, as used in Apple iOS before 8.4 and OS X before 10.10.4 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted TIFF image.	2020-02-12	4.3	<a href="#">CVE-2014-8128</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira_server_and_data_center	The VerifyPopServerConnection!add jsps component in Atlassian Jira Server and Data Center before version 8.7.0 is vulnerable to cross-site request forgery (CSRF). An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	6.8	<a href="#">CVE-2019-20099</a> <a href="#">N/A</a> <a href="#">N/A</a>
atlassian -- jira_server_and_data_center	The VerifySmtServerConnection!add jsps component in Atlassian Jira Server and Data Center before version 8.7.0 is vulnerable to cross-site request forgery (CSRF). An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	6.8	<a href="#">CVE-2019-20098</a> <a href="#">N/A</a> <a href="#">N/A</a>
blackberry -- playbook	BlackBerry PlayBook before 2.1 has an Information Disclosure Vulnerability via a Web browser component error	2020-02-10	4.3	<a href="#">CVE-2012-5828</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	4	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>
bosch -- multiple_products	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR P 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-07	5	<a href="#">CVE-2020-6768</a> <a href="#">CONF RM</a>
bosch -- video_streaming_gateway_and_divar_ip	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This	2020-02-07	6.4	<a href="#">CVE-2020-6769</a> <a href="#">CONF RM</a>

	affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR P all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR P 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.			
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	4.6	<a href="#">CVE-2019-11484</a> MISC MISC
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	6.1	<a href="#">CVE-2019-11481</a> MISC MISC
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	6.8	<a href="#">CVE-2020-1700</a> SUSE CONF RM
chamilo -- chamilo_lms	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	4.3	<a href="#">CVE-2012-4029</a> MISC MISC MISC
cisco -- application_control_engine	Cisco ACE A2(3.6) allows log retention DOS.	2020-02-07	5	<a href="#">CVE-2013-1202</a> MISC
clearcanvas -- clearcanvas	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	4.3	<a href="#">CVE-2020-8788</a> MISC
cypress -- psoc_4_devices	The Bluetooth Low Energy (BLE) stack implementation on Cypress PSoC 4 through 3.62 devices does not properly restrict the BLE Link Layer header and executes certain memory contents upon receiving a packet with a Link Layer D (LLID) equal to zero. This allows attackers within radio range to cause deadlocks, cause anomalous behavior in the BLE state machine, or trigger a buffer overflow via a crafted BLE Link Layer frame.	2020-02-10	6.1	<a href="#">CVE-2019-17061</a> MISC MISC
d-link -- dir865l_devices	D-Link DIR865L v1 03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	4.3	<a href="#">CVE-2013-3096</a> MISC MISC MISC
daum_communications -- potplayer	Potplayer prior to 1 5.39659: DLL Loading Arbitrary Code Execution Vulnerability	2020-02-11	6.8	<a href="#">CVE-2013-3942</a> MISC MISC
dialog -- da14580/1/2/3_devices	The Bluetooth Low Energy implementation on Dialog Semiconductor SDK through 5.0.4 for DA14580/1/2/3 devices does not properly restrict the L2CAP payload length, allowing attackers in radio range to cause a buffer overflow via a crafted Link Layer packet.	2020-02-10	6.1	<a href="#">CVE-2019-17517</a> MISC MISC
dialog -- da1468x_devices	The Bluetooth Low Energy implementation on Dialog Semiconductor SDK through 1.0.14.1081 for DA1468x devices responds to link layer packets with a payload length larger than expected, allowing attackers in radio range to cause a buffer overflow via a crafted packet. This affects, for example, August Smart Lock.	2020-02-10	6.1	<a href="#">CVE-2019-17518</a> MISC MISC
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container Ds.	2020-02-07	4.3	<a href="#">CVE-2014-5278</a> MISC MISC MISC

drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access_basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	4	<a href="#">CVE-2012-5570</a> MISC MISC MISC CONFIRM
filemaker -- filemaker_pro_and_filemaker_pro_advanced	An Authentication Bypass vulnerability exists in the MatchPasswordData function in DBEngine.dll in Filemaker Pro 13.03 and Filemaker Pro Advanced 12.04, which could let a malicious user obtain elevated privileges.	2020-02-11	4.6	<a href="#">CVE-2014-8347</a> MISC MISC MISC MISC
flowplayer -- flowplayer_flash	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	6.8	<a href="#">CVE-2011-3642</a> MISC MISC MISC MISC MISC MISC MISC MISC
fork -- fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	4.3	<a href="#">CVE-2014-9470</a> MISC MISC MISC MISC MISC
fortiguard -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctsched process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	6.6	<a href="#">CVE-2019-16155</a> MISC CONFIRM
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	6.8	<a href="#">CVE-2019-13333</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	6.8	<a href="#">CVE-2019-13334</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	6.8	<a href="#">CVE-2019-17135</a> MISC

foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	6.8	<a href="#">CVE-2019-17136</a> MISC
gizmo5 -- gizmo5	The S P implementation on the Gizmo5 software phone provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "S P Digest Leak" issue.	2020-02-12	4.3	<a href="#">CVE-2009-5139</a> MISC MISC
google -- chrome	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6414</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.	2020-02-11	4.3	<a href="#">CVE-2020-6392</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6393</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6415</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass HTML validators via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6413</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in navigation in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to confuse the user via a crafted domain name.	2020-02-11	6.8	<a href="#">CVE-2020-6410</a> SUSE MISC MISC
google -- chrome	Inappropriate implementation in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker who convinced the user to enter a URI to bypass navigation restrictions via a crafted domain name.	2020-02-11	6.8	<a href="#">CVE-2020-6409</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2020-02-11	6.8	<a href="#">CVE-2020-6402</a> SUSE MISC MISC
google -- chrome	Use after free in V8 in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6379</a> MISC MISC
google -- chrome	Type confusion in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6382</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in storage in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass site isolation via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6385</a> SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.130 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted Chrome Extension.	2020-02-11	6.8	<a href="#">CVE-2020-6380</a> MISC MISC
	Integer overflow in JavaScript in Google			<a href="#">CVE-2020-</a>



google -- chrome	Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6381</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use of uninitialized data in PDFium in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2020-02-11	6.8	<a href="#">CVE-2020-6398</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6390</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.	2020-02-11	6.8	<a href="#">CVE-2020-6389</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds access in WebAudio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6388</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.	2020-02-11	6.8	<a href="#">CVE-2020-6387</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	5.8	<a href="#">CVE-2020-6412</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use after free in speech in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6378</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient data validation in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-02-11	6.8	<a href="#">CVE-2020-6416</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	5.8	<a href="#">CVE-2020-6411</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in installer in Google Chrome prior to 80.0.3987.87 allowed a local attacker to execute arbitrary code via a crafted registry entry.	2020-02-11	4.6	<a href="#">CVE-2020-6417</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to potentially exploit heap corruption via crafted clipboard content.	2020-02-11	4.6	<a href="#">CVE-2020-6404</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2020-02-11	5.8	<a href="#">CVE-2020-6394</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Insufficient validation of untrusted input in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to bypass content security policy via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6391</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds read in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6395</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in Skia in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6396</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in sharing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.	2020-02-11	4.3	<a href="#">CVE-2020-6397</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Inappropriate implementation in CORS in Google Chrome prior to 80.0.3987.87	2020-02-		<a href="#">CVE-2020-6400</a>

	allowed a remote attacker to leak cross-origin data via a crafted HTML page.	11	4.3	SUSE MISC MISC
google -- chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2020-02-11	4.3	CVE-2020-6401 SUSE MISC MISC
google -- chrome	Incorrect implementation in Omnibox in Google Chrome on iOS prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2020-02-11	4.3	CVE-2020-6403 SUSE MISC MISC
google -- chrome	Out of bounds read in SQLite in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2020-02-11	4.3	CVE-2020-6405 SUSE MISC MISC
google -- chrome	Insufficient policy enforcement in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2020-02-11	4.3	CVE-2020-6399 SUSE MISC MISC
hp -- system_event_utility	A potential security vulnerability has been identified with certain versions of HP System Event Utility prior to version 1.4.33. This vulnerability may allow a local attacker to execute arbitrary code via an HP System Event Utility system service.	2020-02-13	4.6	CVE-2019-18915 FULLDISC MISC
htmlunit -- htmlunit	HtmlUnit prior to 2.37.0 contains code execution vulnerabilities. HtmlUnit initializes Rhino engine improperly, hence a malicious JavaScript code can execute arbitrary Java code on the application. Moreover, when embedded in Android application, Android-specific initialization of Rhino engine is done in an improper way, hence a malicious JavaScript code can execute arbitrary Java code on the application.	2020-02-11	6.8	CVE-2020-5529 CONF RM JVN
ibm -- cloud_cli	IBM Cloud CLI 0.6.0 through 0.16.1 windows installers are signed using SHA1 certificate. An attacker might be able to exploit the weak algorithm to generate a installer with malicious software inside. IBM X-Force ID: 162773.	2020-02-12	5	CVE-2019-4427 XF CONF RM
ibm -- content_navigator	IBM Content Navigator 3.0CD is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 172815.	2020-02-12	5	CVE-2019-4741 XF CONF RM
ibm -- infosphere_guardium	InfoSphere Guardium aix_ktap module: DoS	2020-02-10	4.9	CVE-2012-2204 MISC
ispconfig -- ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	6.5	CVE-2013-3629 MISC MISC MISC MISC
jenkins -- jenkins	A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2020-02-12	4	CVE-2020-2118 MLIST CONF RM
jenkins -- jenkins	Jenkins NUnit Plugin 0.25 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks.	2020-02-12	6.5	CVE-2020-2115 MLIST CONF RM
jenkins -- jenkins	Jenkins ECX Copy Data Management Plugin 1.9 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	4	CVE-2020-2128 MLIST CONF RM
jenkins -- jenkins	Jenkins FitNesse Plugin 1.30 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks.	2020-02-12	6.5	CVE-2020-2120 MLIST CONF RM
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers	2020-02-		CVE-2020-2116

	to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	12	<a href="#">6.8</a>	<a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	A missing permission check in Jenkins Pipeline GitHub Notify Step Plugin 1.0.4 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2117</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Debian Package Builder Plugin 1.6.11 and earlier stores a GPG passphrase unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2125</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Google Kubernetes Engine Plugin 0.8.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	2020-02-12	<a href="#">6.5</a>	<a href="#">CVE-2020-2121</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins DigitalOcean Plugin 1.1 and earlier stores a token unencrypted in the global config.xml file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2126</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins BMC Release Package and Deployment Plugin 1.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2127</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Applatix Plugin 1.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2133</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Eagle Tester Plugin 1.0.9 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2129</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Sandbox protection in Jenkins Script Security Plugin 1.69 and earlier could be circumvented during the script compilation phase by applying AST transforming annotations to imports or by using them inside of other annotations.	2020-02-12	<a href="#">6.5</a>	<a href="#">CVE-2020-2110</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Sandbox protection in Jenkins Pipeline: Groovy Plugin 2.78 and earlier can be circumvented through default parameter expressions in CPS-transformed methods.	2020-02-12	<a href="#">6.5</a>	<a href="#">CVE-2020-2109</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores a password unencrypted in its global configuration file on the Jenkins master where it can be viewed by users with access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2130</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Harvest SCM Plugin 0.5.1 and earlier stores passwords unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2131</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins S3 publisher Plugin 0.11.4 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	2020-02-12	<a href="#">5</a>	<a href="#">CVE-2020-2114</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Azure AD Plugin 1.1.2 and earlier transmits configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	2020-02-12	<a href="#">5</a>	<a href="#">CVE-2020-2119</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Parasoft Environment Manager Plugin 2.14 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can be viewed by users with Extended Read permission, or access to the master file system.	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2132</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and earlier stores a password unencrypted in job config.xml files on the Jenkins master where it can	2020-02-12	<a href="#">4</a>	<a href="#">CVE-2020-2124</a> <a href="#">MLIST</a>

	be viewed by users with Extended Read permission, or access to the master file system.			<a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins RadarGun Plugin 1.7 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability.	2020-02-12	<a href="#">6.5</a>	<a href="#">CVE-2020-2123</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
kemp_technologies -- loadmaster	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	<a href="#">6.8</a>	<a href="#">CVE-2014-5288</a> <a href="#">MISC</a> <a href="#">MISC</a>
konqueror -- konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	<a href="#">6.8</a>	<a href="#">CVE-2012-4512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgd -- libgd	gdImageClone in gd.c in libgd 2.1.0-rc2 through 2.2.5 has a NULL pointer dereference allowing attackers to crash an application via a specific function call sequence. Only affects PHP when linked with an external libgd (not bundled).	2020-02-11	<a href="#">5</a>	<a href="#">CVE-2018-14553</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys -- spa2102_devices	The S P implementation on the Linksys SPA2102 phone adapter provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "S P Digest Leak" issue.	2020-02-12	<a href="#">4.3</a>	<a href="#">CVE-2009-5140</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	The int3 handler in the Linux kernel before 3.3 relies on a per-CPU debug stack, which allows local users to cause a denial of service (stack corruption and panic) via a crafted application that triggers certain lock contention.	2020-02-12	<a href="#">4.9</a>	<a href="#">CVE-2012-0810</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
linuxmint -- linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	<a href="#">5</a>	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint -- linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	<a href="#">5</a>	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Upload Center Forms Component of Web File Manager in Rumpus FTP 8.2.9.1. This could allow an attacker to delete, create, and update the upload forms via RAPR/TriggerServerFunction.html.	2020-02-10	<a href="#">5.8</a>	<a href="#">CVE-2019-19669</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Block Clients component of Web File Manager in Rumpus FTP 8.2.9.1 that could allow an attacker to whitelist or block any IP address via RAPR/BlockedClients.html.	2020-02-10	<a href="#">5.8</a>	<a href="#">CVE-2019-19667</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the File Types component of Web File Manager in Rumpus FTP 8.2.9.1 that allows an attacker to add or delete the file types that are used on the server via RAPR/TriggerServerFunction.html.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19668</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the FTP Settings of Web File Manager in Rumpus FTP 8.2.9.1. Exploitation of this vulnerability can result in manipulation of Server FTP settings at RAPR/FTPSettingsSet.html.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19665</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A Cookie based reflected XSS exists in the Web File Manager of Rumpus FTP Server 8.2.9.1, related to RumpusLoginUserName and snp.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19661</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Folder Sets Settings of Web File Manager in Rumpus FTP 8.2.9.1. This allows an attacker to Create/Delete Folders after exploiting it at RAPR/FolderSetsSet.html.	2020-02-10	<a href="#">5.8</a>	<a href="#">CVE-2019-19663</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Event Notices Settings of Web File Manager in Rumpus FTP 8.2.9.1. An attacker can create/update event notices via	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2019-19666</a> <a href="#">MISC</a> <a href="#">MISC</a>



	RAPR/EventNoticesSet.html.			
maxum_development corporation - rumpus_ftp	A CSRF vulnerability exists in the Web File Manager's Network Setting functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can manipulate the SMTP setting and other network settings via RAPR/NetworkSettingsSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19660</a> MISC MISC
maxum_development corporation - rumpus_ftp	A HTTP Response Splitting vulnerability was identified in the Web Settings Component of Web File Manager in Rumpus FTP Server 8.2.9.1. A successful exploit can result in stored XSS, website defacement, etc. via ExtraHTTPHeader to RAPR/WebSettingsGeneralSet.html.	2020-02-10	4.3	<a href="#">CVE-2019-19670</a> MISC MISC
maxum_development corporation - rumpus_ftp_server	A CSRF vulnerability exists in the Web File Manager's Edit Accounts functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can take over a user account by changing the password, update users' details, and escalate privileges via RAPR/DefineUsersSet.html.	2020-02-10	6.8	<a href="#">CVE-2019-19659</a> MISC MISC
mfscripts -- yetishare	MFScripts YetiShare v3 5 2 through v4 5 4 might allow an attacker to reset a password by using a leaked hash (the hash never expires until used).	2020-02-10	5	<a href="#">CVE-2019-20062</a> MISC MISC MISC
mfscripts -- yetishare	MFScripts YetiShare v3 5 2 through v4 5 4 places sensitive information in the Referer header. If this leaks, then third parties may discover password-reset hashes, file-delete links, or other sensitive information.	2020-02-10	5	<a href="#">CVE-2019-20060</a> MISC MISC MISC
mfscripts -- yetishare	The user-introduction email in MFScripts YetiShare v3 5 2 through v4 5 4 may leak the (system-picked) password if this email is sent in cleartext. In other words, the user is not allowed to choose their own initial password.	2020-02-10	5	<a href="#">CVE-2019-20061</a> MISC MISC MISC
mfscripts -- yetishare	payment_manage.ajax.php and various *_manage.ajax.php in MFScripts YetiShare 3 5 2 through 4 5 4 directly insert values from the sSortDir_0 parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection. NOTE: this issue exists because of an incomplete fix for CVE-2019-19732.	2020-02-10	6.8	<a href="#">CVE-2019-20059</a> MISC MISC MISC MISC
microchip_technology -- atsamb11_devices	The Bluetooth Low Energy implementation on Microchip Technology BluSDK Smart through 6.2 for ATSAMB11 devices does not properly restrict link-layer data length on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.	2020-02-10	6.1	<a href="#">CVE-2019-19195</a> MISC MISC
microsoft -- edge	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain. In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'.	2020-02-11	4	<a href="#">CVE-2020-0663</a> MISC
microsoft -- exchange_server_2013, and 2016 and 2019	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0692</a> MISC
microsoft -- internet_explorer_10_and_11	An information disclosure vulnerability exists in the way that affected Microsoft Internet Explorer handles cross-origin requests, aka 'Microsoft Browser Information Disclosure Vulnerability'.	2020-02-11	4.3	<a href="#">CVE-2020-0706</a> MISC
microsoft -- malicious_software_removal_tool	An elevation of privilege vulnerability exists when the Windows Malicious Software Removal Tool (MSRT) improperly handles junctions. To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Malicious Software Removal Tool Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0733</a> MISC
microsoft --	A security feature bypass vulnerability exists in Microsoft Outlook software when			<a href="#">CVE-2020-</a>

multiple_products	it improperly handles the parsing of URI formats, aka 'Microsoft Outlook Security Feature Bypass Vulnerability'.	2020-02-11	4.3	<a href="#">0696 MISC</a>
microsoft -- multiple_windows_products	A security feature bypass vulnerability exists in secure boot, aka 'Microsoft Secure Boot Security Feature Bypass Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0689 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0679, CVE-2020-0682.	2020-02-11	4.6	<a href="#">CVE-2020-0680 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0735 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0668, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.	2020-02-11	4.6	<a href="#">CVE-2020-0669 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Client License Service (ClipSVC) handles objects in memory, aka 'Windows Client License Service Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0701 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0740 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the tapisrv.dll handles objects in memory, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0739.	2020-02-11	4.6	<a href="#">CVE-2020-0737 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749.	2020-02-11	4.6	<a href="#">CVE-2020-0750 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the dssvc.dll handles file creation allowing for a file overwrite or creation in a secured location, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0737.	2020-02-11	4.6	<a href="#">CVE-2020-0739 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0669, CVE-2020-0670, CVE-2020-0671, CVE-2020-0672.	2020-02-11	4.6	<a href="#">CVE-2020-0668 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0742, CVE-2020-0743, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0741 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-	2020-02-11	4.6	<a href="#">CVE-2020-0742 MISC</a>

	2020-0743, CVE-2020-0749, CVE-2020-0750.			
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0749, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0743</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0659.	2020-02-11	4.6	<a href="#">CVE-2020-0747</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Connected Devices Platform Service handles objects in memory, aka 'Connected Devices Platform Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0740, CVE-2020-0741, CVE-2020-0742, CVE-2020-0743, CVE-2020-0750.	2020-02-11	4.6	<a href="#">CVE-2020-0749</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0667, CVE-2020-0735.	2020-02-11	4.6	<a href="#">CVE-2020-0752</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Function Discovery Service handles objects in memory, aka 'Windows Function Discovery Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0680, CVE-2020-0682.	2020-02-11	4.6	<a href="#">CVE-2020-0679</a> MISC
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'.	2020-02-11	5	<a href="#">CVE-2020-0746</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0665</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0754.	2020-02-11	4.6	<a href="#">CVE-2020-0753</a> MISC
microsoft -- multiple_windows_products	A remote code execution vulnerability exists in Microsoft Windows that could allow remote code execution if a .LNK file is processed. An attacker who successfully exploited this vulnerability could gain the same user rights as the local user, aka 'LNK Remote Code Execution Vulnerability'.	2020-02-11	6.8	<a href="#">CVE-2020-0729</a> MISC
microsoft -- multiple_windows_products	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	2020-02-11	5	<a href="#">CVE-2020-0660</a> MISC
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2020-0751.	2020-02-11	5.5	<a href="#">CVE-2020-0661</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Common Log File System (CLFS) driver improperly handles objects in memory, aka 'Windows Common Log File System Driver Elevation of Privilege Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0657</a> MISC

microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka 'Windows Data Sharing Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0747.	2020-02-11	4.6	<a href="#">CVE-2020-0659</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0667, CVE-2020-0735, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0666</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in the way that the Windows Search Indexer handles objects in memory, aka 'Windows Search Indexer Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0666, CVE-2020-0735, CVE-2020-0752.	2020-02-11	4.6	<a href="#">CVE-2020-0667</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0753.	2020-02-11	4.6	<a href="#">CVE-2020-0754</a> MISC
microsoft -- sql_server_2012_and_2014_and_2016	A remote code execution vulnerability exists in Microsoft SQL Server Reporting Services when it incorrectly handles page requests, aka 'Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability'.	2020-02-11	6.5	<a href="#">CVE-2020-0618</a> MISC
microsoft -- surface_hub	A security feature bypass vulnerability exists in Surface Hub when prompting for credentials, aka 'Surface Hub Security Feature Bypass Vulnerability'.	2020-02-11	4.6	<a href="#">CVE-2020-0702</a> MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It mishandled time skew (between the machine hosting the web server and the machine hosting the database) when trying to block a brute-force series of invalid requests.	2020-02-12	4.3	<a href="#">CVE-2020-8890</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It did not canonicalize usernames when trying to block a brute-force series of invalid requests.	2020-02-12	4.3	<a href="#">CVE-2020-8891</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. It did not consider the HTTP PUT method when trying to block a brute-force series of invalid requests.	2020-02-12	6.8	<a href="#">CVE-2020-8892</a> MISC MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. The Galaxy view contained an incorrectly sanitized search string in app/View/Galaxies/view.ctp.	2020-02-12	5	<a href="#">CVE-2020-8893</a> MISC MISC
misp_project -- misp	An issue was discovered in MISP before 2.4.121. ACLs for discussion threads were mishandled in app/Controller/ThreadsController.php and app/Model/Thread.php.	2020-02-12	6.4	<a href="#">CVE-2020-8894</a> MISC MISC
netcracker -- netcracker_resource_management	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h, (3) %2427, (3) h, (4) %2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	6.5	<a href="#">CVE-2015-3423</a> MISC MISC
netsurf -- libnsbmp	Heap-based buffer overflow in the bmp_decode_rle function in libnsbmp.c in Libnsbmp 0.1.2 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the last row of RLE data in a crafted BMP file.	2020-02-12	6.8	<a href="#">CVE-2015-7508</a> MISC MISC
node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	5	<a href="#">CVE-2019-15604</a> MISC CONF RM CONF RM CONF RM



nxp -- kw41z_devices	The Bluetooth Low Energy (BLE) stack implementation on the NXP KW41Z (based on the MCUXpresso SDK with Bluetooth Low Energy Driver 2.1 and earlier) does not properly restrict the BLE Link Layer header and executes certain memory contents upon receiving a packet with a Link Layer D (LL D) equal to zero. This allows attackers within radio range to cause deadlocks, cause anomalous behavior in the BLE state machine, or trigger a buffer overflow via a crafted BLE Link Layer frame.	2020-02-10	6.1	<a href="#">CVE-2019-17060</a> MISC MISC
oberhumer -- libzo2_and_lzo-2	Integer overflow in the LZO algorithm variant in Oberhumer libzo2 and lzo-2 before 2.07 on 32-bit platforms might allow remote attackers to execute arbitrary code via a crafted Literal Run.	2020-02-12	6.8	<a href="#">CVE-2014-4607</a> MISC CONF RM
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	4	<a href="#">CVE-2014-9127</a> MISC
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the VII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	4.3	<a href="#">CVE-2014-9126</a> MISC
openfiler -- openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	4.3	<a href="#">CVE-2011-1086</a> MISC MISC MISC
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	5.5	<a href="#">CVE-2020-1768</a> CONF RM
perforce_software -- p4web	Perforce P4web 2011.1 and 2012.1 has multiple XSS vulnerabilities	2020-02-12	4.3	<a href="#">CVE-2013-1410</a> MISC MISC
phonerlite -- phonerlite	The PhonerLite phone before 2.15 provides hashed credentials in a response to an invalid authentication challenge, which makes it easier for remote attackers to obtain access via a brute-force attack, related to a "SIP Digest Leak" issue.	2020-02-12	4.3	<a href="#">CVE-2014-2560</a> MISC
php -- php	When using certain mbstring functions to convert multibyte encodings, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause function mbf_ffi_conv_big5_wchar to read past the allocated buffer. This may lead to information disclosure or crash.	2020-02-10	6.4	<a href="#">CVE-2020-7060</a> MISC
php -- php	When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7.4.x below 7.4.2 it is possible to supply data that will cause this function to read past the allocated buffer. This may lead to information disclosure or crash.	2020-02-10	6.4	<a href="#">CVE-2020-7059</a> MISC
pragmamx -- pragmamx	Multiple cross-site scripting (XSS) vulnerabilities in pragmaMx 1.x before 1.12.2 allow remote attackers to inject arbitrary web script or HTML via the (1) name parameter to modules.php or (2) img_url to includes/wysiwyg/spaw/editor/plugins/imgpopup/img_popup.php.	2020-02-11	4.3	<a href="#">CVE-2012-2452</a> MISC MISC MISC
prestashop -- prestashop	Cross-site scripting (XSS) vulnerability in PrestaShop before 1.4.9 allows remote attackers to inject arbitrary web script or HTML via the index of the product[] parameter to ajax.php.	2020-02-11	4.3	<a href="#">CVE-2012-2517</a> MISC MISC
	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon			

qualcomm -- multiple_snapdragon_products	Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> CONF RM
qualcomm -- multiple_snapdragon_products	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> CONF RM
railo_technologies -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	6.8	<a href="#">CVE-2014-5468</a> MISC MISC MISC MISC
red_hat -- openshift_entrpise	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-app.	2020-02-07	4.4	<a href="#">CVE-2020-1708</a> CONF RM
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, stores users' information by cleartext in the cookie, which divulges password to attackers.	2020-02-11	5	<a href="#">CVE-2020-3935</a> MISC MISC MISC
secom -- dr.id	Secom Co. Dr.ID, a Door Access Control and Personnel Attendance Management system, allows attackers to enumerate and exam user account in the system.	2020-02-11	5	<a href="#">CVE-2020-3933</a> MISC MISC MISC
siemens -- multiple_scalance_devices	A vulnerability has been identified in SCALANCE S602 (All versions >= V3.0), SCALANCE S612 (All versions >= V3.0), SCALANCE S623 (All versions >= V3.0), SCALANCE S627-2M (All versions >= V3.0). Specially crafted packets sent to port 443/tcp of affected devices could cause a Denial-of-Service condition of the web server.	2020-02-11	5	<a href="#">CVE-2019-13925</a> MISC
siemens -- multiple_scalance_switches	A vulnerability has been identified in SCALANCE X-200 switch family (incl. SIPLUS NET variants) (all versions < 5.2.4), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All versions), SCALANCE X-300 switch family (incl. X408 and S PLUS NET variants) (all versions < 4.1.3). The device does not send the X-Frame-Option Header in the administrative web interface, which makes it vulnerable to Clickjacking attacks. The security vulnerability could be exploited by an attacker that is able to trick an administrative user with a valid session on the target device into clicking on a website controlled by the attacker. The	2020-02-11	4.3	<a href="#">CVE-2019-13924</a> MISC

	vulnerability could allow an attacker to perform administrative actions via the web interface. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- multiple_simatic_devices	A vulnerability has been identified in SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.1), SIMATIC S7-300 PN/DP CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions). Affected devices contain a vulnerability that could cause a Denial-of-Service condition of the web server by sending specially crafted HTTP requests to ports 80/tcp and 443/tcp. The security vulnerability could be exploited by an attacker with network access to an affected device. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device's web server. Beyond the web service, no other functions or interfaces are affected by the Denial-of-Service condition.	2020-02-11	5	<a href="#">CVE-2019-13940</a> <a href="#">MISC</a> <a href="#">MISC</a>
siemens -- ozw672_and_772_web_servers	A vulnerability has been identified in OZW672 (All versions < V10.00), OZW772 (All versions < V10.00). Vulnerable versions of OZW Web Server use predictable path names for project files that legitimately authenticated users have created by using the application's export function. By accessing a specific uniform resource locator on the web servers a remote attacker could be able to download a project file without prior authentication. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected system. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises the confidentiality of the targeted system.	2020-02-11	5	<a href="#">CVE-2019-13941</a> <a href="#">MISC</a>
simple_machines -- simple_machines_forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: Forum admin can read files such as the database config.	2020-02-07	4	<a href="#">CVE-2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
smoothwall - smoothwall_express_3	A cross-site scripting (XSS) vulnerability in Smoothwall Express 3.	2020-02-07	4.3	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall -- smoothwall_express_3	CSRF vulnerability in Smoothwall Express 3.	2020-02-07	6.8	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
socialengine -- socialengine	Multiple cross-site request forgery (CSRF) vulnerabilities in the (1) Forum, (2) Event, and (3) Classifieds plugins in SocialEngine before 4.2.4.	2020-02-11	6.8	<a href="#">CVE-2012-6721</a> <a href="#">MISC</a>
socialengine -- socialengine	Multiple cross-site scripting (XSS) vulnerabilities in SocialEngine before 4.2.4 allow remote attackers to inject arbitrary web script or HTML via the (1) title parameter to music/create, (2) location parameter to events/create, or (3) search parameter to widget/index/content_id/*.	2020-02-11	4.3	<a href="#">CVE-2012-6720</a> <a href="#">MISC</a>
sockjs -- sockjs	htmlfile in lib/transport/htmlfile.js in SockJS before 3.0 is vulnerable to Reflected XSS via the /htmlfile c (aka callback) parameter.	2020-02-10	4.3	<a href="#">CVE-2020-8823</a> <a href="#">MISC</a> <a href="#">MISC</a>
sphider -- sphider	A Command Execution vulnerability exists in Sphider before 1.3.6 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5083 pertains to instances of fwrite in Sphider.	2020-02-10	6.5	<a href="#">CVE-2014-5083</a> <a href="#">MISC</a>
sphider -- sphider_plus	A Command Execution vulnerability exists in Sphider Plus 3.2 due to insufficient sanitization of fwrite to conf.php, which could let a remote malicious user execute arbitrary code. CVE-2014-5085 pertains to instances of fwrite in Sphider Plus, but do not exist in either Sphider or Sphider Pro.	2020-02-10	6.5	<a href="#">CVE-2014-5085</a> <a href="#">MISC</a>

sphider -- sphider_pro	A Command Execution vulnerability exists in Sphider Pro 3.2 due to insufficient sanitization of fwrite, which could let a remote malicious user execute arbitrary code. CVE-2014-5084 pertains to instances of fwrite in Sphider Pro only, but do not exist in either Sphider or Sphider Plus.	2020-02-10	6.5	<a href="#">CVE-2014-5084</a> <a href="#">MISC</a>
statusnet -- statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	5	<a href="#">CVE-2010-4658</a> <a href="#">MISC</a> <a href="#">MISC</a>
suse -- opensuse_wicked	An ni_dhcp4_fsm_process_dhcp4_packet memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets with a different client-id.	2020-02-11	5	<a href="#">CVE-2020-7217</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISCm</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5820</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5822</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a DLL injection vulnerability, which is a type of issue whereby an individual attempts to execute their own code in place of legitimate code as a means to perform an exploit.	2020-02-11	4.6	<a href="#">CVE-2020-5821</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2020-02-11	4.6	<a href="#">CVE-2020-5823</a> <a href="#">MISC</a>
teamviewer -- teamviewer_desktop	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9 x , this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.	2020-02-07	4.4	<a href="#">CVE-2019-18988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
testlink -- testlink	An issue was discovered in TestLink 1.9.19. The relation_type parameter of	2020-02-		<a href="#">CVE-2020-8841</a>



	the lib/requirements/reqSearch.php endpoint is vulnerable to authenticated SQL Injection.	10	<a href="#">6.5</a>	<a href="#">MISC</a> <a href="#">MISC</a>
texas_instruments -- cc2640r2_devices	The Bluetooth Low Energy implementation on Texas Instruments SDK through 3.30.00.20 for CC2640R2 devices does not properly restrict the SM Public Key packet on reception, allowing attackers in radio range to cause a denial of service (crash) via crafted packets.	2020-02-10	<a href="#">6.1</a>	<a href="#">CVE-2019-17520</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
texas_instruments -- multiple_devices	The Bluetooth Low Energy peripheral implementation on Texas Instruments SIMPLELINK-CC2640R2-SDK through 3.30.00.20 and BLE-STACK through 1.5.0 before Q4 2019 for CC2640R2 and CC2540/1 devices does not properly restrict the advertisement connection request packet on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.	2020-02-10	<a href="#">6.1</a>	<a href="#">CVE-2019-19193</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_bug_genie -- the_bug_genie	The Bug Genie before 3.2.6 has Multiple XSS and HTML Injection Vulnerabilities	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2013-1760</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ubiquiti_networks -- unifi_controller	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4) authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the UniFi Controller name via a request to api/set/setting/identity.	2020-02-08	<a href="#">6.8</a>	<a href="#">CVE-2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>
vbseo -- vbseo	vbSeo before 3.6.0PL2 allows XSS via the member.php u parameter.	2020-02-10	<a href="#">4.3</a>	<a href="#">CVE-2012-6666</a> <a href="#">MISC</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	<a href="#">6.5</a>	<a href="#">CVE-2013-3591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
watchguard -- firewire_xtm	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	<a href="#">4.3</a>	<a href="#">CVE-2014-6413</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	<a href="#">6.5</a>	<a href="#">CVE-2015-2062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	A Cross-site Scripting (XSS) vulnerability exists in the All in One SEO Pack plugin before 2.0.3.1 for WordPress via the Search parameter.	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2013-5988</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	<a href="#">6.8</a>	<a href="#">CVE-2013-2009</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	<a href="#">4.3</a>	<a href="#">CVE-2013-2008</a> <a href="#">MISC</a> <a href="#">MISC</a>

				<a href="#">MISC</a>
xiaomi -- mi6_devices	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Xiaomi Browser Prior to 10.4.0. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the miui.share application. The issue results from the lack of proper validation of user-supplied data, which can result in an arbitrary application download. An attacker can leverage this vulnerability to execute code in the context of the user. Was ZDI-CAN-7483.	2020-02-10	<a href="#">6.8</a>	<a href="#">CVE-2019-13322</a> <a href="#">MISC</a>
xiaomi -- mi6_devices	This vulnerability allows network adjacent attackers to execute arbitrary code on affected installations of Xiaomi Browser Prior to 10.4.0. User interaction is required to exploit this vulnerability in that the target must connect to a malicious access point. The specific flaw exists within the handling of HTTP responses to the Captive Portal. A crafted HTML response can cause the Captive Portal to open a browser to a specified location without user interaction. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-7467.	2020-02-10	<a href="#">5.4</a>	<a href="#">CVE-2019-13321</a> <a href="#">MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	<a href="#">6.5</a>	<a href="#">CVE-2013-3628</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Zenphoto before 1.4.3.4 admin-news-articles.php date parameter XSS.	2020-02-11	<a href="#">4.3</a>	<a href="#">CVE-2012-4519</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - applications_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	<a href="#">5</a>	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apport -- apport	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	<a href="#">1.9</a>	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a> <a href="#">MISC</a>
apport -- apport	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	<a href="#">2.1</a>	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a> <a href="#">MISC</a>
apport -- apport	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	<a href="#">2.1</a>	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a> <a href="#">MISC</a>
bludit -- bludit	<b>** DISPUTED **</b> Bludit 3.10.0 allows Editor or Author roles to insert malicious JavaScript on the WYSIWYG editor. NOTE: the vendor's perspective is that this is "not a bug."	2020-02-07	<a href="#">3.5</a>	<a href="#">CVE-2020-8812</a> <a href="#">MISC</a>
cpanel -- cpanel_and_whm	The clientconf.html and detailbw.html pages in x3 in cPanel & WHM 11.34.0 (build 8) have a XSS vulnerability.	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2012-6449</a> <a href="#">MISC</a>
digi_transport -- multiple_devices	Digi TransPort WR21 5.2.2 3, WR44 5.1 6.4, and WR44v2 5.1.6.9 devices	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2020-8822</a>

	allow stored XSS in the web application.			<a href="#">MISC</a>
google -- chrome	Insufficient policy enforcement in CORS in Google Chrome prior to 80.0 3987.87 allowed a local attacker to obtain potentially sensitive information via a crafted HTML page.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-6408</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- hp_systems_insight_manager	HP Systems Insight Manager before 7.0 allows a remote user on adjacent network to access information	2020-02-10	<a href="#">2.7</a>	<a href="#">CVE-2012-1994</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- rational_publishing_engine	IBM Rational Publishing Engine 6 0.6 and 6.0 6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 162888.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2019-4431</a> <a href="#">XE</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Brakeman Plugin 0.12 and earlier did not escape values received from parsed JSON files when rendering them, resulting in a stored cross-site scripting vulnerability exploitable by users able to control the Brakeman post-build step input data.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2122</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Subversion Plugin 2.13.0 and earlier does not escape the error message for the Project Repository Base URL field form validation, resulting in a stored cross-site scripting vulnerability.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2111</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the parameter name shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2112</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
jenkins -- jenkins	Jenkins Git Parameter Plugin 0.9.11 and earlier does not escape the default value shown on the UI, resulting in a stored cross-site scripting vulnerability exploitable by users with Job/Configure permission.	2020-02-12	<a href="#">3.5</a>	<a href="#">CVE-2020-2113</a> <a href="#">MLIST</a> <a href="#">CONF RM</a>
keycloak -- keycloak	It was found in all keycloak versions before 9.0.0 that links to external applications (Application Links) in the admin console are not validated properly and could allow Stored XSS attacks. An authed malicious user could create URLs to trick users in other realms, and possibly conduct further attacks.	2020-02-10	<a href="#">3.5</a>	<a href="#">CVE-2020-1697</a> <a href="#">CONF RM</a>
linksys -- wrt310nv2ne	Linksys WRT310Nv2 2.0 0.1 is vulnerable to XSS.	2020-02-07	<a href="#">3.5</a>	<a href="#">CVE-2013-3067</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows User Profile Service (ProfSvc) improperly handles symlinks, aka 'Windows User Profile Service Elevation of Privilege Vulnerability'.	2020-02-11	<a href="#">3.6</a>	<a href="#">CVE-2020-0730</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Windows Common Log File System (CLFS) driver when it fails to properly handle objects in memory, aka 'Windows Common Log File System Driver Information Disclosure Vulnerability'.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-0658</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0756.	2020-02-11	<a href="#">2.1</a>	<a href="#">CVE-2020-0755</a> <a href="#">MISC</a>
	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to			

microsoft -- multiple_windows_products	properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0675 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0748 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0744 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755.	2020-02-11	2.1	<a href="#">CVE-2020-0756 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0716.	2020-02-11	2.1	<a href="#">CVE-2020-0717 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0717.	2020-02-11	2.1	<a href="#">CVE-2020-0716 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows Network Driver Interface Specification (NDIS) improperly handles memory.To exploit this vulnerability, an attacker would first have to gain execution on the victim system, aka 'Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0705 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Telephony Service improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0698 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory.To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application.The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation	2020-02-11	2.1	<a href="#">CVE-2020-0677 MISC</a>



	Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0676, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.			
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the Cryptography Next Generation (CNG) service when it fails to properly handle objects in memory. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The security update addresses the vulnerability by correcting how the service handles objects in memory., aka 'Windows Key Isolation Service Information Disclosure Vulnerability'. This CVE D is unique from CVE-2020-0675, CVE-2020-0677, CVE-2020-0748, CVE-2020-0755, CVE-2020-0756.	2020-02-11	2.1	<a href="#">CVE-2020-0676</a> MISC
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows kernel does not properly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'.	2020-02-11	2.1	<a href="#">CVE-2020-0736</a> MISC
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0693.	2020-02-11	3.5	<a href="#">CVE-2020-0694</a> MISC
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2020-0694.	2020-02-11	3.5	<a href="#">CVE-2020-0693</a> MISC
microsoft -- windows_10_and_windows_server_products	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate specific malicious data from a user on a guest operating system. To exploit the vulnerability, an attacker who already has a privileged account on a guest operating system, could run a specially crafted application. The security update addresses the vulnerability by resolving the conditions where Hyper-V would fail to handle these requests., aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE D is unique from CVE-2020-0661.	2020-02-11	2.1	<a href="#">CVE-2020-0751</a> MISC
moodle -- moodle	Persistent XSS in /course/modedit.php of Moodle through 3.7.2 allows authenticated users (Teacher and above) to inject JavaScript into the session of another user (e.g., enrolled student or site administrator) via the introeditor[text] parameter. NOTE: the discoverer and vendor disagree on whether Moodle customers have a reasonable expectation that anyone authenticated as a Teacher can be trusted with the ability to add arbitrary JavaScript (this ability is not documented on Moodle's Teacher_role page). Because the vendor has this expectation, they have stated "this report has been closed as a false positive, and not a bug."	2020-02-11	3.5	<a href="#">CVE-2019-18210</a> MISC MISC
mybulletinboard -- mybulletinboard	Cross-site scripting (XSS) vulnerability in MyBB before 1.6.13 allows remote authenticated users to inject arbitrary web script or HTML via the name parameter in the edit action of the config-profile_fields module.	2020-02-11	3.5	<a href="#">CVE-2014-3826</a> MISC
mybulletinboard -- mybulletinboard	Multiple cross-site scripting (XSS) vulnerabilities in the MyBB (aka MyBulletinBoard) before 1.8.4 allow remote authenticated users to inject arbitrary web script or HTML via the title parameter in the (1) edit or (2) add action in the user-users module or the (3) finduser action or the name parameter in an (4) edit action in the user-user module or the (5) editprofile action to modcp.php.	2020-02-11	3.5	<a href="#">CVE-2014-3827</a> CONF RM MISC
netapp --	NetApp Snap Creator Framework before			<a href="#">CVE-2016-</a>

snap_creator_framework	4.3P1 allows remote authenticated users to conduct clickjacking attacks via unspecified vectors.	2020-02-11	3.5	<a href="#">CVE-2020-5710</a> <a href="#">MISC</a>
netcracker -- netcracker_resource_manager	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the (1) ctrl, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8) xname, or (9) mpTransactionId parameter.	2020-02-08	3.5	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>
orange_hrm -- orange_hrm	Orange HRM 2.7.1 allows XSS via the vacancy name.	2020-02-10	3.5	<a href="#">CVE-2013-1353</a> <a href="#">MISC</a>
piwigo -- piwigo	Piwigo 2.10.1 is affected by stored XSS via the Group Name Field to the group_list page.	2020-02-10	3.5	<a href="#">CVE-2020-8089</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0 8.8 has stored XSS	2020-02-07	3.5	<a href="#">CVE-2013-3635</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0 8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	3.5	<a href="#">CVE-2013-3636</a> <a href="#">MISC</a> <a href="#">MISC</a>
projectpier -- projectpier	ProjectPier 0 8.8 does not use the Secure flag for cookies	2020-02-07	3.5	<a href="#">CVE-2013-3637</a> <a href="#">MISC</a>
rakuten -- viber_for_android	An exploitable information disclosure vulnerability exists in the 'Secret Chats' functionality of Rakuten Viber on Android 9.3 0.6. The 'Secret Chats' functionality allows a user to delete all traces of a chat either by using a time trigger or by direct request. There is a bug in this functionality which leaves behind photos taken and shared on the secret chats, even after the chats are deleted. These photos will be stored in the device and accessible to all applications installed on the Android device.	2020-02-13	2.1	<a href="#">CVE-2018-3987</a> <a href="#">MISC</a>
samsung -- knox	This vulnerability allows local attackers to disclose sensitive information on affected installations of Samsung Knox 1.2.02 39 on Samsung Galaxy S9 build G9600ZHS3ARL1 Secure Folder. An attacker must first obtain physical access to the device in order to exploit this vulnerability. The specific flaws exists within the the handling of the lock screen for Secure Folder. The issue results from the lack of proper validation that a user has correctly authenticated. An attacker can leverage this vulnerability to disclose the contents of the secure container. Was ZDI-CAN-7381.	2020-02-10	2.1	<a href="#">CVE-2019-6744</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to a denial of service vulnerability, which is a type of issue whereby a threat actor attempts to tie up the resources of a resident application, thereby making certain functions unavailable.	2020-02-11	2.1	<a href="#">CVE-2020-5824</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5826</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection (SEP) and Symantec Endpoint Protection Small Business Edition (SEP SBE), prior to 14.2 RU2 MP1 and prior to 14.2.5569.2100 respectively, may be susceptible to an arbitrary file write vulnerability, which is a type of issue whereby an attacker is able to overwrite existing files on the resident system without proper privileges.	2020-02-11	3.6	<a href="#">CVE-2020-5825</a> <a href="#">MISC</a>
	Symantec Endpoint Protection Manager			

symantec -- endpoint_protection_manager	(SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5827</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5829</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5830</a> MISC
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5831</a> MISC
symantec -- symantec_endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM), prior to 14.2 RU2 MP1, may be susceptible to an out of bounds vulnerability, which is a type of issue that results in an existing application reading memory outside of the bounds of the memory that had been allocated to the program.	2020-02-11	2.1	<a href="#">CVE-2020-5828</a> MISC
syska -- smart_bulb_devices	Syska Smart Bulb devices through 2017-08-06 receive RGB parameters over cleartext Bluetooth Low Energy (BLE), leading to sniffing, reverse engineering, and replay attacks.	2020-02-10	3.3	<a href="#">CVE-2017-18642</a> MISC
vanilla_forum -- vanilla	index.php? p=/dashboard/settings/branding in Vanilla 2.6 3 allows stored XSS.	2020-02-10	3.5	<a href="#">CVE-2020-8825</a> MISC MISC
wordpress -- wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	3.5	<a href="#">CVE-2015-1394</a> MISC MISC MISC MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll PNG pngread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted PNG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2020-6068</a> MISC
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll JPEG SOFx parser of the Accusoft ImageGear 19.5.0 library. A specially crafted JPEG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6066</a> MISC
	An exploitable out-of-bounds write vulnerability exists in the TIFreadstripdata function of the igcore19d.dll library of Accusoft ImageGear 19 5 0. A specially			<a href="#">CVE-2019-</a>

accusoft -- imagegear	crafted T FF file file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2020-5187</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the uncompress_scan_line function of the igcore19d.dll library of Accusoft ImageGear, version 19.5 0. A specially crafted PCX file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6063</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the bmp_parsing function of the igcore19d.dll library of Accusoft ImageGear, version 19.5.0. A specially crafted BMP file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6065</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the uncompress_scan_line function of the igcore19d.dll library of Accusoft ImageGear, version 19.5 0. A specially crafted PCX file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6064</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d dll JPEG jpegread precision parser of the Accusoft ImageGear 19 5 0 library. A specially crafted JPEG file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6069</a> <a href="#">MISC</a>
accusoft -- imagegear	An exploitable out-of-bounds write vulnerability exists in the igcore19d dll TIFF tifread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted T FF file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.	2020-02-11	not yet calculated	<a href="#">CVE-2020-6067</a> <a href="#">MISC</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to arbitrary file system write.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3762</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3748</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to arbitrary file system write.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3763</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions, 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3742</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2017.011.30156 and earlier, and	2020-02-	not yet calculated	<a href="#">CVE-2020-3743</a>



	2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	13	calculated	<a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3744</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3745</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3746</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3747</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3749</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3750</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to memory leak .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3753</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3754</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3755</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to memory leak .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3756</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code	2020-02-13	not yet calculated	<a href="#">CVE-2020-3751</a> <a href="#">CONFIRM</a>

	execution .			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.021.20061 and earlier, 2017.011.30156 and earlier, 2017.011.30156 and earlier, and 2015.006.30508 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2020-02-13	not yet calculated	<a href="#">CVE-2020-3752</a> <a href="#">CONFIRM</a>
adobe -- digital_editions	Adobe Digital Editions versions 4.5.10 and below have a buffer errors vulnerability. Successful exploitation could lead to information disclosure.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3759</a> <a href="#">CONFIRM</a>
adobe -- digital_editions	Adobe Digital Editions versions 4.5.10 and below have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3760</a> <a href="#">CONFIRM</a>
adobe -- experience_manager	Adobe Experience Manager versions 6.5, and 6.4 have an uncontrolled resource consumption vulnerability. Successful exploitation could lead to denial-of-service.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3741</a> <a href="#">CONFIRM</a>
adobe -- flash_player	Adobe Flash Player versions 32.0.0.321 and earlier, 32.0.0.314 and earlier, 32.0.0.321 and earlier, and 32.0.0.255 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.	2020-02-13	not yet calculated	<a href="#">CVE-2020-3757</a> <a href="#">CONFIRM</a>
ai -- risknet_acquirer	RiskNet Acquirer before hotfix 6.0 b7+ADHOC-443 ApplicationServiceBean contains a service information disclosure.	2020-02-14	not yet calculated	<a href="#">CVE-2013-5687</a> <a href="#">X</a>
amazon -- aws-js-s3-explorer	explorer.js in Amazon AWS JavaScript S3 Explorer (aka aws-js-s3-explorer) v2 alpha before 2019-08-02 allows XSS in certain circumstances.	2020-02-13	not yet calculated	<a href="#">CVE-2019-14652</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
amd -- radeon_amd_user_exp	The AUEPLauncher service in Radeon AMD User Experience Program Launcher through 1.0.0.1 on Windows allows elevation of privilege by placing a crafted file in %PROGRAMDATA%\AMD\PPC\upload and then creating a symbolic link in %PROGRAMDATA%\AMD\PPC\temp that points to an arbitrary folder with an arbitrary file name.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8950</a> <a href="#">MISC</a> <a href="#">MISC</a>
ammy -- ammy_admin	Ammy Admin 3.2 and earlier stores the client ID at a fixed memory location, which might make it easier for user-assisted remote attackers to bypass authentication by running a local program that extracts a field from the AA_v3.2.exe file.	2020-02-11	not yet calculated	<a href="#">CVE-2013-5582</a> <a href="#">MISC</a>
apache -- nifi	In Apache NiFi 0.0.1 to 1.11.0, the flow fingerprint factory generated flow fingerprints which included sensitive property descriptor values. In the event a node attempted to join a cluster and the cluster flow was not inheritable, the flow fingerprint of both the cluster and local flow was printed, potentially containing sensitive values in plaintext.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1942</a> <a href="#">MISC</a>
ariadne -- ariadne	Multiple cross-site scripting (XSS) vulnerabilities in Ariadne 2.7.6 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO parameter to (1) index.php and (2) loader.php.	2020-02-11	not yet calculated	<a href="#">CVE-2011-4938</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
aruba_networks -- intelligent_edge_switch	A remotely exploitable information disclosure vulnerability is present in Aruba Intelligent Edge Switch models 5400, 3810, 2920, 2930, 2530 with GigT port, 2530 10/100 port, or 2540. The vulnerability impacts firmware 16.08.* before 16.08.0009, 16.09.* before 16.09.0007 and 16.10.* before 16.10.0003. The vulnerability allows an attacker to retrieve sensitive system information. This attack can be carried out without user authentication under very specific conditions.	2020-02-13	not yet calculated	<a href="#">CVE-2019-5322</a> <a href="#">MISC</a>
askey -- ap400w_devices	An issue was discovered on Askey AP4000W TDC_V1 01.003 devices. An attacker can perform Remote Code Execution (RCE) by sending a specially crafted network packer to the bd_srv service listening on TCP port 54188.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8614</a> <a href="#">MISC</a>

askpop3d -- askpop3d	A Denial of Service vulnerability exists in askpop3d 0.7.7 in free (psZQuery),	2020-02-13	not yet calculated	<a href="#">CVE-2014-3208</a> <a href="#">MISC</a>
atlassian -- jira_and_greenhopper	Stored XSS vulnerability in UpdateFieldJson.jspa in JIRA 4.4.3 and GreenHopper before 5.9.8 allows an attacker to inject arbitrary script code.	2020-02-13	not yet calculated	<a href="#">CVE-2012-1500</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
atlassian -- jira_server_and_data_center	The Atlassian Application Links plugin is vulnerable to cross-site request forgery (CSRF). The following versions are affected: all versions prior to 5.4.21, from version 6.0.0 before version 6.0.12, from version 6.1.0 before version 6.1.2, from version 7.0.0 before version 7.0.2, and from version 7.1.0 before version 7.1.3. The vulnerable plugin is used by Atlassian Jira Server and Data Center before version 8.7.0. An attacker could exploit this by tricking an administrative user into making malicious HTTP requests, allowing the attacker to enumerate hosts and open ports on the internal network where Jira server is present.	2020-02-12	not yet calculated	<a href="#">CVE-2019-20100</a> <a href="#">N/A</a> <a href="#">N/A</a> <a href="#">N/A</a>
avira -- antivir_engine	A Denial of Service (infinite loop) vulnerability exists in Avira AntiVir Engine before 8.2.12.58 via an unspecified function in the PDF Scanner Engine.	2020-02-12	not yet calculated	<a href="#">CVE-2013-4602</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
barracuda -- web_application_firewall	Barracuda Web Application Firewall (WAF) 7.8.1.013 allows remote attackers to bypass authentication by leveraging a permanent authentication token obtained from a query string.	2020-02-12	not yet calculated	<a href="#">CVE-2014-2595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bearftp -- bearftp	Improper connection handling in the base connection handler in IKTeam BearFTP before v0.3.1 allows a remote attacker to achieve denial of service via a Slowloris approach by sending a large volume of small packets.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
belkin -- n750_routers	Belkin n750 routers have a buffer overflow.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7173</a> <a href="#">MISC</a> <a href="#">MISC</a>
boat_browser -- boat_browser_for_android	The WebView class and use of the WebView.addJavascriptInterface method in the Boat Browser application 8.0 and 8.0.1 for Android allow remote attackers to execute arbitrary code via a crafted web site, a related issue to CVE-2012-6636.	2020-02-12	not yet calculated	<a href="#">CVE-2014-4968</a> <a href="#">MISC</a>
bss -- bs-client_private_client	A Two-Factor Authentication Bypass Vulnerability exists in BS-Client Private Client 2.4 and 2.5 via an XML request that neglects the use of ADPsw D and AD parameters, which could let a malicious user access privileged function.	2020-02-13	not yet calculated	<a href="#">CVE-2014-4198</a> <a href="#">MISC</a>
chiyu_technology -- bf-430_devices	Stored XSS was discovered on CHIYU BF-430 232/485 TCP/ P Converter devices before 1.16.00, as demonstrated by the /if cgi TF_submask field.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8839</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- internetwork_operating_systems	A memory leak vulnerability exists in Cisco IOS before 15.2(1)T due to a memory leak in the HTTP PROXY Server process (aka CSCu52820), when configured with Cisco ISR Web Security with Cisco ScanSafe and User Authentication NTLM configured.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4661</a> <a href="#">MISC</a>
cloud_foundry -- credhub	Cloud Foundry CredHub, versions prior to 2.5.10, connects to a MySQL database without TLS even when configured to use TLS. A malicious user with access to the network between CredHub and its MySQL database may eavesdrop on database connections and thereby gain unauthorized access to CredHub and other components.	2020-02-12	not yet calculated	<a href="#">CVE-2020-5399</a> <a href="#">CONF RM</a>
	Codologic CodoForum through 4.8.4 allows a DOM-based XSS. While creating			

codologic -- codofurm	a new topic as a normal user, it is possible to add a poll that is automatically loaded in the DOM once the thread/topic is opened. Because session cookies lack the HttpOnly flag, it is possible to steal authentication cookies and take over accounts.	2020-02-15	not yet calculated	<a href="#">CVE-2020-7050</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
codologic -- codofurm	Codologic Codoforum through 4.8.4 allows stored XSS in the login area. This is relevant in conjunction with CVE-2020-5842 because session cookies lack the HttpOnly flag. The impact is account takeover.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7051</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	In iTop through 2.6.0, an XSS payload can be delivered in certain fields (such as icon) of the XML file used to build the dashboard. This is similar to CVE-2015-6544 (which is only about the dashboard title).	2020-02-14	not yet calculated	<a href="#">CVE-2019-13966</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	iTop 2.2.0 through 2.6.0 allows remote attackers to cause a denial of service (application outage) via many requests to launch a compile operation. The requests use the pages/exec.php?exec_env=production&exec_module=itop-hub-connector&exec_page=ajax.php&operation=compile URI. This only affects the community version.	2020-02-14	not yet calculated	<a href="#">CVE-2019-13967</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	Because of a lack of sanitization around error messages, multiple Reflective XSS issues exist in iTop through 2.6.0 via the param_file parameter to webservices/export.php, webservices/cron.php, or env-production/itop-backup/backup.php. By default, any XSS sent to the administrator can be transformed to remote command execution because of CVE-2018-10642 (still working through 2.6.0) The Reflective XSS can also become a stored XSS within the same account because of another vulnerability.	2020-02-14	not yet calculated	<a href="#">CVE-2019-13965</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
combodo -- itop	In Combodo iTop 2.2.0 through 2.6.0, if the configuration file is writable, then execution of arbitrary code can be accomplished by calling ajax.dataloader with a maliciously crafted payload. Many conditions can place the configuration file into a writable state: during installation; during upgrade; in certain cases, an error during modification of the file from the web interface leaves the file writable (can be triggered with XSS); a race condition can be triggered by the hub-connector module (community version only from 2.4.1 to 2.6.0); or editing the file in a CLI.	2020-02-14	not yet calculated	<a href="#">CVE-2019-11215</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
cypress -- psoc_4_devices	The Bluetooth Low Energy implementation in Cypress PSoC 4 BLE component 3.61 and earlier processes data channel frames with a payload length larger than the configured link layer maximum RX payload size, which allows attackers (in radio range) to cause a denial of service (crash) via a crafted BLE Link Layer frame.	2020-02-12	not yet calculated	<a href="#">CVE-2019-16336</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-842_rev_c_devices	A stack-based buffer overflow was found on the D-Link DIR-842 REVC with firmware v3.13B09 HOTFIX due to the use of strcpy for LOGINPASSWORD when handling a POST request to the /MTFWU endpoint.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8962</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
digi_international -- connectport_lts_32_mei	Digi International ConnectPort LTS 32 MEI, Firmware Version 1.4.3 (82002228_K 08/09/2018), bios Version 1.2. Successful exploitation of this vulnerability could allow an attacker to upload a malicious file to the application.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6975</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
digi_international -- connectport_lts_32_mei	Digi International ConnectPort LTS 32 MEI, Firmware Version 1.4.3 (82002228_K 08/09/2018), bios Version 1.2. Multiple cross-site scripting vulnerabilities exist that could allow an attacker to cause a denial-of-service condition.	2020-02-13	not yet calculated	<a href="#">CVE-2020-6973</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>
dojo -- dojox	dojox is vulnerable to Cross-site Scripting in all versions before version 1.16.1, 1.15.2, 1.14.5, 1.13.6, 1.12.7 and 1.11.9. This is due to dojox xmpp util.xmlEncode	2020-02-13	not yet calculated	<a href="#">CVE-2019-10785</a> <a href="#">CONFIRMED</a> <a href="#">MISC</a>



	only encoding the first occurrence of each character, not all of them.			<a href="#">MISC</a>
dovecot -- dovecot	The IMAP and LMTP components in Dovecot 2.3.9 before 2.3.9.3 mishandle snippet generation when many characters must be read to compute the snippet and a trailing > character exists. This causes a denial of service in which the recipient cannot read all of their messages.	2020-02-12	not yet calculated	<a href="#">CVE-2020-7957</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
dovecot -- dovecot	lib-smtp in submission-login and lmtp in Dovecot 2.3.9 before 2.3.9.3 mishandles truncated UTF-8 data in command parameters, as demonstrated by the unauthenticated triggering of a submission-login infinite loop.	2020-02-12	not yet calculated	<a href="#">CVE-2020-7046</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
drupal -- drupal	The RESTful Web Services (restws) module 7.x-1.x before 7.x-1.4 and 7.x-2.x before 7.x-2.1 for Drupal does not properly restrict access to entity write operations, which makes it easier for remote authenticated users with the "access resource node" and "create page content" permissions (or equivalents) to conduct cross-site scripting (XSS) or execute arbitrary PHP code via a crafted text field.	2020-02-11	not yet calculated	<a href="#">CVE-2013-4225</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
easyxdm -- easyxdm	Cross-site Scripting (XSS) in EasyXDM before 2.4.18 allows remote attackers to inject arbitrary web script or HTML via the easyxdm.swf file.	2020-02-14	not yet calculated	<a href="#">CVE-2013-5212</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
etherpad -- etherpad	Directory traversal vulnerability in node/Utils/Minify.js in Etherpad 1.1.2 through 1.5.4 allows remote attackers to read arbitrary files with permissions of the user running the service via a .. (dot dot) in the path parameter of HTTP API requests. NOTE: This vulnerability is due to an incomplete fix to CVE-2015-3297.	2020-02-13	not yet calculated	<a href="#">CVE-2015-3309</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
extrun -- ilbo	ilbo App (ilbo App for Android prior to version 1.1.8 and ilbo App for iOS prior to version 1.2.01) allows an attacker on the same network segment to bypass authentication and to view the images which were recorded by the other ilbo user's device via unspecified vectors.	2020-02-14	not yet calculated	<a href="#">CVE-2020-5532</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.	2020-02-10	not yet calculated	<a href="#">CVE-2020-8840</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of text field objects. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9400.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8846</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.2947. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the fxhtml2pdf.exe module. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9560.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8855</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of watermarks in AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this	2020-02-14	not yet calculated	<a href="#">CVE-2020-8845</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	vulnerability to execute code in the context of the current process. Was ZDI-CAN-9358.			
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7 0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of HTML files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9591.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8853</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7 0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of JPEG files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9606.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8854</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6 0.25608. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of watermarks. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9640.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8856</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.7 0.29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9416.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8852</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of form Annotation objects within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9862.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8857</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this	2020-02-14	not yet calculated	<a href="#">CVE-2020-8847</a> <a href="#">MISC</a> <a href="#">MISC</a>

	vulnerability to execute code in the context of the current process. Was ZDI-CAN-9414.			
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9406.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8851</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPG2000 images. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9407.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8848</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9415.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8850</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.0 29455. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of JPEG2000 files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9413.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8849</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxit -- reader	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.6.0 25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of JPEG files within CovertToPDF. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9102.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8844</a> <a href="#">CONF RM</a> <a href="#">MISC</a>
free_reprintables -- articlefr	A Privilege Escalation Vulnerability exists in Free Reprintables ArticleFR 11.06 2014 due to insufficient access restrictions in the data.php script, which could let a remote malicious user obtain access or modify or delete database information.	2020-02-13	not yet calculated	<a href="#">CVE-2014-4170</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
freebsd -- bsd_libc	regcomp in the BSD implementation of libc is vulnerable to denial of service due to stack exhaustion.	2020-02-12	not yet calculated	<a href="#">CVE-2011-3336</a> <a href="#">FULLDISC</a> <a href="#">END</a> <a href="#">MISC</a>

				<a href="#">BUGTRAQ</a>
fujitsu -- multiple_products	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions, Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3, Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.	2020-02-07	not yet calculated	<a href="#">CVE-2019-13163</a> <a href="#">CONFIRM</a>
git -- git	Git before 1 8.5.6, 1.9.x before 1.9.5, 2.0 x before 2.0.5, 2.1 x before 2.1.4, and 2.2 x before 2.2.1 on Windows and OS X; Mercurial before 3.2.3 on Windows and OS X; Apple Xcode before 6.2 beta 3; mine; libgit2; Egit; and JGit allow remote Git servers to execute arbitrary commands via a tree containing a crafted .git/config file with (1) an ignorable Unicode codepoint, (2) a git~1/config representation, or (3) mixed case that is improperly handled on a case-insensitive filesystem.	2020-02-12	not yet calculated	<a href="#">CVE-2014-9390</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab 12.2.2 and below contains a security vulnerability that allows a guest user in a private project to see the merge request D associated to an issue via the activity timeline.	2020-02-14	not yet calculated	<a href="#">CVE-2019-15592</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab	GitLab 11.8 and later contains a security vulnerability that allows a user to obtain details of restricted pipelines via the merge request endpoint.	2020-02-14	not yet calculated	<a href="#">CVE-2019-15594</a> <a href="#">MISC</a> <a href="#">MISC</a>
global_payments -- php-sdk	Gateways/Gateway.php in Heartland & Global Payments PHP SDK before 2.0.0 does not enforce SSL certificate validations.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20455</a> <a href="#">MISC</a> <a href="#">MISC</a>
gocloud -- multiple_devices	Gocloud S2A_WL 4.2.7.16471, S2A 4.2.7.17278, S2A 4.3 0.15815, S2A 4.3 0.17193, S3A K2P MTK 4.2.7.16528, S3A 4.3 0.16572, and ISP3000 4.3 0.17190 devices allows remote attackers to execute arbitrary OS commands via shell metacharacters in a ping operation, as demonstrated by the cgi-bin/webui/admin/tools/app_ping/diag_ping/substring.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8949</a> <a href="#">MISC</a>
google -- android	In notifyNetworkTested and related functions of NetworkMonitor.java, there is a possible bypass of private DNS settings. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-9 Android ID: A-122652057	2020-02-13	not yet calculated	<a href="#">CVE-2020-0028</a> <a href="#">MISC</a>
google -- android	In btm_read_remote_ext_features_complete of btm_acl.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0 Android-8.1 Android-9 Android-10 Android D: A-141552859	2020-02-13	not yet calculated	<a href="#">CVE-2020-0005</a> <a href="#">MISC</a>
google -- android	It is possible for a malicious application to construct a TYPE_TOAST window manually and make that window clickable. This could lead to a local escalation of privilege with no additional execution privileges needed. User action is needed	2020-02-13	not yet calculated	<a href="#">CVE-2020-0014</a> <a href="#">MISC</a>



	for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-128674520			
google -- android	In binder_thread_release of binder.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android kernelAndroid ID: A-145286050References: Upstream kernel	2020-02-13	not yet calculated	<a href="#">CVE-2020-0030</a> MISC
google -- android	The Bluetooth stack in Android before 2.3.6 allows a physically proximate attacker to obtain contact information via an AT phonebook transfer.	2020-02-12	not yet calculated	<a href="#">CVE-2011-2343</a> CONFIRMED MISC
google -- android	In updatePermissions of PermissionManagerService.java, it may be possible for a malicious app to obtain a custom permission from another app due to a permission bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-10Android D: A-67319274	2020-02-13	not yet calculated	<a href="#">CVE-2019-2200</a> MISC
google -- android	In onCreate of CertInstaller.java, there is a possible way to overlay the Certificate Installation dialog by a malicious application. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-139017101	2020-02-13	not yet calculated	<a href="#">CVE-2020-0015</a> MISC
google -- android	In Parcel::continueWrite of Parcel.cpp, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-140419401	2020-02-13	not yet calculated	<a href="#">CVE-2020-0026</a> MISC
google -- android	In multiple places, it was possible for the primary user's dictionary to be visible to and modifiable by secondary users. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-123232892	2020-02-13	not yet calculated	<a href="#">CVE-2020-0017</a> MISC
google -- android	In MotionEvent::appendDescription of InputDispatcher.cpp, there is a possible log information disclosure. This could lead to local disclosure of user input with System execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-139945049	2020-02-13	not yet calculated	<a href="#">CVE-2020-0018</a> MISC
google -- android	In HidRawSensor::batch of HidRawSensor.cpp, there is a possible out of bounds write due to an unexpected switch fallthrough. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-144040966	2020-02-13	not yet calculated	<a href="#">CVE-2020-0027</a> MISC
google -- android	In getAttributeRange of ExifInterface.java, there is a possible failure to redact location information from media files due to an incorrect bounds check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-10Android D: A-143118731	2020-02-13	not yet calculated	<a href="#">CVE-2020-0020</a> MISC
google -- android	In removeUnusedPackagesLPw of PackageManagerService.java, there is a possible permanent denial-of-service due to a missing package dependency test. This could lead to remote denial of service with User execution privileges needed. User interaction is not needed for	2020-02-13	not yet calculated	<a href="#">CVE-2020-0021</a> MISC

	exploitation Product: AndroidVersions: Android-10Android D: A-141413692			
google -- android	In reassemble_and_dispatch of packet_fragmenter.cc, there is possible out of bounds write due to an incorrect bounds calculation. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android D: A-143894715	2020-02-13	not yet calculated	<a href="#">CVE-2020-0022</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
google -- android	In setPhonebookAccessPermission of AdapterService.java, there is a possible disclosure of user contacts over bluetooth due to a missing permission check. This could lead to local information disclosure if a malicious app enables contacts over a bluetooth connection, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145130871	2020-02-13	not yet calculated	<a href="#">CVE-2020-0023</a> <a href="#">MISC</a>
hashicorp -- sentinel	HashiCorp Sentinel up to 0.10.1 incorrectly parsed negation in certain policy expressions. Fixed in 0.10.2.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19879</a> <a href="#">MISC</a>
hcl -- appscan_standard_edition	HCL AppScan Standard Edition 9 0.3.13 and earlier uses hard-coded credentials which can be exploited by attackers to get unauthorized access to the system.	2020-02-14	not yet calculated	<a href="#">CVE-2019-4392</a> <a href="#">MISC</a>
hitachi -- command_suite_and_automation_director	A vulnerability in Hitachi Command Suite prior to 8.7.1-00 and Hitachi Automation Director prior to 8.5.0-00 allow authenticated remote users to expose technical information through error messages. Hitachi Command Suite includes Hitachi Device Manager and Hitachi Compute Systems Manager.	2020-02-14	not yet calculated	<a href="#">CVE-2018-21032</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
hitachi -- multiple_products	A vulnerability in Hitachi Command Suite prior to 8 6.2-00, Hitachi Automation Director prior to 8.6.2-00 and Hitachi Infrastructure Analytics Advisor prior to 4.2 0-00 allow authenticated remote users to load an arbitrary Cascading Style Sheets (CSS) token sequence. Hitachi Command Suite includes Hitachi Device Manager, Hitachi Tiered Storage Manager, Hitachi Replication Manager, Hitachi Tuning Manager, Hitachi Global Link Manager and Hitachi Compute Systems Manager.	2020-02-14	not yet calculated	<a href="#">CVE-2018-21033</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
hp -- linuxki	LinuxKI v6.0-1 and earlier is vulnerable to an XSS which is resolved in release 6.0-2.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7208</a> <a href="#">MISC</a>
hp -- linuxki	LinuxKI v6.0-1 and earlier is vulnerable to a remote code execution which is resolved in release 6 0-2.	2020-02-13	not yet calculated	<a href="#">CVE-2020-7209</a> <a href="#">MISC</a>
ibm -- tivoli_monitoring_service	IBM Tivoli Monitoring Service 6.3.0.7.3 through 6.3 0.7.10 could allow an unauthorized user to access and modify operation aspects of the ITM monitoring server possibly leading to an effective denial of service or disabling of the monitoring server. BM X-Force ID: 167647.	2020-02-13	not yet calculated	<a href="#">CVE-2019-4592</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
ibm -- urbandcode_deploy_and_urbancode_build	IBM UrbanCode Deploy (UCD) 7.0.3 and IBM UrbanCode Build 6.1.5 could allow a local user to obtain sensitive information by unmasking certain secure values in documents. IBM X-Force D: 171248.	2020-02-13	not yet calculated	<a href="#">CVE-2019-4666</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
intel -- converged_security_and_management_engine	Improper Authentication in subsystem in Intel(R) CSME versions 12.0 through 12.0.48 (IOT only: 12 0.56), versions 13.0 through 13.0.20, versions 14.0 through 14.0.10 may allow a privileged user to potentially enable escalation of privilege, denial of service or information disclosure via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2019-14598</a> <a href="#">MISC</a>
intel -- e1000e/82574l_network_processing_state_when_parsing_32_hex_33_hex_or_34_hex_byte_values_at_the_0x47f_offset.	A denial of service vulnerability exists in some motherboard implementations of Intel e1000e/82574L network controller devices through 2013-02-06 where the device can be brought into a non-processing state when parsing 32 hex, 33 hex, or 34 hex byte values at the 0x47f offset. NOTE: A followup statement from Intel suggests that the root cause of this issue was an incorrectly configured	2020-02-13	not yet calculated	<a href="#">CVE-2013-1634</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">SECTRAK</a> <a href="#">XF</a>

	EEPROM image.			
intel -- manycore_platform_sof	Improper permissions in the installer for Intel(R) MPSS before version 3.8.6 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0563</a> MISC
intel -- renesas_electronics_usb	Improper permissions in the installer for the Intel(R) Renesas Electronics(R) USB 3.0 Driver, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0560</a> MISC
intel -- sgx_software_development	Improper initialization in the Intel(R) SGX SDK before v2.6.100.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0561</a> MISC
intel -- raid_web_console_2	Improper permissions in the installer for Intel(R) RWC2, all versions, may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0562</a> MISC
intel -- raid_web_console_3_for_windows	Improper permissions in the installer for Intel(R) RWC3 for Windows before version 7.010.009.000 may allow an authenticated user to potentially enable escalation of privilege via local access.	2020-02-13	not yet calculated	<a href="#">CVE-2020-0564</a> MISC
invision_power_services -- invision_power_board	Invision Power Board (PB) through 3.x allows admin account takeover leading to code execution.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3725</a> MISC
istio -- istio	An issue was discovered in Istio 1.3 through 1.3.6. Under certain circumstances, it is possible to bypass a specifically configured Mixer policy. Istio-proxy accepts the x-istio-attributes header at ingress that can be used to affect policy decisions when Mixer policy selectively applies to a source equal to ingress. To exploit this vulnerability, someone has to encode a source.uid in this header. This feature is disabled by default in Istio 1.3 and 1.4.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8843</a> MISC MISC CONF RM
joomla! -- joomla!	Tiny browser in TinyMCE 3.0 editor in Joomla! before 1.5.13 allows file upload and arbitrary PHP code execution.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4906</a> CONF RM EXPLOIT-DB MISC
joomla! -- joomla!	TinyBrowser plugin for Joomla! before 1.5.13 allows arbitrary file upload via upload.php.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4908</a> MISC EXPLOIT-DB MLIST
jsreport -- jsreport	An unintended require and server-side request forgery vulnerabilities in jsreport version 2.5.0 and earlier allow attackers to execute arbitrary code.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8128</a> MISC
jsreport -- script-manager	An unintended require vulnerability in script-manager npm package version 0.8.6 and earlier may allow attackers to execute arbitrary code.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8129</a> MISC
juniper -- junos_os	Multiple vulnerabilities exist in Juniper Junos J-Web error handling that may lead to cross site scripting (XSS) issues or crash the J-Web service (DoS). This affects Juniper Junos OS 12.1X44 before 12.1X44-D45, 12.1X46 before 12.1X46-D30, 12.1X47 before 12.1X47-D20, 12.3 before 12.3R8, 12.3X48 before 12.3X48-D10, 13.1 before 13.1R5, 13.2 before 13.2R6, 13.3 before 13.3R4, 14.1 before 14.1R3, 14.1X53 before 14.1X53-D10, 14.2 before 14.2R1, and 15.1 before 15.1R1.	2020-02-11	not yet calculated	<a href="#">CVE-2014-6447</a> CONF RM MISC
kaseya -- virtual_system_administrator	Directory traversal vulnerability in Kaseya Virtual System Administrator (VSA) 7.0.0.0 before 7.0.0.33, 8.0.0.0 before 8.0.0.23, 9.0.0.0 before 9.0.0.19, and 9.1.0.0 before 9.1.0.9 allows remote authenticated users to write to and execute arbitrary files due to insufficient restrictions in file paths to json.ashx.	2020-02-13	not yet calculated	<a href="#">CVE-2015-6589</a> MISC MISC MISC MISC
kde -- paste_applet	The %{password(...)} macro in pastemacroexpander.cpp in the KDE Paste Applet before 4.10.5 in kdeplasma-addons does not properly generate passwords, which allows context-dependent attackers to bypass	2020-02-11	not yet calculated	<a href="#">CVE-2013-2120</a> MISC MISC MISC MISC

	authentication via a brute-force attack.			MISC
kde -- paste_applet	The KRandom::random function in KDE Paste Applet after 4.10.5 in kdeplasma-addons uses the GNU C Library rand function's linear congruential generator, which makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms by predicting the generator output.	2020-02-11	not yet calculated	<a href="#">CVE-2013-2213</a> MISC MISC MISC
kinetica -- kinetica	The Admin web application in Kinetica 7.0 9.2.20191118151947 does not properly sanitise the input for the function getLogs. This lack of sanitisation could be exploited to allow an authenticated attacker to run remote code on the underlying operating system. The logFile parameter in the getLogs function was used as a variable in a command to read log files; however, due to poor input sanitisation, it was possible to bypass a replacement and break out of the command.	2020-02-11	not yet calculated	<a href="#">CVE-2020-8429</a> MISC MISC
lenovo -- ez_media_&_backup_center	A vulnerability in the web interface of Lenovo EZ Media & Backup Center, ix2 & ix2-dl version 4.1.406.34763 and prior could allow an unauthenticated, remote attacker to redirect a user to an untrusted web page.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19758</a> CONF RM
lenovo -- multiple_devices	Lenovo was notified of a potential denial of service vulnerability, affecting various versions of BIOS for Lenovo Desktop, Desktop - All in One, and ThinkStation, that could cause PCRs to be cleared intermittently after resuming from sleep (S3) on systems with Intel TXT enabled.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6190</a> CONF RM
lenovo -- xclarity_administrator	An internal product security audit of Lenovo XClarity Administrator (LXCA) discovered a Document Object Model (DOM) based cross-site scripting vulnerability in versions prior to 2.6.6 that could allow JavaScript code to be executed in the user's web browser if a specially crafted link is visited. The JavaScript code is executed on the user's system, not executed on LXCA itself.	2020-02-14	not yet calculated	<a href="#">CVE-2019-19757</a> CONF RM
lenovo -- xclarity_administrator	An XML External Entity (XXE) processing vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.6.6 that could allow information disclosure.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6194</a> CONF RM
lenovo -- xclarity_administrator	An information disclosure vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.6.6 that could allow unauthenticated access to some configuration files which may contain usernames, license keys, IP addresses, and encrypted password hashes.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6193</a> CONF RM
lenovo -- xclarity_controller	An authorization bypass exists in Lenovo XClarity Controller (XCC) versions prior to 3.08 CDI340V, 3.01 TEI392O, 1.71 PSI328N where a valid authenticated user with lesser privileges may be granted read-only access to higher-privileged information if 1) "LDAP Authentication Only with Local Authorization" mode is configured and used by XCC, and 2) a lesser privileged user logs into XCC within 1 minute of a higher privileged user logging out. The authorization bypass does not exist when "Local Authentication and Authorization" or "LDAP Authentication and Authorization" modes are configured and used by XCC.	2020-02-14	not yet calculated	<a href="#">CVE-2019-6195</a> CONF RM
lexmark -- multiple_devices	Lexmark printer MS812 and multiple older generation Lexmark devices have a stored XSS vulnerability in the embedded web server. The vulnerability can be exploited to expose session credentials and other information via the users web browser.	2020-02-13	not yet calculated	<a href="#">CVE-2019-18791</a> MISC CONF RM
libuv -- libuv	The uv_rwlock_t fallback implementation for Windows XP and Server 2003 in libuv before 1.7.4 does not properly prevent threads from releasing the locks of other threads, which allows attackers to cause a denial of service (deadlock) or possibly have unspecified other impact by	2020-02-11	not yet calculated	<a href="#">CVE-2014-9748</a> MISC MISC MISC MISC



	leveraging a race condition.			<a href="#">MISC</a>
linux -- linux_kernel	ext4_protect_reserved_inode in fs/ext4/block_validity.c in the Linux kernel through 5.5.3 allows attackers to cause a denial of service (soft lockup) via a crafted journal size.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8992</a> <a href="#">MISC</a>
lvm2 -- lvm2	vg_lookup in daemons/lvmetad/lvmetad-core.c in LVM2 2.02 mismanages memory, leading to an lvmetad memory leak, as demonstrated by running pvs.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8991</a> <a href="#">MISC</a>
magento -- magento	Zend_XmlRpc Class in Magento before 1.7.0.2 contains an information disclosure vulnerability.	2020-02-13	not yet calculated	<a href="#">CVE-2012-6091</a> <a href="#">MLIST</a> <a href="#">BID</a> <a href="#">XF</a>
mailu -- mailu	In Mailu before version 1.7, an authenticated user can exploit a vulnerability in Mailu fetchmail script and gain full access to a Mailu instance. Mailu servers that have open registration or untrusted users are most impacted. The master and 1.7 branches are patched on our git repository. All Docker images published on docker.io/mailu for tags 1.5, 1.6, 1.7 and master are patched. For detailed instructions about patching and securing the server afterwards, see <a href="https://github.com/Mailu/Mailu/issues/1354">https://github.com/Mailu/Mailu/issues/1354</a>	2020-02-13	not yet calculated	<a href="#">CVE-2020-5239</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
mambo -- mambo_cms	Mambo CMS through 4.6.5 has multiple XSS.	2020-02-12	not yet calculated	<a href="#">CVE-2011-2499</a> <a href="#">MLIST</a>
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability was discovered in the Source Integration plugin before 1.6.2 and 2.x before 2.3.1 for MantisBT. The repo_delete.php Delete Repository page allows execution of arbitrary code via a repo name (if CSP settings permit it). This is related to CVE-2018-16362.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8981</a> <a href="#">MISC</a> <a href="#">MISC</a>
matestack-ui-core_gem_for_ruby_on_rails -- matestack-ui-core_gem_for_ruby_on_rails	matestack-ui-core (RubyGem) before 0.7.14 is vulnerable to XSS/Script injection. This vulnerability is patched in version 0.7.14.	2020-02-13	not yet calculated	<a href="#">CVE-2020-5241</a> <a href="#">CONF RM</a>
maxum_development - rumpus_ftp	A CSRF vulnerability exists in the Web Settings of Web File Manager in Rumpus FTP 8.2.9.1. Exploitation of this vulnerability can result in manipulation of Server Web settings at RAPR/WebSettingsGeneralSet.html.	2020-02-10	not yet calculated	<a href="#">CVE-2019-19664</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development - rumpus_ftp_server	A CSRF vulnerability exists in the Web File Manager's Create/Delete Accounts functionality of Rumpus FTP Server 8.2.9.1. By exploiting it, an attacker can Create and Delete accounts via RAPR/TriggerServerFunction.html.	2020-02-10	not yet calculated	<a href="#">CVE-2019-19662</a> <a href="#">MISC</a> <a href="#">MISC</a>
mcafee -- endpoint_security	Improper access control vulnerability in Configuration Tool in McAfee McAfee Endpoint Security (ENS) Prior to 10.6.1 February 2020 Update allows local users to disable security features via unauthorised use of the configuration tool from older versions of ENS.	2020-02-14	not yet calculated	<a href="#">CVE-2020-7251</a> <a href="#">CONF RM</a>
microsoft -- multiple_windows_products	An information vulnerability exists when Windows Modules Installer Service improperly discloses file information, aka 'Windows Modules Installer Service Information Disclosure Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0728</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0714</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Windows Graphics Component improperly handles objects in memory, aka 'Windows Graphics Component Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2020-0745, CVE-2020-0792.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0715</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when the Connected User Experiences and Telemetry Service improperly handles file operations, aka 'Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0727</a> <a href="#">MISC</a>
	A remote code execution vulnerability exists when the Windows Imaging Library			

microsoft -- multiple_windows_products	improperly handles memory.To exploit this vulnerability, an attacker would first have to coerce a victim to open a specially crafted file.The security update addresses the vulnerability by correcting how the Windows Imaging Library handles memory., aka 'Windows Imaging Library Remote Code Execution Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0708</a> MISC
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE is unique from CVE-2020-0719, CVE-2020-0720, CVE-2020-0721, CVE-2020-0722, CVE-2020-0723, CVE-2020-0724, CVE-2020-0725, CVE-2020-0726, CVE-2020-0731.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0691</a> MISC
microsoft -- office_online_server	A spoofing vulnerability exists when Office Online Server does not validate origin in cross-origin communications correctly, aka 'Microsoft Office Online Server Spoofing Vulnerability'.	2020-02-11	not yet calculated	<a href="#">CVE-2020-0695</a> MISC
microsys -- promotic	Microsys PROMOTIC 8.2.13 contains an ActiveX Control Start Buffer Overflow vulnerability which can lead to denial of service.	2020-02-13	not yet calculated	<a href="#">CVE-2014-1617</a> MISC MISC
mobileiron -- vsp_and_sentry	MobileIron VSP < 5.9.1 and Sentry < 5.0 has an insecure encryption scheme.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7287</a> MISC MISC
mobileiron -- vsp_and_sentry	MobileIron VSP < 5.9.1 and Sentry < 5.0 has a weak password obfuscation algorithm	2020-02-12	not yet calculated	<a href="#">CVE-2013-7286</a> MISC MISC
moxa -- mgate_5105-mb-eip_devices	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Moxa MGate 5105-MB-EIP firmware version 4.1. Authentication is required to exploit this vulnerability. The specific flaw exists within the DestIP parameter within MainPing.asp. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9552.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8858</a> MISC MISC
netgear -- cg3100_devices	A vulnerability exists in Netgear CG3100 devices before 3.9.2421.13.mp3 V0027 via an embed malicious script in an unspecified page, which could let a malicious user obtain sensitive information.	2020-02-13	not yet calculated	<a href="#">CVE-2014-3919</a> MISC
netis -- wf2471_devices	Netis WF2471 v1.2.30142 devices allow an authenticated attacker to execute arbitrary OS commands via shell metacharacters in the /cgi-bin-igdd/sys_log_clean cgi log_3g_type parameter.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8946</a> MISC
nvidia -- graphics_drivers	A Memory Corruption Vulnerability exists in NVIDIA Graphics Drivers 29549 due to an unknown function in the file proc/driver/nvidia/registry.	2020-02-12	not yet calculated	<a href="#">CVE-2012-0951</a> MISC MISC
nxp -- kw41z_devices	The Bluetooth Low Energy implementation on NXP SDK through 2.2.1 for KW41Z devices does not properly restrict the Link Layer payload length, allowing attackers in radio range to cause a buffer overflow via a crafted packet.	2020-02-12	not yet calculated	<a href="#">CVE-2019-17519</a> MISC
openconnect_project - - openconnect_vpn_client	OpenConnect VPN client with GnuTLS before 5.02 contains a heap overflow if MTU is increased on reconnection.	2020-02-13	not yet calculated	<a href="#">CVE-2013-7098</a> CONF RM
openvpn -- access_server	OpenVPN Access Server 2.8.x before 2.8.1 allows LDAP authentication bypass (except when a user is enrolled in two-factor authentication).	2020-02-13	not yet calculated	<a href="#">CVE-2020-8953</a> CONF RM
openx -- openx_ad_server	A Code Execution Vulnerability exists in OpenX Ad Server 2.8.10 due to a backdoor in flowplayer-3.1.1.min.js library, which could let a remote malicious user execute arbitrary PHP code	2020-02-14	not yet calculated	<a href="#">CVE-2013-4211</a> MISC MISC MISC MISC
	A Cross-Site Scripting (XSS) Vulnerability			<a href="#">CVE-2013-</a>

otrs -- itsm_and_faq	exists in OTRS ITSM prior to 3.2.4, 3.1.8, and 3.0.7 and FAQ prior to 2.1.4 and 2.0.8 via changes, workorder items, and FAQ articles, which could let a remote malicious user execute arbitrary code.	2020-02-12	not yet calculated	2637 <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
palo_alto_networks -- expedition_migration_tool	Insufficient Cross-Site Request Forgery (XSRF) protection on Expedition Migration Tool allows remote unauthenticated attackers to hijack the authentication of administrators and to perform actions on the Expedition Migration Tool. This issue affects Expedition Migration Tool 1.1.51 and earlier versions.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1977</a> <a href="#">CONF RM</a>
palo_alto_networks -- globalprotect	A denial-of-service (DoS) vulnerability in Palo Alto Networks GlobalProtect software running on Mac OS allows authenticated local users to cause the Mac OS kernel to hang or crash. This issue affects GlobalProtect 5.0.5 and earlier versions of GlobalProtect 5.0 on Mac OS.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1976</a> <a href="#">CONF RM</a>
palo_alto_networks -- pan-os	Missing XML validation vulnerability in the PAN-OS web interface on Palo Alto Networks PAN-OS software allows authenticated users to inject arbitrary XML that results in privilege escalation. This issue affects PAN-OS 8.1 versions earlier than PAN-OS 8.1.12 and PAN-OS 9.0 versions earlier than PAN-OS 9.0.6. This issue does not affect PAN-OS 7.1, PAN-OS 8.0, or PAN-OS 9.1 or later versions.	2020-02-12	not yet calculated	<a href="#">CVE-2020-1975</a> <a href="#">CONF RM</a>
pcres -- pcre2_jit_compile	An out-of-bounds read was discovered in PCRE before 10.34 when the pattern JIT compiled and used to match specially crafted subjects in non-UTF mode. Applications that use PCRE to parse untrusted input may be vulnerable to this flaw, which would allow an attacker to crash the application. The flaw occurs in do_extuni_no_utf in pcre2_jit_compile.c.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20454</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
podman -- podman	A flaw was discovered in Podman where it incorrectly allows containers when created to overwrite existing files in volumes, even if they are mounted as read-only. When a user runs a malicious container or a container based on a malicious image with an attached volume that is used for the first time, it is possible to trigger the flaw and overwrite files in the volume. This issue was introduced in version 1.6.0.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1726</a> <a href="#">CONF RM</a>
prestashop -- prestashop	PrestaShop before 1.4.11 allows logout CSRF.	2020-02-14	not yet calculated	<a href="#">CVE-2013-4792</a> <a href="#">MISC</a>
prestashop -- prestashop	PrestaShop before 1.4.11 allows Logistician, translators and other low level profiles/accounts to inject a persistent XSS vector on TinyMCE.	2020-02-14	not yet calculated	<a href="#">CVE-2013-4791</a> <a href="#">MISC</a>
prismview -- prismview_system_and_prismview_player	The HTTP API in Prismview System 9.11.10.17.00 and Prismview Player 11.13.09.1100 allows remote code execution by uploading RebootSystem.Ink and requesting /REBOOTSYSTEM or /RESTARTVNC. (Authentication is required but an XML file containing credentials can be downloaded.)	2020-02-10	not yet calculated	<a href="#">CVE-2019-20451</a> <a href="#">MISC</a>
proglottis -- gpgme	The proglottis Go wrapper before 0.1.1 for the GPGME library has a use-after-free, as demonstrated by use for container image pulls by Docker or CRI-O. This leads to a crash or potential code execution during GPG signature verification.	2020-02-12	not yet calculated	<a href="#">CVE-2020-8945</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
progress -- moveit_transfer	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, multiple SQL Injection vulnerabilities have been found in the REST API that could allow an authenticated attacker to gain unauthorized access to MOVEit Transfer's database via the REST API. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database in addition to executing SQL statements that alter or	2020-02-14	not yet calculated	<a href="#">CVE-2020-8611</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>

	destroy database elements.			
progress -- moveit_transfer	In Progress MOVEit Transfer 2019.1 before 2019.1.4 and 2019.2 before 2019.2.1, a REST API endpoint failed to adequately sanitize malicious input, which could allow an authenticated attacker to execute arbitrary code in a victim's browser, aka XSS.	2020-02-14	not yet calculated	<a href="#">CVE-2020-8612</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
python-mode -- python-mode	A Code Execution vulnerability exists in select.py when using python-mode 2012-12-19.	2020-02-12	not yet calculated	<a href="#">CVE-2013-5106</a> <a href="#">MISC</a>
qemu -- qemu	An out-of-bounds heap buffer access flaw was found in the way the iSCSI Block driver in QEMU versions 2.12.0 before 4.2.1 handled a response coming from an iSCSI server while checking the status of a Logical Address Block (LBA) in an iscsi_co_block_status() routine. A remote user could use this flaw to crash the QEMU process, resulting in a denial of service or potential execution of arbitrary code with privileges of the QEMU process on the host.	2020-02-11	not yet calculated	<a href="#">CVE-2020-1711</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a>
qnnap -- viocard-300_devices	QNAP VioCard 300 has hardcoded RSA private keys.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6277</a> <a href="#">MISC</a> <a href="#">MISC</a>
realtek -- ndis_driver_rt64x64.sys	Realtek NDIS driver rt640x64.sys, file version 10.1.505.2015, fails to do any size checking on an input buffer from user space, which the driver assumes has a size greater than zero bytes. To exploit this vulnerability, an attacker must send an RP with a system buffer size of 0.	2020-02-12	not yet calculated	<a href="#">CVE-2019-11867</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openshift_enterprise	The default configuration of broker.conf in Red Hat OpenShift Enterprise 2.x before 2.1 has a password of "mo00" for a Mongo account, which allows remote attackers to hijack the broker by providing this password, related to the openshift.sh script in Openshift Extras before 20130920. NOTE: this may overlap CVE-2013-4253 and CVE-2013-4281.	2020-02-12	not yet calculated	<a href="#">CVE-2014-0234</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
runc -- runc	runc through 1.0.0-rc9 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. (This vulnerability does not affect Docker due to an implementation detail that happens to block the attack.)	2020-02-12	not yet calculated	<a href="#">CVE-2019-19921</a> <a href="#">SUSE</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.10 allows SQL Injection via the SOAP API, the EmailUIAjax interface, or the MailMerge module.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8804</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows Directory Traversal to include arbitrary .php files within the webroot via add_to_prospect_list.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8803</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 has Incorrect Access Control via action_saveHTMLField Bean Manipulation.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8802</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows PHAR Deserialization.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8801</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
salesagility -- suitecrm	SuiteCRM through 7.11.11 allows EmailsControllerActionGetFromFields PHP Object Injection.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung -- s6_edge_smartphone	Multiple buffer overflows in the esa_write function in /dev/seirenin the Exynos Seiren Audio driver, as used in Samsung S6 Edge, allow local users to cause a denial of service (memory corruption) via a large (1) buffer or (2) size parameter.	2020-02-12	not yet calculated	<a href="#">CVE-2015-7890</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap --	Certain settings page(s) in SAP Business Objects Business Intelligence Platform (CMC), version 4.2, generates error	2020-02-	not yet	<a href="#">CVE-2020-6189</a>



business_objects_intelligence_platform	messages that can give enterprise private-network related information which would otherwise be restricted leading to Information Disclosure.	12	calculator	<a href="#">CVE-2020-6183</a> <a href="#">MISC</a>
sap -- enterprise_resource_planning_and_s4hana	VAT Pro-Rata reports in SAP ERP (SAP_APPL versions 600, 602, 603, 604, 605, 606, 616 and SAP_FIN versions 617, 618, 700, 720, 730) and SAP S/4HANA (versions 100, 101, 102, 103, 104) do not perform necessary authorization checks for an authenticated user leading to Missing Authorization Check.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6188</a> <a href="#">MISC</a>
sap -- host_agent	SAP Host Agent, version 7.21, allows an unprivileged user to read the shared memory or write to the shared memory by sending request to the main SAPOSCOL process and receive responses that may contain data read with user root privileges e.g. size of any directory, system hardware and OS details, leading to Missing Authorization Check vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6183</a> <a href="#">MISC</a>
sap -- host_agent	SAP Host Agent, version 7.21, allows an attacker to cause a slowdown in processing of username/password-based authentication requests of the SAP Host Agent, leading to Denial of Service.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6186</a> <a href="#">MISC</a>
sap -- landscape_management	SAP Landscape Management, version 3.0, allows an attacker with admin privileges to execute malicious commands with root privileges in SAP Host Agent via SAP Landscape Management.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6192</a> <a href="#">MISC</a>
sap -- landscape_management	SAP Landscape Management, version 3.0, allows an attacker with admin privileges to execute malicious executables with root privileges in SAP Host Agent via SAP Landscape Management due to Missing Input Validation.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6191</a> <a href="#">MISC</a>
sap -- mobile_platform	SAP Mobile Platform, version 3.0, does not sufficiently validate an XML document accepted from an untrusted source which could lead to partial denial of service. Since SAP Mobile Platform does not allow External-Entity resolving, there is no issue of leaking content of files on the server.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6177</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver (Guided Procedures), versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, does not sufficiently validate an XML document input from a compromised admin, leading to Denial of Service.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6187</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver (Knowledge Management ICE Service), versions 7.30, 7.31, 7.40, 7.50, allows an unauthenticated attacker to execute malicious scripts leading to Reflected Cross-Site Scripting (XSS) vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6193</a> <a href="#">MISC</a>
sap -- netweaver_and_abap_platform	Under some circumstances the SAML SSO implementation in the SAP NetWeaver (SAP_BASIS versions 702, 730, 731, 740 and SAP ABAP Platform (SAP_BASIS versions 750, 751, 752, 753, 754), allows an attacker to include invalidated data in the HTTP response header sent to a Web user, leading to HTTP Response Splitting vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6181</a> <a href="#">MISC</a>
sap -- netweaver_and_s4hana	Under certain conditions, ABAP Online Community in SAP NetWeaver (SAP_BASIS version 7.40) and SAP S/4HANA (SAP_BASIS versions 7.50, 7.51, 7.52, 7.53, 7.54), does not sufficiently encode user-controlled inputs, resulting in Reflected Cross-Site Scripting (XSS) vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6184</a> <a href="#">MISC</a>
sap -- netweaver_and_s4hana	Under certain conditions ABAP Online Community in SAP NetWeaver (SAP_BASIS version 7.40) and SAP S/4HANA (SAP_BASIS versions 7.50, 7.51, 7.52, 7.53, 7.54), allows an authenticated attacker to store a malicious payload which results in Stored Cross Site Scripting vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2020-6185</a> <a href="#">MISC</a>
sap -- netweaver_as_java	Certain vulnerable endpoints in SAP NetWeaver AS Java (Heap Dump Application), versions 7.30, 7.31, 7.40, 7.50, provide valuable information about	2020-02-	not yet	<a href="#">CVE-2020-6190</a>

	the system like hostname, server node and installation path that could be misused by an attacker leading to Information Disclosure.	12	calculator	<a href="#">MISC</a> <a href="#">MISC</a>
shaman -- shaman	Shaman 1.0 9: Users can add the line askforpwd=false to his shaman.conf file, without entering the root password in shaman. The next time shaman is run, root privileges are granted despite the fact that the user never entered the root password.	2020-02-12	not yet calculated	<a href="#">CVE-2011-4338</a> <a href="#">MISC</a> <a href="#">MISC</a>
siemens -- multiple_devices	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All Versions < V4.5), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All Versions < V4.6), PROFINET Driver for Controller (All Versions < V2.1), RUGGEDCOM RM1224 (All versions < V4 3), SCALANCE M-800 / S615 (All versions < V4.3), SCALANCE W700 IEEE 802.11n (All versions <= V6 0.1), SCALANCE X-200 switch family (incl. SIPLUS NET variants) (All versions), SCALANCE X-200IRT switch family (incl. SIPLUS NET variants) (All Versions < V5 3), SCALANCE X-300 switch family (incl. X408 and S PLUS NET variants) (All versions), SCALANCE XB-200, XC-200, XP-200, XF-200BA and XR-300WG (All Versions < V3.0), SCALANCE XM-400 switch family (All Versions < V6.0), SCALANCE XR-500 switch family (All Versions < V6.0), SIMATIC CP 1616 and CP 1604 (All Versions < V2.8), S MATIC CP 343-1 (incl. SIPLUS NET variants) (All versions), SIMATIC CP 343-1 Advanced (incl. SIPLUS NET variants) (All versions), SIMATIC CP 343-1 ERPC (All versions), SIMATIC CP 343-1 LEAN (incl. SIPLUS NET variants) (All versions), SIMATIC CP 443-1 (incl. SIPLUS NET variants) (All versions), SIMATIC CP 443-1 Advanced (incl. S PLUS NET variants) (All versions), S MATIC CP 443-1 OPC UA (All versions), SIMATIC ET200AL M 157-1 PN (All versions), SIMATIC ET200M IM153-4 PN IO HF (incl. SIPLUS variants) (All versions), SIMATIC ET200M IM153-4 PN IO ST (incl. SIPLUS variants) (All versions), S MATIC ET200MP IM155-5 PN HF (incl. S PLUS variants) (All Versions < V4.2.0), SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants) (All Versions < V4.1.0), SIMATIC ET200S (incl. SIPLUS variants) (All versions), SIMATIC ET200SP IM155-6 PN Basic (incl. SIPLUS variants) (All versions), SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants) (All Versions < V3.3.1), SIMATIC ET200SP IM155-6 PN ST (incl. SIPLUS variants) (All Versions < V4.1 0), SIMATIC ET200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0) (All versions), S MATIC ET200pro, IM 154-3 PN HF (All versions), SIMATIC ET200pro, IM 154-4 PN HF (All versions), SIMATIC IPC Support, Package for VxWorks (All versions), SIMATIC MV400 family (All versions), S MATIC PN/PN Coupler 6ES7158-3AD01-0XA0 (incl. SIPLUS NET variant) (All Versions), SIMATIC RF180C (All versions), SIMATIC RF182C (All versions), SIMATIC RF600 family (All versions < V3), SINAMICS DCP (All Versions < V1 3). Profinet-IO (PNIO) stack versions prior V06.00 do not properly limit internal resource allocation when multiple legitimate diagnostic package requests are sent to the DCE-RPC interface. This could lead to a denial of service condition due to lack of memory for devices that include a vulnerable version of the stack. The security vulnerability could be exploited by an attacker with network access to an affected device. Successful	2020-02-11	not yet calculated	<a href="#">CVE-2019-13946</a> <a href="#">MISC</a>

	exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise the availability of the device.			
simple_machines -- simple_machines_forum	Simple Machines Forum (SMF) through 2.0.5 has XSS	2020-02-12	not yet calculated	<a href="#">CVE-2013-4395</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplisafe -- ss3_devices	Authentication bypass using an alternate path or channel in SimpliSafe SS3 firmware 1.4 allows a local, unauthenticated attacker to modify the Wi-Fi network the base station connects to.	2020-02-13	not yet calculated	<a href="#">CVE-2019-3998</a> <a href="#">MISC</a>
skril -- skril	Commerce Skril (Formerly Moneybookers) has an Access bypass vulnerability in all versions prior to 7.x-1.2	2020-02-12	not yet calculated	<a href="#">CVE-2013-1924</a> <a href="#">MISC</a> <a href="#">MISC</a>
sprite_software -- spritebud_and_backup	A Privilege Escalation Vulnerability exists in Sprite Software Spritebud 1.3.24 and 1.3.28 and Backup 2.5.4105 and 2.5.4108 on LG Android smartphones due to a race condition in the spritebud daemon, which could let a local malicious user obtain root privileges.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3685</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sqlite -- android_sqlite	Android SQLite Journal before 4.0.1 has an information disclosure vulnerability.	2020-02-12	not yet calculated	<a href="#">CVE-2011-3901</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
squirrelmail -- squirrelmail	Squirrelmail 4.0 uses the outdated MD5 hash algorithm for passwords.	2020-02-13	not yet calculated	<a href="#">CVE-2012-5623</a> <a href="#">MISC</a> <a href="#">MISC</a>
stem_innovation -- izon_ip_camera	IZON P 2 0.2: hard-coded password vulnerability	2020-02-12	not yet calculated	<a href="#">CVE-2013-6236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
stmicroelectronics -- stm32wb5x_series_devices	The Bluetooth Low Energy implementation on STMicroelectronics BLE Stack through 1.3.1 for STM32WB5x devices does not properly handle consecutive Attribute Protocol (ATT) requests on reception, allowing attackers in radio range to cause an event deadlock or crash via crafted packets.	2020-02-12	not yet calculated	<a href="#">CVE-2019-19192</a> <a href="#">MISC</a>
synergy_systems_&_solutions -- husky_rtu_devices	The Synergy Systems & Solutions PLC & RTU system has a vulnerability in HUSKY RTU 6049-E70 firmware versions 5.0 and prior. Specially crafted malicious packets could cause disconnection of active authentic connections or reboot of device. This is a different issue than CVE-2019-16879 and CVE-2019-20046.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20045</a> <a href="#">MISC</a>
synergy_systems_&_solutions -- husky_rtu_devices	The Synergy Systems & Solutions PLC & RTU system has a vulnerability in HUSKY RTU 6049-E70 firmware versions 5.0 and prior. The affected product does not require adequate authentication, which may allow an attacker to read sensitive information or execute arbitrary code. This is a different issue than CVE-2019-16879 and CVE-2019-20046.	2020-02-14	not yet calculated	<a href="#">CVE-2019-20046</a> <a href="#">MISC</a>
telink -- tslr8x5_and_tslr823x_and_tslr826x_devices	The Bluetooth Low Energy Secure Manager Protocol (SMP) implementation on Telink Semiconductor BLE SDK versions before November 2019 for TSLR8x5x through 3.4.0, TSLR823x through 1.3.0, and TSLR826x through 3.3 devices accepts a pairing request with a key size greater than 16 bytes, allowing an attacker in radio range to cause a buffer overflow and denial of service (crash) via crafted packets.	2020-02-12	not yet calculated	<a href="#">CVE-2019-19196</a> <a href="#">MISC</a> <a href="#">MISC</a>
telink -- tslr8x5_and_tslr823x_and_tslr826x_devices	The Bluetooth Low Energy Secure Manager Protocol (SMP) implementation on Telink Semiconductor BLE SDK versions before November 2019 for TSLR8x5x through 3.4.0, TSLR823x through 1.3.0, and TSLR826x through 3.3 devices installs a zero long term key (LTK) if an out-of-order link-layer encryption request is received during Secure Connections pairing. An attacker in radio range can have arbitrary read/write access to protected GATT service data, cause a device crash, or possibly control a device's function by	2020-02-12	not yet calculated	<a href="#">CVE-2019-19194</a> <a href="#">MISC</a> <a href="#">MISC</a>

	establishing an encrypted session with the zero LTK.			
telligent_systems -- telligent_community	XSS in Telligent Community 5.6 583.20496 via a flash file and related to the allowScriptAccess parameter.	2020-02-13	not yet calculated	<a href="#">CVE-2012-1903</a> MISC
tiki_wiki -- cms_groupware	A Cross-Site Scripting (XSS) vulnerability exists in Tiki Wiki CMG Groupware 11.0 via the id paraZeroClipboard swf, which could let a remote malicious user execute arbitrary code.	2020-02-12	not yet calculated	<a href="#">CVE-2013-6022</a> MISC
timetools -- multiple_deivces	TimeTools SC7105 1 0.007, SC9205 1.0 007, SC9705 1.0.007, SR7110 1.0 007, SR9210 1.0.007, SR9750 1.0 007, SR9850 1.0.007, T100 1.0.003, T300 1.0 003, and T550 1.0.003 devices allow remote attackers to bypass authentication by placing t3axs=TiMEtOOlsj7G3xMm52wB in a t3.cgi request, aka a "hardcoded cookie."	2020-02-13	not yet calculated	<a href="#">CVE-2020-8964</a> MISC
timetools -- multiple_deivces	TimeTools SC7105 1 0.007, SC9205 1.0 007, SC9705 1.0.007, SR7110 1.0 007, SR9210 1.0.007, SR9750 1.0 007, SR9850 1.0.007, T100 1.0.003, T300 1.0 003, and T550 1.0.003 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the t3.cgi srmodel or srtime parameter.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8963</a> MISC
trendnet -- ts- s402_devices	TRENDnet TS-S402 has a backdoor to enable TELNET.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6360</a> MISC
tri-plc -- internet_trilogi_server	Internet TRILOGI Server (unknown versions) could allow a local user to bypass security and create a local user account.	2020-02-13	not yet calculated	<a href="#">CVE-2013-6927</a> MISC
umplayer -- umplayer	A Code Execution Vulnerability exists in UMPlayer 0 98 in wintab32 dll due to insufficient path restrictions when loading external libraries. which could let a malicious user execute arbitrary code.	2020-02-12	not yet calculated	<a href="#">CVE-2013-3494</a> MISC
varnish_software -- varnish_http_cache	Varnish HTTP cache before 3.0.4: ACL bug	2020-02-12	not yet calculated	<a href="#">CVE-2013-4090</a> MISC
visual_it -- tube_map_live_underground	Tube Map Live Underground for Android before 0.22 has an Information Disclosure Vulnerability	2020-02-12	not yet calculated	<a href="#">CVE-2013-6681</a> MISC
voatz -- voatz_for_android	The Voatz application 2020-01-01 for Android allows only 100 million different PINs, which makes it easier for attackers (after using root access to make a copy of the local database) to discover login credentials and voting history via an offline brute-force approach.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8988</a> MISC
voatz -- voatz_for_android	In the Voatz application 2020-01-01 for Android, the amount of data transmitted during a single voter's vote depends on the different lengths of the metadata across the available voting choices, which makes it easier for remote attackers to discover this voter's choice by sniffing the network. For example, a small amount of sniffed data may indicate that a vote was cast for the candidate with the least metadata. An active man-in-the-middle attacker can leverage this behavior to disrupt voters' abilities to vote for a candidate opposed by the attacker.	2020-02-13	not yet calculated	<a href="#">CVE-2020-8989</a> MISC
weechat - weechat	irc_mode_channel_update in plugins/irc-mode.c in WeeChat through 2.7 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a malformed IRC message 324 (channel mode).	2020-02-12	not yet calculated	<a href="#">CVE-2020-8955</a> MISC
wordpress -- wordpress	participants-database.php in the Participants Database plugin 1 9.5.5 and previous versions for WordPress has a time-based SQL injection vulnerability via the ascdesc, list_filter_count, or sortBy parameters. It is possible to exfiltrate data and potentially execute code (if certain conditions are met).	2020-02-11	not yet calculated	<a href="#">CVE-2020-8596</a> MISC
wordpress --	The Ninja Forms plugin 3.4.22 for WordPress has Multiple Stored XSS vulnerabilities via	2020-02-	not yet	<a href="#">CVE-2020-8594</a>



wordpress	ninja_forms[recaptcha_site_key], ninja_forms[recaptcha_secret_key], ninja_forms[recaptcha_lang], or ninja_forms[date_format].	14	calculator	<a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
wordpress -- wordpress	Multiple SQL injection vulnerabilities in CWPPoll.js in WordPress Poll Plugin 34.5 for WordPress allow attackers to execute arbitrary SQL commands via the pollid or poll_id parameter in a viewPollResults or userlogs action.	2020-02-13	not yet calculator	<a href="#">CVE-2013-1400</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">BUGTRAQ</a>
wordpress -- wordpress	Multiple security bypass vulnerabilities in the editAnswer, deleteAnswer, addAnswer, and deletePoll functions in WordPress Poll Plugin 34.5 for WordPress allow a remote attacker to add, edit, and delete an answer and delete a poll.	2020-02-13	not yet calculator	<a href="#">CVE-2013-1401</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">BUGTRAQ</a>
wordpress -- wordpress	WordPress WP Cleanfix Plugin 2.4.4 has CSRF	2020-02-10	not yet calculator	<a href="#">CVE-2013-2108</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress plugin wp-cleanfix has Remote Code Execution	2020-02-10	not yet calculator	<a href="#">CVE-2013-2109</a> <a href="#">MISC</a> <a href="#">MISC</a>
xerox -- colorcube_and_workcenter	Xerox ColorCube and WorkCenter devices in 2013 had hardcoded FTP and shell user accounts.	2020-02-13	not yet calculator	<a href="#">CVE-2013-6362</a> <a href="#">MISC</a> <a href="#">MISC</a>
xilisoft -- video_converter_ultimate	Xilisoft Video Converter Ultimate 7.8.1 build-20140505 has a DLL Hijacking vulnerability	2020-02-12	not yet calculator	<a href="#">CVE-2014-3860</a> <a href="#">MISC</a>
zenoss -- zenoss_core	Multiple format string vulnerabilities in the python module in RRDtool, as used in Zenoss Core before 4.2.5 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted third argument to the rrdtool.graph function, aka ZEN-15415, a related issue to CVE-2013-2131.	2020-02-12	not yet calculator	<a href="#">CVE-2014-6262</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zimbra -- zimbra_collaboration	Zimbra 2013 has XSS in aspell php	2020-02-12	not yet calculator	<a href="#">CVE-2013-1938</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zpanel_project -- zpanel	ZPanel through 10.1.0 has Remote Command Execution	2020-02-12	not yet calculator	<a href="#">CVE-2013-2097</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [trmcginnis@sunnyvale.ca.gov](mailto:trmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20508 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [edigiovanna@sunnyvale.ca.gov](mailto:edigiovanna@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of February 3, 2020  
**Date:** Wednesday, February 12, 2020 12:48:43 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

*\*The tables in Vulnerability Bulletin (SB20-041) have been updated.*

## **Vulnerability Summary for the Week of February 3, 2020**

02/10/2020 07:28 AM EST

Original release date: February 10, 2020 | Last revised: February 12, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	2020-01-31	7.5	<a href="#">CVE-2014-8322</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aruba_networks -- instant	Multiple vulnerabilities exists in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.	2020-01-31	7.5	<a href="#">CVE-2016-2031</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	7.8	<a href="#">CVE-2020-3926</a> <a href="#">CONFIRM</a>

changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	8.5	<a href="#">CVE-2020-3927</a> <a href="#">CONFIRM</a>
cisco -- multiple_ip_phones	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	8.3	<a href="#">CVE-2020-3111</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- video_surveillance_8000_series_ip_cameras	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later.	2020-02-05	8.3	<a href="#">CVE-2020-3110</a> <a href="#">MISC</a> <a href="#">CISCO</a>
coppermine_development -- coppermine_gallery	Coppermine gallery before 1.4.26 has an input validation vulnerability that allows for code execution.	2020-02-05	7.5	<a href="#">CVE-2010-4815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

curling -- curling	All versions of curling.js are vulnerable to Command Injection via the run function. The command argument can be controlled by users without any sanitization.	2020-02-06	<a href="#">10</a>	<a href="#">CVE-2019-10789</a> <a href="#">MISC</a> <a href="#">MISC</a>
django -- django	Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-7471</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
dot-prop -- dot-prop	Prototype pollution vulnerability in dot-prop npm package version 5.1.0 and earlier allows an attacker to add arbitrary properties to JavaScript language constructs such as objects.	2020-02-04	<a href="#">7.5</a>	<a href="#">CVE-2020-8116</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.2.4 is vulnerable to directory traversal, leading to incorrect access control. It allows an attacker to read or execute files under \$TOMCAT_HOME/webapps/ROOT/assets (which should be a protected directory). Additionally, attackers can upload temporary files (e.g., .jsp files) into /webapps/ROOT/assets/tmp_upload, which can lead to remote command execution (with the permissions of the user running the dotCMS application).	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-6754</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
edk2 -- unified_extensible_firmware_interface	Multiple integer overflows in the Pre-EFI Initialization (PEI) boot phase in the Capsule Update feature in the UEFI implementation in EDK2 allow physically proximate attackers to bypass intended access restrictions by providing crafted data that is not properly handled during the coalescing phase.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4860</a> <a href="#">MISC</a>
edk2 -- unified_extensible_firmware_interface	Integer overflow in the Drive Execution Environment (DXE) phase in the Capsule Update feature in the UEFI implementation in EDK2 allows physically proximate attackers to bypass intended access restrictions via crafted data.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4859</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows SQL Injection via the user parameter to com.eg.LoginHelperServlet (aka the Forgot Password feature).	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8592</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows authentication bypass via a com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8591</a> <a href="#">MISC</a>



	request.			
fortinet -- fortimanager	A Command Injection vulnerability exists in FortiManager 5.2.1 and earlier and FortiManager 5.0.10 and earlier via unspecified vectors, which could let a malicious user run systems commands when executing a report.	2020-02-04	9	<a href="#">CVE-2015-3611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- mortimanager	A vulnerability exists in in FortiManager 5.2.1 and earlier and 5.0.10 and earlier in the WebUI FTP backup page	2020-02-04	7.5	<a href="#">CVE-2015-3613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	7.5	<a href="#">CVE-2020-8114</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.2 incorrectly validated role/region associated with TLS certificates used for mTLS RPC, and were susceptible to privilege escalation. Fixed in 0.10.3.	2020-01-31	7.5	<a href="#">CVE-2020-7956</a> <a href="#">MISC</a> <a href="#">MISC</a>
jobberbase -- jobberbase	Jobberbase 2.0 has SQL injection via the PATH_INFO to the jobs-in endpoint.	2020-02-05	7.5	<a href="#">CVE-2019-20447</a> <a href="#">MISC</a> <a href="#">MISC</a>
klona -- klona	Flaw in input validation in npm package klona version 1.1.0 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using klona.	2020-02-04	7.5	<a href="#">CVE-2020-8125</a> <a href="#">MISC</a>
nanopb -- nanopb	There is a potentially exploitable out of memory condition In Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is compiled with PB_ENABLE_MALLOC, the message to be decoded contains a repeated string, bytes or message field and realloc() runs out of memory when expanding the array nanopb can end up calling `free()` on a pointer value that comes from uninitialized memory. Depending on platform this can result in a crash or further memory corruption, which may be exploitable in some cases. This problem is fixed in nanopb-0.4.1, nanopb-0.3.9.5, nanopb-0.2.9.4.	2020-02-04	7.5	<a href="#">CVE-2020-5235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netapp -- oncommand_system_manager	NetApp OnCommand System Manager 2.1 and earlier allows remote attackers to execute arbitrary commands in the Halt/Reboot interface.	2020-01-31	9	<a href="#">CVE-2013-3322</a> <a href="#">XF</a> <a href="#">MISC</a>
norman -- malware_cleaner	nsak64.sys in Norman Malware Cleaner 2.08.08 allows users to call arbitrary kernel functions because the passing of function pointers between user and kernel	2020-02-03	7.5	<a href="#">CVE-2020-8508</a> <a href="#">MISC</a>

	mode is mishandled.			
phpabook -- phpabook	An issue was discovered in phpABook 0.9 Intermediate. On the login page, if one sets a userInfo cookie with the value of admin+1+en (user+perms+lang), one can login as any user without a password.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8510</a> <a href="#">MISC</a> <a href="#">MISC</a>
phplist -- phplist	phplist 3.5.0 allows type juggling for admin login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8547</a> <a href="#">MISC</a>
playsms -- playsms	PlaySMS before 1.4.3 does not sanitize inputs from a malicious string.	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-8644</a> <a href="#">MISC</a> <a href="#">MISC</a>
ppp -- ppp	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8597</a> <a href="#">MISC</a> <a href="#">MLIST</a>
python -- python	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.	2020-02-04	<a href="#">7.1</a>	<a href="#">CVE-2019-9674</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- mdm9206_and_mdm9607_devices	Subsequent additions performed during Module loading while allocating the 9607_devices could lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14051</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14046</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open close in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14044</a> <a href="#">CONFIRM</a>
	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon			

qualcomm -- multiple_snapdragon_products	Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14055</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14002</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> <a href="#">CONFIRM</a>
	Out of bound access due to Invalid inputs to dapm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial			

qualcomm -- multiple_snapdragon_products	IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14063</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Uninitialized stack data gets used if memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14060</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14057</a> <a href="#">CONFIRM</a>



qualcomm -- multiple_snapdragon_products	Stage-2 fault will occur while writing to an ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14049</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> <a href="#">CONFIRM</a>
sap -- netweaver	SAP NetWeaver 7.0 allows Remote Code Execution and Denial of Service caused by an error in the DiagTraceHex() function. By sending a specially-crafted packet, an attacker could exploit this vulnerability to cause the application to crash.	2020-02-05	7.5	<a href="#">CVE-2011-1517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript.com -- simplejobscript.com	controllers/page_apply.php in Simplejobscript.com SJS through 1.66 is prone to unauthenticated Remote Code Execution by uploading a PHP script as a resume.	2020-01-31	7.5	<a href="#">CVE-2020-8440</a> <a href="#">CONFIRM</a>
smartbear -- readyapi_and_soapui	An issue was discovered in SmartBear ReadyAPI through 2.8.2 and 3.0.0 and SoapUI through 5.5. When opening a project, the Groovy "Load Script" is automatically executed. This allows an attacker to execute arbitrary Groovy Language code (Java scripting language)	2020-02-05	9.3	<a href="#">CVE-2019-12180</a> <a href="#">MISC</a>

	on the victim machine by inducing it to open a malicious Project. The same issue is present in the "Save Script" function, which is executed automatically when saving a project.			
squid -- squid	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	2020-02-04	7.5	<a href="#">CVE-2020-8450</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_update_framework -- tuf	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature.	2020-02-05	7.5	<a href="#">CVE-2020-6174</a> <a href="#">CONFIRM</a>
tp-link -- tg-sg105e_devices	The Web Management of TP-Link TP-SG105E V4 1.0.0 Build 20181120 devices allows an unauthenticated attacker to reboot the device via a reboot.cgi request.	2020-02-03	7.8	<a href="#">CVE-2019-16893</a> <a href="#">EXPLOIT-DB</a>
zpanel_project -- zpanel	ZPanel 10.0.1 has insufficient entropy for its password reset process.	2020-02-04	7.5	<a href="#">CVE-2012-5686</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	6.5	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	5	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	4.6	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent --	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch			<a href="#">CVE-2014-</a>

1830_photonic_service	OS 16.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	2020-01-31	<a href="#">4.3</a>	<a href="#">3809 MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-12426 MLIST CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	<a href="#">4.9</a>	<a href="#">CVE-2011-0220 MISC</a>
apple -- safari	A Cross-origin vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2016-4676 MISC MISC MISC CONFIRM MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8505 MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8504 MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2016-2032 MISC MISC MISC MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20104 N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404 N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20400 N/A</a>
	The JMX monitoring flag in Atlassian Jira Server and Data Center before version			<a href="#">CVE-2019-</a>

atlassian -- jira	8.6.0 allows remote attackers to turn the JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	2020-02-06	<a href="#">4.3</a>	<a href="#">20405</a> <a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20403</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20402</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2674</a> <a href="#">MISC</a> <a href="#">XE</a> <a href="#">BID</a>



brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	5	<a href="#">CVE-2013-2672</a> <a href="#">MISC</a> <a href="#">XF</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	4.6	<a href="#">CVE-2013-2673</a> <a href="#">MISC</a> <a href="#">BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	5	<a href="#">CVE-2019-12998</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	5	<a href="#">CVE-2013-2683</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	5	<a href="#">CVE-2013-2680</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	6.8	<a href="#">CVE-2013-2678</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	4.3	<a href="#">CVE-2013-2681</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	4.3	<a href="#">CVE-2013-2682</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	4.3	<a href="#">CVE-2013-2684</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
computer_incident_response -- ail-framework	Global Cyber All framework 2.8 allows path traversal.	2020-02-03	5	<a href="#">CVE-2020-8545</a> <a href="#">MISC</a>
cysharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions	2020-01-31	6.8	<a href="#">CVE-2020-5234</a> <a href="#">MISC</a>

	and stack overflow. Review the linked GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus -- eucalyptus_management_console	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>

evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	6.6	<a href="#">CVE-2013-5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	5	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	4.6	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	5	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	5	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	4.3	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	4	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>



hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 0.10.3 allow unbounded resource usage.	2020-01-31	5	<a href="#">7218</a> <a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	6.5	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information_server	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	5.8	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	6.8	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	6.9	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	6.5	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	6	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	5.8	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or	2020-02-04	5	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

	browser history. IBM X-Force ID: 166623.			
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> XF <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> XF <a href="#">CONFIRM</a>
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> MISC MISC MISC
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> MISC MISC MISC MISC

info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8139</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	4.3	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	6.5	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	5	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	5	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	5	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	6.4	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	5	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be			

joomla! -- joomla!	entered by any user. If it doesn't contain rel="noopener" (or similar attributes such as noreferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	2020-02-03	4.3	<a href="#">CVE-2020-5182</a> <a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	4.3	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	5	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	5	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	6.6	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	6.5	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	4.3	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- rumpus	An issue was discovered in Rumpus 0.2.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	4.3	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to	2020-02-06	4.4	<a href="#">CVE-2019-20406</a>



	write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.			<a href="#">N/A</a>
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	5	<a href="#">4116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	5	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	6.4	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	4.3	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	4.3	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	4	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	6.8	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon			

qualcomm -- multiple_snapdragon_products	Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>

squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- openSUSE_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a>



	to arbitrary websites via a crafted URL.			<a href="#">MISC</a>
telaen -- telaen	Telaen before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted URL request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2624</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browsery" in the page image.php.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	<a href="#">5</a>	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>

	vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

wordpress -- wordpress	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can result in an attacker performing malicious actions such as stealing session tokens.	2020-02-03	<a href="#">4.3</a>	<a href="#">8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	<a href="#">4</a>	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) 5.0.1050 through 5.1.1067 and 6.0.1000 through 6.0.1003 allows Insecure Direct Object Reference (IDOR) by an authenticated sender because of an error in a file-upload feature. This is fixed in 5.1.1068 and 6.0.1004.	2020-01-31	<a href="#">3.5</a>	<a href="#">CVE-2020-8503</a> <a href="#">MISC</a>
bromium -- secure_platform	Bromium client version 4.0.3.2060 and prior to 4.1.7 Update 1 has an out of bound read results in race condition causing Kernel memory leaks or denial of service.	2020-02-03	<a href="#">3.3</a>	<a href="#">CVE-2019-18567</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	A vulnerability in the web-based management interface of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management			

cisco -- digital_network_architecture	interface of an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker needs administrator credentials. This vulnerability affects Cisco DNA Center Software releases earlier than 1.3.0.6 and 1.3.1.4.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2019-15253</a> <a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack on an affected device. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by providing malicious data to a specific field within the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco ISE Software releases 2.7.0 and later contains the fix for this vulnerability.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2020-3149</a> <a href="#">CISCO</a>
cloud-init -- cloud-init	In cloud-init through 19.4, rand_user_password in cloudinit/config/cc_set_passwords.py has a small default pwlen value, which makes it easier for attackers to guess passwords.	2020-02-05	<a href="#">2.1</a>	<a href="#">CVE-2020-8632</a> <a href="#">MISC</a> <a href="#">MISC</a>
cloud-init -- cloud-init	cloud-init through 19.4 relies on Mersenne Twister for a random password, which makes it easier for attackers to predict passwords, because rand_str in cloudinit/util.py calls the random.choice function.	2020-02-05	<a href="#">2.1</a>	<a href="#">CVE-2020-8631</a> <a href="#">MISC</a> <a href="#">MISC</a>
fortinet -- fortimanager	A Cross-site Scripting (XSS) vulnerability exists in FortiManager 5.2.1 and earlier and 5.0.10 and earlier via an unspecified parameter in the FortiWeb auto update service page.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2015-3612</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 163493.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-4451</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
	IBM StoredIQ 7.6.0.17 through 7.6.0.20			



ibm -- storediq	could disclose sensitive information to a local user due to data in certain directories not being encrypted when it contained symbolic links. IBM X-Force ID: 175133.	2020-02-03	<a href="#">2.1</a>	<a href="#">CVE-2020-4224</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8649</a> <a href="#">MISC</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vc_do_resize function in drivers/tty/vt/vt.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8647</a> <a href="#">MISC</a>
linux -- linux_kernel	In a Linux KVM guest that has PV TLB enabled, a process in the guest kernel may be able to read memory locations from another process in the same guest. This problem is limit to the host running linux kernel 4.10 with a guest running linux kernel 4.16 or later. The problem mainly affects AMD processors but Intel CPUs cannot be ruled out.	2020-01-31	<a href="#">1.9</a>	<a href="#">CVE-2019-3016</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8648</a> <a href="#">MISC</a>
nextcloud -- nextcloud	Missing escaping of HTML in the Updater of Nextcloud 15.0.5 allowed a reflected XSS when starting the updater from a malicious location.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-15618</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg	An issue was discovered in PRTG 7.x through 19.4.53. Due to insufficient access control on local registry keys for the Core Server Service, a non-administrative user on the local machine is able to access administrative credentials.	2020-02-03	<a href="#">2.1</a>	<a href="#">CVE-2019-19119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
pandora_fms -- pandora_fms	PandoraFMS 742 suffers from multiple XSS vulnerabilities, affecting the Agent Management, Report Builder, and Graph Builder components. An authenticated user can inject dangerous content into a data store that is later read and included in dynamic content.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-19968</a> <a href="#">MISC</a> <a href="#">MISC</a>
sos -- jobscheduler	A cross-site scripting (XSS) vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to inject arbitrary web script or HTML via JSON properties available from the REST API.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2020-6854</a> <a href="#">MISC</a>
wordpress -- wordpress	A CSRF vulnerability in the Tutor LMS plugin before 1.5.3 for WordPress can result in an attacker approving themselves as an instructor and performing other malicious actions (such	2020-02-04	<a href="#">2.6</a>	<a href="#">CVE-2020-8615</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

as blocking legitimate instructors).

[MISC](#)

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS& Score	Patch Info	Source
arctic_torrent -- arctic_torrent	A vulnerability exists in Arctic Torrent 1.4 via unspecified vectors in .torrent file handling, which could let a malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6309</a> <a href="#">MISC</a>	
atmail -- atmail_webmail_server	Cross-site scripting (XSS) vulnerability in the administrative interface in Atmail Webmail Server 6.4 allows remote attackers to inject arbitrary web script or HTML via the Date field of an email.	2020-02-06	not yet calculated	<a href="#">CVE-2012-2593</a> <a href="#">MISC</a>	
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	not yet calculated	<a href="#">CVE-2013-3091</a> <a href="#">MISC</a>	
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8796</a> <a href="#">MISC</a>	
bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>	
boonex -- dolphin	SQL injection vulnerability in Boonex Dolphin before 7.1.3 allows remote authenticated users to execute arbitrary SQL commands via the 'pathes' parameter in 'categories.php'.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3638</a> <a href="#">BID-XE</a>	
bosch -- bvms_mobile_video_service	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6770</a> <a href="#">CONFIRM</a>	
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP	2020-02-07	not yet calculated	<a href="#">CVE-2020-6768</a> <a href="#">CONFIRM</a>	

	7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.			
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6767</a> CONFIRM
bosch -- video_streaming_gateway	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6769</a> CONFIRM
broadcom -- multiple_devices	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic, a different vulnerability than CVE-2019-9500, CVE-2019-9501, CVE-2019-9502, and CVE-2019-9503.	2020-02-05	not yet calculated	<a href="#">CVE-2019-15126</a> CONFIRM
broadcom - wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. By supplying a vendor information element with a data length larger than 32 bytes, a heap buffer overflow is triggered in wlc_wpa_sup_eapol. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9501</a> MISC CERT. VN
broadcom - wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. If the vendor information element data length is larger than 164 bytes, a heap buffer overflow is triggered in wlc_wpa_plumb_gtk. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9502</a> MISC CERT. VN
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view private IP addresses and other sensitive information.	2020-02-04	not yet calculated	<a href="#">CVE-2013-2676</a> MISC XF BID

brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 devices with Firmware L contain a Frameable response (Clickjacking) vulnerability which could allow remote attackers to obtain sensitive information.	2020-02-05	not yet calculated	<a href="#">CVE-2013-2675</a> <a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a>
c-more -- touch_panels EA9 series	It is possible to unmask credentials and other sensitive information on ?unprotected? project files, which may allow remote attackers to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations.	2020-02-05	not yet calculated	<a href="#">CVE-2020-6969</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11481</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11484</a> <a href="#">MISC</a> <a href="#">MISC</a>
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1700</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cgilua -- cgilua	The session.lua library in CGILua 5.2 alpha 1 and 5.2 alpha 2 uses weak session IDs generated based on OS time, which allows remote attackers to hijack arbitrary sessions via a brute force attack. NOTE: CVE-2014-10300 and CVE-2014-10400 were SPLIT from this ID.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2875</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGILua 5.0.x uses sequential session IDs, which makes it easier for remote attackers to predict the session ID and hijack arbitrary sessions. NOTE:	2020-02-06	not yet calculated	<a href="#">CVE-2014-10400</a> <a href="#">MISC</a>



	this vulnerability was SPLIT from CVE-2014-2875.			<a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.1.x uses the same ID for each session, which allows remote attackers to hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10399</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chamilo -- chamilo_image	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_image -- - servisign	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts.	2020-02-03	not yet calculated	<a href="#">CVE-2020-3925</a> <a href="#">CONFIRM</a>
cisco -- application	Cisco ACE 4.2(3.6) allows log retention DoS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-1202</a> <a href="#">MISC</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3120</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability			

cisco -- cisco_discovery_protocol	exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3119</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- linksys_wrt110	Cross-site request forgery (CSRF) vulnerability in Cisco Linksys WRT110 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3568</a> <a href="#">EXPLOIT-DATABASE.BID.XF</a>
clamav -- clam_antivirus	A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	2020-02-05	not yet calculated	<a href="#">CVE-2020-3123</a> <a href="#">CISCO</a>
corsair -- corsair_icue	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8808</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir865l_devices	D-Link DIR865L v1.03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3096</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dd-wrt -- dd-wrt	Command Injection vulnerability exists via a CSRF in DD-WRT 24-sp2 from specially crafted configuration values containing shell meta-characters, which could let a remote malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6297</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dedicated -- multiple_dvr_products	Dedicated Micros DV-IP Express, SD Advanced, SD, EcoSense, and DS2 devices rely on a GUI warning to help ensure that the administrator configures login credentials, which makes it easier for remote attackers to obtain access by leveraging situations in which this warning was not needed. NOTE: the vendor states "The user is presented with clear warnings on the GUI that they should set usernames and passwords."	2020-02-06	not yet calculated	<a href="#">CVE-2015-2909</a> <a href="#">MISC</a> <a href="#">MISC</a>

dell -- dmc_isilon_ones	Dell EMC Isilon OneFS versions 8.1.2, 8.1.0.4, 8.1.0.3, and 8.0.0.7 contain a vulnerability in some configurations. An attacker may exploit this vulnerability to gain access to restricted files. The non-RAN HTTP and WebDAV file-serving components have a vulnerability wherein when either are enabled, and Basic Authentication is enabled for either or both components, files are accessible without authentication.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5318</a> MISC
dell -- emc_ecs	Dell EMC ECS versions prior to 3.4.0.1 contain an XSS vulnerability. A remote authenticated malicious user could exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5317</a> MISC
dell -- multiple_products	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5319</a> MISC
den_norsk -- im-metadata	im-metadata through 3.0.1 allows remote attackers to execute arbitrary commands via the "exec" argument. It is possible to inject arbitrary commands as part of the metadata options which is given to the "exec" function.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10788</a> CONFIRM MISC
den_norsk -- im-resize	im-resize through 2.3.2 allows remote attackers to execute arbitrary commands via the "exec" argument. The cmd argument used within index.js, can be controlled by user without any sanitization.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10787</a> CONFIRM MISC
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container IDs.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5278</a> MISC MISC MISC
drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	not yet calculated	<a href="#">CVE-2012-5570</a> MISC MISC CONFIRM
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The installation uses the same API key (hardcoded as EONAPI_KEY in include/api_functions.php for API version 2.4.2) by default for all installations, hence allowing an attacker to calculate/guess the admin access token.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8657</a> MISC
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in	2020-02-07	not yet calculated	<a href="#">CVE-2020-8656</a> MISC

	include/api_functions.php.			MISC
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	not yet calculated	CVE-2020-8654 MISC
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	not yet calculated	CVE-2020-8655 MISC
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made.	2020-02-06	not yet calculated	CVE-2020-5854 CONFIRM
flowplayer -- flowplayer	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	not yet calculated	CVE-2011-3642 MISC MISC MISC MISC MISC MISC MISC MISC MISC
fork_cms - fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	not yet calculated	CVE-2014-9470 MISC MISC MISC MISC MISC MISC
fortinet -- forticlient_for_linux	A Denial of service (DoS) vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to cause FortiClient processes running under root privilege to crash via sending specially crafted IPC client requests to the fctschd process due the nanomsg not been correctly validated.	2020-02-06	not yet calculated	CVE-2019-16152 MISC CONFIRM
fortinet -- forticlient_for_linux	A stack buffer overflow vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted "StartAvCustomScan" type IPC client requests to the fctschd process due the argv data not been well sanitized.	2020-02-06	not yet calculated	CVE-2019-17652 MISC CONFIRM
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to run arbitrary commands under root privilege via injecting specially crafted "ExportLogs" type IPC client requests to the fctschd process.	2020-02-06	not yet calculated	CVE-2019-15711 MISC CONFIRM



fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctsched process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	not yet calculated	<a href="#">CVE-2019-16155</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13333</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17136</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13334</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17135</a> <a href="#">MISC</a>
	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions,		not	<a href="#">CVE-</a>

fujitsu -- multiple_products	Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3, Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.	2020-02-07	yet calculated	2019- 13163 CONFIRM
gnome -- librsvg	In xml.rs in GNOME librsvg before 2.46.2, a crafted SVG file with nested patterns can cause denial of service when passed to the library for processing. The attacker constructs pattern elements so that the number of final rendered objects grows exponentially.	2020-02-02	not yet calculated	CVE- 2019- 20446 MISC
gnome -- evolution_and_evolution_data_server	The gpg_ctx_add_recipient function in camel/camel-gpg-context.c in GNOME Evolution 3.8.4 and earlier and Evolution Data Server 3.9.5 and earlier does not properly select the GPG key to use for email encryption, which might cause the email to be encrypted with the wrong key and allow remote attackers to obtain sensitive information.	2020-02-06	not yet calculated	CVE- 2013- 4166 CONFIRM MISC MISC CONFIRM CONFIRM
golang -- go	The net/http library in net/http/transfer.go in Go before 1.4.3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains Content-Length and Transfer-Encoding header fields.	2020-02-08	not yet calculated	CVE- 2015- 5741 MISC MISC MISC MISC MISC MISC
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	CVE- 2014- 7224 MISC MISC MISC MISC
google -- chrome	Google Chrome before 3.0 does not properly handle XML documents, which allows remote attackers to obtain sensitive information via a crafted web site.	2020-02-06	not yet calculated	CVE- 2010- 3917 MISC MISC
hardcoreview - - hardcoreview	A vulnerability exists in HCView (aka Hardcoreview) 1.4 due to a write access violation with a GIF file.	2020-02-06	not yet calculated	CVE- 2012- 6306 MISC MISC
hp -- sitescope	An Information Disclosure vulnerability exists in HP SiteScope 11.2 and 11.3 on Windows, Linux and Solaris, HP Asset Manager 9.30 through 9.32, 9.40 through 9.41, 9.50, and Asset Manager Cloudsystem Chargeback 9.40, which could let a remote malicious user obtain sensitive	2020-02-04	not yet calculated	CVE- 2015- 2802 CONFIRM CONFIRM MISC

	information. This is the TLS vulnerability known as the RC4 cipher Bar Mitzvah vulnerability.			<a href="#">MISC</a> <a href="#">MISC</a>
ibm -- cloud_automation_manager	IBM Cloud Automation Manager 3.2.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http://link to the user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 168644.	2020-02-05	not yet calculated	<a href="#">CVE-2019-4616</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 171511.	2020-02-04	not yet calculated	<a href="#">CVE-2019-4675</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7523</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Stack-based buffer overflow in the WritePSDImage function in coders/psd.c in ImageMagick, possibly 6.8.8-5, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-1947.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2030</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Buffer overflow in the DecodePSDPixels function in coders/psd.c in ImageMagick before 6.8.8-5 might allow remote attackers to execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-2030.	2020-02-06	not yet calculated	<a href="#">CVE-2014-1958</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ispconfig - - ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	not yet	<a href="#">CVE-2013-3629</a> <a href="#">MISC</a>

			calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jpegsnoot - jpegsnoot	A vulnerability exists in JPEGsnoot 1.5.2 due to an unspecified issue in JPEG file handling, which could let a malicious user execute arbitrary code	2020-02-06	not yet calculated	<a href="#">CVE-2012-6307</a> <a href="#">MISC</a> <a href="#">MISC</a>
kemp -- load_master	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5288</a> <a href="#">MISC</a> <a href="#">MISC</a>
konqueror - konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	not yet calculated	<a href="#">CVE-2012-4512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys -- wrt310n_wireless_router	Linksys WRT310Nv2 2.0.0.1 is vulnerable to XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3067</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
mariadb -- mariadb	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.	2020-02-04	not yet calculated	<a href="#">CVE-2020-7221</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mcabber - - mcabber	MCabber before 1.0.4 is vulnerable to roster push attacks, which allows remote attackers to intercept communications, or add themselves as an entity on a 3rd party's roster as	2020-02-06	not yet	<a href="#">CVE-2016-9928</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>



	another user, which will also garner associated privileges, via crafted XMPP packets.		calculated	MISC CONFIRM CONFIRM CONFIRM MISC
mediawiki - mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	not yet calculated	CVE-2012-4381 MISC MISC MISC MISC MISC MISC MISC
mediawiki - mediawiki	The CentralNotice extension for MediaWiki before 1.19.9, 1.20.x before 1.20.8, and 1.21.x before 1.21.3 sets the Cache-Control header to cache session cookies when a user is autocreated, which allows remote attackers to authenticate as the created user.	2020-02-06	not yet calculated	CVE-2013-4572 MISC MISC CONFIRM MISC
mikrotik -- winbox	MikroTik WinBox before 3.21 is vulnerable to a path traversal vulnerability that allows creation of arbitrary files wherever WinBox has write permissions. WinBox is vulnerable to this attack if it connects to a malicious endpoint or if an attacker mounts a man in the middle attack.	2020-02-06	not yet calculated	CVE-2020-5720 MISC
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exastm R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to execute arbitrary code via a crafted packet.	2020-02-05	not yet calculated	CVE-2015-5628 CONFIRM MISC
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exastm R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS	2020-02-05	not yet calculated	CVE-2015-5627 CONFIRM MISC

	R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (process outage) via a crafted packet.			
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (network-communications outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5626</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h_____%2427, (3) h_____%2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-3423</a> <a href="#">MISC</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the system, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8) xname, or (9) mpTransactionId parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wireless_router	An Authentication vulnerability exists in NETGEAR WGR614 wireless router due to a hardcoded credential used for serial programming, a related issue to CVE-2006-1002.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6340</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wireless_router	An Information Disclosure vulnerability exists in the my config file in NetGEAR WGR614 v7 and v9, which could let a malicious user recover all previously used passwords on the device, for both the control panel and WEP/WPA/WPA2, in plaintext. This is a different issue than CVE-2012-6340.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1.2.31805 and V2.2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracert diagnostic tool because of lack of user input sanitizing.	2020-02-07	not yet calculated	<a href="#">CVE-2019-19356</a> <a href="#">MISC</a>
network-manager - network-manager	network-manager through 1.0.2 allows remote attackers to execute arbitrary commands via the "execSync()" argument.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10786</a> <a href="#">MISC</a>

nextcloud -- circles	Improper authorization in the Circles app 0.17.7 causes retaining access when an email address was removed from a circle.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15610</a> MISC
nextcloud -- nextcloud_android	A wrong check for the system time in the Android App 3.9.0 causes a bypass of the lock protection when changing the time of the system to the past.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15615</a> MISC
nextcloud -- nextcloud_android	Not strictly enough sanitization in the Nextcloud Android app 3.6.0 allowed an attacker to get content information from protected tables when using custom queries.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15622</a> MISC
nextcloud -- nextcloud_server	Violation of Secure Design Principles in the iOS App 2.23.0 causes the app to leak its login and token to other Nextcloud services when search e.g. for federated users or registering for push notifications.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15611</a> MISC
nextcloud -- nextcloud_server	Missing sanitization in the iOS App 2.24.4 causes an XSS when opening malicious HTML files.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15614</a> MISC
nextcloud -- nextcloud_server	Improper permissions preservation in Nextcloud Server 16.0.1 causes sharees to be able to reshare with write permissions when sharing the mount point of a share they received, as a public link.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15621</a> MISC
nextcloud -- nextcloud_server	Dangling remote share attempts in Nextcloud 16 allow a DoS/pollution when running long.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15616</a> MISC
nextcloud -- nextcloud_server	A bug in Nextcloud Server 15.0.2 causes pending 2FA logins to not be correctly expired when the password of the user is reset.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15612</a> MISC
nextcloud -- nextcloud_server	A bug in Nextcloud Server 17.0.1 causes the workflow rules to depend their behaviour on the file extension when checking file mimetypes.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15613</a> MISC
nextcloud -- nextcloud_server	A missing check in Nextcloud Server 17.0.0 allowed an attacker to set up a new second factor when trying to login.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15617</a> MISC
nextcloud -- nextcloud_server	Improper Input Validation in Nextcloud Server 15.0.7 allows server admins to create users with IDs of system folders.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15624</a> MISC

				<a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper neutralization of file names, conversation names and board names in Nextcloud Server 16.0.3, Nextcloud Talk 6.0.3 and Nextcloud Desk 0.6.5 causes an XSS when linking them with each others in a project.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A bug in Nextcloud Server 14.0.4 could expose more data in reshared link shares than intended by the sharer.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8121</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	An authenticated server-side request forgery in Nextcloud server 16.0.1 allowed to detect local and remote services when adding a new subscription in the calendar application.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8118</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A missing check in Nextcloud Server 14.0.3 could give recipient the possibility to extend the expiration date of a share they received.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8122</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	nghttp2 before 1.7.1 allows remote attackers to cause a denial of service (memory exhaustion).	2020-02-06	not yet calculated	<a href="#">CVE-2016-1544</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	not yet calculated	<a href="#">CVE-2019-15604</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	Including trailing white space in HTTP header values in Nodejs 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	not yet calculated	<a href="#">CVE-2019-15606</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	not yet calculated	<a href="#">CVE-2019-15605</a> <a href="#">MISC</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a>
nuxeo -- nuxeo_platform	RichFaces implementation in Nuxeo Platform 5.6.0 before HF27 and 5.8.0 before HF-01 does not restrict the classes for which deserialization methods can be called, which allows remote attackers to execute arbitrary code via crafted serialized data. NOTE: this vulnerability may overlap CVE-2013-2165.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4521</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	not yet calculated	<a href="#">CVE-2014-9530</a> <a href="#">CONFIRM</a>
omniauth-weibo-oauth2_gem -- omniauth-weibo-oauth2_gem_for_ruby_on_ra	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	not yet calculated	<a href="#">CVE-2019-17268</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the YII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9126</a> <a href="#">MISC</a>
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9127</a> <a href="#">MISC</a>
openfiler - - openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1086</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openshift-enterprise - openshift-enterprise	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1708</a> <a href="#">CONFIRM</a>
openvas -- openvas_manager	OpenVAS Manager v2.0.3 allows plugin remote code execution.	2020-02-06	not yet calculated	<a href="#">CVE-2011-1597</a> <a href="#">MISC</a>
opopensoc - opopensoc	alplugin - opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple External Entity Injection Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4335</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Starting from the apache user account, it is possible to perform privilege escalation through the lack of correct configuration in the server's sudoers file, which by default allows the execution of programs (e.g. nmap) without the need for a password with sudo.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7954</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Without authentication, it is possible to read server files (e.g.,	2020-02-06	not yet	<a href="#">CVE-2020-7953</a>

	/etc/passwd) due to the use of the nmap -iL (aka input file) option.		calculated	<a href="#">CVE-2019-13636</a> <a href="#">MISC</a>
opservices - opservices	- An issue was discovered in OpServices OpMon 9.3.2 that allows Remote Code Execution .	2020-02-06	not yet calculated	<a href="#">CVE-2020-8636</a> <a href="#">MISC</a>
opwebapiplugin - opwebapiplugin	- opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4334</a> <a href="#">MISC</a>
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1768</a> <a href="#">CONFIRM</a>
percona -- percona_monitoring_and_management	- pmm-server in Percona Monitoring and Management (PMM) 2.2.x before 2.2.1 allows unauthenticated denial of service.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7920</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phppgadmin -- phppgadmin	- phppgadmin through 7.12.1 allows sensitive actions to be performed without validating that the request originated from the application. One such area, "database.php" does not verify the source of an HTTP request. This can be leveraged by a remote attacker to trick a logged-in administrator to visit a malicious page with a CSRF exploit and execute arbitrary system commands on the server.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10784</a> <a href="#">MISC</a>
projectpier - projectpier	- ProjectPier 0.8.8 has stored XSS	2020-02-07	not yet calculated	<a href="#">CVE-2013-3635</a> <a href="#">MISC</a>
projectpier - projectpier	- ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	not yet calculated	<a href="#">CVE-2013-3636</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
projectpier - projectpier	- ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	not yet calculated	<a href="#">CVE-2013-3637</a> <a href="#">MISC</a>
qemu -- qemu	- In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8608</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm --	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		not	<a href="#">CVE-2019-</a>

multiple_snp	Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	yet calculated	<a href="#">14088</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
railo -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5468</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive -- adserver	A reflected XSS vulnerability has been discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.0.3 by Jacopo Tediosi. There are currently no known exploits: the session identifier cannot be accessed as it is stored in an http-only cookie as of v3.2.2. On older versions, however, under specific circumstances, it could be possible to steal the session identifier and gain access to the admin interface. The query string sent to the www/delivery/afr.php script was printed back without proper escaping in a JavaScript context, allowing an attacker to execute arbitrary JS code on the browser of the victim.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8115</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung - - multiple_m	On Samsung mobile devices with O(8.0) and P(9.0) software and an Exynos 8895 chipset, RKP (aka the Samsung Hypervisor EL2 implementation) allows arbitrary memory write operations. The Samsung ID is SVE-2019-16265.	2020-02-04	not yet calculated	<a href="#">CVE-2019-19273</a> <a href="#">CONFIRM</a>
schmid -- zi_620_v400_090 routers	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6760</a> <a href="#">MISC</a>
simple_machines - - simple_machines_forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: Forum admin can read files such as the database config.	2020-02-07	not yet calculated	<a href="#">CVE-2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscrip -- - simplejobscrip	An issue was discovered in Simplejobscrip.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
smoothwall - - smoothwall_express3	A cross-site scripting (XSS) vulnerability in Smoothwall Express3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall - - smoothwall_express	CSRF vulnerability in Smoothwall Express 3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
sphider -- sphider_search_engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 and the engine calls in admin/spiderfuncs.php, which could let a	2020-02-07	not yet	<a href="#">CVE-2014-5087</a>

	remote malicious user execute arbitrary code.		calculated	<a href="#">MISC</a> <a href="#">MISC</a>
status2k -- status2k	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
statusnet - - statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	not yet calculated	<a href="#">CVE-2010-4658</a> <a href="#">MISC</a> <a href="#">MISC</a>
synaptive - - medical_clearcanvas_image_server	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8788</a> <a href="#">MISC</a>
teamviewer -- teamviewer	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9.x, this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2019-18988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tianocore - - edk2	Buffer overflow in the Reclaim function in Tianocore EDK2 before SVN 16280 allows physically proximate attackers to gain privileges via a long variable name.	2020-02-06	not yet calculated	<a href="#">CVE-2014-8271</a> <a href="#">MISC</a> <a href="#">MISC</a>
troglobit -- minisnmpd	A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server.	2020-02-04	not yet calculated	<a href="#">CVE-2020-6060</a> <a href="#">MISC</a>
ubiquiti_networks -	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4)			<a href="#">CVE-</a>



- unifi_controller	authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the Unifi Controller name via a request to api/set/setting/identity.	2020-02-08	not yet calculated	<a href="#">2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>
ui -- edgeswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	not yet calculated	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
unshift -- url-parse	Insufficient validation and sanitization of user input exists in url-parse npm package version 1.4.4 and earlier may allow attacker to bypass security checks.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8124</a> <a href="#">MISC</a>
ushahidi -- ushahidi	Ushahidi before 2.6.1 has insufficient entropy for forgot-password tokens.	2020-02-04	not yet calculated	<a href="#">CVE-2012-5618</a> <a href="#">MISC</a> <a href="#">MISC</a>
videolan -- vlc_media_player	The web interface in VideoLAN VLC media player before 2.0.7 has no access control which allows remote attackers to view directory listings via the 'dir' command or issue other commands without authenticating.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3564</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	Unrestricted file upload vulnerability in the Settings_Vtiger_CompanyDetailsSave_Action class in modules/Settings/Vtiger/actions/CompanyDetailsSave.php in Vtiger CRM 6.3.0 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in test/logo/.	2020-02-06	not yet calculated	<a href="#">CVE-2015-6000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
watchguard -- firewire_xtn	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	not yet calculated	<a href="#">CVE-2014-6413</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
webcalendar - - webcalendar	webcalendar before 1.2.7 shows the reason for a failed login (e.g., "no such user").	2020-02-04	not yet calculated	<a href="#">CVE-2013-1422</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-</a>

wordpress - wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	not yet calculated	<a href="#">2013-2008 MISC MISC MISC</a>
wordpress - wordpress	The Time Capsule plugin before 1.21.16 for WordPress has an authentication bypass. Any request containing IWP_JSON_PREFIX causes the client to be logged in as the first account on the list of administrator accounts.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8771 MISC MISC</a>
wordpress - wordpress	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for WordPress and before 2.0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	2020-02-08	not yet calculated	<a href="#">CVE-2014-8739 MISC MISC MISC MISC MISC MISC MISC MISC</a>
wordpress - wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-2009 MISC MISC MISC MISC MISC</a>
wordpress - wordpress	The InfiniteWP Client plugin before 1.9.4.5 for WordPress has a missing authorization check in iwpm_mmb_set_request in init.php. Any attacker who knows the username of an administrator can log in.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8772 MISC MISC</a>
wordpress - wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2062 MISC MISC MISC MISC</a>
wordpress - wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-1394 MISC MISC MISC MISC MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3628 MISC MISC</a>

				<a href="#">MISC</a>
zoho_manageengine -- applications_manager	Zoho ManageEngine Applications Manager 14 before 14520 allows a remote unauthenticated attacker to disclose OS file names via FailOverHelperServlet.	2020-02-06	not yet calculated	<a href="#">CVE-2019-19800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager_and_ops_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	not yet calculated	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

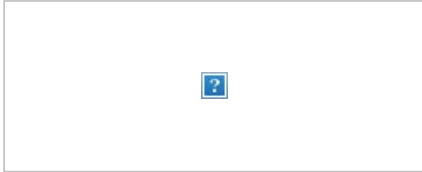
This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of February 3, 2020  
**Date:** Wednesday, February 12, 2020 12:43:22 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

*\*The tables in Vulnerability Bulletin (SB20-041) have been updated.*

## **Vulnerability Summary for the Week of February 3, 2020**

02/10/2020 07:28 AM EST

Original release date: February 10, 2020 | Last revised: February 12, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	2020-01-31	7.5	<a href="#">CVE-2014-8322</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aruba_networks -- instant	Multiple vulnerabilities exists in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.	2020-01-31	7.5	<a href="#">CVE-2016-2031</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	7.8	<a href="#">CVE-2020-3926</a> <a href="#">CONFIRM</a>



changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	8.5	<a href="#">CVE-2020-3927</a> <a href="#">CONFIRM</a>
cisco -- multiple_ip_phones	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	8.3	<a href="#">CVE-2020-3111</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- video_surveillance_8000_series_ip_cameras	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later.	2020-02-05	8.3	<a href="#">CVE-2020-3110</a> <a href="#">MISC</a> <a href="#">CISCO</a>
coppermine_development -- coppermine_gallery	Coppermine gallery before 1.4.26 has an input validation vulnerability that allows for code execution.	2020-02-05	7.5	<a href="#">CVE-2010-4815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

curling -- curling	All versions of curling.js are vulnerable to Command Injection via the run function. The command argument can be controlled by users without any sanitization.	2020-02-06	<a href="#">10</a>	<a href="#">CVE-2019-10789</a> <a href="#">MISC</a> <a href="#">MISC</a>
django -- django	Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-7471</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
dot-prop -- dot-prop	Prototype pollution vulnerability in dot-prop npm package version 5.1.0 and earlier allows an attacker to add arbitrary properties to JavaScript language constructs such as objects.	2020-02-04	<a href="#">7.5</a>	<a href="#">CVE-2020-8116</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.2.4 is vulnerable to directory traversal, leading to incorrect access control. It allows an attacker to read or execute files under \$TOMCAT_HOME/webapps/ROOT/assets (which should be a protected directory). Additionally, attackers can upload temporary files (e.g., .jsp files) into /webapps/ROOT/assets/tmp_upload, which can lead to remote command execution (with the permissions of the user running the dotCMS application).	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-6754</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
edk2 -- unified_extensible_firmware_interface	Multiple integer overflows in the Pre-EFI Initialization (PEI) boot phase in the Capsule Update feature in the UEFI implementation in EDK2 allow physically proximate attackers to bypass intended access restrictions by providing crafted data that is not properly handled during the coalescing phase.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4860</a> <a href="#">MISC</a>
edk2 -- unified_extensible_firmware_interface	Integer overflow in the Drive Execution Environment (DXE) phase in the Capsule Update feature in the UEFI implementation in EDK2 allows physically proximate attackers to bypass intended access restrictions via crafted data.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4859</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows SQL Injection via the user parameter to com.eg.LoginHelperServlet (aka the Forgot Password feature).	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8592</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows authentication bypass via a com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8591</a> <a href="#">MISC</a>

	request.			
fortinet -- fortimanager	A Command Injection vulnerability exists in FortiManager 5.2.1 and earlier and FortiManager 5.0.10 and earlier via unspecified vectors, which could let a malicious user run systems commands when executing a report.	2020-02-04	9	<a href="#">CVE-2015-3611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- mortimanager	A vulnerability exists in in FortiManager 5.2.1 and earlier and 5.0.10 and earlier in the WebUI FTP backup page	2020-02-04	7.5	<a href="#">CVE-2015-3613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	7.5	<a href="#">CVE-2020-8114</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.2 incorrectly validated role/region associated with TLS certificates used for mTLS RPC, and were susceptible to privilege escalation. Fixed in 0.10.3.	2020-01-31	7.5	<a href="#">CVE-2020-7956</a> <a href="#">MISC</a> <a href="#">MISC</a>
jobberbase -- jobberbase	Jobberbase 2.0 has SQL injection via the PATH_INFO to the jobs-in endpoint.	2020-02-05	7.5	<a href="#">CVE-2019-20447</a> <a href="#">MISC</a> <a href="#">MISC</a>
klona -- klona	Flaw in input validation in npm package klona version 1.1.0 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using klona.	2020-02-04	7.5	<a href="#">CVE-2020-8125</a> <a href="#">MISC</a>
nanopb -- nanopb	There is a potentially exploitable out of memory condition In Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is compiled with PB_ENABLE_MALLOC, the message to be decoded contains a repeated string, bytes or message field and realloc() runs out of memory when expanding the array nanopb can end up calling `free()` on a pointer value that comes from uninitialized memory. Depending on platform this can result in a crash or further memory corruption, which may be exploitable in some cases. This problem is fixed in nanopb-0.4.1, nanopb-0.3.9.5, nanopb-0.2.9.4.	2020-02-04	7.5	<a href="#">CVE-2020-5235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netapp -- oncommand_system_manager	NetApp OnCommand System Manager 2.1 and earlier allows remote attackers to execute arbitrary commands in the Halt/Reboot interface.	2020-01-31	9	<a href="#">CVE-2013-3322</a> <a href="#">XF</a> <a href="#">MISC</a>
norman -- malware_cleaner	nsak64.sys in Norman Malware Cleaner 2.08.08 allows users to call arbitrary kernel functions because the passing of function pointers between user and kernel	2020-02-03	7.5	<a href="#">CVE-2020-8508</a> <a href="#">MISC</a>

	mode is mishandled.			
phpabook -- phpabook	An issue was discovered in phpABook 0.9 Intermediate. On the login page, if one sets a userInfo cookie with the value of admin+1+en (user+perms+lang), one can login as any user without a password.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8510</a> <a href="#">MISC</a> <a href="#">MISC</a>
phplist -- phplist	phplist 3.5.0 allows type juggling for admin login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8547</a> <a href="#">MISC</a>
playsms -- playsms	PlaySMS before 1.4.3 does not sanitize inputs from a malicious string.	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-8644</a> <a href="#">MISC</a> <a href="#">MISC</a>
ppp -- ppp	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8597</a> <a href="#">MISC</a> <a href="#">MLIST</a>
python -- python	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.	2020-02-04	<a href="#">7.1</a>	<a href="#">CVE-2019-9674</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- mdm9206_and_mdm9607_devices	Subsequent additions performed during Module loading while allocating the 9607_devices could lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14051</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14046</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open close in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14044</a> <a href="#">CONFIRM</a>
	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon			



qualcomm -- multiple_snapdragon_products	Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14055</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14002</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> <a href="#">CONFIRM</a>
	Out of bound access due to Invalid inputs to dapm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial			

qualcomm -- multiple_snapdragon_products	IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14063</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Uninitialized stack data gets used if memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14060</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14057</a> <a href="#">CONFIRM</a>

qualcomm -- multiple_snapdragon_products	Stage-2 fault will occur while writing to an ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14049</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> <a href="#">CONFIRM</a>
sap -- netweaver	SAP NetWeaver 7.0 allows Remote Code Execution and Denial of Service caused by an error in the DiagTraceHex() function. By sending a specially-crafted packet, an attacker could exploit this vulnerability to cause the application to crash.	2020-02-05	7.5	<a href="#">CVE-2011-1517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript.com -- simplejobscript.com	controllers/page_apply.php in Simplejobscript.com SJS through 1.66 is prone to unauthenticated Remote Code Execution by uploading a PHP script as a resume.	2020-01-31	7.5	<a href="#">CVE-2020-8440</a> <a href="#">CONFIRM</a>
smartbear -- readyapi_and_soapui	An issue was discovered in SmartBear ReadyAPI through 2.8.2 and 3.0.0 and SoapUI through 5.5. When opening a project, the Groovy "Load Script" is automatically executed. This allows an attacker to execute arbitrary Groovy Language code (Java scripting language)	2020-02-05	9.3	<a href="#">CVE-2019-12180</a> <a href="#">MISC</a>

	on the victim machine by inducing it to open a malicious Project. The same issue is present in the "Save Script" function, which is executed automatically when saving a project.			
squid -- squid	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	2020-02-04	7.5	<a href="#">CVE-2020-8450</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_update_framework -- tuf	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature.	2020-02-05	7.5	<a href="#">CVE-2020-6174</a> <a href="#">CONFIRM</a>
tp-link -- tg-sg105e_devices	The Web Management of TP-Link TP-SG105E V4 1.0.0 Build 20181120 devices allows an unauthenticated attacker to reboot the device via a reboot.cgi request.	2020-02-03	7.8	<a href="#">CVE-2019-16893</a> <a href="#">EXPLOIT-DB</a>
zpanel_project -- zpanel	ZPanel 10.0.1 has insufficient entropy for its password reset process.	2020-02-04	7.5	<a href="#">CVE-2012-5686</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	6.5	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	5	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	4.6	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent --	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch			<a href="#">CVE-2014-</a>



1830_photonic_service	OS 16.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	2020-01-31	<a href="#">4.3</a>	<a href="#">3809 MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-12426 MLIST CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	<a href="#">4.9</a>	<a href="#">CVE-2011-0220 MISC</a>
apple -- safari	A Cross-origin vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2016-4676 MISC MISC MISC CONFIRM MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8505 MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8504 MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2016-2032 MISC MISC MISC MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20104 N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404 N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20400 N/A</a>
	The JMX monitoring flag in Atlassian Jira Server and Data Center before version			<a href="#">CVE-2019-</a>

atlassian -- jira	8.6.0 allows remote attackers to turn the JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	2020-02-06	<a href="#">4.3</a>	<a href="#">20405</a> <a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20403</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20402</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2674</a> <a href="#">MISC</a> <a href="#">XE</a> <a href="#">BID</a>

brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	5	<a href="#">CVE-2013-2672</a> <a href="#">MISC</a> <a href="#">XF</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	4.6	<a href="#">CVE-2013-2673</a> <a href="#">MISC</a> <a href="#">BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	5	<a href="#">CVE-2019-12998</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	5	<a href="#">CVE-2013-2683</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	5	<a href="#">CVE-2013-2680</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	6.8	<a href="#">CVE-2013-2678</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	4.3	<a href="#">CVE-2013-2681</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	4.3	<a href="#">CVE-2013-2682</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	4.3	<a href="#">CVE-2013-2684</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
computer_incident_response -- ail-framework	Global Cyber All framework 2.8 allows path traversal.	2020-02-03	5	<a href="#">CVE-2020-8545</a> <a href="#">MISC</a>
cysharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions	2020-01-31	6.8	<a href="#">CVE-2020-5234</a> <a href="#">MISC</a>

	and stack overflow. Review the linked GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus -- eucalyptus_management_console	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>



evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	6.6	<a href="#">CVE-2013-5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	5	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	4.6	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	5	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	5	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	4.3	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	4	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 0.10.3 allow unbounded resource usage.	2020-01-31	5	<a href="#">7218</a> <a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	6.5	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information_server	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	5.8	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	6.8	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	6.9	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	6.5	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	6	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	5.8	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or	2020-02-04	5	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

	browser history. IBM X-Force ID: 166623.			
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> XF <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> XF <a href="#">CONFIRM</a>
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> MISC MISC MISC
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> MISC MISC MISC MISC



info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8139</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	4.3	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	6.5	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	5	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	5	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	5	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	6.4	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	5	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be			

joomla! -- joomla!	entered by any user. If it doesn't contain rel="noopener" (or similar attributes such as noreferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	2020-02-03	4.3	<a href="#">CVE-2020-5182</a> <a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	4.3	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	5	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	5	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	6.6	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	6.5	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	4.3	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- rumpus	An issue was discovered in Rumpus 0.2.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	4.3	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to	2020-02-06	4.4	<a href="#">CVE-2019-20406</a>

	write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.			<a href="#">N/A</a>
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	5	<a href="#">4116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	5	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	6.4	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	4.3	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	4.3	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	4	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	6.8	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon			



qualcomm -- multiple_snapdragon_products	Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>

squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- openSUSE_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a>

	to arbitrary websites via a crafted URL.			<a href="#">MISC</a>
telaen -- telaen	Telaen before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted URL request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2624</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browser_y" in the page image.php.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	<a href="#">5</a>	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>

	vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>



wordpress -- wordpress	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can result in an attacker performing malicious actions such as stealing session tokens.	2020-02-03	<a href="#">4.3</a>	<a href="#">8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	<a href="#">4</a>	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) 5.0.1050 through 5.1.1067 and 6.0.1000 through 6.0.1003 allows Insecure Direct Object Reference (IDOR) by an authenticated sender because of an error in a file-upload feature. This is fixed in 5.1.1068 and 6.0.1004.	2020-01-31	<a href="#">3.5</a>	<a href="#">CVE-2020-8503</a> <a href="#">MISC</a>
bromium -- secure_platform	Bromium client version 4.0.3.2060 and prior to 4.1.7 Update 1 has an out of bound read results in race condition causing Kernel memory leaks or denial of service.	2020-02-03	<a href="#">3.3</a>	<a href="#">CVE-2019-18567</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	A vulnerability in the web-based management interface of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management			

cisco -- digital_network_architecture	interface of an affected device. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker needs administrator credentials. This vulnerability affects Cisco DNA Center Software releases earlier than 1.3.0.6 and 1.3.1.4.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2019-15253</a> <a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack on an affected device. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by providing malicious data to a specific field within the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco ISE Software releases 2.7.0 and later contains the fix for this vulnerability.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2020-3149</a> <a href="#">CISCO</a>
cloud-init -- cloud-init	In cloud-init through 19.4, rand_user_password in cloudinit/config/cc_set_passwords.py has a small default pwlen value, which makes it easier for attackers to guess passwords.	2020-02-05	<a href="#">2.1</a>	<a href="#">CVE-2020-8632</a> <a href="#">MISC</a> <a href="#">MISC</a>
cloud-init -- cloud-init	cloud-init through 19.4 relies on Mersenne Twister for a random password, which makes it easier for attackers to predict passwords, because rand_str in cloudinit/util.py calls the random.choice function.	2020-02-05	<a href="#">2.1</a>	<a href="#">CVE-2020-8631</a> <a href="#">MISC</a> <a href="#">MISC</a>
fortinet -- fortimanager	A Cross-site Scripting (XSS) vulnerability exists in FortiManager 5.2.1 and earlier and 5.0.10 and earlier via an unspecified parameter in the FortiWeb auto update service page.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2015-3612</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 163493.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-4451</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
	IBM StoredIQ 7.6.0.17 through 7.6.0.20			

ibm -- storediq	could disclose sensitive information to a local user due to data in certain directories not being encrypted when it contained symbolic links. IBM X-Force ID: 175133.	2020-02-03	<a href="#">2.1</a>	<a href="#">CVE-2020-4224</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8649</a> <a href="#">MISC</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vc_do_resize function in drivers/tty/vt/vt.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8647</a> <a href="#">MISC</a>
linux -- linux_kernel	In a Linux KVM guest that has PV TLB enabled, a process in the guest kernel may be able to read memory locations from another process in the same guest. This problem is limit to the host running linux kernel 4.10 with a guest running linux kernel 4.16 or later. The problem mainly affects AMD processors but Intel CPUs cannot be ruled out.	2020-01-31	<a href="#">1.9</a>	<a href="#">CVE-2019-3016</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8648</a> <a href="#">MISC</a>
nextcloud -- nextcloud	Missing escaping of HTML in the Updater of Nextcloud 15.0.5 allowed a reflected XSS when starting the updater from a malicious location.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-15618</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg	An issue was discovered in PRTG 7.x through 19.4.53. Due to insufficient access control on local registry keys for the Core Server Service, a non-administrative user on the local machine is able to access administrative credentials.	2020-02-03	<a href="#">2.1</a>	<a href="#">CVE-2019-19119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
pandora_fms -- pandora_fms	PandoraFMS 742 suffers from multiple XSS vulnerabilities, affecting the Agent Management, Report Builder, and Graph Builder components. An authenticated user can inject dangerous content into a data store that is later read and included in dynamic content.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-19968</a> <a href="#">MISC</a> <a href="#">MISC</a>
sos -- jobscheduler	A cross-site scripting (XSS) vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to inject arbitrary web script or HTML via JSON properties available from the REST API.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2020-6854</a> <a href="#">MISC</a>
wordpress -- wordpress	A CSRF vulnerability in the Tutor LMS plugin before 1.5.3 for WordPress can result in an attacker approving themselves as an instructor and performing other malicious actions (such	2020-02-04	<a href="#">2.6</a>	<a href="#">CVE-2020-8615</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

as blocking legitimate instructors).

[MISC](#)

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS& Score	Patch Info	Source
arctic_torrent -- arctic_torrent	A vulnerability exists in Arctic Torrent 1.4 via unspecified vectors in .torrent file handling, which could let a malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6309</a> <a href="#">MISC</a>	
atmail -- atmail_webmail_server	Cross-site scripting (XSS) vulnerability in the administrative interface in Atmail Webmail Server 6.4 allows remote attackers to inject arbitrary web script or HTML via the Date field of an email.	2020-02-06	not yet calculated	<a href="#">CVE-2012-2593</a> <a href="#">MISC</a>	
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	not yet calculated	<a href="#">CVE-2013-3091</a> <a href="#">MISC</a>	
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8796</a> <a href="#">MISC</a>	
bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>	
boonex -- dolphin	SQL injection vulnerability in Boonex Dolphin before 7.1.3 allows remote authenticated users to execute arbitrary SQL commands via the 'pathes' parameter in 'categories.php'.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3638</a> <a href="#">BID-XE</a>	
bosch -- bvms_mobile_video_service	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6770</a> <a href="#">CONFIRM</a>	
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP	2020-02-07	not yet calculated	<a href="#">CVE-2020-6768</a> <a href="#">CONFIRM</a>	



	7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.			
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6767</a> <a href="#">CONFIRM</a>
bosch -- video_streaming_gateway	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6769</a> <a href="#">CONFIRM</a>
broadcom -- multiple_devices	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic, a different vulnerability than CVE-2019-9500, CVE-2019-9501, CVE-2019-9502, and CVE-2019-9503.	2020-02-05	not yet calculated	<a href="#">CVE-2019-15126</a> <a href="#">CONFIRM</a>
broadcom - wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. By supplying a vendor information element with a data length larger than 32 bytes, a heap buffer overflow is triggered in wlc_wpa_sup_eapol. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9501</a> <a href="#">MISC CERT.</a> <a href="#">VN</a>
broadcom - wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. If the vendor information element data length is larger than 164 bytes, a heap buffer overflow is triggered in wlc_wpa_plumb_gtk. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9502</a> <a href="#">MISC CERT.</a> <a href="#">VN</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view private IP addresses and other sensitive information.	2020-02-04	not yet calculated	<a href="#">CVE-2013-2676</a> <a href="#">MISC CERT.</a> <a href="#">XF BID</a>

brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 devices with Firmware L contain a Frameable response (Clickjacking) vulnerability which could allow remote attackers to obtain sensitive information.	2020-02-05	not yet calculated	<a href="#">CVE-2013-2675</a> <a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a>
c-more -- touch_panels EA9 series	It is possible to unmask credentials and other sensitive information on ?unprotected? project files, which may allow remote attackers to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations.	2020-02-05	not yet calculated	<a href="#">CVE-2020-6969</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11481</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11484</a> <a href="#">MISC</a> <a href="#">MISC</a>
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1700</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cgilua -- cgilua	The session.lua library in CGILua 5.2 alpha 1 and 5.2 alpha 2 uses weak session IDs generated based on OS time, which allows remote attackers to hijack arbitrary sessions via a brute force attack. NOTE: CVE-2014-10300 and CVE-2014-10400 were SPLIT from this ID.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2875</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGILua 5.0.x uses sequential session IDs, which makes it easier for remote attackers to predict the session ID and hijack arbitrary sessions. NOTE:	2020-02-06	not yet calculated	<a href="#">CVE-2014-10400</a> <a href="#">MISC</a>

	this vulnerability was SPLIT from CVE-2014-2875.			<a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.1.x uses the same ID for each session, which allows remote attackers to hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10399</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chamilo -- chamilo_image	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_image -- - servisign	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts.	2020-02-03	not yet calculated	<a href="#">CVE-2020-3925</a> <a href="#">CONFIRM</a>
cisco -- application	Cisco ACE 4.2(3.6) allows log retention DoS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-1202</a> <a href="#">MISC</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3120</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability			

cisco -- cisco_discovery_protocol	exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3119</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- linksys_wrt110	Cross-site request forgery (CSRF) vulnerability in Cisco Linksys WRT110 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3568</a> <a href="#">EXPLOIT-DATABASE.BID.XF</a>
clamav -- clam_antivirus	A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	2020-02-05	not yet calculated	<a href="#">CVE-2020-3123</a> <a href="#">CISCO</a>
corsair -- corsair_icue	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8808</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir865l_devices	D-Link DIR865L v1.03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3096</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dd-wrt -- dd-wrt	Command Injection vulnerability exists via a CSRF in DD-WRT 24-sp2 from specially crafted configuration values containing shell meta-characters, which could let a remote malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6297</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dedicated -- multiple_dvr_products	Dedicated Micros DV-IP Express, SD Advanced, SD, EcoSense, and DS2 devices rely on a GUI warning to help ensure that the administrator configures login credentials, which makes it easier for remote attackers to obtain access by leveraging situations in which this warning was not needed. NOTE: the vendor states "The user is presented with clear warnings on the GUI that they should set usernames and passwords."	2020-02-06	not yet calculated	<a href="#">CVE-2015-2909</a> <a href="#">MISC</a> <a href="#">MISC</a>



dell -- dmc_isilon_ones	Dell EMC Isilon OneFS versions 8.1.2, 8.1.0.4, 8.1.0.3, and 8.0.0.7 contain a vulnerability in some configurations. An attacker may exploit this vulnerability to gain access to restricted files. The non-RAN HTTP and WebDAV file-serving components have a vulnerability wherein when either are enabled, and Basic Authentication is enabled for either or both components, files are accessible without authentication.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5318</a> MISC
dell -- emc_ecs	Dell EMC ECS versions prior to 3.4.0.1 contain an XSS vulnerability. A remote authenticated malicious user could exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5317</a> MISC
dell -- multiple_products	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5319</a> MISC
den_norsk -- im-metadata	im-metadata through 3.0.1 allows remote attackers to execute arbitrary commands via the "exec" argument. It is possible to inject arbitrary commands as part of the metadata options which is given to the "exec" function.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10788</a> CONFIRM MISC
den_norsk -- im-resize	im-resize through 2.3.2 allows remote attackers to execute arbitrary commands via the "exec" argument. The cmd argument used within index.js, can be controlled by user without any sanitization.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10787</a> CONFIRM MISC
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container IDs.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5278</a> MISC MISC MISC
drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	not yet calculated	<a href="#">CVE-2012-5570</a> MISC MISC CONFIRM
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The installation uses the same API key (hardcoded as EONAPI_KEY in include/api_functions.php for API version 2.4.2) by default for all installations, hence allowing an attacker to calculate/guess the admin access token.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8657</a> MISC
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in	2020-02-07	not yet calculated	<a href="#">CVE-2020-8656</a> MISC

	include/api_functions.php.			MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	not yet calculated	CVE-2020-8654 MISC
eyesofnetwork -- eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	not yet calculated	CVE-2020-8655 MISC
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made.	2020-02-06	not yet calculated	CVE-2020-5854 CONFIRM
flowplayer -- flowplayer	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	not yet calculated	CVE-2011-3642 MISC MISC MISC MISC MISC MISC MISC MISC MISC
fork_cms -- fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	not yet calculated	CVE-2014-9470 MISC MISC MISC MISC MISC MISC
fortinet -- forticlient_for_linux	A Denial of service (DoS) vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to cause FortiClient processes running under root privilege to crash via sending specially crafted IPC client requests to the fctschd process due the nanomsg not been correctly validated.	2020-02-06	not yet calculated	CVE-2019-16152 MISC CONFIRM
fortinet -- forticlient_for_linux	A stack buffer overflow vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted "StartAvCustomScan" type IPC client requests to the fctschd process due the argv data not been well sanitized.	2020-02-06	not yet calculated	CVE-2019-17652 MISC CONFIRM
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to run arbitrary system commands under root privilege via injecting specially crafted "ExportLogs" type IPC client requests to the fctschd process.	2020-02-06	not yet calculated	CVE-2019-15711 MISC CONFIRM

fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctsched process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	not yet calculated	<a href="#">CVE-2019-16155</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13333</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17136</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13334</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17135</a> <a href="#">MISC</a>
	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions,		not	<a href="#">CVE-</a>

fujitsu -- multiple_products	Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3, Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.	2020-02-07	yet calculated	2019- 13163 CONFIRM
gnome -- librsvg	In xml.rs in GNOME librsvg before 2.46.2, a crafted SVG file with nested patterns can cause denial of service when passed to the library for processing. The attacker constructs pattern elements so that the number of final rendered objects grows exponentially.	2020-02-02	not yet calculated	CVE- 2019- 20446 MISC
gnome -- evolution_and_evolution_data_server	The gpg_ctx_add_recipient function in camel/camel-gpg-context.c in GNOME Evolution 3.8.4 and earlier and Evolution Data Server 3.9.5 and earlier does not properly select the GPG key to use for email encryption, which might cause the email to be encrypted with the wrong key and allow remote attackers to obtain sensitive information.	2020-02-06	not yet calculated	CVE- 2013- 4166 CONFIRM MISC MISC CONFIRM CONFIRM
golang -- go	The net/http library in net/http/transfer.go in Go before 1.4.3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains Content-Length and Transfer-Encoding header fields.	2020-02-08	not yet calculated	CVE- 2015- 5741 MISC MISC MISC MISC MISC MISC
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	CVE- 2014- 7224 MISC MISC MISC MISC
google -- chrome	Google Chrome before 3.0 does not properly handle XML documents, which allows remote attackers to obtain sensitive information via a crafted web site.	2020-02-06	not yet calculated	CVE- 2010- 3917 MISC MISC
hardcoreview - - hardcoreview	A vulnerability exists in HCView (aka Hardcoreview) 1.4 due to a write access violation with a GIF file.	2020-02-06	not yet calculated	CVE- 2012- 6306 MISC MISC
hp -- sitescope	An Information Disclosure vulnerability exists in HP SiteScope 11.2 and 11.3 on Windows, Linux and Solaris, HP Asset Manager 9.30 through 9.32, 9.40 through 9.41, 9.50, and Asset Manager Cloudsystem Chargeback 9.40, which could let a remote malicious user obtain sensitive	2020-02-04	not yet calculated	CVE- 2015- 2802 CONFIRM CONFIRM MISC



	information. This is the TLS vulnerability known as the RC4 cipher Bar Mitzvah vulnerability.			<a href="#">MISC</a> <a href="#">MISC</a>
ibm -- cloud_automation	IBM Cloud Automation Manager 3.2.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http://link to the user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 168644.	2020-02-05	not yet calculated	<a href="#">CVE-2019-4616</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 171511.	2020-02-04	not yet calculated	<a href="#">CVE-2019-4675</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7523</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Stack-based buffer overflow in the WritePSDImage function in coders/psd.c in ImageMagick, possibly 6.8.8-5, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-1947.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2030</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Buffer overflow in the DecodePSDPixels function in coders/psd.c in ImageMagick before 6.8.8-5 might allow remote attackers to execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-2030.	2020-02-06	not yet calculated	<a href="#">CVE-2014-1958</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ispconfig - - ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	not yet	<a href="#">CVE-2013-3629</a> <a href="#">MISC</a>

			calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jpegsnoot - jpegsnoot	A vulnerability exists in JPEGsnoot 1.5.2 due to an unspecified issue in JPEG file handling, which could let a malicious user execute arbitrary code	2020-02-06	not yet calculated	<a href="#">CVE-2012-6307</a> <a href="#">MISC</a> <a href="#">MISC</a>
kemp -- load_master	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5288</a> <a href="#">MISC</a> <a href="#">MISC</a>
konqueror - konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	not yet calculated	<a href="#">CVE-2012-4512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys -- wrt310n_wireless_router	Linksys WRT310Nv2 2.0.0.1 is vulnerable to XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3067</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
mariadb -- mariadb	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.	2020-02-04	not yet calculated	<a href="#">CVE-2020-7221</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mcabber - - mcabber	MCabber before 1.0.4 is vulnerable to roster push attacks, which allows remote attackers to intercept communications, or add themselves as an entity on a 3rd party's roster as	2020-02-06	not yet	<a href="#">CVE-2016-9928</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>

	another user, which will also garner associated privileges, via crafted XMPP packets.		calculated	<a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mediawiki - mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4381</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki - mediawiki	The CentralNotice extension for MediaWiki before 1.19.9, 1.20.x before 1.20.8, and 1.21.x before 1.21.3 sets the Cache-Control header to cache session cookies when a user is autocreated, which allows remote attackers to authenticate as the created user.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4572</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mikrotik -- winbox	MikroTik WinBox before 3.21 is vulnerable to a path traversal vulnerability that allows creation of arbitrary files wherever WinBox has write permissions. WinBox is vulnerable to this attack if it connects to a malicious endpoint or if an attacker mounts a man in the middle attack.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5720</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exastm R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to execute arbitrary code via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5628</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exastm R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS	2020-02-05	not yet calculated	<a href="#">CVE-2015-5627</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (process outage) via a crafted packet.			
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (network-communications outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5626</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h_____%2427, (3) h_____%2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-3423</a> <a href="#">MISC</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the system, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8) xname, or (9) mpTransactionId parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wireless_router	An Authentication vulnerability exists in NETGEAR WGR614 wireless router due to a hardcoded credential used for serial programming, a related issue to CVE-2006-1002.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6340</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wireless_router	An Information Disclosure vulnerability exists in the my config file in NETGEAR WGR614 v7 and v9, which could let a malicious user recover all previously used passwords on the device, for both the control panel and WEP/WPA/WPA2, in plaintext. This is a different issue than CVE-2012-6340.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1.2.31805 and V2.2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracert diagnostic tool because of lack of user input sanitizing.	2020-02-07	not yet calculated	<a href="#">CVE-2019-19356</a> <a href="#">MISC</a>
network-manager - network-manager	network-manager through 1.0.2 allows remote attackers to execute arbitrary commands via the "execSync()" argument.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10786</a> <a href="#">MISC</a>



nextcloud -- circles	Improper authorization in the Circles app 0.17.7 causes retaining access when an email address was removed from a circle.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15610</a> MISC
nextcloud -- nextcloud_android	A wrong check for the system time in the Android App 3.9.0 causes a bypass of the lock protection when changing the time of the system to the past.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15615</a> MISC
nextcloud -- nextcloud_android	Not strictly enough sanitization in the Nextcloud Android app 3.6.0 allowed an attacker to get content information from protected tables when using custom queries.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15622</a> MISC
nextcloud -- nextcloud_server	Violation of Secure Design Principles in the iOS App 2.23.0 causes the app to leak its login and token to other Nextcloud services when search e.g. for federated users or registering for push notifications.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15611</a> MISC
nextcloud -- nextcloud_server	Missing sanitization in the iOS App 2.24.4 causes an XSS when opening malicious HTML files.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15614</a> MISC
nextcloud -- nextcloud_server	Improper permissions preservation in Nextcloud Server 16.0.1 causes sharees to be able to reshare with write permissions when sharing the mount point of a share they received, as a public link.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15621</a> MISC
nextcloud -- nextcloud_server	Dangling remote share attempts in Nextcloud 16 allow a DoS/pollution when running long.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15616</a> MISC
nextcloud -- nextcloud_server	A bug in Nextcloud Server 15.0.2 causes pending 2FA logins to not be correctly expired when the password of the user is reset.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15612</a> MISC
nextcloud -- nextcloud_server	A bug in Nextcloud Server 17.0.1 causes the workflow rules to depend their behaviour on the file extension when checking file mimetypes.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15613</a> MISC
nextcloud -- nextcloud_server	A missing check in Nextcloud Server 17.0.0 allowed an attacker to set up a new second factor when trying to login.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15617</a> MISC
nextcloud -- nextcloud_server	Improper Input Validation in Nextcloud Server 15.0.7 allows server admins to create users with IDs of system folders.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15624</a> MISC

				<a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper neutralization of file names, conversation names and board names in Nextcloud Server 16.0.3, Nextcloud Talk 6.0.3 and Nextcloud Desk 0.6.5 causes an XSS when linking them with each others in a project.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A bug in Nextcloud Server 14.0.4 could expose more data in reshared link shares than intended by the sharer.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8121</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	An authenticated server-side request forgery in Nextcloud server 16.0.1 allowed to detect local and remote services when adding a new subscription in the calendar application.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8118</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A missing check in Nextcloud Server 14.0.3 could give recipient the possibility to extend the expiration date of a share they received.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8122</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	nghttp2 before 1.7.1 allows remote attackers to cause a denial of service (memory exhaustion).	2020-02-06	not yet calculated	<a href="#">CVE-2016-1544</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	not yet calculated	<a href="#">CVE-2019-15604</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	Including trailing white space in HTTP header values in Nodejs 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	not yet calculated	<a href="#">CVE-2019-15606</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	not yet calculated	<a href="#">CVE-2019-15605</a> <a href="#">MISC</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a>
nuxeo -- nuxeo_platform	RichFaces implementation in Nuxeo Platform 5.6.0 before HF27 and 5.8.0 before HF-01 does not restrict the classes for which deserialization methods can be called, which allows remote attackers to execute arbitrary code via crafted serialized data. NOTE: this vulnerability may overlap CVE-2013-2165.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4521</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	not yet calculated	<a href="#">CVE-2014-9530</a> <a href="#">CONFIRM</a>
omniauth-weibo-oauth2_gem -- omniauth-weibo-oauth2_gem_for_ruby_on_ra	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	not yet calculated	<a href="#">CVE-2019-17268</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the YII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9126</a> <a href="#">MISC</a>
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9127</a> <a href="#">MISC</a>
openfiler - - openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1086</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openshift-enterprise - openshift-enterprise	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1708</a> <a href="#">CONFIRM</a>
openvas -- openvas_manager	OpenVAS Manager v2.0.3 allows plugin remote code execution.	2020-02-06	not yet calculated	<a href="#">CVE-2011-1597</a> <a href="#">MISC</a>
opopensoc - opopensoc_plugin -	opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple External Entity Injection Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4335</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Starting from the apache user account, it is possible to perform privilege escalation through the lack of correct configuration in the server's sudoers file, which by default allows the execution of programs (e.g. nmap) without the need for a password with sudo.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7954</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Without authentication, it is possible to read server files (e.g.,	2020-02-06	not yet	<a href="#">CVE-2020-7953</a>

	/etc/passwd) due to the use of the nmap -iL (aka input file) option.		calculated	<a href="#">CVE-2019-13636</a> <a href="#">MISC</a>
opservices - opservices	- An issue was discovered in OpServices OpMon 9.3.2 that allows Remote Code Execution .	2020-02-06	not yet calculated	<a href="#">CVE-2020-8636</a> <a href="#">MISC</a>
opwebapiplugin - opwebapiplugin	- opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4334</a> <a href="#">MISC</a>
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1768</a> <a href="#">CONFIRM</a>
percona -- percona_monitoring_and_management	- pmm-server in Percona Monitoring and Management (PMM) 2.2.x before 2.2.1 allows unauthenticated denial of service.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7920</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phppgadmin -- phppgadmin	- phppgadmin through 7.12.1 allows sensitive actions to be performed without validating that the request originated from the application. One such area, "database.php" does not verify the source of an HTTP request. This can be leveraged by a remote attacker to trick a logged-in administrator to visit a malicious page with a CSRF exploit and execute arbitrary system commands on the server.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10784</a> <a href="#">MISC</a>
projectpier - projectpier	- ProjectPier 0.8.8 has stored XSS	2020-02-07	not yet calculated	<a href="#">CVE-2013-3635</a> <a href="#">MISC</a>
projectpier - projectpier	- ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	not yet calculated	<a href="#">CVE-2013-3636</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
projectpier - projectpier	- ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	not yet calculated	<a href="#">CVE-2013-3637</a> <a href="#">MISC</a>
qemu -- qemu	- In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8608</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm --	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		not	<a href="#">CVE-2019-</a>



multiple_samsung -	Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	yet calculated	<a href="#">14088</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
railo -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5468</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive -- adserver	A reflected XSS vulnerability has been discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.0.3 by Jacopo Tediosi. There are currently no known exploits: the session identifier cannot be accessed as it is stored in an http-only cookie as of v3.2.2. On older versions, however, under specific circumstances, it could be possible to steal the session identifier and gain access to the admin interface. The query string sent to the www/delivery/afr.php script was printed back without proper escaping in a JavaScript context, allowing an attacker to execute arbitrary JS code on the browser of the victim.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8115</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung - multiple_mobile_devices	On Samsung mobile devices with O(8.0) and P(9.0) software and an Exynos 8895 chipset, RKP (aka the Samsung Hypervisor EL2 implementation) allows arbitrary memory write operations. The Samsung ID is SVE-2019-16265.	2020-02-04	not yet calculated	<a href="#">CVE-2019-19273</a> <a href="#">CONFIRM</a>
schmid -- zi_620_v400_090_routers	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6760</a> <a href="#">MISC</a>
simple_machines - simple_machines_forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: Forum admin can read files such as the database config.	2020-02-07	not yet calculated	<a href="#">CVE-2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscrip - simplejobscrip	An issue was discovered in Simplejobscrip.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
smoothwall - smoothwall_express3	A cross-site scripting (XSS) vulnerability in Smoothwall Express3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall - smoothwall_express	CSRF vulnerability in Smoothwall Express 3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
sphider -- sphider_search_engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 and the engine calls in admin/spiderfuncs.php, which could let a	2020-02-07	not yet	<a href="#">CVE-2014-5087</a>

	remote malicious user execute arbitrary code.		calculated	<a href="#">MISC</a> <a href="#">MISC</a>
status2k -- status2k	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
statusnet - - statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	not yet calculated	<a href="#">CVE-2010-4658</a> <a href="#">MISC</a> <a href="#">MISC</a>
synaptive - - medical_clearcanvas_image_server	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8788</a> <a href="#">MISC</a>
teamviewer -- teamviewer	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9.x, this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2019-18988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tianocore - - edk2	Buffer overflow in the Reclaim function in Tianocore EDK2 before SVN 16280 allows physically proximate attackers to gain privileges via a long variable name.	2020-02-06	not yet calculated	<a href="#">CVE-2014-8271</a> <a href="#">MISC</a> <a href="#">MISC</a>
troglobit -- minisnmpd	A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server.	2020-02-04	not yet calculated	<a href="#">CVE-2020-6060</a> <a href="#">MISC</a>
ubiquiti_networks -	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4)			<a href="#">CVE-</a>

- unifi_controller	authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the Unifi Controller name via a request to api/set/setting/identity.	2020-02-08	not yet calculated	<a href="#">2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>
ui -- edgeswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	not yet calculated	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
unshift -- url-parse	Insufficient validation and sanitization of user input exists in url-parse npm package version 1.4.4 and earlier may allow attacker to bypass security checks.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8124</a> <a href="#">MISC</a>
ushahidi -- ushahidi	Ushahidi before 2.6.1 has insufficient entropy for forgot-password tokens.	2020-02-04	not yet calculated	<a href="#">CVE-2012-5618</a> <a href="#">MISC</a> <a href="#">MISC</a>
videolan -- vlc_media_player	The web interface in VideoLAN VLC media player before 2.0.7 has no access control which allows remote attackers to view directory listings via the 'dir' command or issue other commands without authenticating.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3564</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	Unrestricted file upload vulnerability in the Settings_Vtiger_CompanyDetailsSave_Action class in modules/Settings/Vtiger/actions/CompanyDetailsSave.php in Vtiger CRM 6.3.0 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in test/logo/.	2020-02-06	not yet calculated	<a href="#">CVE-2015-6000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
watchguard -- firewire_xtmi	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	not yet calculated	<a href="#">CVE-2014-6413</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
webcalendar - - webcalendar	webcalendar before 1.2.7 shows the reason for a failed login (e.g., "no such user").	2020-02-04	not yet calculated	<a href="#">CVE-2013-1422</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-</a>

wordpress - wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	not yet calculated	<a href="#">2013-2008 MISC MISC MISC</a>
wordpress - wordpress	The Time Capsule plugin before 1.21.16 for WordPress has an authentication bypass. Any request containing IWP_JSON_PREFIX causes the client to be logged in as the first account on the list of administrator accounts.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8771 MISC MISC</a>
wordpress - wordpress	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for WordPress and before 2.0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	2020-02-08	not yet calculated	<a href="#">CVE-2014-8739 MISC MISC MISC MISC MISC MISC MISC MISC</a>
wordpress - wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-2009 MISC MISC MISC MISC MISC</a>
wordpress - wordpress	The InfiniteWP Client plugin before 1.9.4.5 for WordPress has a missing authorization check in iwpm_mmb_set_request in init.php. Any attacker who knows the username of an administrator can log in.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8772 MISC MISC</a>
wordpress - wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2062 MISC MISC MISC MISC</a>
wordpress - wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-1394 MISC MISC MISC MISC MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3628 MISC MISC</a>



				<a href="#">MISC</a>
zoho_manageengine -- applications_manager	Zoho ManageEngine Applications Manager 14 before 14520 allows a remote unauthenticated attacker to disclose OS file names via FailOverHelperServlet.	2020-02-06	not yet calculated	<a href="#">CVE-2019-19800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager_and_ops_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	not yet calculated	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to tmcginnis@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:** [US-CERT](mailto:US-CERT)  
**To:** [wqutarte@ci.sunnyvale.ca.us](mailto:wqutarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of February 3, 2020  
**Date:** Wednesday, February 12, 2020 12:41:58 PM

---



National Cyber Awareness System:

*\*The tables in Vulnerability Bulletin (SB20-041) have been updated.*

## **Vulnerability Summary for the Week of February 3, 2020**

02/10/2020 07:28 AM EST

Original release date: February 10, 2020 | Last revised: February 12, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	2020-01-31	7.5	<a href="#">CVE-2014-8322</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aruba_networks -- instant	Multiple vulnerabilities exists in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.	2020-01-31	7.5	<a href="#">CVE-2016-2031</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	7.8	<a href="#">CVE-2020-3926</a> <a href="#">CONFIRM</a>
changing_information_technology	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API	2020-02-		<a href="#">CVE-2020-</a>

-- servisign	function, they may access arbitrary files on target system via crafted API parameter.	03	<a href="#">8.5</a>	<a href="#">3927 CONFIRM</a>
cisco -- multiple_ip_phones	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	<a href="#">8.3</a>	<a href="#">CVE-2020-3111 MISC CISCO</a>
cisco -- video_surveillance_8000_series_ip_cameras	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later.	2020-02-05	<a href="#">8.3</a>	<a href="#">CVE-2020-3110 MISC CISCO</a>
coppermine_development -- coppermine_gallery	Coppermine gallery before 1.4.26 has an input validation vulnerability that allows for code execution.	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2010-4815 MISC MISC MISC</a>
	All versions of curling.js are vulnerable to Command Injection via the run function.			<a href="#">CVE-2019-</a>

curling -- curling	The command argument can be controlled by users without any sanitization.	2020-02-06	<a href="#">10</a>	<a href="#">10789</a> <a href="#">MISC</a> <a href="#">MISC</a>
django -- django	Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-7471</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
dot-prop -- dot-prop	Prototype pollution vulnerability in dot-prop npm package version 5.1.0 and earlier allows an attacker to add arbitrary properties to JavaScript language constructs such as objects.	2020-02-04	<a href="#">7.5</a>	<a href="#">CVE-2020-8116</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.2.4 is vulnerable to directory traversal, leading to incorrect access control. It allows an attacker to read or execute files under \$TOMCAT_HOME/webapps/ROOT/assets (which should be a protected directory). Additionally, attackers can upload temporary files (e.g., .jsp files) into /webapps/ROOT/assets/tmp_upload, which can lead to remote command execution (with the permissions of the user running the dotCMS application).	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-6754</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
edk2 -- unified_extensible_firmware_interface	Multiple integer overflows in the Pre-EFI Initialization (PEI) boot phase in the Capsule Update feature in the UEFI implementation in EDK2 allow physically proximate attackers to bypass intended access restrictions by providing crafted data that is not properly handled during the coalescing phase.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4860</a> <a href="#">MISC</a>
edk2 -- unified_extensible_firmware_interface	Integer overflow in the Drive Execution Environment (DXE) phase in the Capsule Update feature in the UEFI implementation in EDK2 allows physically proximate attackers to bypass intended access restrictions via crafted data.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4859</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows SQL Injection via the user parameter to com.eg.LoginHelperServlet (aka the Forgot Password feature).	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8592</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows authentication bypass via a com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r request.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8591</a> <a href="#">MISC</a>



fortinet -- fortimanager	A Command Injection vulnerability exists in FortiManager 5.2.1 and earlier and FortiManager 5.0.10 and earlier via unspecified vectors, which could let a malicious user run systems commands when executing a report.	2020-02-04	9	<a href="#">CVE-2015-3611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- mortimanager	A vulnerability exists in in FortiManager 5.2.1 and earlier and 5.0.10 and earlier in the WebUI FTP backup page	2020-02-04	7.5	<a href="#">CVE-2015-3613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	7.5	<a href="#">CVE-2020-8114</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.2 incorrectly validated role/region associated with TLS certificates used for mTLS RPC, and were susceptible to privilege escalation. Fixed in 0.10.3.	2020-01-31	7.5	<a href="#">CVE-2020-7956</a> <a href="#">MISC</a> <a href="#">MISC</a>
jobberbase -- jobberbase	Jobberbase 2.0 has SQL injection via the PATH_INFO to the jobs-in endpoint.	2020-02-05	7.5	<a href="#">CVE-2019-20447</a> <a href="#">MISC</a> <a href="#">MISC</a>
klona -- klona	Flaw in input validation in npm package klona version 1.1.0 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using klona.	2020-02-04	7.5	<a href="#">CVE-2020-8125</a> <a href="#">MISC</a>
nanopb -- nanopb	There is a potentially exploitable out of memory condition In Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is compiled with PB_ENABLE_MALLOC, the message to be decoded contains a repeated string, bytes or message field and realloc() runs out of memory when expanding the array nanopb can end up calling `free()` on a pointer value that comes from uninitialized memory. Depending on platform this can result in a crash or further memory corruption, which may be exploitable in some cases. This problem is fixed in nanopb-0.4.1, nanopb-0.3.9.5, nanopb-0.2.9.4.	2020-02-04	7.5	<a href="#">CVE-2020-5235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netapp -- oncommand_system_manager	NetApp OnCommand System Manager 2.1 and earlier allows remote attackers to execute arbitrary commands in the Halt/Reboot interface.	2020-01-31	9	<a href="#">CVE-2013-3322</a> <a href="#">XF</a> <a href="#">MISC</a>
norman -- malware_cleaner	nsak64.sys in Norman Malware Cleaner 2.08.08 allows users to call arbitrary kernel functions because the passing of function pointers between user and kernel mode is mishandled.	2020-02-03	7.5	<a href="#">CVE-2020-8508</a> <a href="#">MISC</a>

phpabook -- phpabook	An issue was discovered in phpABook 0.9 Intermediate. On the login page, if one sets a userInfo cookie with the value of admin+1+en (user+perms+lang), one can login as any user without a password.	2020-02-03	7.5	<a href="#">CVE-2020-8510</a> <a href="#">MISC</a> <a href="#">MISC</a>
phplist -- phplist	phplist 3.5.0 allows type juggling for admin login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2020-02-03	7.5	<a href="#">CVE-2020-8547</a> <a href="#">MISC</a>
playsms -- playsms	PlaySMS before 1.4.3 does not sanitize inputs from a malicious string.	2020-02-05	7.5	<a href="#">CVE-2020-8644</a> <a href="#">MISC</a> <a href="#">MISC</a>
ppp -- ppp	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.	2020-02-03	7.5	<a href="#">CVE-2020-8597</a> <a href="#">MISC</a> <a href="#">MLIST</a>
python -- python	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.	2020-02-04	7.1	<a href="#">CVE-2019-9674</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- mdm9206_and_mdm9607_devices	Subsequent additions performed during Module loading while allocating the memory could lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	7.2	<a href="#">CVE-2019-14051</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_processors	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	7.2	<a href="#">CVE-2019-14046</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_processors	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open process in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	7.2	<a href="#">CVE-2019-14044</a> <a href="#">CONFIRM</a>
	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,			

qualcomm -- multiple_snapdragon_products	Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14055</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14002</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> <a href="#">CONFIRM</a>
qualcomm --	Out of bound access due to Invalid inputs to dapm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon			<a href="#">CVE-2019-</a>

multiple_snapdragon_products	Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	<a href="#">9.4</a>	<a href="#">14063 CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Uninitialized stack data gets used If memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14060 CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	<a href="#">9.4</a>	<a href="#">CVE-2019-14057 CONFIRM</a>
	Stage-2 fault will occur while writing to an			



qualcomm -- multiple_snapdragon_products	ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14049</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> <a href="#">CONFIRM</a>
sap -- netweaver	SAP NetWeaver 7.0 allows Remote Code Execution and Denial of Service caused by an error in the DiagTraceHex() function. By sending a specially-crafted packet, an attacker could exploit this vulnerability to cause the application to crash.	2020-02-05	7.5	<a href="#">CVE-2011-1517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript.com -- simplejobscript.com	controllers/page_apply.php in Simplejobscript.com SJS through 1.66 is prone to unauthenticated Remote Code Execution by uploading a PHP script as a resume.	2020-01-31	7.5	<a href="#">CVE-2020-8440</a> <a href="#">CONFIRM</a>
smartbear -- readyapi_and_soapui	An issue was discovered in SmartBear ReadyAPI through 2.8.2 and 3.0.0 and SoapUI through 5.5. When opening a project, the Groovy "Load Script" is automatically executed. This allows an attacker to execute arbitrary Groovy Language code (Java scripting language) on the victim machine by inducing it to	2020-02-05	9.3	<a href="#">CVE-2019-12180</a> <a href="#">MISC</a>

	open a malicious Project. The same issue is present in the "Save Script" function, which is executed automatically when saving a project.			
squid -- squid	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	2020-02-04	7.5	<a href="#">CVE-2020-8450</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_update_framework -- tuf	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature.	2020-02-05	7.5	<a href="#">CVE-2020-6174</a> <a href="#">CONFIRM</a>
tp-link -- tg-sg105e_devices	The Web Management of TP-Link TP-SG105E V4 1.0.0 Build 20181120 devices allows an unauthenticated attacker to reboot the device via a reboot.cgi request.	2020-02-03	7.8	<a href="#">CVE-2019-16893</a> <a href="#">EXPLOIT-DB</a>
zpanel_project -- zpanel	ZPanel 10.0.1 has insufficient entropy for its password reset process.	2020-02-04	7.5	<a href="#">CVE-2012-5686</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	6.5	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	5	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	4.6	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent -- 1830_photonic_service (PDS)	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch (PDS) 6.0 and earlier allows remote	2020-01-	4.3	<a href="#">CVE-2014-3809</a>

	attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	31		<a href="#">MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-12426</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	<a href="#">4.9</a>	<a href="#">CVE-2011-0220</a> <a href="#">MISC</a>
apple -- safari	A Cross-origin vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2016-4676</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8505</a> <a href="#">MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8504</a> <a href="#">MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2016-2032</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20104</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404</a> <a href="#">N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20400</a> <a href="#">N/A</a>
atlassian -- jira	The JMX monitoring flag in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to turn the	2020-02-	<a href="#">4.3</a>	<a href="#">CVE-2019-20405</a>

	JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	06		<a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20403</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20402</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2674</a> <a href="#">MISC</a> <a href="#">XE</a> <a href="#">BID</a>
				<a href="#">CVE-2013-</a>



brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	<a href="#">5</a>	<a href="#">2672 MISC XE</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	<a href="#">4.6</a>	<a href="#">CVE-2013-2673 MISC BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-12998 MISC CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2013-2683 MISC BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2013-2680 MISC BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-2678 MISC EXPLOIT-DB BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2013-2681 MISC BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2013-2682 MISC BID XE</a>
cisco -- linksys_e4200	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2013-2684 MISC BID XE</a>
computer_incident_response -- ail-framework	Global Cyber All Framework 2.8 allows path traversal.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2020-8545 MISC</a>
csharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions and stack overflow. Review the linked	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2020-5234 MISC</a>

	GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus -- eucalyptus_management_console	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2013-</a>

evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	<a href="#">6.6</a>	<a href="#">5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	<a href="#">4.6</a>	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

gitlab -- gitlab_enterprise_edition	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	5	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (Issue 2 of 2).	2020-02-05	5	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	4.3	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	6.8	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	5	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	5	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 1.10.3 allow unbounded resource	2020-01-	5	<a href="#">CVE-2020-7218</a>



	usage.	31		<a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	<a href="#">5.8</a>	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	<a href="#">6.9</a>	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	<a href="#">6.5</a>	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	<a href="#">6</a>	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	<a href="#">5.8</a>	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or browser history. IBM X-Force ID: 166623.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
	IBM Security Directory Server 6.4.0 could			

ibm -- security_directory_server	allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute	2020-01-		<a href="#">CVE-2014-8139</a> <a href="#">MISC</a>

	arbitrary code via a crafted zip file in the -t command argument to the unzip command.	31	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	<a href="#">6.4</a>	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be entered by any user. If it doesn't contain rel="noopener" (or similar attributes such	2020-02-	<a href="#">4.3</a>	<a href="#">CVE-2020-5182</a>

	as norereferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	03		<a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	<a href="#">6.6</a>	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- - rumpus	An issue was discovered in Rumpus 0.2.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	<a href="#">4.3</a>	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to write a DLL file in a directory in the global path environmental variable variable to	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20406</a> <a href="#">N/A</a>



	inject code & escalate their privileges via a DLL hijacking vulnerability.			
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	4.3	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	4	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	4.3	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	5	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	4	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	4	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	5	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	4.3	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-4116</a> <a href="#">MISC</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	<a href="#">5</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	<a href="#">6.4</a>	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	<a href="#">4</a>	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,			

qualcomm -- multiple_snapdragon_products	APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>
	An issue was discovered in Squid before			

squid-cache -- squid	4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- openSUSE_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims to arbitrary websites via a crafted URL.	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>



telaen -- telaen	Telean before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted URL request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2624</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browserx" in the page image.php.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	<a href="#">5</a>	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>

	server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress --	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can	2020-02-		<a href="#">CVE-2020-8549</a> <a href="#">MISC</a>

wordpress	result in an attacker performing malicious actions such as stealing session tokens.	03	4.3	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	4.3	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	6.5	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	4	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) 5.0.1050 through 5.1.1067 and 6.0.1000 through 6.0.1003 allows Insecure Direct Object Reference (IDOR) by an authenticated sender because of an error in a file-upload feature. This is fixed in 5.1.1068 and 6.0.1004.	2020-01-31	3.5	<a href="#">CVE-2020-8503</a> <a href="#">MISC</a>
bromium -- secure_platform	Bromium client version 4.0.3.2060 and prior to 4.1.7 Update 1 has an out of bound read results in race condition causing Kernel memory leaks or denial of service.	2020-02-03	3.3	<a href="#">CVE-2019-18567</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- digital_network_architecture	A vulnerability in the web-based management interface of Cisco Digital Network Architecture (DNA) Center could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An	2020-02-	3.5	<a href="#">CVE-2019-15253</a>

	attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker needs administrator credentials. This vulnerability affects Cisco DNA Center Software releases earlier than 1.3.0.6 and 1.3.1.4.	05		<a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack on an affected device. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by providing malicious data to a specific field within the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco ISE Software releases 2.7.0 and later contains the fix for this vulnerability.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2020-3149</a> <a href="#">CISCO</a>
cloud-init -- cloud-init	In cloud-init through 19.4, rand_user_password in cloudinit/config/cc_set_passwords.py has a small default pwlen value, which makes it easier for attackers to guess passwords.	2020-02-05	<a href="#">2.1</a>	<a href="#">CVE-2020-8632</a> <a href="#">MISC</a> <a href="#">MISC</a>
cloud-init -- cloud-init	cloud-init through 19.4 relies on Mersenne Twister for a random password, which makes it easier for attackers to predict passwords, because rand_str in cloudinit/util.py calls the random.choice function.	2020-02-05	<a href="#">2.1</a>	<a href="#">CVE-2020-8631</a> <a href="#">MISC</a> <a href="#">MISC</a>
fortinet -- fortimanager	A Cross-site Scripting (XSS) vulnerability exists in FortiManager 5.2.1 and earlier and 5.0.10 and earlier via an unspecified parameter in the FortiWeb auto update service page.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2015-3612</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 163493.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-4451</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- storediq	IBM StoredIQ 7.6.0.17 through 7.6.0.20 could disclose sensitive information to a local user due to data in certain	2020-02-		<a href="#">CVE-2020-4224</a>



	directories not being encrypted when it contained symbolic links. IBM X-Force ID: 175133.	03	<a href="#">2.1</a>	<a href="#">XE CONFIRM</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/console/vgacon.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8649 MISC</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vc_do_resize function in drivers/tty/vt/vt.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8647 MISC</a>
linux -- linux_kernel	In a Linux KVM guest that has PV TLB enabled, a process in the guest kernel may be able to read memory locations from another process in the same guest. This problem is limit to the host running linux kernel 4.10 with a guest running linux kernel 4.16 or later. The problem mainly affects AMD processors but Intel CPUs cannot be ruled out.	2020-01-31	<a href="#">1.9</a>	<a href="#">CVE-2019-3016 MLIST CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM</a>
linux -- linux_kernel	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.	2020-02-06	<a href="#">3.6</a>	<a href="#">CVE-2020-8648 MISC</a>
nextcloud -- nextcloud	Missing escaping of HTML in the Updater of Nextcloud 15.0.5 allowed a reflected XSS when starting the updater from a malicious location.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-15618 MISC MISC</a>
paessler -- prtg	An issue was discovered in PRTG 7.x through 19.4.53. Due to insufficient access control on local registry keys for the Core Server Service, a non-administrative user on the local machine is able to access administrative credentials.	2020-02-03	<a href="#">2.1</a>	<a href="#">CVE-2019-19119 MISC MISC MISC MISC</a>
pandora_fms -- pandora_fms	PandoraFMS 742 suffers from multiple XSS vulnerabilities, affecting the Agent Management, Report Builder, and Graph Builder components. An authenticated user can inject dangerous content into a data store that is later read and included in dynamic content.	2020-02-04	<a href="#">3.5</a>	<a href="#">CVE-2019-19968 MISC MISC</a>
sos -- jobscheduler	A cross-site scripting (XSS) vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to inject arbitrary web script or HTML via JSON properties available from the REST API.	2020-02-05	<a href="#">3.5</a>	<a href="#">CVE-2020-6854 MISC</a>
wordpress -- wordpress	A CSRF vulnerability in the Tutor LMS plugin before 1.5.3 for WordPress can result in an attacker approving themselves as an instructor and performing other malicious actions (such as blocking legitimate instructors).	2020-02-04	<a href="#">2.6</a>	<a href="#">CVE-2020-8615 MISC MISC MISC MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS& Score	Patch Info	Source
arctic_torrent -- arctic_torrent	A vulnerability exists in Arctic Torrent 1.4 via unspecified vectors in .torrent file handling, which could let a malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6309</a> <a href="#">MISC</a>	
atmail -- atmail_webmail_server	Cross-site scripting (XSS) vulnerability in the administrative interface in Atmail Webmail Server 6.4 allows remote attackers to inject arbitrary web script or HTML via the Date field of an email.	2020-02-06	not yet calculated	<a href="#">CVE-2012-2593</a> <a href="#">MISC</a>	
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	not yet calculated	<a href="#">CVE-2013-3091</a> <a href="#">MISC</a>	
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8796</a> <a href="#">MISC</a>	
bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>	
boonex -- dolphin	SQL injection vulnerability in Boonex Dolphin before 7.1.3 allows remote authenticated users to execute arbitrary SQL commands via the 'pathes' parameter in 'categories.php'.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3638</a> <a href="#">BID</a> <a href="#">XF</a>	
bosch -- bvms_mobile_video_service	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6770</a> <a href="#">CONFIRM</a>	
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS	2020-02-07	not yet calculated	<a href="#">CVE-2020-6768</a> <a href="#">CONFIRM</a>	

	version is installed.			
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6767</a> <a href="#">CONFIRM</a>
bosch -- video_streaming_gateway	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6769</a> <a href="#">CONFIRM</a>
broadcom -- multiple_devices	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic, a different vulnerability than CVE-2019-9500, CVE-2019-9501, CVE-2019-9502, and CVE-2019-9503.	2020-02-05	not yet calculated	<a href="#">CVE-2019-15126</a> <a href="#">CONFIRM</a>
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. By supplying a vendor information element with a data length larger than 32 bytes, a heap buffer overflow is triggered in wlc_wpa_sup_eapol. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9501</a> <a href="#">MISC CERT.</a> <a href="#">VN</a>
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. If the vendor information element data length is larger than 164 bytes, a heap buffer overflow is triggered in wlc_wpa_plumb_gtk. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9502</a> <a href="#">MISC CERT.</a> <a href="#">VN</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view private IP addresses and other sensitive information.	2020-02-04	not yet calculated	<a href="#">CVE-2013-2676</a> <a href="#">MISC CERT.</a> <a href="#">XF BID</a>

brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 devices with Firmware L contain a Frameable response (Clickjacking) vulnerability which could allow remote attackers to obtain sensitive information.	2020-02-05	not yet calculated	<a href="#">CVE-2013-2675</a> <a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a>
c-more -- touch_panels_attacker	It is possible to unmask credentials and other sensitive information on ?unprotected? project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations.	2020-02-05	not yet calculated	<a href="#">CVE-2020-6969</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11481</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11484</a> <a href="#">MISC</a>
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1700</a> <a href="#">USE</a> <a href="#">CONFIRM</a>
cgilua -- cgilua	The session.lua library in CGILua 5.2 alpha 1 and 5.2 alpha 2 uses weak session IDs generated based on OS time, which allows remote attackers to hijack arbitrary sessions via a brute force attack. NOTE: CVE-2014-10300 and CVE-2014-10400 were SPLIT from this ID.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2875</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGILua 5.0.x uses sequential session IDs, which makes it easier for remote attackers to predict the session ID and hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10400</a> <a href="#">MISC</a> <a href="#">MISC</a>



				<a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.1.x uses the same ID for each session, which allows remote attackers to hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10399</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chamilo -- chamilo_image	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_information_application -- servisign	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts.	2020-02-03	not yet calculated	<a href="#">CVE-2020-3925</a> <a href="#">CONFIRM</a>
cisco -- application Cisco ACE 4.6	Cisco ACE 4.6 allows log retention DoS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-1202</a> <a href="#">MISC</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3120</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not			

cisco -- cisco_discovery_protocol	properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3119</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- linksys_wrt110	Cross-site request forgery (CSRF) vulnerability in Cisco Linksys WRT110 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3568</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XF</a>
clamav -- clam_anti_virus	A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	2020-02-05	not yet calculated	<a href="#">CVE-2020-3123</a> <a href="#">CISCO</a>
corsair -- corsair_icue	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8808</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir865l_devices	D-Link DIR865L v1.03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3096</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dd-wrt -- dd-wrt	Command Injection vulnerability exists via a CSRF in DD-WRT 24-sp2 from specially crafted configuration values containing shell meta-characters, which could let a remote malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6297</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dedicated -- multiple_dvr_products	Dedicated Micros DV-IP Express, SD Advanced, SD, EcoSense, and DS2 devices rely on a GUI warning to help ensure that the administrator configures login credentials, which makes it easier for remote attackers to obtain access by leveraging situations in which this warning was not needed. NOTE: the vendor states "The user is presented with clear warnings on the GUI that they should set usernames and passwords."	2020-02-06	not yet calculated	<a href="#">CVE-2015-2909</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Dell EMC Isilon OneFS versions 8.1.2, 8.1.0.4, 8.1.0.3, and			

dell -- dmc_isilon	8.0.0.7 contain a vulnerability in some configurations. An attacker may exploit this vulnerability to gain access to restricted files. The non-RAN HTTP and WebDAV file-serving components have a vulnerability wherein when either are enabled, and Basic Authentication is enabled for either or both components, files are accessible without authentication.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5318</a> MISC
dell -- emc_ecs	Dell EMC ECS versions prior to 3.4.0.1 contain an XSS vulnerability. A remote authenticated malicious user could exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5317</a> MISC
dell -- multiple_products	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5319</a> MISC
den_norsk -- im-metadata	im-metadata through 3.0.1 allows remote attackers to execute arbitrary commands via the "exec" argument. It is possible to inject arbitrary commands as part of the metadata options which is given to the "exec" function.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10788</a> CONFIRM MISC
den_norsk -- im-resize	im-resize through 2.3.2 allows remote attackers to execute arbitrary commands via the "exec" argument. The cmd argument used within index.js, can be controlled by user without any sanitization.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10787</a> CONFIRM MISC
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container IDs.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5278</a> MISC MISC MISC
drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	not yet calculated	<a href="#">CVE-2012-5570</a> MISC MISC CONFIRM
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The installation uses the same API key (hardcoded as EONAPI_KEY in include/api_functions.php for API version 2.4.2) by default for all installations, hence allowing an attacker to calculate/guess the admin access token.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8657</a> MISC
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8656</a> MISC

eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8654</a> <a href="#">MISC</a>	
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8655</a> <a href="#">MISC</a>	
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5854</a> <a href="#">CONFIRM</a>	
flowplayer -- flowplayer	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	not yet calculated	<a href="#">CVE-2011-3642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>	
fork_cms - fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9470</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>	
fortinet -- forticlient_for_linux	A Denial of service (DoS) vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted IPC client requests to the fctschd process due the nanomsg not been correctly validated.	2020-02-06	not yet calculated	<a href="#">CVE-2019-16152</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A stack buffer overflow vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to cause FortiClient processes running under root priviledge crashes via sending specially crafted "StartAvCustomScan" type IPC client requests to the fctschd process due the argv data not been well sanitized.	2020-02-06	not yet calculated	<a href="#">CVE-2019-17652</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to run system commands under root privilege via injecting specially crafted "ExportLogs" type IPC client requests to the fctschd process.	2020-02-06	not yet calculated	<a href="#">CVE-2019-15711</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to			<a href="#">CVE-</a>	



fortinet -- forticlient_for_linux	overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctsched process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	not yet calculated	<a href="#">2019-16155</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13333</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17136</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13334</a> <a href="#">MISC</a>
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17135</a> <a href="#">MISC</a>
fujitsu -- multiple_products	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions, Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3,	2020-02-07	not yet calculated	<a href="#">CVE-2019-13163</a>

	Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.			CONFIRM
gnome -- libsvg	In xml.rs in GNOME libsvg before 2.46.2, a crafted SVG file with nested patterns can cause denial of service when passed to the library for processing. The attacker constructs pattern elements so that the number of final rendered objects grows exponentially.	2020-02-02	not yet calculated	CVE-2019-20446 MISC
gnome -- evolution -- and evolution_data_server	The gpg_ctx_add_recipient function in camel/camel-gpg-context.c in GNOME Evolution 3.8.4 and earlier and Evolution Data Server 3.9.5 and earlier does not properly select the GPG key to use for email encryption, which might cause the email to be encrypted with the wrong key and allow remote attackers to obtain sensitive information.	2020-02-06	not yet calculated	CVE-2013-4166 CONFIRM MISC MISC CONFIRM CONFIRM
golang -- go	The net/http library in net/http/transfer.go in Go before 1.4.3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains Content-Length and Transfer-Encoding header fields.	2020-02-08	not yet calculated	CVE-2015-5741 MISC MISC MISC MISC MISC MISC
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	CVE-2014-7224 MISC MISC MISC
google -- chrome	Google Chrome before 3.0 does not properly handle XML documents, which allows remote attackers to obtain sensitive information via a crafted web site.	2020-02-06	not yet calculated	CVE-2010-3917 MISC
hardcoreview - - hardcoreview	A vulnerability exists in HCView (aka Hardcoreview) 1.4 due to a write access violation with a GIF file.	2020-02-06	not yet calculated	CVE-2012-6306 MISC
hp -- sitescope	An Information Disclosure vulnerability exists in HP SiteScope 11.2 and 11.3 on Windows, Linux and Solaris, HP Asset Manager 9.30 through 9.32, 9.40 through 9.41, 9.50, and Asset Manager Cloudsystem Chargeback 9.40, which could let a remote malicious user obtain sensitive information. This is the TLS vulnerability known as the RC4 cipher Bar Mitzvah vulnerability.	2020-02-04	not yet calculated	CVE-2015-2802 CONFIRM CONFIRM MISC MISC MISC

ibm -- cloud_automation	IBM Cloud Automation Manager 3.2.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http://link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 168644.	2020-02-05	not yet calculated	<a href="#">CVE-2019-4616</a> <a href="#">X-CVE-2019-4616</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 contains hard-coded credentials, such as a password or cryptographic key, which can be used to bypass its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 171511.	2020-02-04	not yet calculated	<a href="#">CVE-2019-4675</a> <a href="#">X-CVE-2019-4675</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7523</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Stack-based buffer overflow in the WritePSDImage function coders/psd.c in ImageMagick, possibly 6.8.8-5, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-1947.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2030</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Buffer overflow in the DecodePSDPixels function in coders/psd.c in ImageMagick before 6.8.8-5 might allow remote attackers to execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-2030.	2020-02-06	not yet calculated	<a href="#">CVE-2014-1958</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ispconfig - - ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

				MISC
jpegsnoop - jpegsnoop	A vulnerability exists in JPEGsnoop 1.5.2 due to an unspecified issue in JPEG file handling, which could let a malicious user execute arbitrary code	2020-02-06	not yet calculated	CVE-2012-6307 MISC
kemp --load_master	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	not yet calculated	CVE-2014-5288 MISC
konqueror - konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	not yet calculated	CVE-2012-4512 MISC MISC MISC MISC MISC MISC MISC MISC MISC
linksys --wrt310n_wireless_router	Linksys WRT310Nv2 2.0.0.1 is vulnerable to XSS.	2020-02-07	not yet calculated	CVE-2013-3067 MISC MISC
linuxmint - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	not yet calculated	CVE-2012-1567 MISC
linuxmint - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	not yet calculated	CVE-2012-1566 MISC
mariadb --mariadb	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.	2020-02-04	not yet calculated	CVE-2020-7221 MISC CONFIRM MISC
mcabber - mcabber	MCabber before 1.0.4 is vulnerable to roster push attacks, which allows remote attackers to intercept communications, or add themselves as an entity on a 3rd party's roster as another user, which will also garner associated privileges, via crafted XMPP packets.	2020-02-06	not yet calculated	CVE-2016-9928 CONFIRM MISC MISC MISC CONFIRM



				<a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mediawiki - mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4381</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki - mediawiki	The CentralNotice extension for MediaWiki before 1.19.9, 1.20.x before 1.20.8, and 1.21.x before 1.21.3 sets the Cache-Control header to cache session cookies when a user is autocreated, which allows remote attackers to authenticate as the created user.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4572</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mikrotik -- winbox	MikroTik WinBox before 3.21 is vulnerable to a path traversal vulnerability that allows creation of arbitrary files wherever WinBox has write permissions. WinBox is vulnerable to this attack if it connects to a malicious endpoint or if an attacker mounts a man in the middle attack.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5720</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasnoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to execute arbitrary code via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5628</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasnoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause	2020-02-05	not yet calculated	<a href="#">CVE-2015-5627</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	a denial of service (process outage) via a crafted packet.			
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (network-communications outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5626</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h_____%2427, (3) h_____%2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-3423</a> <a href="#">MISC</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the (1) ctrl, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8) xname, or (9) mpTransactionId parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wifi_router	An Authentication vulnerability exists in NETGEAR WGR614 v7 and v9 due to a hardcoded credential used for serial programming, a related issue to CVE-2006-1002.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6340</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wifi_router	An Information Disclosure vulnerability exists in the my config file in NETGEAR WGR614 v7 and v9, which could let a malicious user recover all previously used passwords on the device, for both the control panel and WEP/WPA/WPA2, in plaintext. This is a different issue than CVE-2012-6340.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1.2.31805 and V2.2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracer diagnostic tool because of lack of user input sanitizing.	2020-02-07	not yet calculated	<a href="#">CVE-2019-19356</a> <a href="#">MISC</a>
network-manager - network-manager	network-manager through 1.0.2 allows remote attackers to execute arbitrary commands via the "execSync()" argument.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10786</a> <a href="#">MISC</a>
nextcloud	Improper authorization in the Circles app 0.17.7 causes		not	<a href="#">CVE-2019-</a>

-- circles	retaining access when an email address was removed from a circle.	2020-02-04	yet calculated	<a href="#">CVE-2019-15610</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	A wrong check for the system time in the Android App 3.9.0 causes a bypass of the lock protection when changing the time of the system to the past.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15615</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	Not strictly enough sanitization in the Nextcloud Android app 3.6.0 allowed an attacker to get content information from protected tables when using custom queries.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15622</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Violation of Secure Design Principles in the iOS App 2.23.0 causes the app to leak its login and token to other Nextcloud services when search e.g. for federated users or registering for push notifications.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15611</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Missing sanitization in the iOS App 2.24.4 causes an XSS when opening malicious HTML files.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15614</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper permissions preservation in Nextcloud Server 16.0.1 causes sharees to be able to reshare with write permissions when sharing the mount point of a share they received, as a public link.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15621</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Dangling remote share attempts in Nextcloud 16 allow a DoS/pollution when running long.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15616</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 15.0.2 causes pending 2FA logins to not be correctly expired when the password of the user is reset.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15612</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 17.0.1 causes the workflow rules to depend their behaviour on the file extension when checking file mimetypes.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15613</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A missing check in Nextcloud Server 17.0.0 allowed an attacker to set up a new second factor when trying to login.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15617</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper Input Validation in Nextcloud Server 15.0.7 allows group admins to create users with IDs of system folders.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15624</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-</a>

nextcloud -- nextcloud	Improper neutralization of file names, conversation names and board names in Nextcloud Server 16.0.3, Nextcloud Talk 16.0.3 and Nextcloud Deck 0.6.5 causes an XSS when linking them with each others in a project.	2020-02-04	not yet calculated	<a href="#">2019-15619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A bug in Nextcloud Server 14.0.4 could expose more data in reshared link shares than intended by the sharer.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8121</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	An authenticated server-side request forgery in Nextcloud server 16.0.1 allowed to detect local and remote services when adding a new subscription in the calendar application.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8118</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A missing check in Nextcloud Server 14.0.3 could give recipient the possibility to extend the expiration date of a share they received.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8122</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	nghttp2 before 1.7.1 allows remote attackers to cause a denial of service (memory exhaustion).	2020-02-06	not yet calculated	<a href="#">CVE-2016-1544</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	not yet calculated	<a href="#">CVE-2019-15604</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	Including trailing white space in HTTP header values in Nodejs 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	not yet calculated	<a href="#">CVE-2019-15606</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	not yet calculated	<a href="#">CVE-2019-15605</a> <a href="#">MISC</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a>
nuxeo -- nuxeo_platform	RichFaces implementation in Nuxeo Platform 5.6.0 before HF27 and 5.8.0 before HF-01 does not restrict the classes for which deserialization methods can be called, which allows remote attackers to execute arbitrary code via crafted serialized data. NOTE: this vulnerability may overlap CVE-2013-2165.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4521</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified	2020-02-07	not yet	<a href="#">CVE-2014-9530</a>



	impact.		calculated	<a href="#">CONFIRM</a>
omniauth-weibo-oauth2_gem -- omniauth-weibo-oauth2_gem_for_ruby_on_ra	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	not yet calculated	<a href="#">CVE-2019-17268</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the YII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9126</a> <a href="#">MISC</a>
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9127</a> <a href="#">MISC</a>
openfiler - openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1086</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openshift-enterprise - openshift-enterprise	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1708</a> <a href="#">CONFIRM</a>
openvas -- openvas_manager	OpenVAS Manager v2.0.3 allows plugin remote code execution.	2020-02-06	not yet calculated	<a href="#">CVE-2011-1597</a> <a href="#">MISC</a>
opopensocialplugin - opopensocialplugin	opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple XML External Entity Injection Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4335</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Starting from the apache user account, it is possible to perform privilege escalation through the lack of correct configuration in the server's sudoers file, which by default allows the execution of programs (e.g. nmap) without the need for a password with sudo.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7954</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Without authentication, it is possible to read server files (e.g., /etc/passwd) due to the use of the nmap -iL (aka input file) option.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7953</a> <a href="#">MISC</a> <a href="#">MISC</a>

opservices - opservices - opservices -	An issue was discovered in OpServices OpMon 9.3.2 that allows Remote Code Execution .	2020-02-06	not yet calculated	<a href="#">CVE-2020-8636</a> <a href="#">MISC</a>
opwebapiplugin - opwebapiplugin	opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4334</a> <a href="#">MISC</a>
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1768</a> <a href="#">CONFIRM</a>
percona -- percona_monitoring_and_management	pmm-server in Percona Monitoring and Management (PMM) 2.2.x before 2.2.1 allows unauthenticated denial of service.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7920</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phppgadmin -- phppgadmin	phppgadmin through 7.12.1 allows sensitive actions to be performed without validating that the request originated from the application. One such area, "database.php" does not verify the source of an HTTP request. This can be leveraged by a remote attacker to trick a logged-in administrator to visit a malicious page with a CSRF exploit and execute arbitrary system commands on the server.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10784</a> <a href="#">MISC</a>
projectpier - projectpier	ProjectPier 0.8.8 has stored XSS	2020-02-07	not yet calculated	<a href="#">CVE-2013-3635</a> <a href="#">MISC</a>
projectpier - projectpier	ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	not yet calculated	<a href="#">CVE-2013-3636</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
projectpier - projectpier	ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	not yet calculated	<a href="#">CVE-2013-3637</a> <a href="#">MISC</a>
qemu -- qemu	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8608</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24,	2020-02-07	not yet calculated	<a href="#">CVE-2019-14088</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	SM8150, SXR1130			
railo -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5468</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive -- adserver	A reflected XSS vulnerability has been discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.0.3 by Jacopo Tediosi. There are currently no known exploits: the session identifier cannot be accessed as it is stored in an http-only cookie as of v3.2.2. On older versions, however, under specific circumstances, it could be possible to steal the session identifier and gain access to the admin interface. The query string sent to the www/delivery/afr.php script was printed back without proper escaping in a JavaScript context, allowing an attacker to execute arbitrary JS code on the browser of the victim.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8115</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung - multiple_mobile_devices	On Samsung mobile devices with O(8.0) and P(9.0) software and an Exynos 8895 chipset, RKP (aka the Samsung Hypervisor EL2 implementation) allows arbitrary memory write operations. The Samsung ID is SVE-2019-16265.	2020-02-04	not yet calculated	<a href="#">CVE-2019-19273</a> <a href="#">CONFIRM</a>
schmid -- zi_620_v400_090_routers	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6760</a> <a href="#">MISC</a>
simple_machines - simple_machines_forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: Forum forum can read files such as the database config.	2020-02-07	not yet calculated	<a href="#">CVE-2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscrip - simplejobscrip	An issue was discovered in Simplejobscrip.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
smoothwall - smoothwall_express3	A cross-site scripting (XSS) vulnerability in Smoothwall Express3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall - smoothwall_express	CSRF vulnerability in Smoothwall Express 3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
sphider -- sphider_search_engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 where the search engine calls in admin/spiderfuncs.php, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5087</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-</a>

status2k -- status2k	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	not yet calculated	<a href="#">2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
statusnet - - statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	not yet calculated	<a href="#">CVE-2010-4658</a> <a href="#">MISC</a> <a href="#">MISC</a>
synaptive - - medical_clearcanvas_image_server	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8788</a> <a href="#">MISC</a>
teamviewer -- teamviewer	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9.x , this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2019-18988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tianocore - - edk2	Buffer overflow in the Reclaim function in Tianocore EDK2 before SVN 16280 allows physically proximate attackers to gain privileges via a long variable name.	2020-02-06	not yet calculated	<a href="#">CVE-2014-8271</a> <a href="#">MISC</a> <a href="#">MISC</a>
troglobit -- minisnmpd	A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server.	2020-02-04	not yet calculated	<a href="#">CVE-2020-6060</a> <a href="#">MISC</a>
ubiquiti_networks - unifi_controller	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4) authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via	2020-02-08	not yet calculated	<a href="#">CVE-2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>



	a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the Unifi Controller name via a request to api/set/setting/identity.			
ui -- edgeswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	not yet calculated	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
unshift -- url-parse	Insufficient validation and sanitization of user input exists in url-parse npm package version 1.4.4 and earlier may allow attacker to bypass security checks.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8124</a> <a href="#">MISC</a>
ushahidi -- ushahidi	Ushahidi before 2.6.1 has insufficient entropy for forgot-password tokens.	2020-02-04	not yet calculated	<a href="#">CVE-2012-5618</a> <a href="#">MISC</a>
videolan -- vlc_media_player	The web interface in VideoLAN VLC media player before 2.0.7 has no access control which allows remote attackers to view directory listings via the 'dir' command or issue other commands without authenticating.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3564</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	Unrestricted file upload vulnerability in the Settings_Vtiger_CompanyDetailsSave_Action class in modules/Settings/Vtiger/actions/CompanyDetailsSave.php in Vtiger CRM 6.3.0 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in test/logo/.	2020-02-06	not yet calculated	<a href="#">CVE-2015-6000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
watchguard - firewire_xtm	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	not yet calculated	<a href="#">CVE-2014-6413</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
webcalendar - webcalendar	webcalendar before 1.2.7 shows the reason for a failed login (e.g., "no such user").	2020-02-04	not yet calculated	<a href="#">CVE-2013-1422</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-2008</a> <a href="#">MISC</a> <a href="#">MISC</a>

				<a href="#">MISC</a>
wordpress - wordpress	The Time Capsule plugin before 1.21.16 for WordPress has an authentication bypass. Any request containing IWP_JSON_PREFIX causes the client to be logged in as the first account on the list of administrator accounts.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8771</a> <a href="#">MISC</a>
wordpress - wordpress	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for WordPress and before 2.0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	2020-02-08	not yet calculated	<a href="#">CVE-2014-8739</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-2009</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	The InfiniteWP Client plugin before 1.9.4.5 for WordPress has a missing authorization check in iwp_mmb_set_request in init.php. Any attacker who knows the username of an administrator can log in.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8772</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-1394</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3628</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine --	Zoho ManageEngine Applications Manager 14 before 14520 allows a remote unauthenticated attacker to disclose OS file	2020-02-06	not yet	<a href="#">CVE-2019-19800</a>

applications_manager	names via FailOverHelperServlet.		calculated	MISC MISC MISC
zoho_manageengine -- applications_manager and ops_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	not yet calculated	CVE-2014-7863 MISC MISC MISC MISC MISC MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:** [US-CERT](#)  
**To:** [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of February 3, 2020  
**Date:** Monday, February 10, 2020 3:15:45 PM

---



National Cyber Awareness System:

## **Vulnerability Summary for the Week of February 3, 2020**

02/10/2020 07:28 AM EST

Original release date: February 10, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	2020-01-31	7.5	<a href="#">CVE-2014-8322</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aruba_networks -- instant	Multiple vulnerabilities exists in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.	2020-01-31	7.5	<a href="#">CVE-2016-2031</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	7.8	<a href="#">CVE-2020-3926</a> <a href="#">CONFIRM</a>
changing_information_technology	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API	2020-02-		<a href="#">CVE-2020-</a>



-- servisign	function, they may access arbitrary files on target system via crafted API parameter.	03	<a href="#">8.5</a>	<a href="#">3927 CONFIRM</a>
cisco -- multiple_ip_phones	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	<a href="#">8.3</a>	<a href="#">CVE-2020-3111 MISC CISCO</a>
cisco -- video_surveillance_8000_series_ip_cameras	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later.	2020-02-05	<a href="#">8.3</a>	<a href="#">CVE-2020-3110 MISC CISCO</a>
coppermine_development -- coppermine_gallery	Coppermine gallery before 1.4.26 has an input validation vulnerability that allows for code execution.	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2010-4815 MISC MISC MISC</a>
	All versions of curling.js are vulnerable to Command Injection via the run function.			<a href="#">CVE-2019-</a>

curling -- curling	The command argument can be controlled by users without any sanitization.	2020-02-06	<a href="#">10</a>	<a href="#">10789</a> <a href="#">MISC</a> <a href="#">MISC</a>
django -- django	Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-7471</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
dot-prop -- dot-prop	Prototype pollution vulnerability in dot-prop npm package version 5.1.0 and earlier allows an attacker to add arbitrary properties to JavaScript language constructs such as objects.	2020-02-04	<a href="#">7.5</a>	<a href="#">CVE-2020-8116</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.2.4 is vulnerable to directory traversal, leading to incorrect access control. It allows an attacker to read or execute files under \$TOMCAT_HOME/webapps/ROOT/assets (which should be a protected directory). Additionally, attackers can upload temporary files (e.g., .jsp files) into /webapps/ROOT/assets/tmp_upload, which can lead to remote command execution (with the permissions of the user running the dotCMS application).	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-6754</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
edk2 -- unified_extensible_firmware_interface	Multiple integer overflows in the Pre-EFI Initialization (PEI) boot phase in the Capsule Update feature in the UEFI implementation in EDK2 allow physically proximate attackers to bypass intended access restrictions by providing crafted data that is not properly handled during the coalescing phase.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4860</a> <a href="#">MISC</a>
edk2 -- unified_extensible_firmware_interface	Integer overflow in the Drive Execution Environment (DXE) phase in the Capsule Update feature in the UEFI implementation in EDK2 allows physically proximate attackers to bypass intended access restrictions via crafted data.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4859</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows SQL Injection via the user parameter to com.eg.LoginHelperServlet (aka the Forgot Password feature).	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8592</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows authentication bypass via a com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r request.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8591</a> <a href="#">MISC</a>

fortinet -- fortimanager	A Command Injection vulnerability exists in FortiManager 5.2.1 and earlier and FortiManager 5.0.10 and earlier via unspecified vectors, which could let a malicious user run systems commands when executing a report.	2020-02-04	9	<a href="#">CVE-2015-3611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- mortimanager	A vulnerability exists in in FortiManager 5.2.1 and earlier and 5.0.10 and earlier in the WebUI FTP backup page	2020-02-04	7.5	<a href="#">CVE-2015-3613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	7.5	<a href="#">CVE-2020-8114</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.2 incorrectly validated role/region associated with TLS certificates used for mTLS RPC, and were susceptible to privilege escalation. Fixed in 0.10.3.	2020-01-31	7.5	<a href="#">CVE-2020-7956</a> <a href="#">MISC</a> <a href="#">MISC</a>
jobberbase -- jobberbase	Jobberbase 2.0 has SQL injection via the PATH_INFO to the jobs-in endpoint.	2020-02-05	7.5	<a href="#">CVE-2019-20447</a> <a href="#">MISC</a> <a href="#">MISC</a>
klona -- klona	Flaw in input validation in npm package klona version 1.1.0 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using klona.	2020-02-04	7.5	<a href="#">CVE-2020-8125</a> <a href="#">MISC</a>
nanopb -- nanopb	There is a potentially exploitable out of memory condition In Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is compiled with PB_ENABLE_MALLOC, the message to be decoded contains a repeated string, bytes or message field and realloc() runs out of memory when expanding the array nanopb can end up calling `free()` on a pointer value that comes from uninitialized memory. Depending on platform this can result in a crash or further memory corruption, which may be exploitable in some cases. This problem is fixed in nanopb-0.4.1, nanopb-0.3.9.5, nanopb-0.2.9.4.	2020-02-04	7.5	<a href="#">CVE-2020-5235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netapp -- oncommand_system_manager	NetApp OnCommand System Manager 2.1 and earlier allows remote attackers to execute arbitrary commands in the Halt/Reboot interface.	2020-01-31	9	<a href="#">CVE-2013-3322</a> <a href="#">XF</a> <a href="#">MISC</a>
norman -- malware_cleaner	nsak64.sys in Norman Malware Cleaner 2.08.08 allows users to call arbitrary kernel functions because the passing of function pointers between user and kernel mode is mishandled.	2020-02-03	7.5	<a href="#">CVE-2020-8508</a> <a href="#">MISC</a>

phpabook -- phpabook	An issue was discovered in phpABook 0.9 Intermediate. On the login page, if one sets a userInfo cookie with the value of admin+1+en (user+perms+lang), one can login as any user without a password.	2020-02-03	7.5	<a href="#">CVE-2020-8510</a> <a href="#">MISC</a> <a href="#">MISC</a>
phplist -- phplist	phplist 3.5.0 allows type juggling for admin login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2020-02-03	7.5	<a href="#">CVE-2020-8547</a> <a href="#">MISC</a>
playsms -- playsms	PlaySMS before 1.4.3 does not sanitize inputs from a malicious string.	2020-02-05	7.5	<a href="#">CVE-2020-8644</a> <a href="#">MISC</a> <a href="#">MISC</a>
ppp -- ppp	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.	2020-02-03	7.5	<a href="#">CVE-2020-8597</a> <a href="#">MISC</a> <a href="#">MLIST</a>
python -- python	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.	2020-02-04	7.1	<a href="#">CVE-2019-9674</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- mdm9206_and_mdm9607_devices	Subsequent additions performed during Module loading while allocating the memory could lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	7.2	<a href="#">CVE-2019-14051</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_processors	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	7.2	<a href="#">CVE-2019-14046</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_processors	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open process in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	7.2	<a href="#">CVE-2019-14044</a> <a href="#">CONFIRM</a>
	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT,			



qualcomm -- multiple_snapdragon_products	Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14055</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14002</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> <a href="#">CONFIRM</a>
qualcomm --	Out of bound access due to Invalid inputs to dapm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon			<a href="#">CVE-2019-</a>

multiple_snapdragon_products	Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	<a href="#">9.4</a>	<a href="#">14063</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Uninitialized stack data gets used If memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14060</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	<a href="#">9.4</a>	<a href="#">CVE-2019-14057</a> <a href="#">CONFIRM</a>
	Stage-2 fault will occur while writing to an			

qualcomm -- multiple_snapdragon_products	ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14049</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> <a href="#">CONFIRM</a>
sap -- netweaver	SAP NetWeaver 7.0 allows Remote Code Execution and Denial of Service caused by an error in the DiagTraceHex() function. By sending a specially-crafted packet, an attacker could exploit this vulnerability to cause the application to crash.	2020-02-05	7.5	<a href="#">CVE-2011-1517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript.com -- simplejobscript.com	controllers/page_apply.php in Simplejobscript.com SJS through 1.66 is prone to unauthenticated Remote Code Execution by uploading a PHP script as a resume.	2020-01-31	7.5	<a href="#">CVE-2020-8440</a> <a href="#">CONFIRM</a>
smartbear -- readyapi_and_soapui	An issue was discovered in SmartBear ReadyAPI through 2.8.2 and 3.0.0 and SoapUI through 5.5. When opening a project, the Groovy "Load Script" is automatically executed. This allows an attacker to execute arbitrary Groovy Language code (Java scripting language) on the victim machine by inducing it to	2020-02-05	9.3	<a href="#">CVE-2019-12180</a> <a href="#">MISC</a>

	open a malicious Project. The same issue is present in the "Save Script" function, which is executed automatically when saving a project.			
squid -- squid	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	2020-02-04	7.5	<a href="#">CVE-2020-8450</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_update_framework -- tuf	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature.	2020-02-05	7.5	<a href="#">CVE-2020-6174</a> <a href="#">CONFIRM</a>
tp-link -- tg-sg105e_devices	The Web Management of TP-Link TP-SG105E V4 1.0.0 Build 20181120 devices allows an unauthenticated attacker to reboot the device via a reboot.cgi request.	2020-02-03	7.8	<a href="#">CVE-2019-16893</a> <a href="#">EXPLOIT-DB</a>
zpanel_project -- zpanel	ZPanel 10.0.1 has insufficient entropy for its password reset process.	2020-02-04	7.5	<a href="#">CVE-2012-5686</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	6.5	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	5	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	4.6	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent -- 1830_photonic_service (PDS)	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch (PDS) 6.0 and earlier allows remote	2020-01-	4.3	<a href="#">CVE-2014-3809</a>



	attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	31		<a href="#">MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-12426</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	<a href="#">4.9</a>	<a href="#">CVE-2011-0220</a> <a href="#">MISC</a>
apple -- safari	A Cross-origin vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2016-4676</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8505</a> <a href="#">MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8504</a> <a href="#">MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2016-2032</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20104</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404</a> <a href="#">N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20400</a> <a href="#">N/A</a>
atlassian -- jira	The JMX monitoring flag in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to turn the	2020-02-	<a href="#">4.3</a>	<a href="#">CVE-2019-20405</a>

	JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	06		<a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20403</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20402</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2674</a> <a href="#">MISC</a> <a href="#">XE</a> <a href="#">BID</a>
				<a href="#">CVE-2013-</a>

brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	<a href="#">5</a>	<a href="#">2672 MISC XE</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	<a href="#">4.6</a>	<a href="#">CVE-2013-2673 MISC BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-12998 MISC CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2013-2683 MISC BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2013-2680 MISC BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-2678 MISC EXPLOIT-DB BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2013-2681 MISC BID XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2013-2682 MISC BID XE</a>
cisco -- linksys_e4200	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2013-2684 MISC BID XE</a>
computer_incident_response -- ail-framework	Global Cyber All Framework 2.8 allows path traversal.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2020-8545 MISC</a>
csharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions and stack overflow. Review the linked	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2020-5234 MISC</a>

	GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus -- eucalyptus_management_console	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2013-</a>



evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	<a href="#">6.6</a>	<a href="#">5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	<a href="#">4.6</a>	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

gitlab -- gitlab_enterprise_edition	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	5	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (Issue 2 of 2).	2020-02-05	5	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	4.3	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	6.8	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	5	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	5	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 1.10.3 allow unbounded resource	2020-01-	5	<a href="#">CVE-2020-7218</a>

	usage.	31		<a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	<a href="#">5.8</a>	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	<a href="#">6.9</a>	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	<a href="#">6.5</a>	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	<a href="#">6</a>	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	<a href="#">5.8</a>	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or browser history. IBM X-Force ID: 166623.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
	IBM Security Directory Server 6.4.0 could			

ibm -- security_directory_server	allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute	2020-01-		<a href="#">CVE-2014-8139</a> <a href="#">MISC</a>

	arbitrary code via a crafted zip file in the -t command argument to the unzip command.	31	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	<a href="#">6.4</a>	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be entered by any user. If it doesn't contain rel="noopener" (or similar attributes such	2020-02-	<a href="#">4.3</a>	<a href="#">CVE-2020-5182</a>



	as norereferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	03		<a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	<a href="#">6.6</a>	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- - rumpus	An issue was discovered in Rumpus 0.2.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	<a href="#">4.3</a>	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to write a DLL file in a directory in the global path environmental variable variable to	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20406</a> <a href="#">N/A</a>

	inject code & escalate their privileges via a DLL hijacking vulnerability.			
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	4.3	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	4	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	4.3	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	5	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	4	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	4	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	5	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	4.3	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-4116</a> <a href="#">MISC</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	<a href="#">5</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	<a href="#">6.4</a>	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	<a href="#">4</a>	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,			

qualcomm -- multiple_snapdragon_products	APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>
	An issue was discovered in Squid before			

squid-cache -- squid	4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- openSUSE_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims to arbitrary websites via a crafted URL.	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>



telaen -- telaen	Telean before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted URL request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2624</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browserx" in the page image.php.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	<a href="#">5</a>	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>

	server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress --	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can	2020-02-		<a href="#">CVE-2020-8549</a> <a href="#">MISC</a>

wordpress	result in an attacker performing malicious actions such as stealing session tokens.	03	4.3	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	4.3	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	6.5	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	4	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	6.5	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	5	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	4.6	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent -- 1830_photonic_service (PSS)	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch before 6.0 and earlier allows remote attackers to inject arbitrary web script or	2020-01-31	4.3	<a href="#">CVE-2014-3809</a> <a href="#">MISC</a>

	HTML via the myurl parameter to menu/pop.html.			
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	5	<a href="#">CVE-2019-12426</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	4.9	<a href="#">CVE-2011-0220</a> <a href="#">MISC</a>
apple -- safari	A Cross-origins vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	5	<a href="#">CVE-2016-4676</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	4.3	<a href="#">CVE-2020-8505</a> <a href="#">MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	4.3	<a href="#">CVE-2020-8504</a> <a href="#">MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	5	<a href="#">CVE-2016-2032</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	5	<a href="#">CVE-2019-20104</a> <a href="#">N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	4.4	<a href="#">CVE-2019-20400</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	5	<a href="#">CVE-2019-20403</a> <a href="#">N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System Administrator user without requiring the user to re-enter their password via an	2020-02-06	4	<a href="#">CVE-2019-20402</a> <a href="#">N/A</a>

	improper authorization vulnerability.			
atlassian -- jira	The JMX monitoring flag in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to turn the JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20405</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2672</a> <a href="#">MISC</a> <a href="#">XF</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view sensitive information	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2674</a> <a href="#">MISC</a> <a href="#">XF</a>



	from referrer logs due to inadequate handling of HTTP referrer headers.			<a href="#">BID</a>
brother -- mfc-9970cdw	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	<a href="#">4.6</a>	<a href="#">CVE-2013-2673</a> <a href="#">MISC</a> <a href="#">BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-12998</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2013-2680</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2013-2683</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XE</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-2678</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XE</a>
cisco -- linksys_e4200_devices	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2013-2681</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XE</a>
cisco -- linksys_e4200_devices	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2013-2684</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XE</a>
cisco -- linksys_e4200_devices	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2013-2682</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XE</a>
computer_incident_response -- ail-framework	Global Cyber Alliance framework 2.8 allows path traversal.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2020-8545</a> <a href="#">MISC</a>
cysharp -- messagepack_for_csharp_and_mono	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can be used to cause a DoS attack due to hash collisions and stack overflow. Review the linked GitHub Security Advisory for more	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2020-5234</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	information and remediation steps.			
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	5	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	5	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	6.8	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	6.8	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	4.3	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	4.3	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	5	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	4.9	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus_eucalyptus	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) 4.0.x before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	6.8	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>
evernote_corporation -	Evernote prior to 5.5.1 has insecure	2020-01-		<a href="#">CVE-2013-5116</a>

- evernote	password change	31	6.6	MISC MISC MISC
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	5	<a href="#">CVE-2020-5856</a> CONFIRM
f5 -- big-ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	4.6	<a href="#">CVE-2020-5855</a> CONFIRM
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	5	<a href="#">CVE-2020-6833</a> MISC CONFIRM
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7973</a> MISC CONFIRM MISC
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	5	<a href="#">CVE-2020-7978</a> MISC CONFIRM
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	5	<a href="#">CVE-2020-7966</a> MISC CONFIRM
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7968</a> MISC CONFIRM
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	4	<a href="#">CVE-2020-7967</a> MISC CONFIRM
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7974</a> MISC CONFIRM
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7976</a> MISC CONFIRM
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).	2020-02-05	5	<a href="#">CVE-2020-7972</a> MISC CONFIRM
				<a href="#">CVE-2020-</a>

gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	<a href="#">5</a>	<a href="#">7969</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise 1.0.10.3 allow unbounded resource	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7218</a> <a href="#">MISC</a>

	usage.			<a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	<a href="#">5.8</a>	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-4613</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	<a href="#">6.9</a>	<a href="#">CVE-2019-4732</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	<a href="#">6.5</a>	<a href="#">CVE-2019-4541</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	<a href="#">6</a>	<a href="#">CVE-2020-4163</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	<a href="#">5.8</a>	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or browser history. IBM X-Force ID: 166623.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-4562</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
	IBM Security Directory Server 6.4.0 does			<a href="#">CVE-2019-</a>



ibm -- security_directory_server	not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">4551</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute	2020-01-		<a href="#">CVE-2014-8139</a> <a href="#">MISC</a>

	arbitrary code via a crafted zip file in the -t command argument to the unzip command.	31	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	<a href="#">6.4</a>	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be entered by any user. If it doesn't contain rel="noopener" (or similar attributes such	2020-02-	<a href="#">4.3</a>	<a href="#">CVE-2020-5182</a>

	as norereferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	03		<a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	<a href="#">6.6</a>	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- - rumpus	An issue was discovered in Rumpus 0.2.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	<a href="#">4.3</a>	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to write a DLL file in a directory in the global path environmental variable variable to	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20406</a> <a href="#">N/A</a>

	inject code & escalate their privileges via a DLL hijacking vulnerability.			
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	4.3	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	4.3	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	4	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	4	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	5	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	4	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	5	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	4.3	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-4116</a> <a href="#">MISC</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	<a href="#">5</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	<a href="#">6.4</a>	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	<a href="#">4</a>	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,			



qualcomm -- multiple_snapdragon_products	APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>
	An issue was discovered in Squid before			

squid-cache -- squid	4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- opensuse_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Telean before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted URL request.	2020-02-03	5	<a href="#">CVE-2013-2624</a> <a href="#">XF</a> <a href="#">MISC</a>

telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims to arbitrary websites via a crafted URL.	2020-02-03	<a href="#">5.8</a>	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browserx" in the page image.php.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	<a href="#">5</a>	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>

	server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress --	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can	2020-02-		<a href="#">CVE-2020-8549</a> <a href="#">MISC</a>

wordpress	result in an attacker performing malicious actions such as stealing session tokens.	03	4.3	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	4.3	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	6.5	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	4	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS & Score	Source Patch Info
arctic_torrent -- arctic_torrent	A vulnerability exists in Arctic Torrent 1.4 via unspecified vectors in .torrent file handling, which could let a malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6309</a> <a href="#">MISC</a>
atmail -- atmail_webmail_server	Cross-site scripting (XSS) vulnerability in the administrative interface in Atmail Webmail Server 6.4 allows remote attackers to inject arbitrary web script or HTML via the Date field of an email.	2020-02-06	not yet calculated	<a href="#">CVE-2012-2593</a> <a href="#">MISC</a> <a href="#">MISC</a>
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	not yet calculated	<a href="#">CVE-2013-3091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8796</a> <a href="#">MISC</a>
bludit --			not	<a href="#">CVE-</a>



bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	yet calculated	<a href="#">2020-8811-MISC</a>
boonex -- dolphin	SQL injection vulnerability in Boonex Dolphin before 7.1.3 allows remote authenticated users to execute arbitrary SQL commands via the 'pathes' parameter in 'categories.php'.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3638</a> <a href="#">BID 58456</a>
bosch -- bvms_mob	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6770</a> <a href="#">CONFIRM</a>
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6768</a> <a href="#">CONFIRM</a>
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6767</a> <a href="#">CONFIRM</a>
bosch -- video_streaming_gateway	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6769</a> <a href="#">CONFIRM</a>
broadcom -- multiple_devices	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic, a different vulnerability than CVE-2019-9500,	2020-02-05	not yet calculated	<a href="#">CVE-2019-15126</a> <a href="#">CONFIRM</a>

	CVE-2019-9501, CVE-2019-9502, and CVE-2019-9503.			
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. By supplying a vendor information element with a data length larger than 32 bytes, a heap buffer overflow is triggered in wlc_wpa_sup_eapol. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9501</a> <a href="#">MISC</a> <a href="#">CERT</a> <a href="#">VN</a>
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. If the vendor information element data length is larger than 164 bytes, a heap buffer overflow is triggered in wlc_wpa_plumb_gtk. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9502</a> <a href="#">MISC</a> <a href="#">CERT</a> <a href="#">VN</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view private IP addresses and other sensitive information.	2020-02-04	not yet calculated	<a href="#">CVE-2013-2676</a> <a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 devices with Firmware L contain a Frameable response (Clickjacking) vulnerability which could allow remote attackers to obtain sensitive information.	2020-02-05	not yet calculated	<a href="#">CVE-2013-2675</a> <a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a>
c-more -- touch_panels EA9 series	It is possible to unmask credentials and other sensitive information on ?unprotected? project files, which may allow attackers to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations.	2020-02-05	not yet calculated	<a href="#">CVE-2020-6969</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11481</a> <a href="#">MISC</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a> <a href="#">MISC</a>

canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11484</a> <a href="#">MISC</a> <a href="#">MISC</a>
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1700</a> <a href="#">BUG</a> <a href="#">CONFIRM</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.2 alpha 1 and 5.2 alpha 2 uses weak session IDs generated based on OS time, which allows remote attackers to hijack arbitrary sessions via a brute force attack. NOTE: CVE-2014-10300 and CVE-2014-10400 were SPLIT from this ID.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2875</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.0.x uses sequential session IDs, which makes it easier for remote attackers to predict the session ID and hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10400</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.1.x uses the same ID for each session, which allows remote attackers to hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10399</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chamilo -- chamilo_image	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_indesignated_applications - servisign	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts.	2020-02-03	not yet calculated	<a href="#">CVE-2020-3925</a> <a href="#">CONFIRM</a>
cisco -- application	Cisco ACE 4.6(3.6) allows log retention DoS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-1202</a> <a href="#">MISC</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an	2020-02-05	not yet calculated	<a href="#">CVE-2020-3120</a> <a href="#">MISC</a> <a href="#">MISC</a>

	affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).			<a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	not yet calculated	<a href="#">CVE-2020-3119</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- linksys_wrt110	Cross-site request forgery (CSRF) vulnerability in Cisco Linksys WRT110 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3568</a> <a href="#">EXPLOIT-DATA</a> <a href="#">BID</a> <a href="#">XE</a>
clamav -- clam_anti_virus	A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.	2020-02-05	not yet calculated	<a href="#">CVE-2020-3123</a> <a href="#">CISCO</a>
corsair -- corsair_icue	The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to read and write to arbitrary physical memory locations, and	2020-02-07	not yet calculated	<a href="#">CVE-2020-8808</a> <a href="#">MISC</a>

	consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.			<a href="#">MISC</a>
d-link -- dir865l_devices	D-Link DIR865L v1.03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3096</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dd-wrt -- dd-wrt	Command Injection vulnerability exists via a CSRF in DD-WRT 24-sp2 from specially crafted configuration values containing shell meta-characters, which could let a remote malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6297</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dedicated -- multiple_dvt_products	Dedicated Micros DV-IP Express, SD Advanced, SD, EcoSense, and DS2 devices rely on a GUI warning to help ensure that the administrator configures login credentials, which makes it easier for remote attackers to obtain access by leveraging situations in which this warning was not needed. NOTE: the vendor states "The user is presented with clear warnings on the GUI that they should set usernames and passwords."	2020-02-06	not yet calculated	<a href="#">CVE-2015-2909</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- dmc_isilon_ones	Dell EMC Isilon OneFS versions 8.1.2, 8.1.0.4, 8.1.0.3, and 8.0.0.7 contain a vulnerability in some configurations. An attacker may exploit this vulnerability to gain access to restricted files. The non-RAN HTTP and WebDAV file-serving components have a vulnerability wherein when either are enabled, and Basic Authentication is enabled for either or both components, files are accessible without authentication.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5318</a> <a href="#">MISC</a>
dell -- emc_ecs	Dell EMC ECS versions prior to 3.4.0.1 contain an XSS vulnerability. A remote authenticated malicious user could exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5317</a> <a href="#">MISC</a>
dell -- multiple_products	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5319</a> <a href="#">MISC</a>
den_norskenturistoring -- im-metadata	im-metadata through 3.0.1 allows remote attackers to execute arbitrary commands via the "exec" argument. It is possible to inject arbitrary commands as part of the metadata options which is given to the "exec" function.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10788</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
den_norskenturistoring -- im-resize	im-resize through 2.3.2 allows remote attackers to execute arbitrary commands via the "exec" argument. The cmd argument used within index.js, can be controlled by user	2020-02-04	not yet calculated	<a href="#">CVE-2019-10787</a> <a href="#">CONFIRM</a>



	without any sanitization.			<a href="#">MISC</a>
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container IDs.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5278</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	not yet calculated	<a href="#">CVE-2012-5570</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The installation uses the same API key (hardcoded as EONAPI_KEY in include/api_functions.php for API version 2.4.2) by default for all installations, hence allowing an attacker to calculate/guess the admin access token.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8657</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8656</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8654</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8655</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tm m crashes under certain circumstances when using the connector profile if a specific sequence of connections are made.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5854</a> <a href="#">CONFIRM</a>
flowplayer -- flowplayer	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	not yet calculated	<a href="#">CVE-2011-3642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Cross-site scripting (XSS) vulnerability in the loadForm			<a href="#">CVE-2014-9470</a>

fork_cms - - fork_cms	function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>	
fortinet -- forticlient_for_linux	A Denial of service (DoS) vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to cause FortiClient processes running under root privilege to crash via sending specially crafted IPC client requests to the fctschd process due the nanomsg not been correctly validated.	2020-02-06	not yet calculated	<a href="#">CVE-2019-16152</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A stack buffer overflow vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted "StartAvCustomScan" type IPC client requests to the fctschd process due the argv data not been well sanitized.	2020-02-06	not yet calculated	<a href="#">CVE-2019-17652</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to run system commands under root privilege via injecting specially crafted "ExportLogs" type IPC client requests to the fctschd process.	2020-02-06	not yet calculated	<a href="#">CVE-2019-15711</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctschd process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	not yet calculated	<a href="#">CVE-2019-16155</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13333</a> <a href="#">MISC</a>	
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17136</a> <a href="#">MISC</a>	
foxit --	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or		not	<a href="#">CVE-</a>	



google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-7224</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Google Chrome before 3.0 does not properly handle XML documents, which allows remote attackers to obtain sensitive information via a crafted web site.	2020-02-06	not yet calculated	<a href="#">CVE-2010-3917</a> <a href="#">MISC</a> <a href="#">MISC</a>
hardcoreview - - hardcoreview	A vulnerability exists in HCView (aka Hardcoreview) 1.4 due to a write access violation with a GIF file.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6306</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- sitescope	An Information Disclosure vulnerability exists in HP SiteScope 11.2 and 11.3 on Windows, Linux and Solaris, HP Asset Manager 9.30 through 9.32, 9.40 through 9.41, 9.50, and Asset Manager Cloudsystem Chargeback 9.40, which could let a remote malicious user obtain sensitive information. This is the TLS vulnerability known as the RC4 cipher Bar Mitzvah vulnerability.	2020-02-04	not yet calculated	<a href="#">CVE-2015-2802</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- cloud_automation_manager	IBM Cloud Automation Manager 3.2.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http://link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 168644.	2020-02-05	not yet calculated	<a href="#">CVE-2019-4616</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 contains hard-coded credentials, such as a password or cryptographic key, which initiates its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 171511.	2020-02-04	not yet calculated	<a href="#">CVE-2019-4675</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7523</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2014-</a>

imagemagick - imagemagick	Stack-based buffer overflow in the WritePSDImage function in coders/psd.c in ImageMagick, possibly 6.8.8-5, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-1947.	2020-02-06	not yet calculated	<a href="#">2030</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Buffer overflow in the DecodePSDPixels function in coders/psd.c in ImageMagick before 6.8.8-5 might allow remote attackers to execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-2030.	2020-02-06	not yet calculated	<a href="#">CVE-2014-1958</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ispconfig - ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jpegsnoop - jpegsnoop	A vulnerability exists in JPEGsnoop 1.5.2 due to an unspecified issue in JPEG file handling, which could let a malicious user execute arbitrary code	2020-02-06	not yet calculated	<a href="#">CVE-2012-6307</a> <a href="#">MISC</a> <a href="#">MISC</a>
kemp --load_master	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5288</a> <a href="#">MISC</a> <a href="#">MISC</a>
konqueror - konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	not yet calculated	<a href="#">CVE-2012-4512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys --wrt310n_wireless_router	Linksys WRT310Nv2 2.0.0.1 is vulnerable to XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3067</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a> <a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
mariadb -- mariadb	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.	2020-02-04	not yet calculated	<a href="#">CVE-2020-7221</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mcabber - - mcabber	MCabber before 1.0.4 is vulnerable to roster push attacks, which allows remote attackers to intercept communications, or add themselves as an entity on a 3rd party's roster as another user, which will also garner associated privileges, via crafted XMPP packets.	2020-02-06	not yet calculated	<a href="#">CVE-2016-9928</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mediawiki - mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4381</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki - mediawiki	The CentralNotice extension for MediaWiki before 1.19.9, 1.20.x before 1.20.8, and 1.21.x before 1.21.3 sets the Cache-Control header to cache session cookies when a user is autocreated, which allows remote attackers to authenticate as the created user.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4572</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mikrotik -- winbox	MikroTik WinBox before 3.21 is vulnerable to a path traversal vulnerability that allows creation of arbitrary files wherever WinBox has write permissions. WinBox is vulnerable to this attack if it connects to a malicious endpoint or if an attacker mounts a man in the middle attack.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5720</a> <a href="#">MISC</a>
	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and			

multiple_vendors - multiple_products	Earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to execute arbitrary code via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5628</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (process outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5627</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (network-communications outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5626</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h_____%2427, (3) h_____%2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-3423</a> <a href="#">MISC</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the system, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8) xname, or (9) mpTransactionId parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>

netgear -- wgr614_wireless_router	An Authentication vulnerability exists in NETGEAR WGR614 v7 and v9 due to a hardcoded credential used for serial programming, a related issue to CVE-2006-1002.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6340</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wireless_router	An Information Disclosure vulnerability exists in the my config file in NETGEAR WGR614 v7 and v9, which could let a malicious user recover all previously used passwords on the device, for both the control panel and WEP/WPA/WPA2, in plaintext. This is a different issue than CVE-2012-6340.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1.2.31805 and V2.2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracer diagnostic tool because of lack of user input sanitizing.	2020-02-07	not yet calculated	<a href="#">CVE-2019-19356</a> <a href="#">MISC</a>
network-manager - network-manager	network-manager through 1.0.2 allows remote attackers to execute arbitrary commands via the "execSync()" argument.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10786</a> <a href="#">MISC</a>
nextcloud -- circles	Improper authorization in the Circles app 0.17.7 causes retaining access when an email address was removed from a circle.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15610</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	A wrong check for the system time in the Android App 3.9.0 causes a bypass of the lock protection when changing the time of the system to the past.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15615</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	Not strictly enough sanitization in the Nextcloud Android app 3.6.0 allowed an attacker to get content information from protected tables when using custom queries.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15622</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_ios	Violation of Secure Design Principles in the iOS App 2.23.0 causes the app to leak its login and token to other Nextcloud services when search e.g. for federated users or registering for push notifications.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15611</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_ios	Missing sanitization in the iOS App 2.24.4 causes an XSS when opening malicious HTML files.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15614</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper permissions preservation in Nextcloud Server 16.0.1 causes sharees to be able to reshare with write permissions when sharing the mount point of a share they received, as a public link.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15621</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud --	Dangling remote share attempts in Nextcloud 16 allow a		not	<a href="#">CVE-2019-</a>

nextcloud_server	Denial of service pollution when running long.	2020-02-04	yet calculated	<a href="#">CVE-2020-15616</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 15.0.2 causes pending 2FA logins to not be correctly expired when the password of the user is reset.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15612</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 17.0.1 causes the workflow rules to depend their behaviour on the file extension when checking file mimetypes.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15613</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A missing check in Nextcloud Server 17.0.0 allowed an attacker to set up a new second factor when trying to login.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15617</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper Input Validation in Nextcloud Server 15.0.7 allows server admins to create users with IDs of system folders.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15624</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server and Nextcloud Desktop	Improper neutralization of file names, conversation names and board names in Nextcloud Server 16.0.3, Nextcloud Talk 6.0.3 and Nextcloud Desktop 0.6.5 causes an XSS when linking them with each others in a project.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A bug in Nextcloud Server 14.0.4 could expose more data in reshared link shares than intended by the sharer.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8121</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	An authenticated server-side request forgery in Nextcloud server 16.0.1 allowed to detect local and remote services when adding a new subscription in the calendar application.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8118</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A missing check in Nextcloud Server 14.0.3 could give recipient the possibility to extend the expiration date of a share they received.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8122</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	nghttp2 before 1.7.1 allows remote attackers to cause a denial of service (memory exhaustion).	2020-02-06	not yet calculated	<a href="#">CVE-2016-1544</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	not yet calculated	<a href="#">CVE-2019-15604</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	Including trailing white space in HTTP header values in Node.js 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	not yet calculated	<a href="#">CVE-2019-15606</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	not yet calculated	<a href="#">CVE-2019-15605</a> <a href="#">MISC</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a>
nuxeo -- nuxeo_platform	RichFaces implementation in Nuxeo Platform 5.6.0 before HF27 and 5.8.0 before HF-01 does not restrict the classes for which deserialization methods can be called, which allows remote attackers to execute arbitrary code via crafted serialized data. NOTE: this vulnerability may overlap CVE-2013-2165.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4521</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	not yet calculated	<a href="#">CVE-2014-9530</a> <a href="#">CONFIRM</a>
omniauth-weibo-oauth2_gem -- omniauth-weibo-oauth2_gem	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	not yet calculated	<a href="#">CVE-2019-17268</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the YII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9126</a> <a href="#">MISC</a>
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9127</a> <a href="#">MISC</a>
openfiler - - openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1086</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openshift-enterprise -	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to make them modifiable by users other than root. An attacker	2020-02-07	not yet	<a href="#">CVE-2020-</a>



openshift-enterprise	with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb.		calculated	<a href="#">1708</a> <a href="#">CONFIRM</a>
openvas -- openvas_manager	OpenVAS Manager v2.0.3 allows plugin remote code execution.	2020-02-06	not yet calculated	<a href="#">CVE-2011-1597</a> <a href="#">MISC</a>
opopensoc - opopensoc -	alplugin - opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple External Entity Injection Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4335</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Starting from the apache user account, it is possible to perform privilege escalation through the lack of correct configuration in the server's sudoers file, which by default allows the execution of programs (e.g. nmap) without the need for a password with sudo.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7954</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Without authentication, it is possible to read server files (e.g., /etc/passwd) due to the use of the nmap -iL (aka input file) option.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7953</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opservices -	An issue was discovered in OpServices OpMon 9.3.2 that allows Remote Code Execution .	2020-02-06	not yet calculated	<a href="#">CVE-2020-8636</a> <a href="#">MISC</a>
opwebapip - opwebapip -	ugin - opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4334</a> <a href="#">MISC</a> <a href="#">MISC</a>
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1768</a> <a href="#">CONFIRM</a>
percona -- percona -	pmm-server in Percona Monitoring and Management (PMM) 2.2.x before 2.2.1 allows unauthenticated denial of service.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7920</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phppgadmin -- phppgadmin	phppgadmin through 7.12.1 allows sensitive actions to be performed without validating that the request originated from the application. One such area, "database.php" does not verify the source of an HTTP request. This can be leveraged by a remote attacker to trick a logged-in administrator to visit a malicious page with a CSRF exploit and execute arbitrary system commands on the server.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10784</a> <a href="#">MISC</a>
projectpier -			not	<a href="#">CVE-2013-</a>

projectpier	ProjectPier 0.8.8 has stored XSS	2020-02-07	yet calculated	<a href="#">CVE-2020-3635</a> <a href="#">MISC</a>
projectpier - projectpier	ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	not yet calculated	<a href="#">CVE-2013-3636</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
projectpier - projectpier	ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	not yet calculated	<a href="#">CVE-2013-3637</a> <a href="#">MISC</a>
qemu -- qemu	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8608</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- multiple_snapdragon_products	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	not yet calculated	<a href="#">CVE-2019-14088</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
railo -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5468</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
revive -- adserver	A reflected XSS vulnerability has been discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.0.3 by Jacopo Tediosi. There are currently no known exploits: the session identifier cannot be accessed as it is stored in an http-only cookie as of v3.2.2. On older versions, however, under specific circumstances, it could be possible to steal the session identifier and gain access to the admin interface. The query string sent to the www/delivery/afr.php script was printed back without proper escaping in a JavaScript context, allowing an attacker to execute arbitrary JS code on the browser of the victim.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8115</a> <a href="#">MISC</a> <a href="#">MISC</a>
samsung - multiple_mobile_devices	On Samsung mobile devices with O(8.0) and P(9.0) software and an Exynos 8895 chipset, RKP (aka the Samsung Hypervisor-L2 implementation) allows arbitrary memory write operations. The Samsung ID is SVE-2019-16265.	2020-02-04	not yet calculated	<a href="#">CVE-2019-19273</a> <a href="#">CONFIRM</a>
schmid -- zi_620_v400_090_routers	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6760</a> <a href="#">MISC</a>
				<a href="#">CVE-</a>

simple_machines - - simple_machines_forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: Forum forum can read files such as the database config.	2020-02-07	not yet calculated	<a href="#">2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscrip - - simplejobscrip	An issue was discovered in Simplejobscrip.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
smoothwall - - smoothwall	- A cross-site scripting (XSS) vulnerability in Smoothwall Express3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall - - smoothwall	- CSRF vulnerability in Smoothwall Express 3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
sphider -- - sphider_search_engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 and before 1.3.6.1. The search function calls in admin/spiderfuncs.php, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5087</a> <a href="#">MISC</a>
status2k -- - status2k	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
statusnet - - statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	not yet calculated	<a href="#">CVE-2010-4658</a> <a href="#">MISC</a>
synaptive - - medical_clearcanvas_image_server	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8788</a> <a href="#">MISC</a>
teamviewer -- - teamviewer	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9.x , this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the	2020-02-07	not yet calculated	<a href="#">CVE-2019-18988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.			
tianocore - - edk2	Buffer overflow in the Reclaim function in Tianocore EDK2 before SVN 16280 allows physically proximate attackers to gain privileges via a long variable name.	2020-02-06	not yet calculated	<a href="#">CVE-2014-8271</a> <a href="#">MISC</a> <a href="#">MISC</a>
troglobit -- minisnmpd	A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server.	2020-02-04	not yet calculated	<a href="#">CVE-2020-6060</a> <a href="#">MISC</a>
ubiquiti_networks - unifi_controller	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4) authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the Unifi Controller name via a request to api/set/setting/identity.	2020-02-08	not yet calculated	<a href="#">CVE-2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>
ui -- edgeswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	not yet calculated	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
unshift -- url-parse	Insufficient validation and sanitization of user input exists in url-parse npm package version 1.4.4 and earlier may allow attacker to bypass security checks.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8124</a> <a href="#">MISC</a>
ushahidi -- ushahidi	Ushahidi before 2.6.1 has insufficient entropy for forgot-password tokens.	2020-02-04	not yet calculated	<a href="#">CVE-2012-5618</a> <a href="#">MISC</a> <a href="#">MISC</a>
videolan -- vlc_media_player	The web interface in VideoLAN VLC media player before 2.0.7 has no access control which allows remote attackers to view directory listings via the 'dir' command or issue other commands without authenticating.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3564</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	Unrestricted file upload vulnerability in the Settings_Vtiger_CompanyDetailsSave_Action class in modules/Settings/Vtiger/actions/CompanyDetailsSave.php in Vtiger CRM 6.3.0 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request	2020-02-06	not yet calculated	<a href="#">CVE-2015-6000</a> <a href="#">MISC</a> <a href="#">MISC</a>

	to the file in test/logo/.			MISC
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3591</a> MISC MISC MISC
watchguard - firewire_xtn	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	not yet calculated	<a href="#">CVE-2014-6413</a> MISC MISC MISC
webcalendar - webcalendar	webcalendar before 1.2.7 shows the reason for a failed login (e.g., "no such user").	2020-02-04	not yet calculated	<a href="#">CVE-2013-1422</a> MISC MISC MISC
wordpress - wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-2008</a> MISC MISC MISC
wordpress - wordpress	The Time Capsule plugin before 1.21.16 for WordPress has an authentication bypass. Any request containing IWP_JSON_PREFIX causes the client to be logged in as the first account on the list of administrator accounts.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8771</a> MISC MISC
wordpress - wordpress	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for WordPress and before 2.0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	2020-02-08	not yet calculated	<a href="#">CVE-2014-8739</a> MISC MISC MISC MISC MISC MISC MISC
wordpress - wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-2009</a> MISC MISC MISC MISC
wordpress - wordpress	The InfiniteWP Client plugin before 1.9.4.5 for WordPress has a missing authorization check in iwpm_mmb_set_request in init.php. Any attacker who knows the username of an	2020-02-06	not yet	<a href="#">CVE-2020-8772</a>



	administrator can log in.		calculator	<a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-1394</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3628</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager	Zoho ManageEngine Applications Manager 14 before 14520 allows a remote unauthenticated attacker to disclose OS file names via FailOverHelperServlet.	2020-02-06	not yet calculated	<a href="#">CVE-2019-19800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	not yet calculated	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of: United States  
Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:** [US-CERT](#)  
**To:** [edigiovanna@sunnyvale.ca.gov](mailto:edigiovanna@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of February 3, 2020  
**Date:** Monday, February 10, 2020 3:12:04 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## **Vulnerability Summary for the Week of February 3, 2020**

02/10/2020 07:28 AM EST

Original release date: February 10, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	2020-01-31	7.5	<a href="#">CVE-2014-8322</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aruba_networks -- instant	Multiple vulnerabilities exists in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.	2020-01-31	7.5	<a href="#">CVE-2016-2031</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	7.8	<a href="#">CVE-2020-3926</a> <a href="#">CONFIRM</a>

changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	8.5	<a href="#">CVE-2020-3927</a> <a href="#">CONFIRM</a>
cisco -- multiple_ip_phones	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	8.3	<a href="#">CVE-2020-3111</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- video_surveillance_8000_series_ip_cameras	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later.	2020-02-05	8.3	<a href="#">CVE-2020-3110</a> <a href="#">MISC</a> <a href="#">CISCO</a>
coppermine_development -- coppermine_gallery	Coppermine gallery before 1.4.26 has an input validation vulnerability that allows for code execution.	2020-02-05	7.5	<a href="#">CVE-2010-4815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

curling -- curling	All versions of curling.js are vulnerable to Command Injection via the run function. The command argument can be controlled by users without any sanitization.	2020-02-06	<a href="#">10</a>	<a href="#">CVE-2019-10789</a> <a href="#">MISC</a> <a href="#">MISC</a>
django -- django	Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-7471</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
dot-prop -- dot-prop	Prototype pollution vulnerability in dot-prop npm package version 5.1.0 and earlier allows an attacker to add arbitrary properties to JavaScript language constructs such as objects.	2020-02-04	<a href="#">7.5</a>	<a href="#">CVE-2020-8116</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.2.4 is vulnerable to directory traversal, leading to incorrect access control. It allows an attacker to read or execute files under \$TOMCAT_HOME/webapps/ROOT/assets (which should be a protected directory). Additionally, attackers can upload temporary files (e.g., .jsp files) into /webapps/ROOT/assets/tmp_upload, which can lead to remote command execution (with the permissions of the user running the dotCMS application).	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-6754</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
edk2 -- unified_extensible_firmware_interface	Multiple integer overflows in the Pre-EFI Initialization (PEI) boot phase in the Capsule Update feature in the UEFI implementation in EDK2 allow physically proximate attackers to bypass intended access restrictions by providing crafted data that is not properly handled during the coalescing phase.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4860</a> <a href="#">MISC</a>
edk2 -- unified_extensible_firmware_interface	Integer overflow in the Drive Execution Environment (DXE) phase in the Capsule Update feature in the UEFI implementation in EDK2 allows physically proximate attackers to bypass intended access restrictions via crafted data.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4859</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows SQL Injection via the user parameter to com.eg.LoginHelperServlet (aka the Forgot Password feature).	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8592</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows authentication bypass via a com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8591</a> <a href="#">MISC</a>



	request.			
fortinet -- fortimanager	A Command Injection vulnerability exists in FortiManager 5.2.1 and earlier and FortiManager 5.0.10 and earlier via unspecified vectors, which could let a malicious user run systems commands when executing a report.	2020-02-04	9	<a href="#">CVE-2015-3611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- mortimanager	A vulnerability exists in in FortiManager 5.2.1 and earlier and 5.0.10 and earlier in the WebUI FTP backup page	2020-02-04	7.5	<a href="#">CVE-2015-3613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	7.5	<a href="#">CVE-2020-8114</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.2 incorrectly validated role/region associated with TLS certificates used for mTLS RPC, and were susceptible to privilege escalation. Fixed in 0.10.3.	2020-01-31	7.5	<a href="#">CVE-2020-7956</a> <a href="#">MISC</a> <a href="#">MISC</a>
jobberbase -- jobberbase	Jobberbase 2.0 has SQL injection via the PATH_INFO to the jobs-in endpoint.	2020-02-05	7.5	<a href="#">CVE-2019-20447</a> <a href="#">MISC</a> <a href="#">MISC</a>
klona -- klona	Flaw in input validation in npm package klona version 1.1.0 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using klona.	2020-02-04	7.5	<a href="#">CVE-2020-8125</a> <a href="#">MISC</a>
nanopb -- nanopb	There is a potentially exploitable out of memory condition In Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is compiled with PB_ENABLE_MALLOC, the message to be decoded contains a repeated string, bytes or message field and realloc() runs out of memory when expanding the array nanopb can end up calling `free()` on a pointer value that comes from uninitialized memory. Depending on platform this can result in a crash or further memory corruption, which may be exploitable in some cases. This problem is fixed in nanopb-0.4.1, nanopb-0.3.9.5, nanopb-0.2.9.4.	2020-02-04	7.5	<a href="#">CVE-2020-5235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netapp -- oncommand_system_manager	NetApp OnCommand System Manager 2.1 and earlier allows remote attackers to execute arbitrary commands in the Halt/Reboot interface.	2020-01-31	9	<a href="#">CVE-2013-3322</a> <a href="#">XF</a> <a href="#">MISC</a>
norman -- malware_cleaner	nsak64.sys in Norman Malware Cleaner 2.08.08 allows users to call arbitrary kernel functions because the passing of function pointers between user and kernel	2020-02-03	7.5	<a href="#">CVE-2020-8508</a> <a href="#">MISC</a>

	mode is mishandled.			
phpabook -- phpabook	An issue was discovered in phpABook 0.9 Intermediate. On the login page, if one sets a userInfo cookie with the value of admin+1+en (user+perms+lang), one can login as any user without a password.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8510</a> <a href="#">MISC</a> <a href="#">MISC</a>
phplist -- phplist	phplist 3.5.0 allows type juggling for admin login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8547</a> <a href="#">MISC</a>
playsms -- playsms	PlaySMS before 1.4.3 does not sanitize inputs from a malicious string.	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-8644</a> <a href="#">MISC</a> <a href="#">MISC</a>
ppp -- ppp	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8597</a> <a href="#">MISC</a> <a href="#">MLIST</a>
python -- python	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.	2020-02-04	<a href="#">7.1</a>	<a href="#">CVE-2019-9674</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- mdm9206_and_mdm9607_devices	Subsequent additions performed during Module loading while allocating the 9607_devices would lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14051</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14046</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open close in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14044</a> <a href="#">CONFIRM</a>
	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon			

qualcomm -- multiple_snapdragon_products	Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14055</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14002</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> <a href="#">CONFIRM</a>
	Out of bound access due to Invalid inputs to dapm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial			

qualcomm -- multiple_snapdragon_products	IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14063</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Uninitialized stack data gets used if memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14060</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14057</a> <a href="#">CONFIRM</a>

qualcomm -- multiple_snapdragon_products	Stage-2 fault will occur while writing to an ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14049</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> <a href="#">CONFIRM</a>
sap -- netweaver	SAP NetWeaver 7.0 allows Remote Code Execution and Denial of Service caused by an error in the DiagTraceHex() function. By sending a specially-crafted packet, an attacker could exploit this vulnerability to cause the application to crash.	2020-02-05	7.5	<a href="#">CVE-2011-1517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript.com -- simplejobscript.com	controllers/page_apply.php in Simplejobscript.com SJS through 1.66 is prone to unauthenticated Remote Code Execution by uploading a PHP script as a resume.	2020-01-31	7.5	<a href="#">CVE-2020-8440</a> <a href="#">CONFIRM</a>
smartbear -- readyapi_and_soapui	An issue was discovered in SmartBear ReadyAPI through 2.8.2 and 3.0.0 and SoapUI through 5.5. When opening a project, the Groovy "Load Script" is automatically executed. This allows an attacker to execute arbitrary Groovy Language code (Java scripting language)	2020-02-05	9.3	<a href="#">CVE-2019-12180</a> <a href="#">MISC</a>



	on the victim machine by inducing it to open a malicious Project. The same issue is present in the "Save Script" function, which is executed automatically when saving a project.			
squid -- squid	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	2020-02-04	7.5	<a href="#">CVE-2020-8450</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_update_framework -- tuf	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature.	2020-02-05	7.5	<a href="#">CVE-2020-6174</a> <a href="#">CONFIRM</a>
tp-link -- tg-sg105e_devices	The Web Management of TP-Link TP-SG105E V4 1.0.0 Build 20181120 devices allows an unauthenticated attacker to reboot the device via a reboot.cgi request.	2020-02-03	7.8	<a href="#">CVE-2019-16893</a> <a href="#">EXPLOIT-DB</a>
zpanel_project -- zpanel	ZPanel 10.0.1 has insufficient entropy for its password reset process.	2020-02-04	7.5	<a href="#">CVE-2012-5686</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	6.5	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	5	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	4.6	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent --	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch			<a href="#">CVE-2014-</a>

1830_photonic_service	OS 16.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	2020-01-31	<a href="#">4.3</a>	<a href="#">3809 MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-12426 MLIST CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	<a href="#">4.9</a>	<a href="#">CVE-2011-0220 MISC</a>
apple -- safari	A Cross-origin vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2016-4676 MISC MISC MISC CONFIRM MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8505 MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8504 MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2016-2032 MISC MISC MISC MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20104 N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404 N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20400 N/A</a>
	The JMX monitoring flag in Atlassian Jira Server and Data Center before version			<a href="#">CVE-2019-</a>

atlassian -- jira	8.6.0 allows remote attackers to turn the JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	2020-02-06	<a href="#">4.3</a>	<a href="#">20405</a> <a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20403</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20402</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2674</a> <a href="#">MISC</a> <a href="#">XE</a> <a href="#">BID</a>

brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	5	<a href="#">CVE-2013-2672</a> <a href="#">MISC</a> <a href="#">XF</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	4.6	<a href="#">CVE-2013-2673</a> <a href="#">MISC</a> <a href="#">BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	5	<a href="#">CVE-2019-12998</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	5	<a href="#">CVE-2013-2683</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	5	<a href="#">CVE-2013-2680</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	6.8	<a href="#">CVE-2013-2678</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	4.3	<a href="#">CVE-2013-2681</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	4.3	<a href="#">CVE-2013-2682</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	4.3	<a href="#">CVE-2013-2684</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
computer_incident_response -- ail-framework	Global Cyber All framework 2.8 allows path traversal.	2020-02-03	5	<a href="#">CVE-2020-8545</a> <a href="#">MISC</a>
cysharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions	2020-01-31	6.8	<a href="#">CVE-2020-5234</a> <a href="#">MISC</a>

	and stack overflow. Review the linked GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus -- eucalyptus_management_console	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>



evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	6.6	<a href="#">CVE-2013-5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	5	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	4.6	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	5	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	5	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	4.3	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	4	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 0.10.3 allow unbounded resource usage.	2020-01-31	5	<a href="#">7218</a> <a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	6.5	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information_server	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	5.8	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	6.8	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	6.9	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	6.5	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	6	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	5.8	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or	2020-02-04	5	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

	browser history. IBM X-Force ID: 166623.			
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> XF <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> XF <a href="#">CONFIRM</a>
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> MISC MISC MISC
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> MISC MISC MISC MISC

info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8139</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	4.3	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	6.5	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	5	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	5	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	5	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	6.4	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	5	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be			



joomla! -- joomla!	entered by any user. If it doesn't contain rel="noopener" (or similar attributes such as noreferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	2020-02-03	4.3	<a href="#">CVE-2020-5182</a> <a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	4.3	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	5	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	5	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	6.6	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	6.5	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	4.3	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- rumpus	An issue was discovered in Rumpus 0.2.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	4.3	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to	2020-02-06	4.4	<a href="#">CVE-2019-20406</a>

	write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.			<a href="#">N/A</a>
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	5	<a href="#">4116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	5	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	6.4	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	4.3	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	4.3	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	4	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	6.8	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon			

qualcomm -- multiple_snapdragon_products	Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>

squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- openSUSE_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a>



	to arbitrary websites via a crafted URL.			<a href="#">MISC</a>
telaen -- telaen	Telaen before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted URL request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2624</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browser_y" in the page image.php.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	<a href="#">5</a>	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>

	vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

wordpress -- wordpress	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can result in an attacker performing malicious actions such as stealing session tokens.	2020-02-03	<a href="#">4.3</a>	<a href="#">8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	<a href="#">4</a>	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	<a href="#">4.6</a>	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent --	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch	2020-01-		<a href="#">CVE-2014-</a>

1830_photonic_service	Before 16.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	31	4.3	<a href="#">3809 MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	5	<a href="#">CVE-2019-12426 MLIST CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	4.9	<a href="#">CVE-2011-0220 MISC</a>
apple -- safari	A Cross-origins vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	5	<a href="#">CVE-2016-4676 MISC MISC MISC CONFIRM MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	4.3	<a href="#">CVE-2020-8505 MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	4.3	<a href="#">CVE-2020-8504 MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	5	<a href="#">CVE-2016-2032 MISC MISC MISC MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	5	<a href="#">CVE-2019-20104 N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	4.4	<a href="#">CVE-2019-20400 N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	5	<a href="#">CVE-2019-20403 N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System	2020-02-	4	<a href="#">CVE-2019-20402</a>

	Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	06		<a href="#">N/A</a>
atlassian -- jira	The JMX monitoring flag in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to turn the JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20405</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2672</a> <a href="#">MISC</a> <a href="#">XF</a>
brother -- mfc-	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure			<a href="#">CVE-2013-2674</a>



9970cdw_devices	vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	5	<a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a>
brother -- mfc-9970cdw	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	4.6	<a href="#">CVE-2013-2673</a> <a href="#">MISC</a> <a href="#">BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	5	<a href="#">CVE-2019-12998</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	5	<a href="#">CVE-2013-2680</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	5	<a href="#">CVE-2013-2683</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	6.8	<a href="#">CVE-2013-2678</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200_devices	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	4.3	<a href="#">CVE-2013-2681</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200_devices	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	4.3	<a href="#">CVE-2013-2684</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200_devices	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	4.3	<a href="#">CVE-2013-2682</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
computer_incident_response -- ail-framework	Global Cyber Alliance framework 2.8 allows path traversal.	2020-02-03	5	<a href="#">CVE-2020-8545</a> <a href="#">MISC</a>
cysharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions	2020-01-31	6.8	<a href="#">CVE-2020-5234</a> <a href="#">MISC</a>

	and stack overflow. Review the linked GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus_eucalyptus	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) 4.0.x before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>

evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	6.6	<a href="#">CVE-2013-5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	5	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	4.6	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	5	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	5	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	5	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	4	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).	2020-02-05	5	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 0.10.3 allow unbounded resource usage.	2020-01-31	5	<a href="#">7218</a> <a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	6.5	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information_server	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	5.8	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	6.8	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	6.9	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	6.5	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	6	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	5.8	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or	2020-02-04	5	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>



	browser history. IBM X-Force ID: 166623.			
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> XF CONFIRM
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> XF CONFIRM
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> XF CONFIRM
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> XF CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> XF CONFIRM
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> XF CONFIRM
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> XF CONFIRM
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> MISC MISC MISC
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> MISC MISC MISC MISC

info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8139</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	4.3	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	6.5	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	5	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	5	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	5	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	6.4	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	5	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be			

joomla! -- joomla!	entered by any user. If it doesn't contain rel="noopener" (or similar attributes such as noreferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	2020-02-03	4.3	<a href="#">CVE-2020-5182</a> <a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	4.3	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	5	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	5	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	6.6	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	6.5	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	4.3	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- rumpus	An issue was discovered in Rumpus 2.0.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	4.3	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to	2020-02-06	4.4	<a href="#">CVE-2019-20406</a>

	write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.			<a href="#">N/A</a>
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	5	<a href="#">4116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	5	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	6.4	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	4.3	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	4.3	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	4	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	6.8	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon			



qualcomm -- multiple_snapdragon_products	Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>

squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- opensuse_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Telean before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted	2020-02-03	5	<a href="#">CVE-2013-2624</a> <a href="#">XF</a>

	URL request.			MISC
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims to arbitrary websites via a crafted URL.	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	4.3	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	5	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	4	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browsery" in the page image.php.	2020-02-03	5	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	5	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	5	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	6.4	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this	2020-02-04	6.4	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>

	vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

wordpress -- wordpress	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can result in an attacker performing malicious actions such as stealing session tokens.	2020-02-03	4.3	<a href="#">8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	4.3	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	6.5	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	4	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS& Score	Source Patch Info
arctic_torrent -- arctic_torrent	A vulnerability exists in Arctic Torrent 1.4 via unspecified vectors in .torrent file handling, which could let a malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6309</a> <a href="#">MISC</a>
atmail -- atmail_webmail_server	Cross-site scripting (XSS) vulnerability in the administrative interface in Atmail Webmail Server 6.4 allows remote attackers to inject arbitrary web script or HTML via the Date field of an email.	2020-02-06	not yet calculated	<a href="#">CVE-2012-2593</a> <a href="#">MISC</a> <a href="#">MISC</a>
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	not yet calculated	<a href="#">CVE-2013-3091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8796</a> <a href="#">MISC</a>



bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>
boonex -- dolphin	SQL injection vulnerability in Boonex Dolphin before 7.1.3 allows remote authenticated users to execute arbitrary SQL commands via the 'pathes' parameter in 'categories.php'.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3638</a> <a href="#">BID</a> <a href="#">XE</a>
bosch -- bvms_mob	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6770</a> <a href="#">CONFIRM</a>
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6768</a> <a href="#">CONFIRM</a>
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6767</a> <a href="#">CONFIRM</a>
bosch -- video_streaming_gateway	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6769</a> <a href="#">CONFIRM</a>
broadcom -- multiple_devices	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete	2020-02-05	not yet calculated	<a href="#">CVE-2019-15126</a>

	set of traffic, a different vulnerability than CVE-2019-9500, CVE-2019-9501, CVE-2019-9502, and CVE-2019-9503.			<a href="#">CONFIRM</a>
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. By supplying a vendor information element with a data length larger than 32 bytes, a heap buffer overflow is triggered in wlc_wpa_sup_eapol. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9501</a> <a href="#">MISC CERT. VN</a>
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. If the vendor information element data length is larger than 164 bytes, a heap buffer overflow is triggered in wlc_wpa_plumb_gtk. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9502</a> <a href="#">MISC CERT. VN</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view private IP addresses and other sensitive information.	2020-02-04	not yet calculated	<a href="#">CVE-2013-2676</a> <a href="#">MISC XF BID</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 devices with Firmware L contain a Frameable response (Clickjacking) vulnerability which could allow remote attackers to obtain sensitive information.	2020-02-05	not yet calculated	<a href="#">CVE-2013-2675</a> <a href="#">MISC XF BID</a>
c-more -- touch_panel_driver	It is possible to unmask credentials and other sensitive information on ?unprotected? project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations.	2020-02-05	not yet calculated	<a href="#">CVE-2020-6969</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11481</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a>

				<a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11484</a> <a href="#">MISC</a> <a href="#">MISC</a>
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1700</a> <a href="#">CLASSIFIED</a> <a href="#">CONFIRM</a>
cgilua -- cgilua	The session.lua library in CGILua 5.2 alpha 1 and 5.2 alpha 2 uses weak session IDs generated based on OS time, which allows remote attackers to hijack arbitrary sessions via a brute force attack. NOTE: CVE-2014-10300 and CVE-2014-10400 were SPLIT from this ID.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2875</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGILua 5.0.x uses sequential session IDs, which makes it easier for remote attackers to predict the session ID and hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10400</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGILua 5.1.x uses the same ID for each session, which allows remote attackers to hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10399</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chamilo -- chamilo_Im	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_infrastructure -- servisign	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts.	2020-02-03	not yet calculated	<a href="#">CVE-2020-3925</a> <a href="#">CONFIRM</a>
cisco -- application	Cisco ACE (3.6) allows log retention DoS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-1202</a> <a href="#">MISC</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by	2020-02-05	not yet	<a href="#">CVE-2020-3120</a>

	<p>sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).</p>		calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	<p>A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).</p>	2020-02-05	not yet calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	<p>A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).</p>	2020-02-05	not yet calculated	<a href="#">CVE-2020-3119</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- linksys_wrt110	<p>Cross-site request forgery (CSRF) vulnerability in Cisco Linksys WRT110 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors.</p>	2020-02-06	not yet calculated	<a href="#">CVE-2013-3568</a> <a href="#">EXPLOIT-DATA</a> <a href="#">BID</a> <a href="#">XF</a>
clamav -- clam_anti_virus	<p>A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.</p>	2020-02-05	not yet calculated	<a href="#">CVE-2020-3123</a> <a href="#">CISCO</a>
corsair -- corsair_icue	<p>The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to</p>	2020-02-07	not yet	<a href="#">CVE-2020-8808</a>

	read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.		calculated	<a href="#">CVE-2019-10787</a> <a href="#">MISC</a>
d-link --dir865l_devices	D-Link DIR865L v1.03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3096</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dd-wrt --dd-wrt	Command Injection vulnerability exists via a CSRF in DD-WRT 24-sp2 from specially crafted configuration values containing shell meta-characters, which could let a remote malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6297</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dedicated --multiple_dvr_products	Dedicated Micros DV-IP Express, SD Advanced, SD, EcoSense, and DS2 devices rely on a GUI warning to help ensure that the administrator configures login credentials, which makes it easier for remote attackers to obtain access by leveraging situations in which this warning was not needed. NOTE: the vendor states "The user is presented with clear warnings on the GUI that they should set usernames and passwords."	2020-02-06	not yet calculated	<a href="#">CVE-2015-2909</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell --dmc_isilon_ones	Dell EMC Isilon OneFS versions 8.1.2, 8.1.0.4, 8.1.0.3, and 8.0.0.7 contain a vulnerability in some configurations. An attacker may exploit this vulnerability to gain access to restricted files. The non-RAN HTTP and WebDAV file-serving components have a vulnerability wherein when either are enabled, and Basic Authentication is enabled for either or both components, files are accessible without authentication.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5318</a> <a href="#">MISC</a>
dell --emc_ecs	Dell EMC ECS versions prior to 3.4.0.1 contain an XSS vulnerability. A remote authenticated malicious user could exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5317</a> <a href="#">MISC</a>
dell --multiple_products	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5319</a> <a href="#">MISC</a>
den_norskenturistoring --im-metadata	im-metadata through 3.0.1 allows remote attackers to execute arbitrary commands via the "exec" argument. It is possible to inject arbitrary commands as part of the metadata options which is given to the "exec" function.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10788</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
den_norskenturistoring --im-metadata	im-metadata through 2.3.2 allows remote attackers to execute arbitrary commands via the "exec" argument. The cmd	2020-02-04	not yet	<a href="#">CVE-2019-10787</a>



resize	argument used within index.js, can be controlled by user without any sanitization.		calculated	<a href="#">CONFIRM</a> <a href="#">CVE-2014-5278</a> <a href="#">MISC</a>
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container IDs.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5278</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	not yet calculated	<a href="#">CVE-2012-5570</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The installation uses the same API key (hardcoded as EONAPI_KEY in include/api_functions.php for API version 2.4.2) by default for all installations, hence allowing an attacker to calculate/guess the admin access token.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8657</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8656</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8654</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8655</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5854</a> <a href="#">CONFIRM</a>
flowplayer -- flowplayer	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	not yet calculated	<a href="#">CVE-2011-3642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2014-</a>

fork_cms - - fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	not yet calculated	<a href="#">9470</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>	
fortinet -- forticlient_for_linux	A Denial of service (DoS) vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted IPC client requests to the fctschd process due the nanomsg not been correctly validated.	2020-02-06	not yet calculated	<a href="#">CVE-2019-16152</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A stack buffer overflow vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted "StartAvCustomScan" type IPC client requests to the fctschd process due the argv data not been well sanitized.	2020-02-06	not yet calculated	<a href="#">CVE-2019-17652</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to run system commands under root privilege via injecting specially crafted "ExportLogs" type IPC client requests to the fctschd process.	2020-02-06	not yet calculated	<a href="#">CVE-2019-15711</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctschd process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	not yet calculated	<a href="#">CVE-2019-16155</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13333</a> <a href="#">MISC</a>	
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17136</a> <a href="#">MISC</a>	
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this				

foxit --phantompdf	vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13334</a> MISC
foxit --phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17135</a> MISC
fujitsu --multiple_products	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions, Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3, Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.	2020-02-07	not yet calculated	<a href="#">CVE-2019-13163</a> CONFIRM
gnome --libsvg	In xml.rs in GNOME libsvg before 2.46.2, a crafted SVG file with nested patterns can cause denial of service when passed to the library for processing. The attacker constructs pattern elements so that the number of final rendered objects grows exponentially.	2020-02-02	not yet calculated	<a href="#">CVE-2019-20446</a> MISC
gnome --evolution_and_evolution_data_server	The <code>gpg_ctx_add_recipient</code> function in <code>camel/camel-gpg-context.c</code> in GNOME Evolution 3.8.4 and earlier and Evolution Data Server 3.9.5 and earlier does not properly select the GPG key to use for email encryption, which might cause the email to be encrypted with the wrong key and allow remote attackers to obtain sensitive information.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4166</a> CONFIRM MISC CONFIRM CONFIRM
golang --go	The <code>net/http</code> library in <code>net/http/transfer.go</code> in Go before 1.4.3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains Content-Length and Transfer-Encoding header fields.	2020-02-08	not yet calculated	<a href="#">CVE-2015-5741</a> MISC MISC MISC MISC MISC

				<a href="#">MISC</a>
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-7224</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Google Chrome before 3.0 does not properly handle XML documents, which allows remote attackers to obtain sensitive information via a crafted web site.	2020-02-06	not yet calculated	<a href="#">CVE-2010-3917</a> <a href="#">MISC</a> <a href="#">MISC</a>
hardcoreview - - hardcoreview	A vulnerability exists in HCView (aka Hardcoreview) 1.4 due to a write access violation with a GIF file.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6306</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- sitescope	An Information Disclosure vulnerability exists in HP SiteScope 11.2 and 11.3 on Windows, Linux and Solaris, HP Asset Manager 9.30 through 9.32, 9.40 through 9.41, 9.50, and Asset Manager Cloudsystem Chargeback 9.40, which could let a remote malicious user obtain sensitive information. This is the TLS vulnerability known as the RC4 cipher Bar Mitzvah vulnerability.	2020-02-04	not yet calculated	<a href="#">CVE-2015-2802</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- cloud_automation_manager	IBM Cloud Automation Manager 3.2.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http://link to the user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 168644.	2020-02-05	not yet calculated	<a href="#">CVE-2019-4616</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 contains hard-coded credentials, such as a password or cryptographic key, which can be used to bypass authentication, inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 171511.	2020-02-04	not yet calculated	<a href="#">CVE-2019-4675</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7523</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-</a>

imagemagick - imagemagick	Stack-based buffer overflow in the WritePSDImage function in coders/psd.c in ImageMagick, possibly 6.8.8-5, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-1947.	2020-02-06	not yet calculated	<a href="#">2014-2030</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Buffer overflow in the DecodePSDPixels function in coders/psd.c in ImageMagick before 6.8.8-5 might allow remote attackers to execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-2030.	2020-02-06	not yet calculated	<a href="#">CVE-2014-1958</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ispconfig - ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jpegsnoop - jpegsnoop	A vulnerability exists in JPEGsnoop 1.5.2 due to an unspecified issue in JPEG file handling, which could let a malicious user execute arbitrary code	2020-02-06	not yet calculated	<a href="#">CVE-2012-6307</a> <a href="#">MISC</a> <a href="#">MISC</a>
kemp -- load_master	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5288</a> <a href="#">MISC</a> <a href="#">MISC</a>
konqueror - konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	not yet calculated	<a href="#">CVE-2012-4512</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys -- wrt310n_wireless_router	Linksys WRT310Nv2 2.0.0.1 is vulnerable to XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3067</a> <a href="#">MISC</a> <a href="#">MISC</a>



				<a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
mariadb -- mariadb	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.	2020-02-04	not yet calculated	<a href="#">CVE-2020-7221</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mcabber - - mcabber	MCabber before 1.0.4 is vulnerable to roster push attacks, which allows remote attackers to intercept communications, or add themselves as an entity on a 3rd party's roster as another user, which will also garner associated privileges, via crafted XMPP packets.	2020-02-06	not yet calculated	<a href="#">CVE-2016-9928</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mediawiki - mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4381</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki - mediawiki	The CentralNotice extension for MediaWiki before 1.19.9, 1.20.x before 1.20.8, and 1.21.x before 1.21.3 sets the Cache-Control header to cache session cookies when a user is autocreated, which allows remote attackers to authenticate as the created user.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4572</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mikrotik -- winbox	MikroTik WinBox before 3.21 is vulnerable to a path traversal vulnerability that allows creation of arbitrary files wherever WinBox has write permissions. WinBox is vulnerable to this attack if it connects to a malicious endpoint or if an attacker mounts a man in the middle attack.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5720</a> <a href="#">MISC</a>
	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier,			

multiple_vendors - multiple_products	Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to execute arbitrary code via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5628</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (process outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5627</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (network-communications outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5626</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h_____%2427, (3) h_____%2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-3423</a> <a href="#">MISC</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the (1) ctrl, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8)	2020-02-08	not yet calculated	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>

	xname, or (9) mpTransactionId parameter.			
netgear -- wgr614_wireless_router	An Authentication vulnerability exists in NETGEAR WGR614 v7 and v9 due to a hardcoded credential used for serial programming, a related issue to CVE-2006-1002.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6340</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wireless_router	An Information Disclosure vulnerability exists in the my config file in NETGEAR WGR614 v7 and v9, which could let a malicious user recover all previously used passwords on the device, for both the control panel and WEP/WPA/WPA2, in plaintext. This is a different issue than CVE-2012-6340.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1.2.31805 and V2.2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracert diagnostic tool because of lack of user input sanitizing.	2020-02-07	not yet calculated	<a href="#">CVE-2019-19356</a> <a href="#">MISC</a>
network-manager - network-manager	network-manager through 1.0.2 allows remote attackers to execute arbitrary commands via the "execSync()" argument.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10786</a> <a href="#">MISC</a>
nextcloud -- circles	Improper authorization in the Circles app 0.17.7 causes retaining access when an email address was removed from a circle.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15610</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	A wrong check for the system time in the Android App 3.9.0 causes a bypass of the lock protection when changing the time of the system to the past.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15615</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	Not strictly enough sanitization in the Nextcloud Android app 3.6.0 allowed an attacker to get content information from protected tables when using custom queries.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15622</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_ios	Violation of Secure Design Principles in the iOS App 2.23.0 causes the app to leak its login and token to other Nextcloud services when search e.g. for federated users or registering for push notifications.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15611</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_ios	Missing sanitization in the iOS App 2.24.4 causes an XSS when opening malicious HTML files.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15614</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper permissions preservation in Nextcloud Server 16.0.1 causes sharees to be able to reshare with write permissions when sharing the mount point of a share they received, as a public link.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15621</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud				<a href="#">CVE-</a>

-- nextcloud_server	Dangling remote share attempts in Nextcloud 16 allow a DNS pollution when running long.	2020-02-04	not yet calculated	<a href="#">2019-15616</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 15.0.2 causes pending 2FA logins to not be correctly expired when the password of the user is reset.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15612</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 17.0.1 causes the workflow rules to depend their behaviour on the file extension when checking file mimetypes.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15613</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A missing check in Nextcloud Server 17.0.0 allowed an attacker to set up a new second factor when trying to login.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15617</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper Input Validation in Nextcloud Server 15.0.7 allows server admins to create users with IDs of system folders.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15624</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server and Nextcloud Desktop	Improper neutralization of file names, conversation names and board names in Nextcloud Server 16.0.3, Nextcloud Talk 6.0.3 and Nextcloud Deck 0.6.5 causes an XSS when linking them with each others in a project.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A bug in Nextcloud Server 14.0.4 could expose more data in reshared link shares than intended by the sharer.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8121</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	An authenticated server-side request forgery in Nextcloud server 16.0.1 allowed to detect local and remote services when adding a new subscription in the calendar application.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8118</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A missing check in Nextcloud Server 14.0.3 could give recipient the possibility to extend the expiration date of a share they received.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8122</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	nghttp2 before 1.7.1 allows remote attackers to cause a denial of service (memory exhaustion).	2020-02-06	not yet calculated	<a href="#">CVE-2016-1544</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	not yet calculated	<a href="#">CVE-2019-15604</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	Including trailing white space in HTTP header values in Node.js 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	not yet calculated	<a href="#">CVE-2019-15606</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	not yet calculated	<a href="#">CVE-2019-15605</a> <a href="#">MISC</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a>
nuxeo -- nuxeo_platform	RichFaces implementation in Nuxeo Platform 5.6.0 before HF27 and 5.8.0 before HF-01 does not restrict the classes for which deserialization methods can be called, which allows remote attackers to execute arbitrary code via crafted serialized data. NOTE: this vulnerability may overlap CVE-2013-2165.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4521</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	not yet calculated	<a href="#">CVE-2014-9530</a> <a href="#">CONFIRM</a>
omniauth- weibo- oauth2_gem -- omniauth- weibo- oauth2_gem	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	not yet calculated	<a href="#">CVE-2019-17268</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open- school -- open- school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the YII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9126</a> <a href="#">MISC</a>
open- school -- open- school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9127</a> <a href="#">MISC</a>
openfiler - - openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1086</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openshift- enterprise -	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to		not	<a href="#">CVE-2020-</a>



openshift-enterprise	make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb.	2020-02-07	yet calculated	<a href="#">1708 CONFIRM</a>
openvas -- openvas_manager	OpenVAS Manager v2.0.3 allows plugin remote code execution.	2020-02-06	not yet calculated	<a href="#">CVE-2011-1597 MISC</a>
opopensoc - opopensoc	alplugin - opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple External Entity Injection Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4335 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Starting from the apache user account, it is possible to perform privilege escalation through the lack of correct configuration in the server's sudoers file, which by default allows the execution of programs (e.g. nmap) without the need for a password with sudo.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7954 MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Without authentication, it is possible to read server files (e.g., /etc/passwd) due to the use of the nmap -iL (aka input file) option.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7953 MISC</a> <a href="#">MISC</a>
opservices - opservices	An issue was discovered in OpServices OpMon 9.3.2 that allows Remote Code Execution .	2020-02-06	not yet calculated	<a href="#">CVE-2020-8636 MISC</a> <a href="#">MISC</a>
opwebapi - opwebapi	ugin - opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4334 MISC</a> <a href="#">MISC</a>
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1768 CONFIRM</a>
percona -- percona_monitoring	pmm-server in Percona Monitoring and Management (PMM) 2.2.x before 2.2.1 allows unauthenticated denial of service.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7920 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phppgadmin -- phppgadmin	phppgadmin through 7.12.1 allows sensitive actions to be performed without validating that the request originated from the application. One such area, "database.php" does not verify the source of an HTTP request. This can be leveraged by a remote attacker to trick a logged-in administrator to visit a malicious page with a CSRF exploit and execute arbitrary system commands on the server.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10784 MISC</a>
projectpier -			not	<a href="#">CVE-</a>

- projectpier	ProjectPier 0.8.8 has stored XSS	2020-02-07	yet calculated	<a href="#">2013-3635 MISC</a>	
projectpier - projectpier	ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	not yet calculated	<a href="#">CVE-2013-3636 MISC</a>	
projectpier - projectpier	ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	not yet calculated	<a href="#">CVE-2013-3637 MISC</a>	
qemu -- qemu	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8608 MISC</a>	
qualcomm -- multiple_snapdragon_products	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	not yet calculated	<a href="#">CVE-2019-14088 MISC</a>	CONFIRM
railo -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5468 MISC</a>	
revive -- adserver	A reflected XSS vulnerability has been discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.0.3 by Jacopo Tediosi. There are currently no known exploits: the session identifier cannot be accessed as it is stored in an http-only cookie as of v3.2.2. On older versions, however, under specific circumstances, it could be possible to steal the session identifier and gain access to the admin interface. The query string sent to the www/delivery/afr.php script was printed back without proper escaping in a JavaScript context, allowing an attacker to execute arbitrary JS code on the browser of the victim.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8115 MISC</a>	
samsung - multiple_mobile_devices	On Samsung mobile devices with O(8.0) and P(9.0) software and an Exynos 8895 chipset, RKP (aka the Samsung Hypervisor-L2 implementation) allows arbitrary memory write operations. The Samsung ID is SVE-2019-16265.	2020-02-04	not yet calculated	<a href="#">CVE-2019-19273 MISC</a>	CONFIRM
schmid -- zi_620_v400_090_routers	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6760 MISC</a>	
				<a href="#">CVE-</a>	

simple_machines - - simple_machines Forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: simple_machines Forum can read files such as the database config.	2020-02-07	not yet calculated	<a href="#">2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript -- - simplejobscript.com	An issue was discovered in Simplejobscript.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
smoothwall -- - smoothwall Express3	- A cross-site scripting (XSS) vulnerability in Smoothwall Express3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall -- - smoothwall Express	- CSRF vulnerability in Smoothwall Express 3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
sphider -- - sphider search engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 where the sphider_engine calls in admin/spiderfuncs.php, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5087</a> <a href="#">MISC</a>
status2k -- - status2k	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
statusnet -- - statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	not yet calculated	<a href="#">CVE-2010-4658</a> <a href="#">MISC</a>
synaptive -- - medical_clearcanvas_image_server	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8788</a> <a href="#">MISC</a>
teamviewer -- - teamviewer	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9.x , this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the	2020-02-07	not yet calculated	<a href="#">CVE-2019-18988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.			
tianocore - - edk2	Buffer overflow in the Reclaim function in Tianocore EDK2 before SVN 16280 allows physically proximate attackers to gain privileges via a long variable name.	2020-02-06	not yet calculated	<a href="#">CVE-2014-8271</a> <a href="#">MISC</a>
troglobit -- minisnmpd	A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server.	2020-02-04	not yet calculated	<a href="#">CVE-2020-6060</a> <a href="#">MISC</a>
ubiquiti_networks - unifi_controller	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4) authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the Unifi Controller name via a request to api/set/setting/identity.	2020-02-08	not yet calculated	<a href="#">CVE-2014-2225</a> <a href="#">MISC</a>
ui -- edgeswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	not yet calculated	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
unshift -- url-parse	Insufficient validation and sanitization of user input exists in url-parse npm package version 1.4.4 and earlier may allow attacker to bypass security checks.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8124</a> <a href="#">MISC</a>
ushahidi -- ushahidi	Ushahidi before 2.6.1 has insufficient entropy for forgot-password tokens.	2020-02-04	not yet calculated	<a href="#">CVE-2012-5618</a> <a href="#">MISC</a>
videolan -- vlc_media_player	The web interface in VideoLAN VLC media player before 2.0.7 has no access control which allows remote attackers to view directory listings via the 'dir' command or issue other commands without authenticating.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3564</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	Unrestricted file upload vulnerability in the Settings_Vtiger_CompanyDetailsSave_Action class in modules/Settings/Vtiger/actions/CompanyDetailsSave.php in Vtiger CRM 6.3.0 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request	2020-02-06	not yet calculated	<a href="#">CVE-2015-6000</a> <a href="#">MISC</a>

	to the file in test/logo/.			MISC
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3591</a> MISC MISC MISC
watchguard - firewire_xtn	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	not yet calculated	<a href="#">CVE-2014-6413</a> MISC MISC MISC
webcalendar - webcalendar	webcalendar before 1.2.7 shows the reason for a failed login (e.g., "no such user").	2020-02-04	not yet calculated	<a href="#">CVE-2013-1422</a> MISC MISC MISC
wordpress - wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-2008</a> MISC MISC MISC
wordpress - wordpress	The Time Capsule plugin before 1.21.16 for WordPress has an authentication bypass. Any request containing IWP_JSON_PREFIX causes the client to be logged in as the first account on the list of administrator accounts.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8771</a> MISC MISC
wordpress - wordpress	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for WordPress and before 2.0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	2020-02-08	not yet calculated	<a href="#">CVE-2014-8739</a> MISC MISC MISC MISC MISC MISC MISC
wordpress - wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-2009</a> MISC MISC MISC MISC
wordpress - wordpress	The InfiniteWP Client plugin before 1.9.4.5 for WordPress has a missing authorization check in iwpm_mmb_set_request in init.php. Any attacker who knows the username of an	2020-02-06	not yet	<a href="#">CVE-2020-8772</a>



	administrator can log in.		calculator	<a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-1394</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3628</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager	Zoho ManageEngine Applications Manager 14 before 14520 allows a remote unauthenticated attacker to disclose OS file names via FailOverHelperServlet.	2020-02-06	not yet calculated	<a href="#">CVE-2019-19800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	not yet calculated	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States  
Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of February 3, 2020  
**Date:** Monday, February 10, 2020 3:12:03 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## **Vulnerability Summary for the Week of February 3, 2020**

02/10/2020 07:28 AM EST

Original release date: February 10, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the tcp_test function in aireplay-ng.c in Aircrack-ng before 1.2 RC 1 allows remote attackers to execute arbitrary code via a crafted length parameter value.	2020-01-31	7.5	<a href="#">CVE-2014-8322</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
aruba_networks -- instant	Multiple vulnerabilities exists in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.	2020-01-31	7.5	<a href="#">CVE-2016-2031</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	7.8	<a href="#">CVE-2020-3926</a> <a href="#">CONFIRM</a>

changing_information_technology -- servisign	An arbitrary-file-access vulnerability exists in ServiSign security plugin, as long as the attackers learn the specific API function, they may access arbitrary files on target system via crafted API parameter.	2020-02-03	8.5	<a href="#">CVE-2020-3927</a> <a href="#">CONFIRM</a>
cisco -- multiple_ip_phones	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco IP Phone could allow an unauthenticated, adjacent attacker to remotely execute code with root privileges or cause a reload of an affected IP phone. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a crafted Cisco Discovery Protocol packet to the targeted IP phone. A successful exploit could allow the attacker to remotely execute code with root privileges or cause a reload of an affected IP phone, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	2020-02-05	8.3	<a href="#">CVE-2020-3111</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- video_surveillance_8000_series_ip_cameras	A vulnerability in the Cisco Discovery Protocol implementation for the Cisco Video Surveillance 8000 Series IP Cameras could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP Camera. The vulnerability is due to missing checks when processing Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to the targeted IP Camera. A successful exploit could allow the attacker to expose the affected IP Camera for remote code execution or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). This vulnerability is fixed in Video Surveillance 8000 Series IP Camera Firmware Release 1.0.7 and later.	2020-02-05	8.3	<a href="#">CVE-2020-3110</a> <a href="#">MISC</a> <a href="#">CISCO</a>
coppermine_development -- coppermine_gallery	Coppermine gallery before 1.4.26 has an input validation vulnerability that allows for code execution.	2020-02-05	7.5	<a href="#">CVE-2010-4815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

curling -- curling	All versions of curling.js are vulnerable to Command Injection via the run function. The command argument can be controlled by users without any sanitization.	2020-02-06	<a href="#">10</a>	<a href="#">CVE-2019-10789</a> <a href="#">MISC</a> <a href="#">MISC</a>
django -- django	Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-7471</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
dot-prop -- dot-prop	Prototype pollution vulnerability in dot-prop npm package version 5.1.0 and earlier allows an attacker to add arbitrary properties to JavaScript language constructs such as objects.	2020-02-04	<a href="#">7.5</a>	<a href="#">CVE-2020-8116</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.2.4 is vulnerable to directory traversal, leading to incorrect access control. It allows an attacker to read or execute files under \$TOMCAT_HOME/webapps/ROOT/assets (which should be a protected directory). Additionally, attackers can upload temporary files (e.g., .jsp files) into /webapps/ROOT/assets/tmp_upload, which can lead to remote command execution (with the permissions of the user running the dotCMS application).	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-6754</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
edk2 -- unified_extensible_firmware_interface	Multiple integer overflows in the Pre-EFI Initialization (PEI) boot phase in the Capsule Update feature in the UEFI implementation in EDK2 allow physically proximate attackers to bypass intended access restrictions by providing crafted data that is not properly handled during the coalescing phase.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4860</a> <a href="#">MISC</a>
edk2 -- unified_extensible_firmware_interface	Integer overflow in the Drive Execution Environment (DXE) phase in the Capsule Update feature in the UEFI implementation in EDK2 allows physically proximate attackers to bypass intended access restrictions via crafted data.	2020-01-31	<a href="#">7.2</a>	<a href="#">CVE-2014-4859</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows SQL Injection via the user parameter to com.eg.LoginHelperServlet (aka the Forgot Password feature).	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8592</a> <a href="#">MISC</a>
eg_innovations -- eg_manager	eG Manager 7.1.2 allows authentication bypass via a com.egurkha.EgLoginServlet?uname=admin&upass=&accessKey=eGm0n1t0r	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8591</a> <a href="#">MISC</a>



	request.			
fortinet -- fortimanager	A Command Injection vulnerability exists in FortiManager 5.2.1 and earlier and FortiManager 5.0.10 and earlier via unspecified vectors, which could let a malicious user run systems commands when executing a report.	2020-02-04	9	<a href="#">CVE-2015-3611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
fortinet -- mortimanager	A vulnerability exists in in FortiManager 5.2.1 and earlier and 5.0.10 and earlier in the WebUI FTP backup page	2020-02-04	7.5	<a href="#">CVE-2015-3613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	7.5	<a href="#">CVE-2020-8114</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise up to 0.10.2 incorrectly validated role/region associated with TLS certificates used for mTLS RPC, and were susceptible to privilege escalation. Fixed in 0.10.3.	2020-01-31	7.5	<a href="#">CVE-2020-7956</a> <a href="#">MISC</a> <a href="#">MISC</a>
jobberbase -- jobberbase	Jobberbase 2.0 has SQL injection via the PATH_INFO to the jobs-in endpoint.	2020-02-05	7.5	<a href="#">CVE-2019-20447</a> <a href="#">MISC</a> <a href="#">MISC</a>
klona -- klona	Flaw in input validation in npm package klona version 1.1.0 and earlier may allow prototype pollution attack that may result in remote code execution or denial of service of applications using klona.	2020-02-04	7.5	<a href="#">CVE-2020-8125</a> <a href="#">MISC</a>
nanopb -- nanopb	There is a potentially exploitable out of memory condition In Nanopb before 0.4.1, 0.3.9.5, and 0.2.9.4. When nanopb is compiled with PB_ENABLE_MALLOC, the message to be decoded contains a repeated string, bytes or message field and realloc() runs out of memory when expanding the array nanopb can end up calling `free()` on a pointer value that comes from uninitialized memory. Depending on platform this can result in a crash or further memory corruption, which may be exploitable in some cases. This problem is fixed in nanopb-0.4.1, nanopb-0.3.9.5, nanopb-0.2.9.4.	2020-02-04	7.5	<a href="#">CVE-2020-5235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netapp -- oncommand_system_manager	NetApp OnCommand System Manager 2.1 and earlier allows remote attackers to execute arbitrary commands in the Halt/Reboot interface.	2020-01-31	9	<a href="#">CVE-2013-3322</a> <a href="#">XF</a> <a href="#">MISC</a>
norman -- malware_cleaner	nsak64.sys in Norman Malware Cleaner 2.08.08 allows users to call arbitrary kernel functions because the passing of function pointers between user and kernel	2020-02-03	7.5	<a href="#">CVE-2020-8508</a> <a href="#">MISC</a>

	mode is mishandled.			
phpabook -- phpabook	An issue was discovered in phpABook 0.9 Intermediate. On the login page, if one sets a userInfo cookie with the value of admin+1+en (user+perms+lang), one can login as any user without a password.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8510</a> <a href="#">MISC</a> <a href="#">MISC</a>
phplist -- phplist	phplist 3.5.0 allows type juggling for admin login bypass because == is used instead of === for password hashes, which mishandles hashes that begin with 0e followed by exclusively numerical characters.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8547</a> <a href="#">MISC</a>
playsms -- playsms	PlaySMS before 1.4.3 does not sanitize inputs from a malicious string.	2020-02-05	<a href="#">7.5</a>	<a href="#">CVE-2020-8644</a> <a href="#">MISC</a> <a href="#">MISC</a>
ppp -- ppp	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.	2020-02-03	<a href="#">7.5</a>	<a href="#">CVE-2020-8597</a> <a href="#">MISC</a> <a href="#">MLIST</a>
python -- python	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.	2020-02-04	<a href="#">7.1</a>	<a href="#">CVE-2019-9674</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm -- mdm9206_and_mdm9607_devices	Subsequent additions performed during Module loading while allocating the 9607 devices could lead to integer overflow and then to buffer overflow in Snapdragon Industrial IOT in MDM9206, MDM9607	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14051</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while allocating memory for an array in camera due to improper validation of elements parameters in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in QCS605, SDM439, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14046</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access due to access of uninitialized memory segment in an array of pointers while normal camera open close in Snapdragon Consumer IOT, Snapdragon Mobile in QCS605, SDM439, SDM630, SDM636, SDM660, SDX24	2020-02-07	<a href="#">7.2</a>	<a href="#">CVE-2019-14044</a> <a href="#">CONFIRM</a>
	Possibility of use-after-free and double free because of not marking buffer as NULL after freeing can lead to dangling pointer access in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon			

qualcomm -- multiple_snapdragon_products	Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8939, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS605, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14055</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	APKs without proper permission may bind to CallEnhancementService and can lead to unauthorized access to call status in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6574AU, QCS605, QM215, SA6155P, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SM6150, SM8150, SM8250, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14002</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	There is a way to deceive the GPU kernel driver into thinking there is room in the GPU ringbuffer and overwriting existing commands could allow unintended GPU opcodes to be executed in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-10567</a> <a href="#">CONFIRM</a>
	Out of bound access due to Invalid inputs to dapm mux settings which results into kernel failure in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial			

qualcomm -- multiple_snapdragon_products	IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9607, Nicobar, QCS405, Rennell, SA6155P, Saipan, SC8180X, SDM630, SDM636, SDM660, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14063</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Uninitialized stack data gets used if memory is not allocated for blob or if the allocated blob is less than the struct size required due to lack of check of return value for read or write blob in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8098, IPQ4019, IPQ6018, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	7.2	<a href="#">CVE-2019-14060</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer Over read of codec private data while parsing an mkv file due to lack of check of buffer size before read in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	9.4	<a href="#">CVE-2019-14057</a> <a href="#">CONFIRM</a>

qualcomm -- multiple_snapdragon_products	Stage-2 fault will occur while writing to an ION system allocation which has been assigned to non-HLOS memory which is non-standard in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MSM8953, QCN7605, QCS605, SC8180X, SDA845, SDM429, SDM439, SDM450, SDM632, SDX20, SDX24, SDX55, SM8150, SXR1130	2020-02-07	7.2	<a href="#">CVE-2019-14049</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access while parsing dts atom, which is non-standard as it does not have valid number of tracks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	10	<a href="#">CVE-2019-10590</a> <a href="#">CONFIRM</a>
sap -- netweaver	SAP NetWeaver 7.0 allows Remote Code Execution and Denial of Service caused by an error in the DiagTraceHex() function. By sending a specially-crafted packet, an attacker could exploit this vulnerability to cause the application to crash.	2020-02-05	7.5	<a href="#">CVE-2011-1517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript.com -- simplejobscript.com	controllers/page_apply.php in Simplejobscript.com SJS through 1.66 is prone to unauthenticated Remote Code Execution by uploading a PHP script as a resume.	2020-01-31	7.5	<a href="#">CVE-2020-8440</a> <a href="#">CONFIRM</a>
smartbear -- readyapi_and_soapui	An issue was discovered in SmartBear ReadyAPI through 2.8.2 and 3.0.0 and SoapUI through 5.5. When opening a project, the Groovy "Load Script" is automatically executed. This allows an attacker to execute arbitrary Groovy Language code (Java scripting language)	2020-02-05	9.3	<a href="#">CVE-2019-12180</a> <a href="#">MISC</a>



	on the victim machine by inducing it to open a malicious Project. The same issue is present in the "Save Script" function, which is executed automatically when saving a project.			
squid -- squid	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.	2020-02-04	7.5	<a href="#">CVE-2020-8450</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_update_framework -- tuf	TUF (aka The Update Framework) through 0.12.1 has Improper Verification of a Cryptographic Signature.	2020-02-05	7.5	<a href="#">CVE-2020-6174</a> <a href="#">CONFIRM</a>
tp-link -- tg-sg105e_devices	The Web Management of TP-Link TP-SG105E V4 1.0.0 Build 20181120 devices allows an unauthenticated attacker to reboot the device via a reboot.cgi request.	2020-02-03	7.8	<a href="#">CVE-2019-16893</a> <a href="#">EXPLOIT-DB</a>
zpanel_project -- zpanel	ZPanel 10.0.1 has insufficient entropy for its password reset process.	2020-02-04	7.5	<a href="#">CVE-2012-5686</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	6.5	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	5	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	4.6	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent --	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch			<a href="#">CVE-2014-</a>

1830_photonic_service	OS 16.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	2020-01-31	<a href="#">4.3</a>	<a href="#">3809 MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-12426 MLIST CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	<a href="#">4.9</a>	<a href="#">CVE-2011-0220 MISC</a>
apple -- safari	A Cross-origin vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2016-4676 MISC MISC MISC CONFIRM MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8505 MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/mysql through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2020-8504 MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2016-2032 MISC MISC MISC MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20104 N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404 N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	<a href="#">4.4</a>	<a href="#">CVE-2019-20400 N/A</a>
	The JMX monitoring flag in Atlassian Jira Server and Data Center before version			<a href="#">CVE-2019-</a>

atlassian -- jira	8.6.0 allows remote attackers to turn the JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	2020-02-06	<a href="#">4.3</a>	<a href="#">20405</a> <a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	<a href="#">5</a>	<a href="#">CVE-2019-20403</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20402</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2674</a> <a href="#">MISC</a> <a href="#">XE</a> <a href="#">BID</a>

brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	5	<a href="#">CVE-2013-2672</a> <a href="#">MISC</a> <a href="#">XF</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	4.6	<a href="#">CVE-2013-2673</a> <a href="#">MISC</a> <a href="#">BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	5	<a href="#">CVE-2019-12998</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	5	<a href="#">CVE-2013-2683</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	5	<a href="#">CVE-2013-2680</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	6.8	<a href="#">CVE-2013-2678</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	4.3	<a href="#">CVE-2013-2681</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	4.3	<a href="#">CVE-2013-2682</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	4.3	<a href="#">CVE-2013-2684</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
computer_incident_response -- ail-framework	Global Cyber All framework 2.8 allows path traversal.	2020-02-03	5	<a href="#">CVE-2020-8545</a> <a href="#">MISC</a>
cysharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions	2020-01-31	6.8	<a href="#">CVE-2020-5234</a> <a href="#">MISC</a>

	and stack overflow. Review the linked GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus -- eucalyptus_management_console	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>



evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	6.6	<a href="#">CVE-2013-5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	5	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	4.6	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	5	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	5	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	4.3	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	4	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 0.10.3 allow unbounded resource usage.	2020-01-31	5	<a href="#">7218</a> <a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	6.5	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information_server	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	5.8	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	6.8	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	6.9	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	6.5	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	6	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	5.8	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or	2020-02-04	5	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

	browser history. IBM X-Force ID: 166623.			
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> XF <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> XF <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> XF <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> XF <a href="#">CONFIRM</a>
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> MISC MISC MISC
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> MISC MISC MISC MISC

info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8139</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	4.3	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	6.5	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	5	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	5	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	5	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	6.4	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	5	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be			



joomla! -- joomla!	entered by any user. If it doesn't contain rel="noopener" (or similar attributes such as noreferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	2020-02-03	4.3	<a href="#">CVE-2020-5182</a> <a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	4.3	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	5	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	5	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	6.6	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	6.5	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	4.3	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- rumpus	An issue was discovered in Rumpus 0.2.0 on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	4.3	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to	2020-02-06	4.4	<a href="#">CVE-2019-20406</a>

	write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.			<a href="#">N/A</a>
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	5	<a href="#">4116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	5	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	6.4	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	4.3	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	4.3	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	4	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	6.8	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon			

qualcomm -- multiple_snapdragon_products	Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>

squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- openSUSE_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a>



	to arbitrary websites via a crafted URL.			<a href="#">MISC</a>
telaen -- telaen	Telaen before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted URL request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2624</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	<a href="#">4</a>	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browser_y" in the page image.php.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	<a href="#">5</a>	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this	2020-02-04	<a href="#">6.4</a>	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>

	vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

wordpress -- wordpress	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can result in an attacker performing malicious actions such as stealing session tokens.	2020-02-03	<a href="#">4.3</a>	<a href="#">8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	<a href="#">4</a>	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1up -- oneupuploaderbundle	oneup/uploader-bundle before 1.9.3 and 2.1.5, can be exploited to upload files to arbitrary folders on the filesystem. The assembly process can further be misused with some restrictions to delete and copy files to other locations. This is fixed in versions 1.9.3 and 2.1.5.	2020-02-05	<a href="#">6.5</a>	<a href="#">CVE-2020-5237</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
abrt -- abrt	ABRT might allow attackers to obtain sensitive information from crash reports.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2011-4088</a> <a href="#">MISC</a> <a href="#">MISC</a>
aircrack-ng -- aircrack-ng	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.	2020-01-31	<a href="#">4.6</a>	<a href="#">CVE-2014-8321</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
alcatel-lucent --	Cross-site scripting (XSS) vulnerability in the management interface in Alcatel-Lucent 1830 Photonic Service Switch	2020-01-		<a href="#">CVE-2014-</a>

1830_photonic_service	Before 16.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the myurl parameter to menu/pop.html.	31	4.3	<a href="#">3809 MISC</a>
apache -- ofbiz	an unauthenticated user could get access to information of some backend screens by invoking setSessionLocale in Apache OFBiz 16.11.01 to 16.11.06	2020-02-06	5	<a href="#">CVE-2019-12426 MLIST CONFIRM</a>
apple -- bonjour	Apple Bonjour before 2011 allows a crash via a crafted multicast DNS packet.	2020-02-05	4.9	<a href="#">CVE-2011-0220 MISC</a>
apple -- safari	A Cross-origins vulnerability exists in WebKit in Apple Safari before 10.0.1 when processing location attributes, which could let a remote malicious user obtain sensitive information.	2020-02-03	5	<a href="#">CVE-2016-4676 MISC MISC MISC CONFIRM MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=deleteadmin CSRF to delete a user.	2020-01-31	4.3	<a href="#">CVE-2020-8505 MISC</a>
aroxsolution -- school_management_software_php/mysql	School Management Software PHP/MySQL through 2019-03-14 allows office_admin/?action=addadmin CSRF to add an administrative user.	2020-01-31	4.3	<a href="#">CVE-2020-8504 MISC</a>
aruba -- airwave_management_platform	A vulnerability exists in the Aruba AirWave Management Platform 8.x prior to 8.2 in the management interface of an underlying system component called RabbitMQ, which could let a malicious user obtain sensitive information. This interface listens on TCP port 15672 and 55672	2020-01-31	5	<a href="#">CVE-2016-2032 MISC MISC MISC MISC</a>
atlassian -- crowd	The OpenID client application in Atlassian Crowd before version 3.6.2, and from version 3.7.0 before 3.7.1 allows remote attackers to perform a Denial of Service attack via an XML Entity Expansion vulnerability.	2020-02-06	5	<a href="#">CVE-2019-20104 N/A</a>
atlassian -- jira	The usage of Tomcat in Jira before version 8.5.2 allows local attackers with permission to write a dll file to a directory in the global path environmental variable can inject code into via a DLL hijacking vulnerability.	2020-02-06	4.4	<a href="#">CVE-2019-20400 N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to determine if a Jira project key exists or not via an information disclosure vulnerability.	2020-02-06	5	<a href="#">CVE-2019-20403 N/A</a>
atlassian -- jira	Support zip files in Atlassian Jira Server and Data Center before version 8.6.0 could be downloaded by a System	2020-02-	4	<a href="#">CVE-2019-20402</a>

	Administrator user without requiring the user to re-enter their password via an improper authorization vulnerability.	06		<a href="#">N/A</a>
atlassian -- jira	The JMX monitoring flag in Atlassian Jira Server and Data Center before version 8.6.0 allows remote attackers to turn the JMX monitoring flag off or on via a Cross-site request forgery (CSRF) vulnerability.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20405</a> <a href="#">N/A</a>
atlassian -- jira	The API in Atlassian Jira Server and Data Center before version 8.6.0 allows authenticated remote attackers to determine project titles they do not have access to via an improper authorization vulnerability.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20404</a> <a href="#">N/A</a>
atlassian -- jira	Comment properties in Atlassian Jira Server and Data Center before version 7.13.12, from 8.0.0 before version 8.5.4, and 8.6.0 before version 8.6.1 allows remote attackers to make comments on a ticket to which they do not have commenting permissions via a broken access control bug.	2020-02-06	<a href="#">4</a>	<a href="#">CVE-2019-20106</a> <a href="#">N/A</a>
atlassian -- jira	Various installation setup resources in Jira before version 8.5.2 allow remote attackers to configure a Jira instance, which has not yet finished being installed, via Cross-site request forgery (CSRF) vulnerabilities.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2019-20401</a> <a href="#">N/A</a>
auth0 -- auth0_lock	Auth0 Lock before 11.21.0 allows XSS when additionalSignUpFields is used with an untrusted placeholder.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-20174</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
batavi -- batavi	Batavi before 1.0 has CSRF.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2011-0525</a> <a href="#">MISC</a> <a href="#">MISC</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v7.4.2f, v8.2.2a, v8.1.2j and v8.2.1d could expose external passwords, common secrets or authentication keys used between the switch and an external server.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16204</a> <a href="#">CONFIRM</a>
brocade -- fabric_os	Brocade Fabric OS Versions before v8.2.2a and v8.2.1d could expose the credentials of the remote ESRS server when these credentials are given as a command line option when configuring the ESRS client.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2019-16203</a> <a href="#">CONFIRM</a>
brother -- mfc-9970cdw_devices	Brother MFC-9970CDW devices with firmware 0D allow cleartext submission of passwords.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2013-2672</a> <a href="#">MISC</a> <a href="#">XF</a>
brother -- mfc-	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure			<a href="#">CVE-2013-2674</a>



9970cdw_devices	vulnerability which allows remote attackers to view sensitive information from referrer logs due to inadequate handling of HTTP referrer headers.	2020-02-03	5	<a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a>
brother -- mfc-9970cdw	Brother MFC-9970CDW 1.10 firmware L devices contain a security bypass vulnerability which allows physically proximate attackers to gain unauthorized access.	2020-02-03	4.6	<a href="#">CVE-2013-2673</a> <a href="#">MISC</a> <a href="#">BID</a>
c-lightning -- c-lightning	c-lightning before 0.7.1 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "It can be used for testing, but it should not be used for real funds."	2020-01-31	5	<a href="#">CVE-2019-12998</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices store passwords in cleartext allowing remote attackers to obtain sensitive information.	2020-02-05	5	<a href="#">CVE-2013-2680</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 devices contain an Information Disclosure Vulnerability which allows remote attackers to obtain private IP addresses and other sensitive information.	2020-02-06	5	<a href="#">CVE-2013-2683</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200	Cisco Linksys E4200 1.0.05 Build 7 routers contain a Local File Include Vulnerability which could allow remote attackers to obtain sensitive information or execute arbitrary code by sending a crafted URL request to the apply.cgi script using the submit_type parameter.	2020-02-04	6.8	<a href="#">CVE-2013-2678</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200_devices	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Security Bypass Vulnerability which could allow remote attackers to gain unauthorized access.	2020-02-05	4.3	<a href="#">CVE-2013-2681</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200_devices	Cross-site Scripting (XSS) in Cisco Linksys E4200 1.0.05 Build 7 devices allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-02-06	4.3	<a href="#">CVE-2013-2684</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
cisco -- linksys_e4200_devices	Cisco Linksys E4200 1.0.05 Build 7 devices contain a Clickjacking Vulnerability which allows remote attackers to obtain sensitive information.	2020-02-05	4.3	<a href="#">CVE-2013-2682</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">XF</a>
computer_incident_response -- ail-framework	Global Cyber Alliance framework 2.8 allows path traversal.	2020-02-03	5	<a href="#">CVE-2020-8545</a> <a href="#">MISC</a>
cysharp -- messagepack_for_csharp_and_unity	MessagePack for C# and Unity before version 1.9.3 and 2.1.80 has a vulnerability where untrusted data can add a DoS attack due to hash collisions	2020-01-31	6.8	<a href="#">CVE-2020-5234</a> <a href="#">MISC</a>

	and stack overflow. Review the linked GitHub Security Advisory for more information and remediation steps.			<a href="#">CONFIRM</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07 has PPTP and poe information disclosure	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7055</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: security bypass via an error in the cliget.cgi script	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2013-7052</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi security bypass due to failure to check authentication parameters	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi CSRF	2020-02-04	<a href="#">6.8</a>	<a href="#">CVE-2013-7053</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-100_devices	D-Link DIR-100 4.03B07: cli.cgi XSS	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2013-7054</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	Cross-site scripting (XSS) vulnerability in vwrooms/js/jsor-jcarousel/examples/special_textscroller.php in the VideoWhisper Webcam plugins for Drupal 7.x allows remote attackers to inject arbitrary web script or HTML via a URL to a crafted SVG file in the feed parameter.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2014-8338</a> <a href="#">MISC</a> <a href="#">MISC</a>
eclair -- eclair	Eclair through 0.3 allows attackers to trigger loss of funds because of Incorrect Access Control. NOTE: README.md states "it is beta-quality software and don't put too much money in it."	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2019-13000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ens_domains -- ens	A user who owns an ENS domain can set a trapdoor, allowing them to transfer ownership to another user, and later regain ownership without the new owners consent or awareness. A new ENS deployment is being rolled out that fixes this vulnerability in the ENS registry.	2020-01-31	<a href="#">4.9</a>	<a href="#">CVE-2020-5232</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eucalyptus_eucalyptus	Cross-site scripting (XSS) vulnerability in Eucalyptus Management Console (EMC) 4.0.x before 4.0.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	<a href="#">6.8</a>	<a href="#">CVE-2014-5039</a> <a href="#">CONFIRM</a>

evernote_corporation - - evernote	Evernote prior to 5.5.1 has insecure password change	2020-01-31	6.6	<a href="#">CVE-2013-5116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1 and 14.1.0-14.1.2.2, while processing specifically crafted traffic using the default 'xnet' driver, Virtual Edition instances hosted in Amazon Web Services (AWS) may experience a TMM restart.	2020-02-06	5	<a href="#">CVE-2020-5856</a> <a href="#">CONFIRM</a>
f5 -- big-ip ip_edge_client_for_windows	When the Windows Logon Integration feature is configured for all versions of BIG-IP Edge Client for Windows, unauthorized users who have physical access to an authorized user's machine can get shell access under unprivileged user.	2020-02-06	4.6	<a href="#">CVE-2020-5855</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab EE 11.3 and later. A GitLab Workhorse bypass could lead to package and file disclosure via request smuggling.	2020-02-05	5	<a href="#">CVE-2020-6833</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	GitLab through 12.7.2 allows XSS.	2020-02-05	4.3	<a href="#">CVE-2020-7973</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.6 and later through 12.7.2 allows Denial of Service.	2020-02-05	5	<a href="#">CVE-2020-7978</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 11.11 and later through 12.7.2 allows Directory Traversal.	2020-02-05	5	<a href="#">CVE-2020-7966</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7968</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 through 12.7.2 has Insecure Permissions (issue 1 of 2).	2020-02-05	4	<a href="#">CVE-2020-7967</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 10.1 through 12.7.2 allows Information Disclosure.	2020-02-05	5	<a href="#">CVE-2020-7974</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.4 and later through 12.7.2 has Incorrect Access Control.	2020-02-05	5	<a href="#">CVE-2020-7976</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 12.2 has Insecure Permissions (issue 2 of 2).	2020-02-05	5	<a href="#">CVE-2020-7972</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.0 and later through 12.7.2 allows Information Disclosure.	2020-02-05	<a href="#">5</a>	<a href="#">CVE-2020-7969</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 11.0 and later through 12.7.2 allows XSS.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7971</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 8.8 and later through 12.7.2 has Insecure Permissions.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7977</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_enterprise	GitLab EE 8.9 and later through 12.7.2 has Insecure Permission	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2020-7979</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
google -- android	An issue was discovered in the Bluetooth component of the Cypress (formerly owned by Broadcom) Wireless IoT codebase. Extended Inquiry Responses (EIRs) are improperly handled, which causes a heap-based buffer overflow during device inquiry. This overflow can be used to overwrite existing functions with arbitrary code. The Reserved for Future Use (RFU) bits are not discarded by eir_handleRx(), and are included in an EIR's length. Therefore, one can exceed the expected 240 bytes, which leads to a heap-based buffer overflow in eir_getReceivedEIR() called by bthci_event_SendInquiryResultEvent(). In order to exploit this bug, an attacker must repeatedly connect to the victim's device in a short amount of time from different source addresses. This will cause the victim's Bluetooth stack to resolve the device names and therefore allocate buffers with attacker-controlled data. Due to the heap corruption, the name will be eventually written to an attacker-controlled location, leading to a write-what-where condition.	2020-02-05	<a href="#">6.8</a>	<a href="#">CVE-2019-11516</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise 1.4.1 through 1.6.2 did not uniformly enforce ACLs across all API endpoints, resulting in potential unintended information disclosure. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7955</a> <a href="#">MISC</a> <a href="#">MISC</a>
hashicorp -- consul_and_consul_enterprise	HashiCorp Consul and Consul Enterprise up to 1.6.2 HTTP/RPC services allowed unbounded resource usage, and were susceptible to unauthenticated denial of service. Fixed in 1.6.3.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2020-7219</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

hashicorp -- nomad_and_nomad_enterprise	HashiCorp Nomad and Nomad Enterprise before 0.10.3 allow unbounded resource usage.	2020-01-31	5	<a href="#">7218</a> <a href="#">MISC</a> <a href="#">MISC</a>
htcondor -- mrg_grid	The scheduler in HTCondor before 8.2.6 allows remote authenticated users to execute arbitrary code.	2020-01-31	6.5	<a href="#">CVE-2014-8126</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- infosphere_information_server	IBM InfoSphere Information Server 8.1, 8.5, 8.7, 9.1 has a Session Fixation Vulnerability	2020-02-05	5.8	<a href="#">CVE-2013-0507</a> <a href="#">MISC</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 168524.	2020-02-05	6.8	<a href="#">CVE-2019-4613</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sdk_java_technology	IBM SDK, Java Technology Edition Version 7.0.0.0 through 7.0.10.55, 7.1.0.0 through 7.1.4.55, and 8.0.0.0 through 8.0.6.0 could allow a local authenticated attacker to execute arbitrary code on the system, caused by DLL search order hijacking vulnerability in Microsoft Windows client. By placing a specially-crafted file in a compromised folder, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 172618.	2020-02-03	6.9	<a href="#">CVE-2019-4732</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 165814.	2020-02-04	6.5	<a href="#">CVE-2019-4541</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.	2020-02-04	6	<a href="#">CVE-2020-4163</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- workflow_for_bluemix	IBM Workflow for Bluemix does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2020-02-05	5.8	<a href="#">CVE-2015-0102</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 stores sensitive information in URLs. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referer header or	2020-02-04	5	<a href="#">CVE-2019-4562</a> <a href="#">XF</a> <a href="#">CONFIRM</a>



	browser history. IBM X-Force ID: 166623.			
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM X-Force ID: 165953.	2020-02-04	5	<a href="#">CVE-2019-4551</a> XF CONFIRM
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 165950.	2020-02-04	4.3	<a href="#">CVE-2019-4548</a> XF CONFIRM
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 is deployed with active debugging code that can create unintended entry points. IBM X-Force ID: 165952.	2020-02-04	5	<a href="#">CVE-2019-4550</a> XF CONFIRM
ibm -- security_directory_server	IBM Security Directory Server 6.4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 165813.	2020-02-04	5	<a href="#">CVE-2019-4540</a> XF CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 171510.	2020-02-04	4	<a href="#">CVE-2019-4674</a> XF CONFIRM
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume all available memory. IBM X-Force ID: 172125.	2020-01-31	5	<a href="#">CVE-2019-4720</a> XF CONFIRM
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to obtain sensitive information caused by improper data representation. IBM X-Force ID: 171319.	2020-02-05	4	<a href="#">CVE-2019-4670</a> XF CONFIRM
icewarp -- webmail_server	In IceWarp Webmail Server through 11.4.4.1, there is XSS in the /webmail/ color parameter.	2020-02-01	4.3	<a href="#">CVE-2020-8512</a> MISC MISC MISC
info-zip -- unzip	Heap-based buffer overflow in the test_compr_eb function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8140</a> MISC MISC MISC MISC

info-zip -- unzip	Heap-based buffer overflow in the CRC32 verification in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8139</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
info-zip -- unzip	Heap-based buffer overflow in the getZip64Data function in Info-ZIP UnZip 6.0 and earlier allows remote attackers to execute arbitrary code via a crafted zip file in the -t command argument to the unzip command.	2020-01-31	6.8	<a href="#">CVE-2014-8141</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
infoware -- mapsuite_mapapi	Cross-site scripting (XSS) vulnerability in infoware MapSuite MapAPI 1.0.x before 1.0.36 and 1.1.x before 1.1.49 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2020-01-31	4.3	<a href="#">CVE-2014-2843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ipmitool -- ipmitool	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.	2020-02-05	6.5	<a href="#">CVE-2020-5208</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
jetbrains -- intellij_idea	In JetBrains IntelliJ IDEA 2019.2, an XSLT debugger plugin misconfiguration allows arbitrary file read operations over the network. This issue was fixed in 2019.3.	2020-01-31	5	<a href="#">CVE-2020-7914</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla! -- joomla!	Joomla! 1.7.1 has core information disclosure due to inadequate error checking.	2020-02-04	5	<a href="#">CVE-2011-4937</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! core 1.7.1 allows information disclosure due to weak encryption	2020-02-04	5	<a href="#">CVE-2011-3629</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! 1.6.0 is vulnerable to SQL Injection via the filter_order and filer_order_Dir parameters.	2020-02-05	6.4	<a href="#">CVE-2011-1151</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla!	Joomla! com_mailto 1.5.x through 1.5.13 has an automated mail timeout bypass.	2020-02-04	5	<a href="#">CVE-2011-4912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The J-BusinessDirectory extension before 5.2.9 for Joomla! allows Reverse Tabnabbing. In some configurations, the link to the business website can be			

joomla! -- joomla!	entered by any user. If it doesn't contain rel="noopener" (or similar attributes such as noreferrer), the tabnabbing may occur. To reproduce the bug, create a business with a website link that contains JavaScript to exploit the window.opener property (for example, by setting window.opener.location).	2020-02-03	4.3	<a href="#">CVE-2020-5182</a> <a href="#">CONFIRM</a>
kubernetes -- kubernetes	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.	2020-02-03	4.3	<a href="#">CVE-2019-11251</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
libvncserver -- libvncserver	A NULL pointer dereference flaw was found in the way LibVNCServer before 0.9.9 handled certain ClientCutText message. A remote attacker could use this flaw to crash the VNC server by sending a specially crafted ClientCutText message from a VNC client.	2020-02-05	5	<a href="#">CVE-2010-5304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lightning_labs -- lightning_network_daemon	Lightning Network Daemon (Ind) before 0.7 allows attackers to trigger loss of funds because of Incorrect Access Control.	2020-01-31	5	<a href="#">CVE-2019-12999</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
logmein -- lastpass	LastPass prior to 2.5.1 allows secure wipe bypass.	2020-01-31	6.6	<a href="#">CVE-2013-5114</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lotus_core -- lotus_core_cms	Lotus Core CMS 1.0.1 allows authenticated Local File Inclusion of .php files via directory traversal in the index.php page_slug parameter.	2020-02-05	6.5	<a href="#">CVE-2020-8641</a> <a href="#">MISC</a>
masscode -- masscode	massCode 1.0.0-alpha.6 allows XSS via crafted Markdown text, with resultant remote code execution (because nodeIntegration in webPreferences is true).	2020-02-03	4.3	<a href="#">CVE-2020-8548</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development -- rumpus	An issue was discovered in Rumpus on macOS. By crafting a directory name, it is possible to activate JavaScript in the context of the web application after invoking the rename folder functionality.	2020-02-02	4.3	<a href="#">CVE-2020-8514</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_operating_system	The usage of Tomcat in Confluence on the Microsoft Windows operating system before version 7.0.5, and from version 7.1.0 before version 7.1.1 allows local system attackers who have permission to	2020-02-06	4.4	<a href="#">CVE-2019-20406</a>

	write a DLL file in a directory in the global path environmental variable variable to inject code & escalate their privileges via a DLL hijacking vulnerability.			<a href="#">N/A</a>
movable_type -- multiple_products	Cross-site scripting vulnerability in Movable Type series (Movable Type 7 r.4603 and earlier (Movable Type 7), Movable Type 6.5.2 and earlier (Movable Type 6.5), Movable Type Advanced 7 r.4603 and earlier (Movable Type Advanced 7), Movable Type Advanced 6.5.2 and earlier (Movable Type Advanced 6.5), Movable Type Premium 1.26 and earlier (Movable Type Premium), and Movable Type Premium Advanced 1.26 and earlier (Movable Type Premium Advanced)) allows remote attackers to inject arbitrary web script or HTML in the block editor and the rich text editor via a specially crafted URL.	2020-02-06	<a href="#">4.3</a>	<a href="#">CVE-2020-5528</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.	2020-02-04	<a href="#">4.3</a>	<a href="#">CVE-2020-8120</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper preservation of permissions in Nextcloud Server 14.0.3 causes the event details to be leaked when sharing a non-public event.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8117</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper authorization in Nextcloud server 17.0.0 causes leaking of previews and files when a file-drop share link is opened via the gallery app.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2020-8119</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Exposure of Private Information in Nextcloud Server 16.0.1 causes the server to send it's domain and user IDs to the Nextcloud Lookup Server without any further data when the Lookup server is disabled.	2020-02-04	<a href="#">5</a>	<a href="#">CVE-2019-15623</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- talk	Improper access control in Nextcloud Talk 6.0.3 leaks the existence and the name of private conversations when linked them to another shared item via the projects feature.	2020-02-04	<a href="#">4</a>	<a href="#">CVE-2019-15620</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-xchange -- ox_app_suite	Multiple absolute path traversal vulnerabilities in documentconverter in Open-Xchange (OX) AppSuite before 7.4.2-rev10 and 7.6.x before 7.6.0-rev10 allow remote attackers to read application files via a full pathname in a crafted (1) OLE Object or (2) image in an OpenDocument text file.	2020-01-31	<a href="#">5</a>	<a href="#">CVE-2014-5236</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openwall -- openwall	bbPress through 1.0.2 has XSS in /bb-login.php url via the re parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1150</a> <a href="#">MISC</a>
				<a href="#">CVE-2011-</a>

perl -- perl	_is_safe in the File::Temp module for Perl does not properly handle symlinks.	2020-01-31	5	<a href="#">4116</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	The Batch::BatchRun module 1.03 for Perl does not properly handle temporary files.	2020-01-31	5	<a href="#">CVE-2011-4117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
perl -- perl	Parallel::ForkManager module before 1.0.0 for Perl does not properly handle temporary files.	2020-01-31	6.4	<a href="#">CVE-2011-4115</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phpshop -- phpshop	PHPShop through 0.8.1 has XSS.	2020-02-05	4.3	<a href="#">CVE-2011-1069</a> <a href="#">MISC</a>
pmwiki -- pmwiki	PmWiki before 2.2.21 has XSS.	2020-02-05	4.3	<a href="#">CVE-2010-4662</a> <a href="#">MISC</a> <a href="#">MISC</a>
prototype -- prototype	Prototype 1.6.0.1 allows remote authenticated users to forge ticket creation (on behalf of other user accounts) via a modified email ID field.	2020-02-03	4	<a href="#">CVE-2020-7993</a> <a href="#">MISC</a> <a href="#">MISC</a>
pylons_project -- waitress	Waitress version 1.4.2 allows a DOS attack When waitress receives a header that contains invalid characters. When a header like "Bad-header: xxxxxxxxxxxxxx\x10" is received, it will cause the regular expression engine to catastrophically backtrack causing the process to use 100% CPU time and blocking any other interactions. This allows an attacker to send a single request with an invalid header and take the service offline. This issue was introduced in version 1.4.2 when the regular expression was updated to attempt to match the behaviour required by errata associated with RFC7230. The regular expression that is used to validate incoming headers has been updated in version 1.4.3, it is recommended that people upgrade to the new version of Waitress as soon as possible.	2020-02-04	6.8	<a href="#">CVE-2020-5236</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	Using memory after being freed in qsee due to wrong implementation can lead to unexpected behavior such as execution of unknown code in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon			



qualcomm -- multiple_snapdragon_products	Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, QCS605, QM215, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SM8150, SXR1130	2020-02-07	4.6	<a href="#">CVE-2019-14040</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	During listener modified response processing, a buffer overrun occurs due to lack of buffer size verification when updating message buffer with physical address information in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996AU, Nicobar, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SC8180X, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2020-02-07	4.6	<a href="#">CVE-2019-14041</a> <a href="#">CONFIRM</a>
senior -- rubiweb	Remote Authentication Bypass in Senior Rubiweb 6.2.34.28 and 6.2.34.37 allows admin access to sensitive information of affected users using vulnerable versions. The attacker only needs to provide the correct URL.	2020-01-31	5	<a href="#">CVE-2019-19550</a> <a href="#">CONFIRM</a>
sos -- jobscheduler	A large or infinite loop vulnerability in the JOC Cockpit component of SOS JobScheduler 1.11 and 1.13.2 allows attackers to parameterize housekeeping jobs in a way that exhausts system resources and results in a denial of service.	2020-02-06	6.8	<a href="#">CVE-2020-6855</a> <a href="#">MISC</a>
sos -- jobscheduler	An XML External Entity (XEE) vulnerability exists in the JOC Cockpit component of SOS JobScheduler 1.12 and 1.13.2 allows attackers to read files from the server via an entity declaration in any of the XML documents that are used to specify the run-time settings of jobs and orders.	2020-02-06	4	<a href="#">CVE-2020-6856</a> <a href="#">MISC</a>

squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, the NTLM authentication credentials parser in ext_lm_group_acl may write to memory outside the credentials buffer. On systems with memory access protections, this can result in the helper process being terminated unexpectedly. This leads to the Squid process also terminating and a denial of service for all clients using the proxy.	2020-02-04	5	<a href="#">CVE-2020-8517</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. Due to incorrect input validation, it can interpret crafted HTTP requests in unexpected ways to access server resources prohibited by earlier security filters.	2020-02-04	5	<a href="#">CVE-2020-8449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.	2020-02-04	5	<a href="#">CVE-2019-12528</a> <a href="#">CONFIRM</a>
strapi -- strapi	A denial of service exists in strapi v3.0.0-beta.18.3 and earlier that can be abused in the admin console using admin rights can lead to arbitrary restart of the application.	2020-02-04	4	<a href="#">CVE-2020-8123</a> <a href="#">MISC</a>
suse -- opensuse_wicked	An ni_dhcp4_parse_response memory leak in openSUSE wicked 0.6.55 and earlier allows network attackers to cause a denial of service by sending DHCP4 packets without a message type option.	2020-02-05	5	<a href="#">CVE-2020-7216</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SQL Injection in SysJust Syuan-Gu-Da-Shih, versions before 20191223, allowing attackers to perform unwanted SQL queries and access arbitrary file in the database.	2020-02-04	5	<a href="#">CVE-2020-3937</a> <a href="#">MISC</a>
sysjust_syuan-gu-d-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Request Forgery, allowing attackers to launch inquiries into network architecture or system files of the server via forged inquests.	2020-02-04	5	<a href="#">CVE-2020-3938</a> <a href="#">MISC</a>
sysjust_syuan-gu-da-shih -- sysjust_syuan-gu-da-shih	SysJust Syuan-Gu-Da-Shih, versions before 20191223, contain vulnerability of Cross-Site Scripting(XSS), personal information may be leaked to attackers via the vulnerability.	2020-02-04	4.3	<a href="#">CVE-2020-3939</a> <a href="#">MISC</a>
telaen -- telaen	Telean before 1.3.1 contains a full path disclosure vulnerability which could allow remote attackers to obtain sensitive information through a specially crafted	2020-02-03	5	<a href="#">CVE-2013-2624</a> <a href="#">XF</a>

	URL request.			MISC
telaen -- telaen	Open Redirection Vulnerability in the redir.php script in Telaen before 1.3.1 allows remote attackers to redirect victims to arbitrary websites via a crafted URL.	2020-02-03	5.8	<a href="#">CVE-2013-2621</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
telaen -- telaen	Cross-site Scripting (XSS) in Telaen before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the "f_email" parameter in index.php.	2020-02-03	4.3	<a href="#">CVE-2013-2623</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">MISC</a>
the_citytv_video_application -- the_citytv_video_application	The Citytv Video application 4.08.0 for Android and 3.35 for iOS sends Unencrypted Analytics.	2020-02-05	5	<a href="#">CVE-2020-8507</a> <a href="#">MISC</a> <a href="#">MISC</a>
the_global_tv_application -- the_global_tv_application	The Global TV application 2.3.2 for Android and 4.7.5 for iOS sends Unencrypted Analytics.	2020-02-05	4	<a href="#">CVE-2020-8506</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinywebgallery -- tinywebgallery	TinyWebGallery (TWG) 1.8.9 and earlier contains a full path disclosure vulnerability which allows remote attackers to obtain sensitive information through the parameters "twg_browserx" and "twg_browsery" in the page image.php.	2020-02-03	5	<a href="#">CVE-2013-2631</a> <a href="#">MISC</a> <a href="#">MISC</a>
torproject -- tor	The daemon in Tor through 0.4.1.8 and 0.4.2.x through 0.4.2.6 does not verify that a rendezvous node is known before attempting to connect to it, which might make it easier for remote attackers to discover circuit information.	2020-02-02	5	<a href="#">CVE-2020-8516</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_v1_120405	TP-LINK TL-WR1043ND V1_120405 devices contain an unspecified denial of service vulnerability.	2020-02-03	5	<a href="#">CVE-2013-2646</a> <a href="#">BID</a>
troglobit -- minisnmpd	An exploitable out-of-bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out-of-bounds memory read, which can result in the disclosure of sensitive information and denial of service. To trigger this vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.	2020-02-04	6.4	<a href="#">CVE-2020-6058</a> <a href="#">MISC</a>
troglobit -- minisnmpd	An exploitable out of bounds read vulnerability exists in the way MiniSNMPD version 1.4 parses incoming SNMP packets. A specially crafted SNMP request can trigger an out of bounds memory read which can result in sensitive information disclosure and Denial Of Service. In order to trigger this	2020-02-04	6.4	<a href="#">CVE-2020-6059</a> <a href="#">MISC</a>

	vulnerability, an attacker needs to send a specially crafted packet to the vulnerable server.			
typo3 -- typo3	The default configuration in the Dynamic Content Elements (dce) extension before 0.11.5 for TYPO3 allows remote attackers to obtain sensitive installation environment information by reading the update check request.	2020-02-03	<a href="#">5</a>	<a href="#">CVE-2014-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
uebimiau -- uebimiau	Cross-site Scripting (XSS) in UebiMiau 2.7.11 and earlier allows remote attackers to inject arbitrary web script or HTML via the "selected_theme" parameter in error.php.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2013-2622</a> <a href="#">XF</a> <a href="#">MISC</a>
unisys -- unisys_stealth	In Unisys Stealth (core) 3.4.108.0, 3.4.209.x, 4.0.027.x and 4.0.114, key material may be inadvertently logged if certain diagnostics are enabled.	2020-02-03	<a href="#">4.3</a>	<a href="#">CVE-2019-18193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vanilla_forums -- vanilla_forums	Vanilla Forums 2.0.17.1 through 2.0.17.5 has XSS in /vanilla/index.php via the p parameter.	2020-02-05	<a href="#">4.3</a>	<a href="#">CVE-2011-1009</a> <a href="#">MISC</a>
videolan -- vlc_media_player	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP Interface in VideoLAN VLC Media Player before 2.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) command parameter to requests/vlm_cmd.xml, (2) dir parameter to requests/browse.xml, or (3) URI in a request, which is returned in an error message through share/lua/intf/http.lua.	2020-01-31	<a href="#">4.3</a>	<a href="#">CVE-2013-3565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
web2project -- web2project	Multiple SQL injection vulnerabilities in web2Project 3.1 and earlier allow remote authenticated users to execute arbitrary SQL commands via the (1) search_string parameter in the contacts module to index.php or allow remote attackers to execute arbitrary SQL commands via the updatekey parameter to (2) do_updatecontact.php or (3) updatecontact.php.	2020-01-31	<a href="#">6.5</a>	<a href="#">CVE-2014-3119</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The BestWebSoft Htaccess plugin through 1.8.1 for WordPress allows wp-admin/admin.php?page=htaccess.php&action=htaccess_editor CSRF. The flag htccss_nonce_name passes the nonce to WordPress but the plugin does not validate it correctly, resulting in a wrong implementation of anti-CSRF protection. In this way, an attacker is able to direct the victim to a malicious web page that modifies the .htaccess file, and takes control of the website.	2020-02-06	<a href="#">6.8</a>	<a href="#">CVE-2020-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2020-</a>

wordpress -- wordpress	Stored XSS in the Strong Testimonials plugin before 2.40.1 for WordPress can result in an attacker performing malicious actions such as stealing session tokens.	2020-02-03	4.3	<a href="#">8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Auth0 wp-auth0 plugin 3.11.x before 3.11.3 for WordPress allows XSS via a wle parameter associated with wp-login.php.	2020-02-05	4.3	<a href="#">CVE-2019-20173</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zeuscart -- zeuscart	Multiple SQL injection vulnerabilities in ZeusCart 4.x.	2020-01-31	6.5	<a href="#">CVE-2014-3868</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - - remote_access_plus	An authorization issue was discovered in the Credential Manager feature in Zoho ManageEngine Remote Access Plus before 10.0.450. A user with the Guest role can extract the collection of all defined credentials of remote machines: the credential name, credential type, user name, domain/workgroup name, and description (but not the password).	2020-01-31	4	<a href="#">CVE-2020-8422</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS& Score	Source Patch Info
arctic_torrent -- arctic_torrent	A vulnerability exists in Arctic Torrent 1.4 via unspecified vectors in .torrent file handling, which could let a malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6309</a> <a href="#">MISC</a>
atmail -- atmail_webmail_server	Cross-site scripting (XSS) vulnerability in the administrative interface in Atmail Webmail Server 6.4 allows remote attackers to inject arbitrary web script or HTML via the Date field of an email.	2020-02-06	not yet calculated	<a href="#">CVE-2012-2593</a> <a href="#">MISC</a> <a href="#">MISC</a>
belkin -- n300_router	An Authentication Bypass vulnerability in Belkin N300 (F7D7301v1) router allows remote attackers to bypass authentication using "Javascript debugging."	2020-02-07	not yet calculated	<a href="#">CVE-2013-3091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
biscom -- biscom_secure_file_transfer	Biscom Secure File Transfer (SFT) before 5.1.1071 and 6.0.1005 allows Remote Code Execution on the server.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8796</a> <a href="#">MISC</a>



bludit -- bludit	ajax/profile-picture-upload.php in Bludit 3.10.0 allows authenticated users to change other users' profile pictures.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8811</a> <a href="#">MISC</a>
boonex -- dolphin	SQL injection vulnerability in Boonex Dolphin before 7.1.3 allows remote authenticated users to execute arbitrary SQL commands via the 'pathes' parameter in 'categories.php'.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3638</a> <a href="#">BID</a> <a href="#">XE</a>
bosch -- bvms_mob	Deserialization of Untrusted Data in the BVMS Mobile Video Service (BVMS MVS) allows an unauthenticated remote attacker to execute arbitrary code on the system. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000 and DIVAR IP 7000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6770</a> <a href="#">CONFIRM</a>
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) NoTouch deployment allows an unauthenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6768</a> <a href="#">CONFIRM</a>
bosch -- video_management_system	A path traversal vulnerability in the Bosch Video Management System (BVMS) FileTransferService allows an authenticated remote attacker to read arbitrary files from the Central Server. This affects Bosch BVMS versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch BVMS Viewer versions 10.0 <= 10.0.0.1225, 9.0 <= 9.0.0.827, 8.0 <= 8.0.329 and 7.5 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable BVMS version is installed.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6767</a> <a href="#">CONFIRM</a>
bosch -- video_streaming_gateway	Missing Authentication for Critical Function in the Bosch Video Streaming Gateway (VSG) allows an unauthenticated remote attacker to retrieve and set arbitrary configuration data of the Video Streaming Gateway. A successful attack can impact the confidentiality and availability of live and recorded video data of all cameras configured to be controlled by the VSG as well as the recording storage associated with the VSG. This affects Bosch Video Streaming Gateway versions 6.45 <= 6.45.08, 6.44 <= 6.44.022, 6.43 <= 6.43.0023 and 6.42.10 and older. This affects Bosch DIVAR IP 3000, DIVAR IP 7000 and DIVAR IP all-in-one 5000 if a vulnerable VSG version is installed with BVMS. This affects Bosch DIVAR IP 2000 <= 3.62.0019 and DIVAR IP 5000 <= 3.80.0039 if the corresponding port 8023 has been opened in the device's firewall.	2020-02-07	not yet calculated	<a href="#">CVE-2020-6769</a> <a href="#">CONFIRM</a>
broadcom -- multiple_devices	An issue was discovered on Broadcom Wi-Fi client devices. Specifically timed and handcrafted traffic can cause internal errors (related to state transitions) in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete	2020-02-05	not yet calculated	<a href="#">CVE-2019-15126</a>

	set of traffic, a different vulnerability than CVE-2019-9500, CVE-2019-9501, CVE-2019-9502, and CVE-2019-9503.			<a href="#">CONFIRM</a>
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. By supplying a vendor information element with a data length larger than 32 bytes, a heap buffer overflow is triggered in wlc_wpa_sup_eapol. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9501</a> <a href="#">MISC CERT. VN</a>
broadcom -- wi_wifi_driver	The Broadcom wl WiFi driver is vulnerable to a heap buffer overflow. If the vendor information element data length is larger than 164 bytes, a heap buffer overflow is triggered in wlc_wpa_plumb_gtk. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.	2020-02-03	not yet calculated	<a href="#">CVE-2019-9502</a> <a href="#">MISC CERT. VN</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 firmware L devices contain an information disclosure vulnerability which allows remote attackers to view private IP addresses and other sensitive information.	2020-02-04	not yet calculated	<a href="#">CVE-2013-2676</a> <a href="#">MISC XF BID</a>
brother -- mfc-9970cdw_device	Brother MFC-9970CDW 1.10 devices with Firmware L contain a Frameable response (Clickjacking) vulnerability which could allow remote attackers to obtain sensitive information.	2020-02-05	not yet calculated	<a href="#">CVE-2013-2675</a> <a href="#">MISC XF BID</a>
c-more -- touch_panel_driver	It is possible to unmask credentials and other sensitive information on ?unprotected? project files, which may allow an attacker to remotely access the C-More Touch Panels EA9 series: firmware versions prior to 6.53 and manipulate system configurations.	2020-02-05	not yet calculated	<a href="#">CVE-2020-6969</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport's lock file was in a world-writable director which allowed all users to prevent crash handling.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11485</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered Apport mishandled crash dumps originating from containers. This could be used by a local attacker to generate a crash report for a privileged process that is readable by an unprivileged user.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11483</a> <a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered that apport would read a user-supplied configuration file with elevated privileges. By replacing the file with a symbolic link, a user could get apport to read any file on the system as root, with unknown consequences.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11481</a> <a href="#">MISC</a>
canonical -- ubuntu	Sander Bos discovered a time of check to time of use (TOCTTOU) vulnerability in apport that allowed a user to cause core files to be written in arbitrary directories.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11482</a> <a href="#">MISC</a>

				<a href="#">MISC</a>
canonical -- ubuntu	Kevin Backhouse discovered an integer overflow in bson_ensure_space, as used in whoopsie.	2020-02-08	not yet calculated	<a href="#">CVE-2019-11484</a> <a href="#">MISC</a> <a href="#">MISC</a>
ceph -- rgw_beast	A flaw was found in the way the Ceph RGW Beast front-end handles unexpected disconnects. An authenticated attacker can abuse this flaw by making multiple disconnect attempts resulting in a permanent leak of a socket connection by radosgw. This flaw could lead to a denial of service condition by pile up of CLOSE_WAIT sockets, eventually leading to the exhaustion of available resources, preventing legitimate users from connecting to the system.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1700</a> <a href="#">CLASSIFIED</a> <a href="#">CONFIRM</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.2 alpha 1 and 5.2 alpha 2 uses weak session IDs generated based on OS time, which allows remote attackers to hijack arbitrary sessions via a brute force attack. NOTE: CVE-2014-10300 and CVE-2014-10400 were SPLIT from this ID.	2020-02-06	not yet calculated	<a href="#">CVE-2014-2875</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.0.x uses sequential session IDs, which makes it easier for remote attackers to predict the session ID and hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10400</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cgilua -- cgilua	The session.lua library in CGI Lua 5.1.x uses the same ID for each session, which allows remote attackers to hijack arbitrary sessions. NOTE: this vulnerability was SPLIT from CVE-2014-2875.	2020-02-06	not yet calculated	<a href="#">CVE-2014-10399</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chamilo -- chamilo_Im	Cross-site scripting (XSS) vulnerability in main/dropbox/index.php in Chamilo LMS before 1.8.8.6 allows remote attackers to inject arbitrary web script or HTML via the category_name parameter in an addsentcategory action.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
changing_infrastructure -- servisign	A Remote Code Execution(RCE) vulnerability exists in some designated applications in ServiSign security plugin, as long as the interface is captured, attackers are able to launch RCE and executes arbitrary command on target system via malicious crafted scripts.	2020-02-03	not yet calculated	<a href="#">CVE-2020-3925</a> <a href="#">CONFIRM</a>
cisco -- application	Cisco ACE 4.3(6) allows log retention DoS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-1202</a> <a href="#">MISC</a>
cisco -- cisco_discovery_protocol	A vulnerability in the Cisco Discovery Protocol implementation for Cisco FXOS Software, Cisco IOS XR Software, and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to a missing check when the affected software processes Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by	2020-02-05	not yet	<a href="#">CVE-2020-3120</a>

	<p>sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to exhaust system memory, causing the device to reload. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).</p>		calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	<p>A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability is due to improper validation of string input from certain fields in Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).</p>	2020-02-05	not yet calculated	<a href="#">CVE-2020-3118</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- cisco_discovery_protocol	<p>A vulnerability in the Cisco Discovery Protocol implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device. The vulnerability exists because the Cisco Discovery Protocol parser does not properly validate input for certain fields in a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. An successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).</p>	2020-02-05	not yet calculated	<a href="#">CVE-2020-3119</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- linksys_wrt110	<p>Cross-site request forgery (CSRF) vulnerability in Cisco Linksys WRT110 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors.</p>	2020-02-06	not yet calculated	<a href="#">CVE-2013-3568</a> <a href="#">EXPLOIT-DATA</a> <a href="#">BID</a> <a href="#">XF</a>
clamav -- clam_anti_virus	<p>A vulnerability in the Data-Loss-Prevention (DLP) module in Clam AntiVirus (ClamAV) Software versions 0.102.1 and 0.102.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to an out-of-bounds read affecting users that have enabled the optional DLP feature. An attacker could exploit this vulnerability by sending a crafted email file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.</p>	2020-02-05	not yet calculated	<a href="#">CVE-2020-3123</a> <a href="#">CISCO</a>
corsair -- corsair_icue	<p>The CorsairLLAccess64.sys and CorsairLLAccess32.sys drivers in CORSAIR iCUE before 3.25.60 allow local non-privileged users (including low-integrity level processes) to</p>	2020-02-07	not yet	<a href="#">CVE-2020-8808</a>

	read and write to arbitrary physical memory locations, and consequently gain NT AUTHORITY\SYSTEM privileges, via a function call such as MmMapIoSpace.		calculated	<a href="#">CVE-2019-10780</a> <a href="#">MISC</a>
d-link --dir865l_devices	D-Link DIR865L v1.03 suffers from an "Unauthenticated Hardware Linking" vulnerability.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3096</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dd-wrt --dd-wrt	Command Injection vulnerability exists via a CSRF in DD-WRT 24-sp2 from specially crafted configuration values containing shell meta-characters, which could let a remote malicious user cause a Denial of Service.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6297</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dedicated --multiple_dvr_products	Dedicated Micros DV-IP Express, SD Advanced, SD, EcoSense, and DS2 devices rely on a GUI warning to help ensure that the administrator configures login credentials, which makes it easier for remote attackers to obtain access by leveraging situations in which this warning was not needed. NOTE: the vendor states "The user is presented with clear warnings on the GUI that they should set usernames and passwords."	2020-02-06	not yet calculated	<a href="#">CVE-2015-2909</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell --dmc_isilon_ones	Dell EMC Isilon OneFS versions 8.1.2, 8.1.0.4, 8.1.0.3, and 8.0.0.7 contain a vulnerability in some configurations. An attacker may exploit this vulnerability to gain access to restricted files. The non-RAN HTTP and WebDAV file-serving components have a vulnerability wherein when either are enabled, and Basic Authentication is enabled for either or both components, files are accessible without authentication.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5318</a> <a href="#">MISC</a>
dell --emc_ecs	Dell EMC ECS versions prior to 3.4.0.1 contain an XSS vulnerability. A remote authenticated malicious user could exploit this vulnerability to store malicious HTML or JavaScript code in a trusted application data store. When victim users access the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5317</a> <a href="#">MISC</a>
dell --multiple_products	Dell EMC Unity, Dell EMC Unity XT, and Dell EMC UnityVSA versions prior to 5.0.2.0.5.009 contain a Denial of Service vulnerability on NAS Server SSH implementation that is used to provide SFTP service on a NAS server. A remote unauthenticated attacker may potentially exploit this vulnerability and cause a Denial of Service (Storage Processor Panic) by sending an out of order SSH protocol sequence.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5319</a> <a href="#">MISC</a>
den_norskenturistoring --im-metadata	im-metadata through 3.0.1 allows remote attackers to execute arbitrary commands via the "exec" argument. It is possible to inject arbitrary commands as part of the metadata options which is given to the "exec" function.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10788</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
den_norskenturistoring --im-metadata	im-metadata through 2.3.2 allows remote attackers to execute arbitrary commands via the "exec" argument. The cmd	2020-02-04	not yet	<a href="#">CVE-2019-10787</a>



resize	argument used within index.js, can be controlled by user without any sanitization.		calculated	<a href="#">CONFIRM</a> <a href="#">CVE-2014-5278</a> <a href="#">MISC</a>
docker -- docker	A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container IDs.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5278</a> <a href="#">MISC</a> <a href="#">MISC</a>
drupal -- drupal	The Basic webmail module 6.x-1.x before 6.x-1.2 for Drupal allows remote authenticated users with the "access basic_webmail" permission to read arbitrary users' email addresses.	2020-02-08	not yet calculated	<a href="#">CVE-2012-5570</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The installation uses the same API key (hardcoded as EONAPI_KEY in include/api_functions.php for API version 2.4.2) by default for all installations, hence allowing an attacker to calculate/guess the admin access token.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8657</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The EyesOfNetwork API 2.4.2 is prone to SQL injection, allowing an unauthenticated attacker to perform various tasks such as authentication bypass via the username field to getApiKey in include/api_functions.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8656</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. An authenticated web user with sufficient privileges could abuse the AutoDiscovery module to run arbitrary OS commands via the /module/module_frame/index.php autodiscovery.php target field.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8654</a> <a href="#">MISC</a>
eyesofnetwork - eyesofnetwork	An issue was discovered in EyesOfNetwork 5.3. The sudoers configuration is prone to a privilege escalation vulnerability, allowing the apache user to run arbitrary commands as root via a crafted NSE script for nmap 7.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8655</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 15.0.0-15.0.1.1, 14.1.0-14.1.2.2, 14.0.0-14.0.1, 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.6.0-11.6.5.1, the tmm crashes under certain circumstances when using the connector profile if a specific sequence of connections are made.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5854</a> <a href="#">CONFIRM</a>
flowplayer -- flowplayer	Cross-site scripting (XSS) vulnerability in Flowplayer Flash 3.2.7 through 3.2.16, as used in the News system (news) extension for TYPO3 and Mahara, allows remote attackers to inject arbitrary web script or HTML via the plugin configuration directive in a reference to an external domain plugin.	2020-02-08	not yet calculated	<a href="#">CVE-2011-3642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2014-</a>

fork_cms - - fork_cms	Cross-site scripting (XSS) vulnerability in the loadForm function in Frontend/Modules/Search/Actions/Index.php in Fork CMS before 3.8.4 allows remote attackers to inject arbitrary web script or HTML via the q_widget parameter to en/search.	2020-02-08	not yet calculated	<a href="#">9470</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>	
fortinet -- forticlient_for_linux	A Denial of service (DoS) vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted IPC client requests to the fctschd process due the nanomsg not been correctly validated.	2020-02-06	not yet calculated	<a href="#">CVE-2019-16152</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A stack buffer overflow vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to cause FortiClient processes running under root privilege crashes via sending specially crafted "StartAvCustomScan" type IPC client requests to the fctschd process due the argv data not been well sanitized.	2020-02-06	not yet calculated	<a href="#">CVE-2019-17652</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow an user with low privilege to run system commands under root privilege via injecting specially crafted "ExportLogs" type IPC client requests to the fctschd process.	2020-02-06	not yet calculated	<a href="#">CVE-2019-15711</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
fortinet -- forticlient_for_linux	A privilege escalation vulnerability in FortiClient for Linux 6.2.1 and below may allow a user with low privilege to overwrite system files as root with arbitrary content through system backup file via specially crafted "BackupConfig" type IPC client requests to the fctschd process. Further more, FortiClient for Linux 6.2.2 and below allow low privilege user write the system backup file under root privilege through GUI thus can cause root system file overwrite.	2020-02-07	not yet calculated	<a href="#">CVE-2019-16155</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>	
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8773.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13333</a> <a href="#">MISC</a>	
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8776.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17136</a> <a href="#">MISC</a>	
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this				

foxit -- phantompdf	vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8774.	2020-02-08	not yet calculated	<a href="#">CVE-2019-13334</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8775.	2020-02-08	not yet calculated	<a href="#">CVE-2019-17135</a> MISC
fujitsu -- multiple_products	The Fujitsu TLS library allows a man-in-the-middle attack. This affects Interstage Application Development Cycle Manager V10 and other versions, Interstage Application Server V12 and other versions, Interstage Business Application Manager V2 and other versions, Interstage Information Integrator V11 and other versions, Interstage Job Workload Server V8, Interstage List Works V10 and other versions, Interstage Studio V12 and other versions, Interstage Web Server Express V11, Linkexpress V5, Safeauthor V3, ServerView Resource Orchestrator V3, Systemwalker Cloud Business Service Management V1, Systemwalker Desktop Keeper V15, Systemwalker Desktop Patrol V15, Systemwalker IT Change Manager V14, Systemwalker Operation Manager V16 and other versions, Systemwalker Runbook Automation V15 and other versions, Systemwalker Security Control V1, and Systemwalker Software Configuration Manager V15.	2020-02-07	not yet calculated	<a href="#">CVE-2019-13163</a> CONFIRM
gnome -- libsvg	In xml.rs in GNOME libsvg before 2.46.2, a crafted SVG file with nested patterns can cause denial of service when passed to the library for processing. The attacker constructs pattern elements so that the number of final rendered objects grows exponentially.	2020-02-02	not yet calculated	<a href="#">CVE-2019-20446</a> MISC
gnome -- evolution_and_evolution_data_server	The <code>gpg_ctx_add_recipient</code> function in <code>camel/camel-gpg-context.c</code> in GNOME Evolution 3.8.4 and earlier and Evolution Data Server 3.9.5 and earlier does not properly select the GPG key to use for email encryption, which might cause the email to be encrypted with the wrong key and allow remote attackers to obtain sensitive information.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4166</a> CONFIRM MISC CONFIRM CONFIRM
golang -- go	The <code>net/http</code> library in <code>net/http/transfer.go</code> in Go before 1.4.3 does not properly parse HTTP headers, which allows remote attackers to conduct HTTP request smuggling attacks via a request that contains <code>Content-Length</code> and <code>Transfer-Encoding</code> header fields.	2020-02-08	not yet calculated	<a href="#">CVE-2015-5741</a> MISC MISC MISC MISC MISC

				<a href="#">MISC</a>
google -- android	A Code Execution vulnerability exists in Android prior to 4.4.0 related to the addJavascriptInterface method and the accessibility and accessibilityTraversal objects, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-7224</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Google Chrome before 3.0 does not properly handle XML documents, which allows remote attackers to obtain sensitive information via a crafted web site.	2020-02-06	not yet calculated	<a href="#">CVE-2010-3917</a> <a href="#">MISC</a> <a href="#">MISC</a>
hardcoreview - - hardcoreview	A vulnerability exists in HCView (aka Hardcoreview) 1.4 due to a write access violation with a GIF file.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6306</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- sitescope	An Information Disclosure vulnerability exists in HP SiteScope 11.2 and 11.3 on Windows, Linux and Solaris, HP Asset Manager 9.30 through 9.32, 9.40 through 9.41, 9.50, and Asset Manager Cloudsystem Chargeback 9.40, which could let a remote malicious user obtain sensitive information. This is the TLS vulnerability known as the RC4 cipher Bar Mitzvah vulnerability.	2020-02-04	not yet calculated	<a href="#">CVE-2015-2802</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- cloud_automation_manager	IBM Cloud Automation Manager 3.2.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http://link to the user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 168644.	2020-02-05	not yet calculated	<a href="#">CVE-2019-4616</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 contains hard-coded credentials, such as a password or cryptographic key, which can be used to bypass authentication, inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 171511.	2020-02-04	not yet calculated	<a href="#">CVE-2019-4675</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7523</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	coders/meta.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2020-02-06	not yet calculated	<a href="#">CVE-2016-7524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-</a>

imagemagick - imagemagick	Stack-based buffer overflow in the WritePSDImage function in coders/psd.c in ImageMagick, possibly 6.8.8-5, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-1947.	2020-02-06	not yet calculated	<a href="#">2014-2030 CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
imagemagick - imagemagick	Buffer overflow in the DecodePSDPixels function in coders/psd.c in ImageMagick before 6.8.8-5 might allow remote attackers to execute arbitrary code via a crafted PSD image, involving the L%06ld string, a different vulnerability than CVE-2014-2030.	2020-02-06	not yet calculated	<a href="#">CVE-2014-1958 CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ispconfig - ispconfig	ISPConfig 3.0.5.2 has Arbitrary PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-3629 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jpegsnoop - jpegsnoop	A vulnerability exists in JPEGsnoop 1.5.2 due to an unspecified issue in JPEG file handling, which could let a malicious user execute arbitrary code	2020-02-06	not yet calculated	<a href="#">CVE-2012-6307 MISC</a> <a href="#">MISC</a>
kemp -- load_master	A CSRF Vulnerability exists in Kemp Load Master before 7.0-18a via unspecified vectors in administrative pages.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5288 MISC</a> <a href="#">MISC</a>
konqueror - konqueror	The CSS parser (khtml/css/cssparser.cpp) in Konqueror in KDE 4.7.3 allows remote attackers to cause a denial of service (crash) and possibly read memory via a crafted font face source, related to "type confusion."	2020-02-08	not yet calculated	<a href="#">CVE-2012-4512 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linksys -- wrt310n_wireless_router	Linksys WRT310Nv2 2.0.0.1 is vulnerable to XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-3067 MISC</a> <a href="#">MISC</a>



				<a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintUpdate.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1567</a> <a href="#">MISC</a>
linuxmint - - linuxmint	LinuxMint as of 2012-03-19 has temporary file creation vulnerabilities in mintNanny.	2020-02-07	not yet calculated	<a href="#">CVE-2012-1566</a> <a href="#">MISC</a>
mariadb -- mariadb	mysql_install_db in MariaDB 10.4.7 through 10.4.11 allows privilege escalation from the mysql user account to root because chown and chmod are performed unsafely, as demonstrated by a symlink attack on a chmod 04755 of auth_pam_tool_dir/auth_pam_tool. NOTE: this does not affect the Oracle MySQL product, which implements mysql_install_db differently.	2020-02-04	not yet calculated	<a href="#">CVE-2020-7221</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mcabber - - mcabber	MCabber before 1.0.4 is vulnerable to roster push attacks, which allows remote attackers to intercept communications, or add themselves as an entity on a 3rd party's roster as another user, which will also garner associated privileges, via crafted XMPP packets.	2020-02-06	not yet calculated	<a href="#">CVE-2016-9928</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mediawiki - mediawiki	MediaWiki before 1.18.5, and 1.19.x before 1.19.2 saves passwords in the local database, (1) which could make it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack or, (2) when an authentication plugin returns a false in the strict function, could allow remote attackers to use old passwords for non-existing accounts in an external authentication system via unspecified vectors.	2020-02-08	not yet calculated	<a href="#">CVE-2012-4381</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki - mediawiki	The CentralNotice extension for MediaWiki before 1.19.9, 1.20.x before 1.20.8, and 1.21.x before 1.21.3 sets the Cache-Control header to cache session cookies when a user is autocreated, which allows remote attackers to authenticate as the created user.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4572</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mikrotik -- winbox	MikroTik WinBox before 3.21 is vulnerable to a path traversal vulnerability that allows creation of arbitrary files wherever WinBox has write permissions. WinBox is vulnerable to this attack if it connects to a malicious endpoint or if an attacker mounts a man in the middle attack.	2020-02-06	not yet calculated	<a href="#">CVE-2020-5720</a> <a href="#">MISC</a>
	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier,			

multiple_vendors - multiple_products	Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to execute arbitrary code via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5628</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (process outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5627</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
multiple_vendors - multiple_products	Stack-based buffer overflow in Yokogawa CENTUM CS 1000 R3.08.70 and earlier, CENTUM CS 3000 R3.09.50 and earlier, CENTUM CS 3000 Entry R3.09.50 and earlier, CENTUM VP R5.04.20 and earlier, CENTUM VP Entry R5.04.20 and earlier, ProSafe-RS R3.02.10 and earlier, Exaopc R3.72.00 and earlier, Exaquantum R2.85.00 and earlier, Exaquantum/Batch R2.50.30 and earlier, Exapilot R3.96.10 and earlier, Exaplog R3.40.00 and earlier, Exasmoc R4.03.20 and earlier, Exarqe R4.03.20 and earlier, Field Wireless Device OPC Server R2.01.02 and earlier, PRM R3.12.00 and earlier, STARDOM VDS R7.30.01 and earlier, STARDOM OPC Server for Windows R3.40 and earlier, FAST/TOOLS R10.01 and earlier, B/M9000CS R5.05.01 and earlier, B/M9000 VP R7.03.04 and earlier, and FieldMate R1.01 or R1.02 allows remote attackers to cause a denial of service (network-communications outage) via a crafted packet.	2020-02-05	not yet calculated	<a href="#">CVE-2015-5626</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple SQL injection vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to execute arbitrary SQL commands via the (1) ctrl, (2) h____%2427, (3) h____%2439, (4) param0, (5) param1, (6) param2, (7) param3, (8) param4, (9) filter_INSERT_COUNT, (10) filter_MINOR_FALLOUT, (11) filter_UPDATE_COUNT, (12) sort, or (13) sessid parameter.	2020-02-08	not yet calculated	<a href="#">CVE-2015-3423</a> <a href="#">MISC</a> <a href="#">MISC</a>
netcracker - resource_management_system	Multiple cross-site scripting (XSS) vulnerabilities in NetCracker Resource Management System before 8.2 allow remote authenticated users to inject arbitrary web script or HTML via the (1) ctrl, (2) t90001_0_theform_selection, (3) _scroll, (4) tableName, (5) parent, (6) circuit, (7) return, (8)	2020-02-08	not yet calculated	<a href="#">CVE-2015-2207</a> <a href="#">MISC</a> <a href="#">MISC</a>

	xname, or (9) mpTransactionId parameter.			
netgear -- wgr614_wireless_router	An Authentication vulnerability exists in NETGEAR WGR614 v7 and v9 due to a hardcoded credential used for serial programming, a related issue to CVE-2006-1002.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6340</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netgear -- wgr614_wireless_router	An Information Disclosure vulnerability exists in the my config file in NETGEAR WGR614 v7 and v9, which could let a malicious user recover all previously used passwords on the device, for both the control panel and WEP/WPA/WPA2, in plaintext. This is a different issue than CVE-2012-6340.	2020-02-06	not yet calculated	<a href="#">CVE-2012-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- wf2419_router	Netis WF2419 is vulnerable to authenticated Remote Code Execution (RCE) as root through the router Web management page. The vulnerability has been found in firmware version V1.2.31805 and V2.2.36123. After one is connected to this page, it is possible to execute system commands as root through the tracert diagnostic tool because of lack of user input sanitizing.	2020-02-07	not yet calculated	<a href="#">CVE-2019-19356</a> <a href="#">MISC</a>
network-manager - network-manager	network-manager through 1.0.2 allows remote attackers to execute arbitrary commands via the "execSync()" argument.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10786</a> <a href="#">MISC</a>
nextcloud -- circles	Improper authorization in the Circles app 0.17.7 causes retaining access when an email address was removed from a circle.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15610</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	A wrong check for the system time in the Android App 3.9.0 causes a bypass of the lock protection when changing the time of the system to the past.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15615</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android	Not strictly enough sanitization in the Nextcloud Android app 3.6.0 allowed an attacker to get content information from protected tables when using custom queries.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15622</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_ios	Violation of Secure Design Principles in the iOS App 2.23.0 causes the app to leak its login and token to other Nextcloud services when search e.g. for federated users or registering for push notifications.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15611</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_ios	Missing sanitization in the iOS App 2.24.4 causes an XSS when opening malicious HTML files.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15614</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper permissions preservation in Nextcloud Server 16.0.1 causes sharees to be able to reshare with write permissions when sharing the mount point of a share they received, as a public link.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15621</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud				<a href="#">CVE-</a>

-- nextcloud_server	Dangling remote share attempts in Nextcloud 16 allow a DNS pollution when running long.	2020-02-04	not yet calculated	<a href="#">2019-15616</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 15.0.2 causes pending 2FA logins to not be correctly expired when the password of the user is reset.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15612</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A bug in Nextcloud Server 17.0.1 causes the workflow rules to depend their behaviour on the file extension when checking file mimetypes.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15613</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A missing check in Nextcloud Server 17.0.0 allowed an attacker to set up a new second factor when trying to login.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15617</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	Improper Input Validation in Nextcloud Server 15.0.7 allows server admins to create users with IDs of system folders.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15624</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server and Nextcloud Desktop	Improper neutralization of file names, conversation names and board names in Nextcloud Server 16.0.3, Nextcloud Talk 6.0.3 and Nextcloud Deck 0.6.5 causes an XSS when linking them with each others in a project.	2020-02-04	not yet calculated	<a href="#">CVE-2019-15619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A bug in Nextcloud Server 14.0.4 could expose more data in reshared link shares than intended by the sharer.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8121</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	An authenticated server-side request forgery in Nextcloud server 16.0.1 allowed to detect local and remote services when adding a new subscription in the calendar application.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8118</a> <a href="#">MISC</a> <a href="#">MISC</a>
nextcloud - nextcloud_server	A missing check in Nextcloud Server 14.0.3 could give recipient the possibility to extend the expiration date of a share they received.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8122</a> <a href="#">MISC</a> <a href="#">MISC</a>
nghttp2 -- nghttp2	nghttp2 before 1.7.1 allows remote attackers to cause a denial of service (memory exhaustion).	2020-02-06	not yet calculated	<a href="#">CVE-2016-1544</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

node.js -- node.js	Improper Certificate Validation in Node.js 10, 12, and 13 causes the process to abort when sending a crafted X.509 certificate	2020-02-07	not yet calculated	<a href="#">CVE-2019-15604</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	Including trailing white space in HTTP header values in Node.js 10, 12, and 13 causes bypass of authorization based on header value comparisons	2020-02-07	not yet calculated	<a href="#">CVE-2019-15606</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
node.js -- node.js	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed	2020-02-07	not yet calculated	<a href="#">CVE-2019-15605</a> <a href="#">MISC</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a>
nuxeo -- nuxeo_platform	RichFaces implementation in Nuxeo Platform 5.6.0 before HF27 and 5.8.0 before HF-01 does not restrict the classes for which deserialization methods can be called, which allows remote attackers to execute arbitrary code via crafted serialized data. NOTE: this vulnerability may overlap CVE-2013-2165.	2020-02-06	not yet calculated	<a href="#">CVE-2013-4521</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
nw.js -- nw.js	A vulnerability exists in nw.js before 0.11.3 when calling nw methods from normal frames, which has an unspecified impact.	2020-02-07	not yet calculated	<a href="#">CVE-2014-9530</a> <a href="#">CONFIRM</a>
omniauth-weibo-oauth2_gem -- omniauth-weibo-oauth2_gem_for_ruby_on_ra	The omniauth-weibo-oauth2 gem 0.4.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. Versions through 0.4.5, and 0.5.1 and later, are unaffected.	2020-02-07	not yet calculated	<a href="#">CVE-2019-17268</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
open-school -- open-school_community_edition	Multiple cross-site scripting (XSS) vulnerabilities in Open-School Community Edition 2.2 allow remote attackers to inject arbitrary web script or HTML via the YII_CSRF_TOKEN HTTP cookie or the StudentDocument, StudentCategories, StudentPreviousDatas parameters to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9126</a> <a href="#">MISC</a>
open-school -- open-school_community_edition	Open-School Community Edition 2.2 does not properly restrict access to the export functionality, which allows remote authenticated users to obtain sensitive information via the r parameter with the value export to index.php.	2020-02-08	not yet calculated	<a href="#">CVE-2014-9127</a> <a href="#">MISC</a>
openfiler - - openfiler	Cross-site scripting (XSS) vulnerability in admin/system.html in Openfiler 2.3 allows remote attackers to inject arbitrary web script or HTML via the device parameter.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1086</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openshift-enterprise -	It has been found in openshift-enterprise version 3.11 and all openshift-enterprise versions from 4.1 to, including 4.3, that multiple containers modify the permissions of /etc/passwd to		not	<a href="#">CVE-2020-</a>



openshift-enterprise	make them modifiable by users other than root. An attacker with access to the running container can exploit this to modify /etc/passwd to add a user and escalate their privileges. This CVE is specific to the openshift/mysql-apb.	2020-02-07	yet calculated	<a href="#">1708 CONFIRM</a>
openvas -- openvas_manager	OpenVAS Manager v2.0.3 allows plugin remote code execution.	2020-02-06	not yet calculated	<a href="#">CVE-2011-1597 MISC</a>
opopensoc - opopensoc_plugin	alplugin - opOpenSocialPlugin 0.8.2.1, > 0.9.9.2, 0.9.13, 1.2.6: Multiple External Entity Injection Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4335 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Starting from the apache user account, it is possible to perform privilege escalation through the lack of correct configuration in the server's sudoers file, which by default allows the execution of programs (e.g. nmap) without the need for a password with sudo.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7954 MISC</a> <a href="#">MISC</a>
opservices - opmon	An issue was discovered in OpServices OpMon 9.3.2. Without authentication, it is possible to read server files (e.g., /etc/passwd) due to the use of the nmap -iL (aka input file) option.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7953 MISC</a> <a href="#">MISC</a>
opservices - opservices_plugins	An issue was discovered in OpServices OpMon 9.3.2 that allows Remote Code Execution .	2020-02-06	not yet calculated	<a href="#">CVE-2020-8636 MISC</a> <a href="#">MISC</a>
opwebapiplugin - opwebapiplugin	ugin - opWebAPIPlugin 0.5.1, 0.4.0, and 0.1.0: XXE Vulnerabilities	2020-02-07	not yet calculated	<a href="#">CVE-2013-4334 MISC</a> <a href="#">MISC</a>
otrs -- otrs	The external frontend system uses numerous background calls to the backend. Each background request is treated as user activity so the SessionMaxIdleTime will not be reached. This issue affects: OTRS 7.0.x version 7.0.14 and prior versions.	2020-02-07	not yet calculated	<a href="#">CVE-2020-1768 CONFIRM</a>
percona -- percona_monitoring_and_management	pmm-server in Percona Monitoring and Management (PMM) 2.2.x before 2.2.1 allows unauthenticated denial of service.	2020-02-06	not yet calculated	<a href="#">CVE-2020-7920 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
phppgadmin -- phppgadmin	phppgadmin through 7.12.1 allows sensitive actions to be performed without validating that the request originated from the application. One such area, "database.php" does not verify the source of an HTTP request. This can be leveraged by a remote attacker to trick a logged-in administrator to visit a malicious page with a CSRF exploit and execute arbitrary system commands on the server.	2020-02-04	not yet calculated	<a href="#">CVE-2019-10784 MISC</a>
projectpier -			not	<a href="#">CVE-</a>

- projectpier	ProjectPier 0.8.8 has stored XSS	2020-02-07	yet calculated	<a href="#">2013-3635 MISC</a>	
projectpier - projectpier	ProjectPier 0.8.8 has a Remote Information Disclosure Weakness because of the lack of the HttpOnly cookie flag	2020-02-07	not yet calculated	<a href="#">CVE-2013-3636 MISC</a>	
projectpier - projectpier	ProjectPier 0.8.8 does not use the Secure flag for cookies	2020-02-07	not yet calculated	<a href="#">CVE-2013-3637 MISC</a>	
qemu -- qemu	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses snprintf return values, leading to a buffer overflow in later code.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8608 MISC</a>	
qualcomm -- multiple_snapdragon_products	Possible use after free issue while CRM is accessing the link pointer from device private data due to lack of resource protection in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, MDM9206, MDM9207C, MDM9607, QCS605, SDM429W, SDX24, SM8150, SXR1130	2020-02-07	not yet calculated	<a href="#">CVE-2019-14088 MISC</a>	CONFIRM
railo -- railo	A File Inclusion vulnerability exists in Railo 4.2.1 and earlier via a specially-crafted URL request to the thumbnail.cfm to specify a malicious PNG file, which could let a remote malicious user obtain sensitive information or execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5468 MISC</a>	
revive -- adserver	A reflected XSS vulnerability has been discovered in the publicly accessible afr.php delivery script of Revive Adserver <= 5.0.3 by Jacopo Tediosi. There are currently no known exploits: the session identifier cannot be accessed as it is stored in an http-only cookie as of v3.2.2. On older versions, however, under specific circumstances, it could be possible to steal the session identifier and gain access to the admin interface. The query string sent to the www/delivery/afr.php script was printed back without proper escaping in a JavaScript context, allowing an attacker to execute arbitrary JS code on the browser of the victim.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8115 MISC</a>	
samsung - multiple_mobile_devices	On Samsung mobile devices with O(8.0) and P(9.0) software and an Exynos 8895 chipset, RKP (aka the Samsung Hypervisor-L2 implementation) allows arbitrary memory write operations. The Samsung ID is SVE-2019-16265.	2020-02-04	not yet calculated	<a href="#">CVE-2019-19273 MISC</a>	CONFIRM
schmid -- zi_620_v400_090_routers	Schmid ZI 620 V400 VPN 090 routers allow an attacker to execute OS commands as root via shell metacharacters to an entry on the SSH subcommand menu, as demonstrated by ping.	2020-02-06	not yet calculated	<a href="#">CVE-2020-6760 MISC</a>	
				<a href="#">CVE-</a>	

simple_machines - - simple_machines Forum	File Disclosure in SMF (SimpleMachines Forum) <= 2.0.3: simple_machines Forum can read files such as the database config.	2020-02-07	not yet calculated	<a href="#">2013-0192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplejobscript -- - simplejobscript.com	An issue was discovered in Simplejobscript.com SJS through 1.66. There is an unauthenticated SQL injection via the job applications search function. The vulnerable parameter is job_id. The function is getJobApplicationsByJobId(). The file is _lib/class.JobApplication.php.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8645</a> <a href="#">MISC</a>
smoothwall -- - smoothwall Express3	- A cross-site scripting (XSS) vulnerability in Smoothwall Express3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1084</a> <a href="#">MISC</a>
smoothwall -- - smoothwall Express	- CSRF vulnerability in Smoothwall Express 3.	2020-02-07	not yet calculated	<a href="#">CVE-2011-1085</a> <a href="#">MISC</a>
sphider -- - sphider search engine	A vulnerability exists in Sphider Search Engine prior to 1.3.6 where the engine calls in admin/spiderfuncs.php, which could let a remote malicious user execute arbitrary code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5087</a> <a href="#">MISC</a>
status2k -- - status2k	A vulnerability exists in Status2K 2.5 Server Monitoring Software via the multies parameter to includes/functions.php, which could let a malicious user execute arbitrary PHP code.	2020-02-07	not yet calculated	<a href="#">CVE-2014-5091</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
statusnet -- - statusnet	statusnet through 2010 allows attackers to spoof syslog messages via newline injection attacks.	2020-02-07	not yet calculated	<a href="#">CVE-2010-4658</a> <a href="#">MISC</a> <a href="#">MISC</a>
synaptive -- - medical_clearcanvas_image_server	Synaptive Medical ClearCanvas ImageServer 3.0 Alpha allows XSS (and HTML injection) via the Default.aspx UserName parameter. NOTE: the issues/227 reference does not imply that the affected product can be downloaded from GitHub. It was simply a convenient location for a public bug report.	2020-02-07	not yet calculated	<a href="#">CVE-2020-8788</a> <a href="#">MISC</a>
teamviewer -- - teamviewer	TeamViewer Desktop through 14.7.1965 allows a bypass of remote-login access control because the same key is used for different customers' installations. It used a shared AES key for all installations since at least as far back as v7.0.43148, and used it for at least OptionsPasswordAES in the current version of the product. If an attacker were to know this key, they could decrypt protect information stored in the registry or configuration files of TeamViewer. With versions before v9.x , this allowed for attackers to decrypt the Unattended Access password to the system (which allows for remote login to the system as well as headless file browsing). The latest version still uses the same key for OptionPasswordAES but appears to have changed how the	2020-02-07	not yet calculated	<a href="#">CVE-2019-18988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	Unattended Access password is stored. While in most cases an attacker requires an existing session on a system, if the registry/configuration keys were stored off of the machine (such as in a file share or online), an attacker could then decrypt the required password to login to the system.			
tianocore - - edk2	Buffer overflow in the Reclaim function in Tianocore EDK2 before SVN 16280 allows physically proximate attackers to gain privileges via a long variable name.	2020-02-06	not yet calculated	<a href="#">CVE-2014-8271</a> <a href="#">MISC</a> <a href="#">MISC</a>
troglobit -- minisnmpd	A stack buffer overflow vulnerability exists in the way MiniSNMPD version 1.4 handles multiple connections. A specially timed sequence of SNMP connections can trigger a stack overflow, resulting in a denial of service. To trigger this vulnerability, an attacker needs to simply initiate multiple connections to the server.	2020-02-04	not yet calculated	<a href="#">CVE-2020-6060</a> <a href="#">MISC</a>
ubiquiti_networks - unifi_controller	Multiple cross-site request forgery (CSRF) vulnerabilities in Ubiquiti Networks UniFi Controller before 3.2.1 allow remote attackers to hijack the authentication of administrators for requests that (1) create a new admin user via a request to api/add/admin; (2) have unspecified impact via a request to api/add/wlanconf; change the guest (3) password, (4) authentication method, or (5) restricted subnets via a request to api/set/setting/guest_access; (6) block, (7) unblock, or (8) reconnect users by MAC address via a request to api/cmd/stamgr; change the syslog (9) server or (10) port via a request to api/set/setting/rsyslogd; (11) have unspecified impact via a request to api/set/setting/smtp; change the syslog (12) server, (13) port, or (14) authentication settings via a request to api/cmd/cfgmgr; or (15) change the Unifi Controller name via a request to api/set/setting/identity.	2020-02-08	not yet calculated	<a href="#">CVE-2014-2225</a> <a href="#">MISC</a> <a href="#">MISC</a>
ui -- edgeswitch	A privilege escalation in the EdgeSwitch prior to version 1.7.1, an CGI script don't fully sanitize the user input resulting in local commands execution, allowing an operator user (Privilege-1) to escalate privileges and became administrator (Privilege-15).	2020-02-07	not yet calculated	<a href="#">CVE-2020-8126</a> <a href="#">MISC</a>
unshift -- url-parse	Insufficient validation and sanitization of user input exists in url-parse npm package version 1.4.4 and earlier may allow attacker to bypass security checks.	2020-02-04	not yet calculated	<a href="#">CVE-2020-8124</a> <a href="#">MISC</a>
ushahidi -- ushahidi	Ushahidi before 2.6.1 has insufficient entropy for forgot-password tokens.	2020-02-04	not yet calculated	<a href="#">CVE-2012-5618</a> <a href="#">MISC</a> <a href="#">MISC</a>
videolan -- vlc_media_player	The web interface in VideoLAN VLC media player before 2.0.7 has no access control which allows remote attackers to view directory listings via the 'dir' command or issue other commands without authenticating.	2020-02-06	not yet calculated	<a href="#">CVE-2013-3564</a> <a href="#">MISC</a>
vtiger -- vtiger_crm	Unrestricted file upload vulnerability in the Settings_Vtiger_CompanyDetailsSave_Action class in modules/Settings/Vtiger/actions/CompanyDetailsSave.php in Vtiger CRM 6.3.0 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request	2020-02-06	not yet calculated	<a href="#">CVE-2015-6000</a> <a href="#">MISC</a> <a href="#">MISC</a>

	to the file in test/logo/.			MISC
vtiger -- vtiger_crm	vTiger CRM 5.3 and 5.4: 'files' Upload Folder Arbitrary PHP Code Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3591</a> MISC MISC MISC
watchguard - firewire_xtn	A Cross-site Scripting (XSS) vulnerability exists in WatchGuard XTM 11.8.3 via the poll_name parameter in the firewall/policy script.	2020-02-07	not yet calculated	<a href="#">CVE-2014-6413</a> MISC MISC MISC
webcalendar - webcalendar	webcalendar before 1.2.7 shows the reason for a failed login (e.g., "no such user").	2020-02-04	not yet calculated	<a href="#">CVE-2013-1422</a> MISC MISC MISC
wordpress - wordpress	WordPress Super Cache Plugin 1.3 has XSS.	2020-02-07	not yet calculated	<a href="#">CVE-2013-2008</a> MISC MISC MISC
wordpress - wordpress	The Time Capsule plugin before 1.21.16 for WordPress has an authentication bypass. Any request containing IWP_JSON_PREFIX causes the client to be logged in as the first account on the list of administrator accounts.	2020-02-06	not yet calculated	<a href="#">CVE-2020-8771</a> MISC MISC
wordpress - wordpress	Unrestricted file upload vulnerability in server/php/UploadHandler.php in the jQuery File Upload Plugin 6.4.4 for jQuery, as used in the Creative Solutions Creative Contact Form (formerly Sexy Contact Form) before 1.0.0 for WordPress and before 2.0.1 for Joomla!, allows remote attackers to execute arbitrary code by uploading a PHP file with an PHP extension, then accessing it via a direct request to the file in files/, as exploited in the wild in October 2014.	2020-02-08	not yet calculated	<a href="#">CVE-2014-8739</a> MISC MISC MISC MISC MISC MISC MISC
wordpress - wordpress	WordPress WP Super Cache Plugin 1.2 has Remote PHP Code Execution	2020-02-07	not yet calculated	<a href="#">CVE-2013-2009</a> MISC MISC MISC MISC
wordpress - wordpress	The InfiniteWP Client plugin before 1.9.4.5 for WordPress has a missing authorization check in iwpm_mmb_set_request in init.php. Any attacker who knows the username of an	2020-02-06	not yet	<a href="#">CVE-2020-8772</a>



	administrator can log in.		calculator	<a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple SQL injection vulnerabilities in the Huge-IT Slider (slider-image) plugin before 2.7.0 for WordPress allow remote administrators to execute arbitrary SQL commands via the removeslide parameter in a popup_posts or edit_cat action in the sliders_huge_it_slider page to wp-admin/admin.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-2062</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress - wordpress	Multiple cross-site scripting (XSS) vulnerabilities in the Photo Gallery plugin before 1.2.11 for WordPress allow remote authenticated users to inject arbitrary web script or HTML via the (1) sort_by, (2) sort_order, (3) items_view, (4) dir, (5) clipboard_task, (6) clipboard_files, (7) clipboard_src, or (8) clipboard_dest parameters in an addImages action to wp-admin/admin-ajax.php.	2020-02-08	not yet calculated	<a href="#">CVE-2015-1394</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zabbix -- zabbix	Zabbix 2.0.9 has an Arbitrary Command Execution Vulnerability	2020-02-07	not yet calculated	<a href="#">CVE-2013-3628</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager	Zoho ManageEngine Applications Manager 14 before 14520 allows a remote unauthenticated attacker to disclose OS file names via FailOverHelperServlet.	2020-02-06	not yet calculated	<a href="#">CVE-2019-19800</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- applications_manager	The FailOverHelperServlet (aka FailServlet) servlet in ZOHO ManageEngine Applications Manager before 11.9 build 11912, OpManager 8 through 11.5 build 11400, and IT360 10.5 and earlier does not properly restrict access, which allows remote attackers and remote authenticated users to (1) read arbitrary files via the fileName parameter in a copyfile operation or (2) obtain sensitive information via a directory listing in a listdirectory operation to servlet/FailOverHelperServlet.	2020-02-08	not yet calculated	<a href="#">CVE-2014-7863</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to tmcginnis@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States  
Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



**From:**

[The Washington Post](#)

**To:**

[aaquino@sunnyvale.ca.gov](mailto:aaquino@sunnyvale.ca.gov)

**Subject:**

The Daily 202: Democratic debate pits Bidenism vs. Bernieism – with the others staking out spaces in between  
**Date:** Wednesday, January 15, 2020 8:14:40 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you're having trouble reading this, [click here](#).

---

# The Daily 202

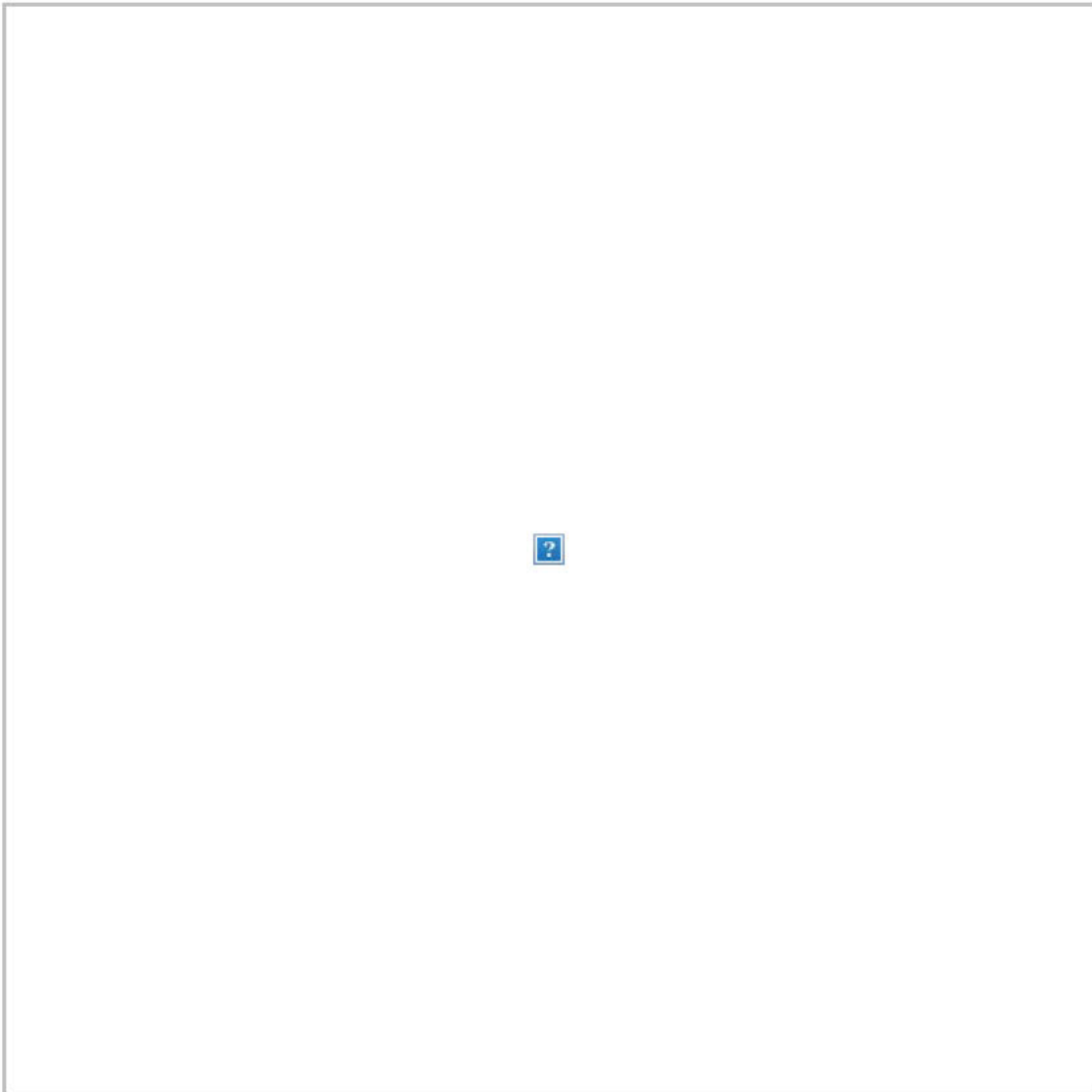


Share:  

 Listen to The Big Idea



## **Democratic debate pits Bidenism vs. Bernieism – with the others staking out spaces in between**



Elizabeth Warren and Bernie Sanders exchange words as Tom Steyer looks on after the debate. (Scott Olson/Getty Images)



**BY JAMES HOHMANN**

*with Mariana Alfaro*

**THE BIG IDEA:** What people will remember from the final debate before the Iowa caucuses is Elizabeth Warren declining to shake Bernie Sanders's outstretched hand after their **brief onstage clash** over whether he really told her during a one-on-one dinner more than a year ago that a woman cannot get elected president. While that made for compelling television, it also distracted from a starker ideological choice that looms for Democratic voters in the weeks ahead.

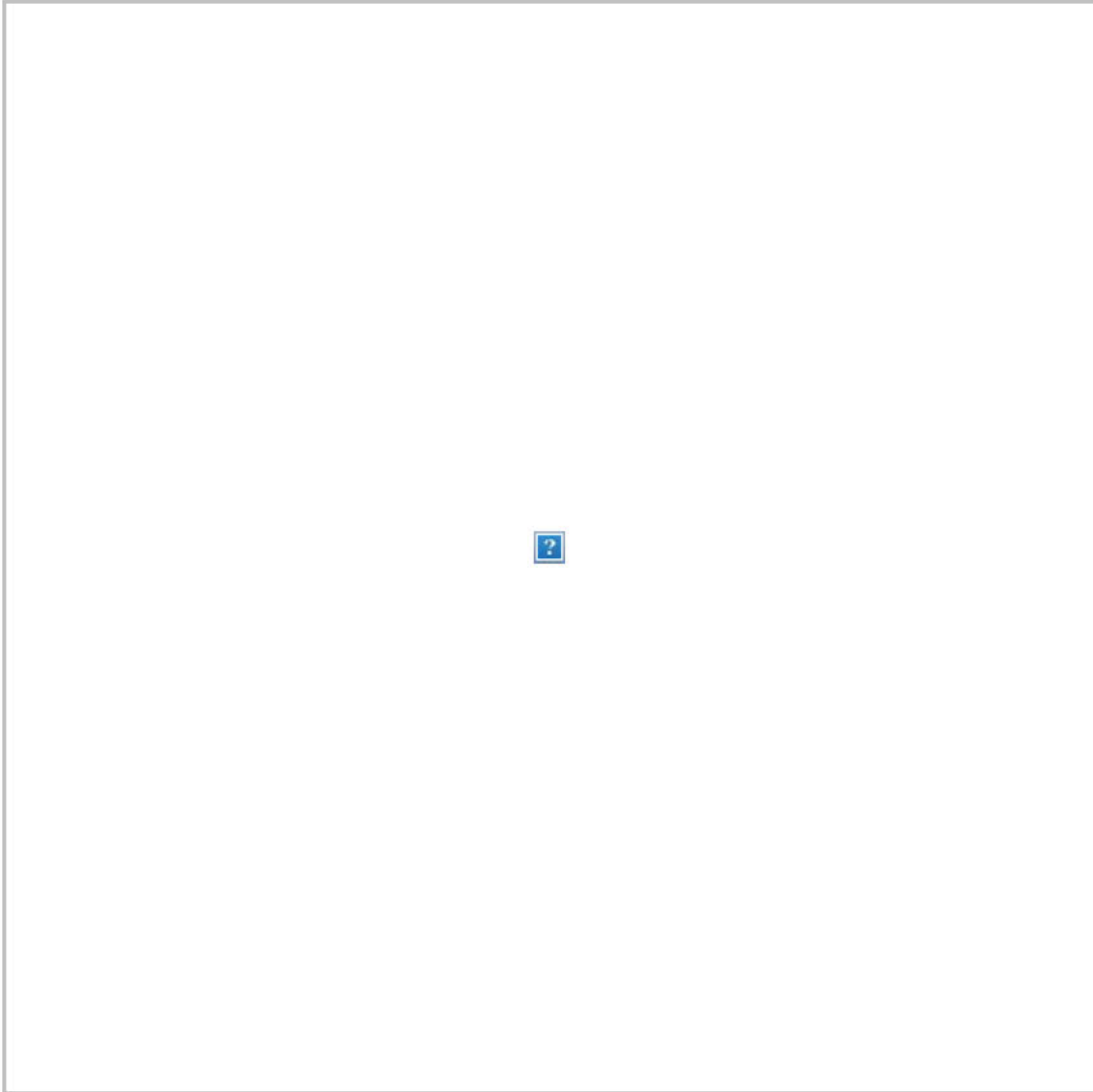
The more substantive portions of the two-hour debate at Drake University in Des Moines put in stark relief the chasm between the approaches of Sanders and Joe Biden – the two leaders in Iowa and national polling – on the biggest issues that face a president, including foreign policy, health care and trade.

It also highlighted continuing tensions between the two men over experience vs. judgment, incrementalism vs. radicalism and whether Democrats are more likely to win in November by igniting the base or appealing to disenchanted moderates who defected to Donald Trump in 2016.

Whomever is coronated at the convention in Milwaukee six months from now will chart the future of the party as its standard-bearer. In Sanders's case, he has spent decades **proudly resisting pressure** to register as a Democrat. He remains an independent who caucuses with the Democrats in the Senate.



Iowa looks like a jump ball, with the latest polls showing no overwhelming favorite and many voters either undecided or willing to change their minds. The next three weeks would be an unpredictable free-for-all in the Hawkeye State anyway. But the impeachment trial threatens to strand a handful of senators in Washington for days at a time with only Sundays away from the chamber.



Joe Biden cracks a smile as Bernie Sanders attacks him during the Democratic debate at Drake University in Des Moines on Tuesday night. (Scott Olson/Getty Images)

**-- It is conceivable that neither Biden nor Sanders ultimately wins the Feb. 3 caucuses. Nevertheless, the two septuagenarians represent the ideological goalposts and the outer bounds – Sanders on the left and the Biden on the right (which, to be clear, is still left-of-center) – of what party regulars will abide.**

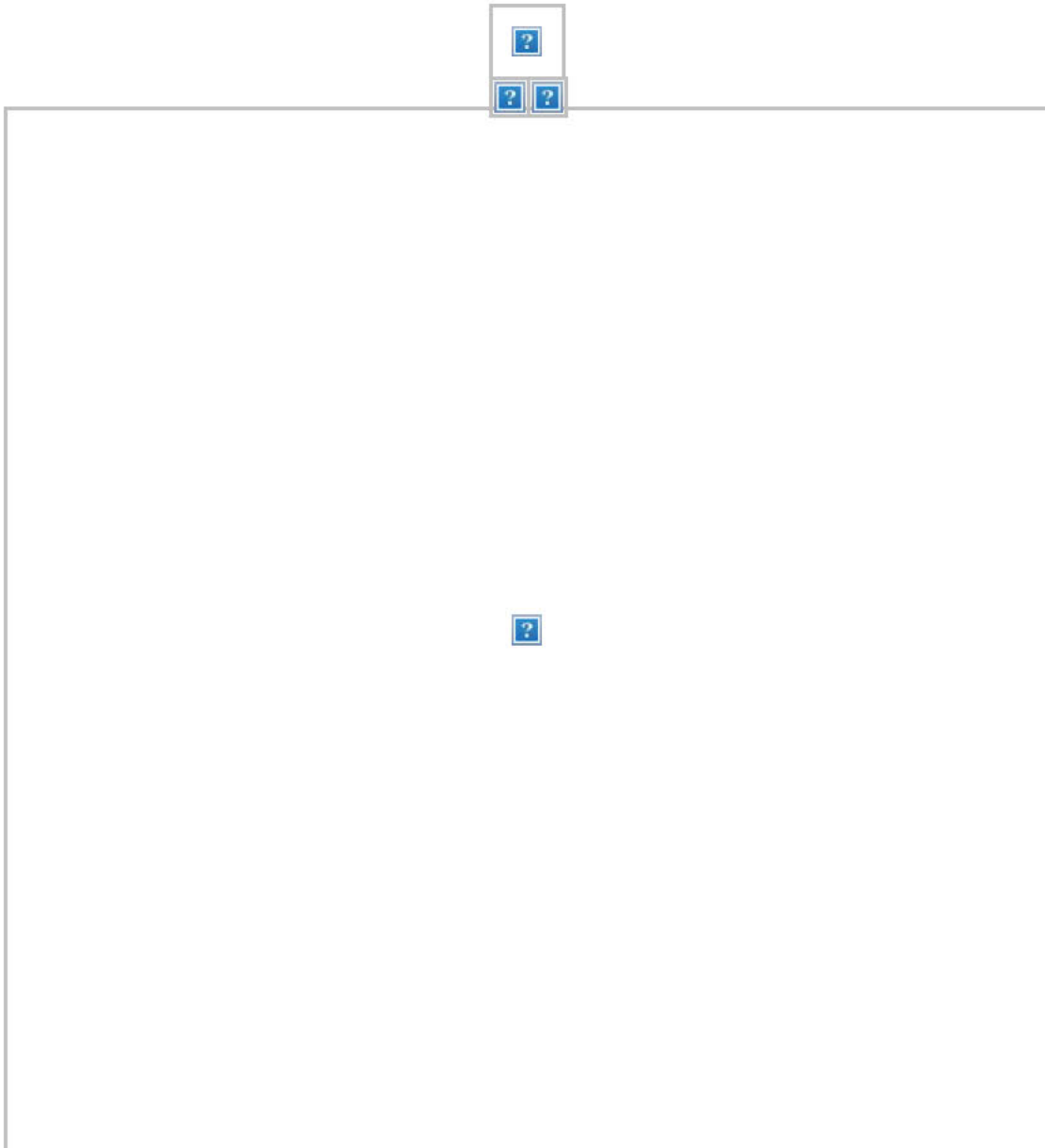
“Joe and I have a fundamental disagreement here, in case you haven't noticed,” Sanders said last night during the round on trade, a salient issue in a farm state where children are taught in school that Iowa is a net exporter. The line, though, can be applied to most every other flashpoint in Democratic politics.

**Just as he opposed the North American Free Trade Agreement, which Biden voted for, Sanders now opposes its replacement, the U.S.-Mexico-Canada trade deal.** This iteration just passed the Democratic-controlled House and won the endorsement of the AFL-CIO. It's awaiting a vote in the Senate. “The answer is we could do much better than a Trump-led trade bill,” Sanders said. “If this is passed, I think it will set us back a number of years.”

**Biden, who supports the new deal, accused Sanders of knee-jerk opposition to everything.** “I don't know that there's any trade agreement that the senator would ever think made any sense, but the problem is that 95 percent of the customers are out there,” Biden said, referring to the rest of the world. “So we better figure out how we begin to write the rules of the road, not China.”

Sanders attacked Biden for voting to ratify multiple agreements over the years that he said have helped large multinational corporations at the expense of workers. Biden compared Sanders's approach to

“poking our finger in the eye of all of our friends and allies” by not trying to negotiate trade agreements with the rest of the world, which he argued empowers China.



Candidates take on foreign policy, trade, electability at seventh Democratic debate

**-- The trade clash was particularly interesting to watch because Sanders proudly stood alone onstage among the top-tier candidates in opposing the USMCA deal. Pete Buttigieg, Amy**



**Klobuchar and even Warren endorsed it.** Trying to show that she has a pragmatic streak, Warren called the deal imperfect but reasoned that “it will give some relief” to farmers and workers. “We get up the next day and fight for a better trade deal,” she said.

**It was a reminder of the extent to which the other candidates have all sought to position themselves somewhere between the poles of Sanders and Biden, and this played out repeatedly.** In theory, Biden and Sanders occupy separate “lanes,” to use the parlance of the operative class. But both men see the other as a direct threat. The Sanders team, in particular, has believed all election cycle that they’re competing for Biden voters just as much as Warren voters.

**Warren also tried to distinguish herself at one point by noting that she was the only candidate onstage who has defeated a Republican incumbent in the last 30 years.** She ousted Republican Scott Brown in 2012 to take back Ted Kennedy’s Senate seat in Massachusetts. Sanders chimed in to say that he defeated a GOP incumbent in Vermont to win a House seat in 1990. An amused Warren, once a high school debate state champion in Oklahoma, noted that this was why she specified 30 years. Then Biden added that he won a major upset in 1972 – 48 years ago – over a Republican incumbent to win his Senate seat.

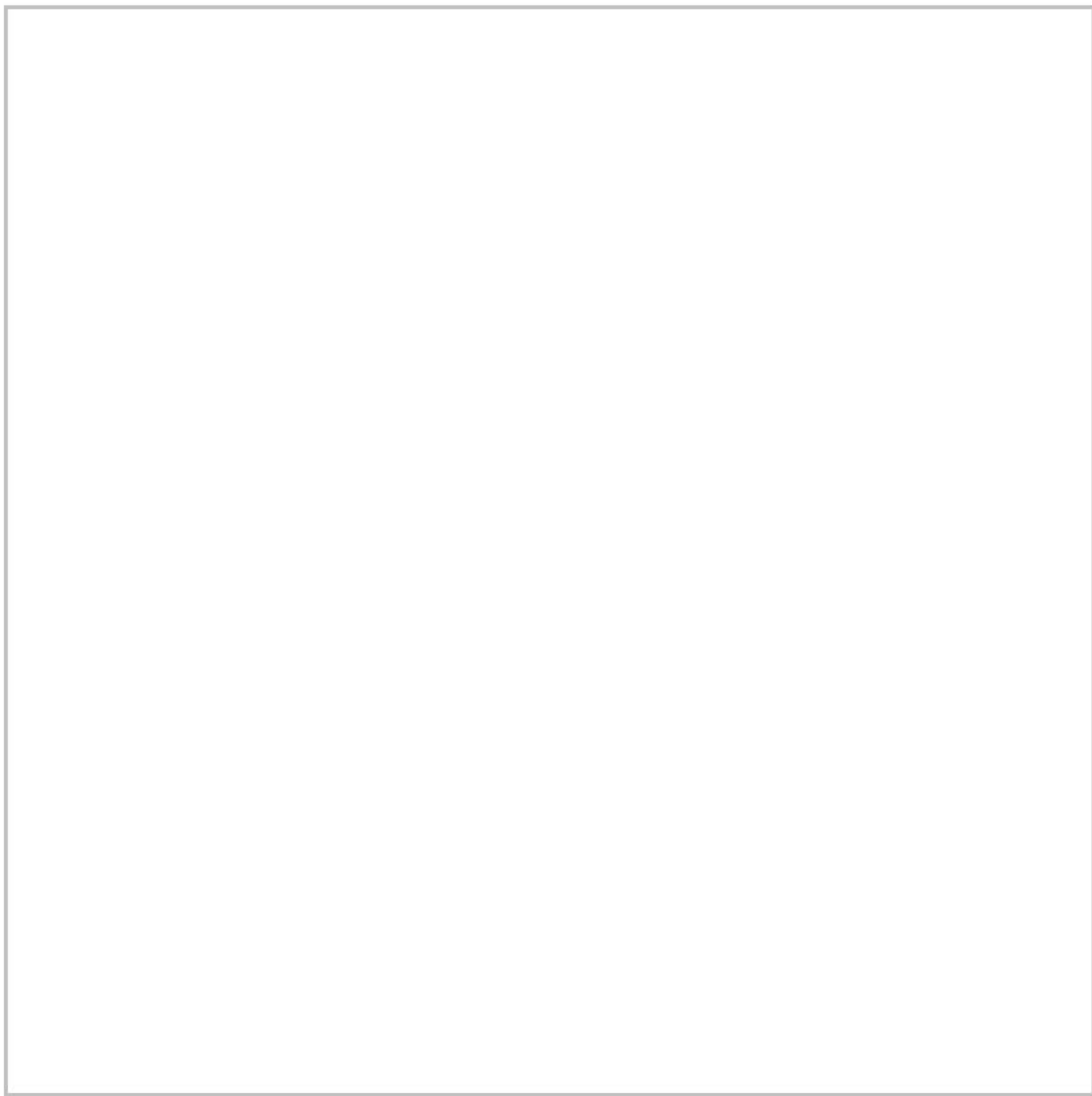
**-- Biden often sounds like he’s promising a return to the pre-Trump status quo, when he was vice president.** “We can overcome four years of Donald Trump, but eight years of Donald Trump will be an absolute disaster and fundamentally change this nation,” he said. “We have to restore America’s soul, as I’ve said from the moment I

announced.”

**Sanders counters that “this is the moment when we have got to think big, not small”:** “This is the moment when we have got to have the courage to take on the 1 percent, take on the greed and take on the corruption of the corporate elite,” he said in his closing, “and create an economy and create a government that works for all of us, not just the 1 percent.”

**CNN’s Abby Phillip also noted that Sanders identifies as a democratic socialist and pointed to a poll that showed about two-thirds of Americans don’t like the idea of voting for a socialist.** She wondered, “Doesn’t that put your chances of beating Donald Trump at risk?” Sanders replied, “Nope, not at all.” He pivoted to attack Trump, displaying the moral certitude that his supporters love but Democratic establishmentarians loathe.





Iran takes center stage at Democratic debate

**-- The gulf between Sanders and Biden was apparent from the opening question of the debate.** The crisis in Iran has prompted the leading candidates to re-litigate the 2002 debate over whether to go to war with Iraq. "Joe and I listened to what Dick Cheney and George Bush and [Donald] Rumsfeld had to say," Sanders said. "I thought they were lying. I didn't believe them for a moment. I took to the floor. I did everything I could to prevent that war. Joe saw it differently."

**Biden emphasized his work bringing troops home from Iraq as**

**Barack Obama's vice president.** "It was a mistake to trust that they weren't going to go to war," he said, referring to the Bush administration. "They said they were not going to go to war. ... It was a mistake, and I acknowledge that."

**-- The well-trod debate over health care was similar, as Biden and Sanders went at it again over the price tag for Medicare-for-all and the other candidates staked out ground in between them.** Phillip, one of three moderators, asked Sanders about a study that said his policy proposals would double federal spending as a share of GDP to a level not seen since World War II. "No, my plan would not bankrupt the country," he answered. "I think you should show how you're going to pay for things, Bernie," replied Klobuchar.

**Warren sponsored Sanders's Medicare-for-all bill, but she moved away from it in the face of questions about how she'd implement it without raising taxes on the middle class or kicking people off their private insurance.** Warren ultimately proposed a three-year transition period to Medicare-for-all, but this only led to attacks from her left and right. Last night, Warren and Buttigieg bickered about who would get covered and how much it would cost.



Fact-Checking the January Democratic debate



-- Our Fact Checker team **calls out Biden and Sanders**, more than the other candidates, for making multiple misleading or false **statements**. For example, Biden did not provide an accurate description of what Bush said before the 2002 vote that allowed for war. Biden also boasted about getting troops out of Iraq under Obama without noting that this allowed for the emergence of the Islamic State,

which required the Obama-Biden administration to send combat troops back into the country. The Fact Checker team faults Sanders for claiming that Medicare-for-all will cost less than the status quo, for significantly exaggerating the number of people who go bankrupt because of medical bills and for incorrectly claiming that the United States spends twice as much per person on health care as “any other country.” It’s only true compared to the developed world.

**-- Warren, Buttigieg and Klobuchar are trying to varying degrees to position themselves as unity candidates between Sanders and Biden who can win support from both sides and therefore beat Trump.**

“It is easy to draw lines in the sand and sketch out grand ideological visions that will never see the light of day,” said Klobuchar. “What is hard is bringing people together and finding common ground instead of scorched earth. ... If you are tired of the extremes in our politics and the noise and the nonsense, you have a home with me.”

“We cannot take the risk with so much on the line of trying to confront this president with the same Washington mindset and political warfare that led us to this point,” said Buttigieg. “If you are watching this at home and you are exhausted by the spectacle of division and dysfunction, I’m asking you to join me to help turn the page on our politics.”





Sanders denies he told Warren a woman couldn't win the presidency

**-- Here's what you need to know about the Warren vs. Sanders kerfuffle: Sanders's campaign manager Faiz Shakir told The Post that Warren "came to raise a concern" with him after the debate.** "And he said let's talk about that later," Shakir said, declining to provide further details about the conversation captured in a viral video.

"Warren said Sanders disagreed with her view that a woman could win the presidential election. Sanders contends that he merely outlined what he said would be Trump's efforts to defeat another



female candidate, and in the debate, he said, ‘Of course a woman can win,’” [Annie Linskey and Sean Sullivan report](#). “The video ... shows Sanders extending his hand as Warren approaches him onstage. Rather than shaking it, Warren clasps her hands together and speaks to Sanders. He responds, as Tom Steyer walks toward them. ... Warren and Sanders then separate. Steyer and Sanders shake hands on one side of the stage. Nearby, Warren shakes hands with [Buttigieg]. ... Representatives for the Warren campaign declined to comment. After the debate, Steyer told MSNBC’s Chris Matthews that he did not know what Warren and Sanders said to each other.”

**-- Dan Balz notes that the Warren-Sanders clash was inevitable, and they remain on a collision course after last night:** “For the past few months, Warren found herself looking at Buttigieg as a more immediate threat in Iowa. She took a lead in a September Iowa poll by the Des Moines Register and CNN, only to see Buttigieg overtake her in the November poll. She and the mayor seemed to be competing in Iowa for the support of more-affluent voters with college degrees. Sanders’s campaign saw that as an opening and seized it.”

**New Hampshire could be even more consequential because Warren and Sanders both come from neighboring states and have invested heavily.** “That gives both of them a potential edge, and whoever finishes behind the other will have suffered a significant setback,” Dan notes.

**-- Warren spoke the most during the debate:**

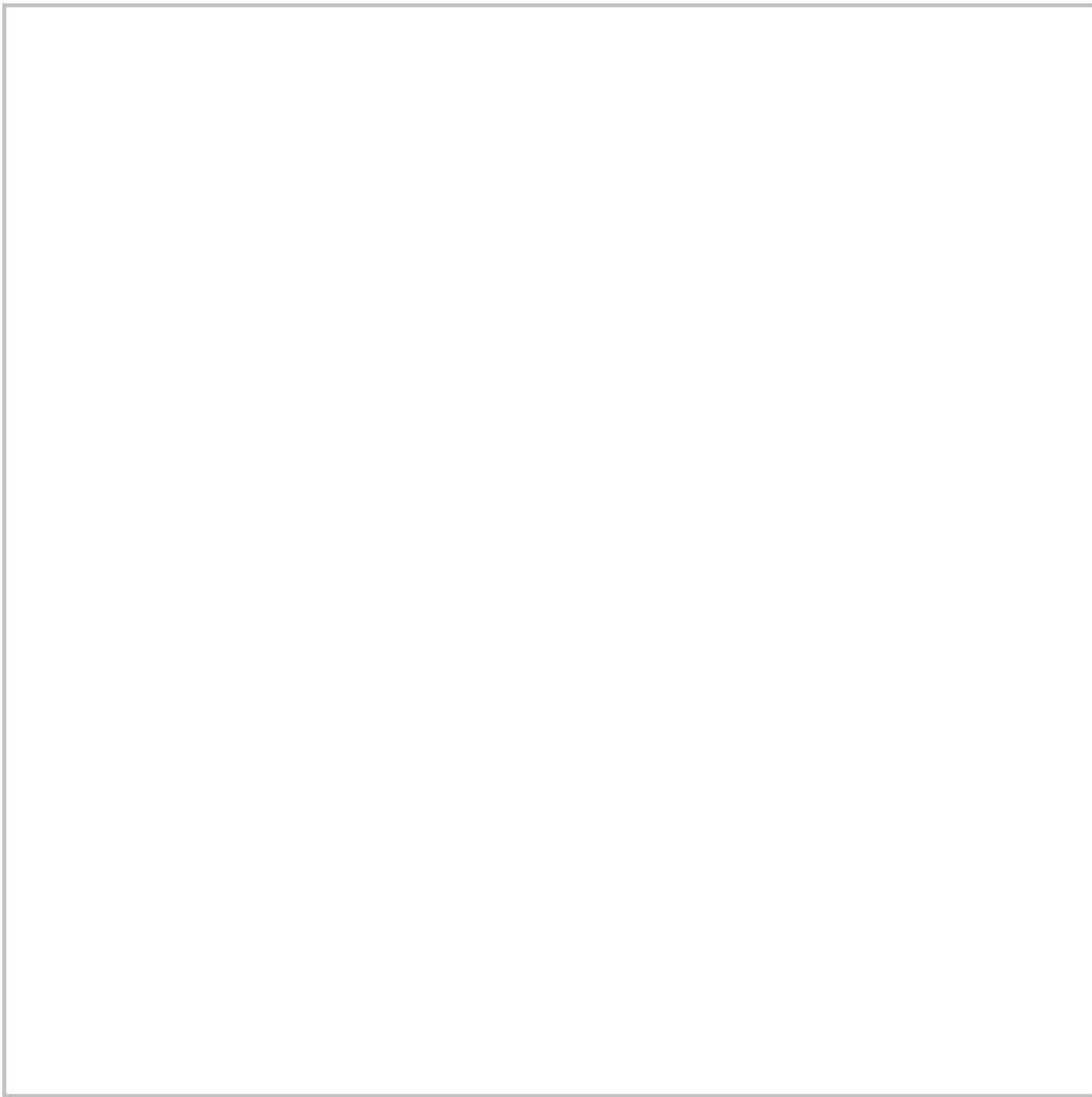
(Dan Keating and Kevin Schaul)



(Dan Keating and Kevin Schaul)

**-- The Post's opinion columnists largely focused on Warren vs. Sanders.** "Can a woman be elected president? Let's put that silly question behind us," wrote [Karen Tumulty](#). "Sanders vs. Warren shows the difference between identifying sexism and giving in to it," declared [Ruth Marcus](#). "There's a reason Bernie Sanders said Elizabeth Warren is lying," noted [David Von Drehle](#). "Democratic officials have reason to hope for a happy ending," said [Eugene Robinson](#). "The debate shows why."

-- Pundits are all over the place in their lists of winners and losers, suggesting that the muddled debate will do little to alter the trajectory of the race. [The Fix's Aaron Blake](#) considered Warren's sly attack on Sanders *and* Sanders's response winning moves. He said Buttigieg lost and Biden was "in the middle." [CNN's Chris Cillizza](#) thought Buttigieg, Warren and Klobuchar won, but Biden, Sanders and Steyer lost. But [Politico's campaign reporters](#) agreed with one another that Biden had the best night. [Fox News's Bret Baier](#) said Biden's performance was lackluster and Klobuchar "actually had a really good night" while Sanders "took a lot of incoming." [Vox](#) put Sanders and Buttigieg on its winners list and named Steyer as the losing candidate. Biden was on neither. [Jennifer Rubin](#) said Klobuchar and Biden shined. "The rest, not so much," she wrote.



Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



Pelosi announces impeachment managers

## **THE LATEST ON IMPEACHMENT:**

**-- Speaker Nancy Pelosi named the seven House Democrats who will serve as impeachment managers during the Senate trial:**

Intelligence Committee Chairman Adam Schiff (Calif.), Judiciary Committee Chairman Jerry Nadler (N.Y.), Hakeem Jeffries (N.Y.), Sylvia Garcia (Tex.), Val Demings (Fla.), Zoe Lofgren (Calif.) and Jason Crow (Colo.). Trump's defense team is expected to be led by White House counsel Pat Cipollone. Notably, Rep. Justin Amash, the



Republican-turned-independent who voted for impeachment, is not one of the managers. Lofgren worked on Richard Nixon's impeachment as a House staffer and was on the House Judiciary Committee during Bill Clinton's impeachment. ([We'll update our liveblog with more news all day.](#))



Rudy Giuliani, the president's personal lawyer, brought Lev Parnas, left, as his guest to the state funeral service for former president George H.W. Bush at the Washington National Cathedral in December 2018. (Al Drago/Bloomberg News)

**-- New materials released last night by House Democrats appear**

**to show Ukraine's top prosecutor offering one of Rudy Giuliani's associates damaging information related to Joe Biden if the Trump administration recalled the U.S. ambassador to Ukraine.** [Paul Sonne, Rosalind S. Helderman and Tom Hamburger report](#): "The text messages and documents provided to Congress by former Giuliani associate Lev Parnas also show that before the ambassador, Marie Yovanovitch, was removed from her post, **a Parnas associate now running for Congress sent menacing text messages suggesting that he had Yovanovitch under surveillance in Ukraine.** A lawyer for Yovanovitch said Tuesday that the episode should be investigated. ...

**"Among the revelations in the documents released Tuesday: a message from Giuliani to Parnas saying he had involved a person he called "no 1" — possibly Trump himself — in an effort to lift a U.S. visa ban on a former Ukrainian prosecutor [who was planning to come to the United States](#) to make claims about Biden.** The materials also include a letter Giuliani wrote to Ukraine's then-president-elect, Volodymyr Zelensky, requesting a May 14 meeting with the new leader in Giuliani's "capacity as personal counsel to President Trump and with his knowledge and consent." Giuliani scrapped his planned trip, and the meeting never took place. Another document released by the House investigators appears to show Parnas directly involved with efforts to get Zelensky to announce investigations related to Biden. In handwritten notes on a piece of stationery from the Ritz-Carlton Hotel in Vienna, Parnas wrote, 'get Zalenksy [sic] to Annouce [sic] that the Biden case will be Investigated.' ...

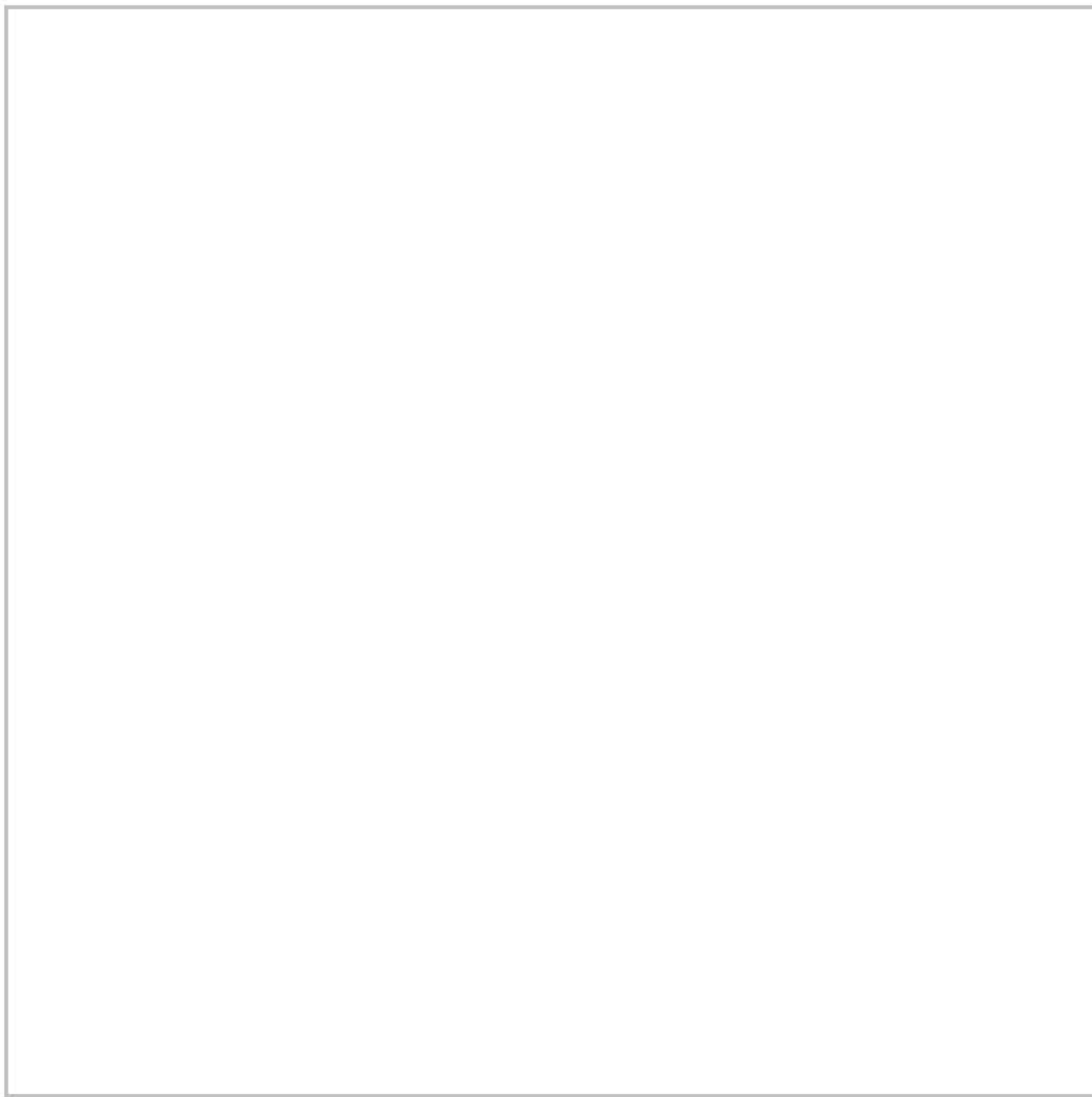


**"The materials show that Parnas, a Russian-speaker who helped coordinate Giuliani's outreach to Ukrainian sources, was directly communicating with an array of top Ukrainian officials.** Among them was Yuri Lutsenko, at the time Ukraine's top prosecutor and a close political ally of then-Ukrainian President Petro Poroshenko, who was running for reelection. Lutsenko wanted to get rid of Yovanovitch, the U.S. ambassador, in part because she had been critical of his office and supported a quasi-independent anti-corruption bureau he despised. The messages, written in Russian, show Lutsenko urging Parnas to force out Yovanovitch in exchange for cooperation regarding Biden. At one point, Lutsenko suggests he won't make any helpful public statements unless 'madam' is removed.

**"The new documents also introduced a new character in the drama over the ambassador's ouster: a Republican congressional candidate from Connecticut who asserted to Parnas in messages that he had Yovanovitch under physical and electronic surveillance.** 'Wow. Can't believe Trumo [sic] hasn't fired this b----,' Robert F. Hyde wrote in an encrypted message to Parnas on March 23. 'I'll get right [on] that.' Hyde described having contact with a 'private security' team located near the embassy that was apparently monitoring the ambassador's movements. 'She's talked to three people. Her phone is off. Computer is off,' he wrote in one message. 'They will let me know when she's on the move,' he said in another. Later, he alerted Parnas that he had been told Yovanovitch would not be moved to a 'special security unit.' 'They are willing to help if we/you would like a price,' he said in one note. 'Guess you can do anything in the Ukraine with money . . . what I was told.' Hyde did not explain how his team might 'help' Parnas, who responded only

with 'lol.' When asked for comment by The Washington Post in a text message, Hyde replied: 'Sorry I can't talk right now.' Hyde is one of three Republicans running to unseat an incumbent Democrat in the 5th Congressional District in Connecticut. He frequently tweets about his support for Trump and posted photos of himself with the president." ([Review the full cache of material for yourself here.](#))

**-- All the president's men, cont.: Former Trump national security adviser Michael Flynn asked a federal judge for permission to withdraw his guilty plea of lying to the FBI about this Russian contacts during special counsel Bob Mueller's probe.** [Spencer S. Hsu reports](#): "The stunning reversal — more than two years after Flynn pleaded guilty Dec. 1, 2017, and two weeks before he faces sentencing — threatens to sidetrack, if not derail, the prosecution of the highest-ranking Trump official charged and one of the first to cooperate with Mueller's office."



Russian Prime Minister Dmitry Medvedev holds a Russian-made weapon during a visit to the Promtehnologiya firearms company in Moscow in 2013. Medvedev resigned today as part of a shake-up orchestrated by Vladimir Putin. (Dmitry Astakhov/Sputnik/AFP via Getty Images)

**-- Russia's prime minister submitted his resignation today as part of a surprise government shake-up directed by President Vladimir Putin.** [Isabelle Khurshudyan reports from Moscow](#): "Putin accepted the resignation of the prime minister, Dmitry Medvedev, and asked the members of Medvedev's Cabinet to remain in place until a new government is formed ... The sweeping moves came shortly after



Putin gave his annual address to Russia's lower house of parliament and proposed constitutional changes to boost the powers of prime ministers and Cabinet members. ... Earlier, Putin proposed sweeping changes to the constitution Wednesday, including strengthening parliament and revamping the country's state council, possibly hinting at his plans for after he leaves power in 2024. In his annual address to lawmakers, Putin again suggested limiting presidential term limits to two, indicating that 20 years after he first became president, he won't attempt to seek a third consecutive term. But **Putin's plan to give constitutional status to the state council, a top advisory body to the president he created in 2000, and transfer more power to parliament, including naming the country's prime minister, could be a path for him to maintain significant influence in a different capacity once this presidential term is finished.** As the Russian constitution stands now, the president has the sole power to appoint the prime minister."



'There is little or no sentiment' among GOP for dismissing Senate trial, McConnell says

**-- Mitch McConnell is trying to balance the feuding factions within the Senate Republican Conference over whether to vote on calling witnesses.** [Seung Min Kim, Elise Viebeck and Robert Costa report:](#) "On one end, a group of influential swing GOP senators — Sens. Susan Collins of Maine, Lisa Murkowski of Alaska, Mitt Romney of Utah and Lamar Alexander of Tennessee — are pushing to hold a vote on whether to call witnesses later in the proceedings. Democrats have vowed to exert pressure on the group to break with

their party on witnesses and other issues, such as obtaining documents. At the same time, the Senate's right flank is increasingly making the case to [McConnell] and other GOP leaders for a more aggressive posture in defense of Trump. In a private meeting with McConnell on Tuesday, Sen. Ted Cruz (Tex.) argued that if Democrats press the case for potentially damaging witnesses — such as former national security adviser John Bolton — the GOP should insist on incendiary witnesses of their own, such as Hunter Biden ... McConnell appeared receptive to Cruz's pitch ...

“Despite their role as potential swing GOP votes in a narrowly divided Senate, the group of moderates has yet to defect in any significant fashion from party leaders ... **In a nod to the moderates, there is expected to be a provision guaranteeing a vote on whether the Senate could consider subpoenaing witnesses**, according to two GOP officials familiar with the matter ... GOP leaders are confident that once voting begins to set the scope of the trial — called an organizing resolution — that no Republicans will defect, with the moderates placated by a guaranteed decision on witnesses later. That calculus could change once the Senate goes through the grind of opening arguments and a litany of questions, and if key GOP senators become dissatisfied that they hadn't gotten enough information from the trial proceedings.”

**-- Capitol Hill reporters are protesting unexpected restrictions on their access to the Senate during the impeachment trial.** [Derek Hawkins](#), [Felicia Sonmez](#) and [Fred Barbash](#) report: “The organization representing daily reporters on Capitol Hill is protesting restrictions expected to be imposed on the news media during the Senate



impeachment trial, saying the security crackdown will severely limit access to lawmakers and stifle coverage of the proceedings. ... Capitol security officials are [reportedly] considering measures that are all but certain to make it harder for journalists to report on the trial and question senators about their actions. A magnetometer in the Senate press gallery will require reporters to trickle into the chamber one at a time. Electronic devices will be banned, leaving reporters to scuttle in and out of the room to send tweets and emails. Reporters will be placed in pens, roping them off and restricting their ability to speak freely with senators as they enter and exit. ... Details about the nature and scope of the restrictions under consideration remained unclear, as neither the Senate sergeant at arms nor the Senate Committee on Rules and Administration, which are responsible for them, has issued a formal document.”

**-- Trump’s impeachment trial is a perilous duty for Chief Justice John Roberts because any signs of partisanship could further erode the Supreme Court's legitimacy. [From the New York Times](#):** “The chief justice’s responsibilities at the trial are fluid and ill-defined, and they will probably turn out to be largely ceremonial. ... The managers will march the articles over to the Senate chamber, touching off a series of steps that will initiate the trial. But before it can get underway Chief Justice **Roberts will be sworn in as the presiding officer and, in his first official act, administer an oath to senators in which they swear to do ‘impartial justice’ in the trial, with the real work not expected to begin until Tuesday.** ... Roberts has plenty on his plate already, much of it related to Mr. Trump. He is working on a Supreme Court docket crowded with divisive issues, including three cases on whether to allow release of Mr. Trump’s

financial records and one on Mr. Trump's efforts to withdraw protection from deportation for young immigrants. ... And Chief Justice Roberts has exchanged sharp remarks with Mr. Trump, laying bare a fundamental disagreement about the independence of federal judges."



Democrats have enough Republican votes to pass war resolution, says Kaine

## **THE IRAN CRISIS:**

**-- The Senate is poised to pass a resolution limiting Trump's**



**military authority on Iran, as four Republicans say they will vote with Democrats to assert Congress's war powers under the Constitution.** [Karoun Demirjian reports](#): “Congress cannot be sidelined on these important decisions,” said [Collins] who on Tuesday declared her support for the measure. She joins Sens. Todd C. Young (R-Ind.), Mike Lee (R-Utah) and Rand Paul (R-Ky.) and all 47 Democrats. A vote could come as soon as next week. ... The resolution is ‘privileged,’ meaning Republicans opposed to the measure cannot block it from coming to a vote once it is ‘ripe.’ It also means that supporters must secure only a simple majority of the Senate, 51 votes, for it to pass. **But it is almost certain that Trump will veto the measure and that Congress will not have the votes to override a veto.** ... Trump’s deputies and supporters said that such resolutions send a negative message to the troops and seemingly project support for the Iranian regime despite its sponsorship of terrorist activities that have led to the deaths of U.S. service members ... Supporters of the war powers measures have taken pains to say they believe [Iranian commander, Maj. Gen. Qasem] Soleimani was reprehensible as they argue that Trump cannot trample on Congress’s right to declare war.” (Kaine and Lee make the case for the resolution in [an op-ed in today’s newspaper](#).)

**-- [New video](#) shows two Iranian missiles hit the downed Ukrainian plane last week.** The [Times reports](#): “The missiles were launched from an Iranian military site around eight miles from the plane. The new video fills a gap about why the plane’s transponder stopped working, seconds before it was hit by a second missile. ... Neither strike downed the plane immediately. The new video shows the airliner on fire, circling back toward Tehran’s international airport.

Minutes later it exploded and crashed down, narrowly missing the village of Khalaj Abad ... The Times has confirmed that the new video was filmed by a camera on the roof of a building near the village of Bidkaneh, four miles from an Iranian military site. Amir Ali Hajizadeh, commander of the Islamic Revolutionary Guards Corps' airspace unit, said that missiles were launched from a base near there." ([Watch the video here.](#))

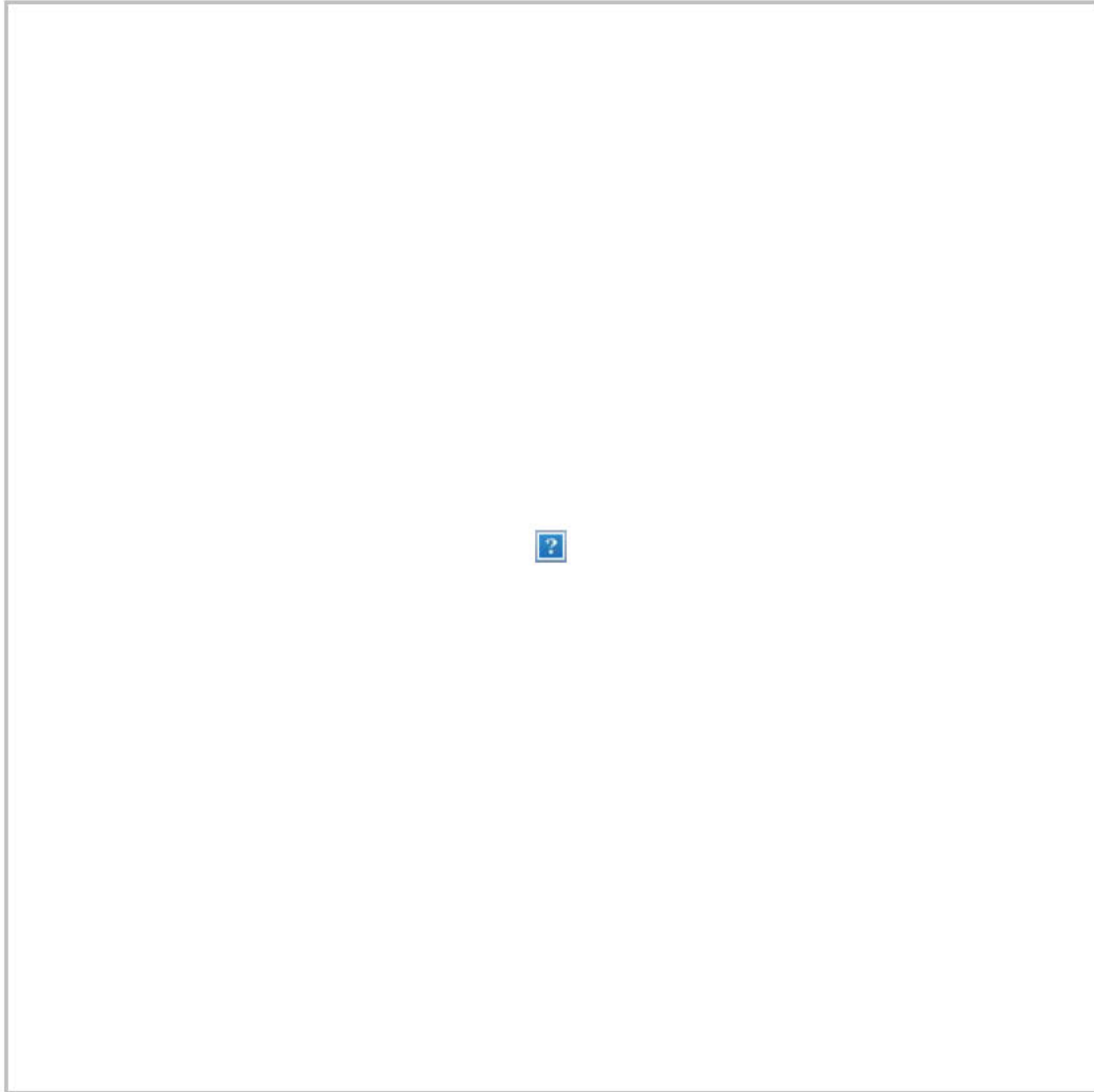
**-- The Iranian people, disturbed by the downing of the plane and the killing of Soleimani, have shown that it is possible to be angry at both their government and the United States at the same time.** [Erin Cunningham explains](#): "On Tuesday, student protesters at the University of Tehran chanted anti-government slogans as officials scrambled to find a way to quell the growing unrest. ... The efforts by senior officials to calm the public are in stark contrast to the defiant tones struck by Tehran amid an outpouring of grief this month for Soleimani at his funeral procession ... Iran is often presented 'as a monolith ... a country where all of its citizens move as one,' said Reza Akbari, a researcher of Iranian politics at the Institute for War and Peace Reporting in Washington. 'But Iranians are capable of condemning U.S. attacks against their sovereignty while protesting the gross negligence of their government,' he said. For many Iranians, Soleimani's killing in a U.S. drone strike in Baghdad was a national affront and came amid widespread resentment over harsh economic sanctions imposed on Iran by the Trump administration ... At the same time, the protests over the downed airliner, Akbari said, align with longer-term demands from the Iranian population for transparency, justice and accountability."



**-- The repressive Iranian regime arrested someone for recording a video of the missile strike that brought down the plane.** [From the Times](#): “The Islamic Revolutionary Guards Corps, a powerful arm of Iran’s military, said it had arrested a person it identified as having recorded a video ... which undercut the military’s initial denials that Iran was responsible. The arrest was announced by Iranian media outlets affiliated with the Guards. The contradictory messages from the president, who is elected, and the Guards, who answer to Iran’s clerical leaders, reflect the competing power centers in the Iranian government. ... In an apparent criticism of the military, [Hassan] Rouhani, a moderate, urged that an official inquiry be candid about its findings. But some hard-line lawmakers have lashed out at his administration, demanding resignations.”

**-- Officials at the State and Defense departments have discussed possible cuts of \$250 million in military aid to Iraq if U.S. troops are asked to leave,** [according to emails reviewed by the Wall Street Journal](#): “The emails indicate that the State Department’s Bureau of Near Eastern Affairs is working to cut all \$250 million in funds under the U.S. foreign military financing program for Iraq for the current fiscal year. The bureau also plans to ask the White House Office of Management and Budget whether it can eliminate the \$100 million request for fiscal year 2021, ‘due to current optics on the ground,’ according to the emails. ‘This does not preclude further congressional consideration of foreign assistance should the situation change in Iraq,’ one of the emails said. The emails assert that no final decision has been made, but top administration officials have ordered a review of what funds may be held or reallocated in the event Iraq requires the U.S. troops be removed. One of the emails said Secretary of State

Mike Pompeo directed that the 2020 foreign military financing funds be repurposed, or used elsewhere.”



Gun rights protesters hold signs at a meeting of the Virginia Senate Judiciary Committee in Richmond. (Steve Helber/AP)

## **DOMESTIC DEVELOPMENTS THAT SHOULDN'T BE OVERSHADOWED:**

-- Virginia Gov. Ralph Northam (D) will ban guns from the grounds of the state's capitol, at least temporarily. [Laura Vozzella and Gregory S. Schneider report](#): “The move comes just days after



newly empowered Democrats banned guns from the Capitol building and an adjacent legislative office building. And **it comes just ahead of a gun rights rally planned for Monday, which organizers say will draw tens of thousands to Capitol Square. The rally has drawn interest from militias and extremist groups across the country**, raising security concerns in Richmond. ... Security has been unusually tight during the General Assembly session that kicked off last week, as Democrats ... consider far-reaching gun-control legislation.”

**-- More than 100 billion doses of pain medication oxycodone and hydrocodone were shipped nationwide from 2006 through 2014, saturating the nation with 24 billion more doses than previously known to the public.** [Steven Rich, Scott Higham and Sari Horwitz report](#): “The Washington Post and the company that owns the Charleston Gazette-Mail in West Virginia first obtained the data, collected by the Drug Enforcement Administration, from 2006 through 2012 after waging a year-long legal fight. In July, The Post reported that the data revealed that the nation’s drug companies had manufactured and distributed more than 76 billion pain pills. The two additional years of information — 2013 and 2014 — was recently posted by a data analytics company managed by lawyers for the plaintiffs in a massive lawsuit against the opioid industry. ... The newly released data, which traces the path of pills from manufacturers and distributors to pharmacies across the country, confirms again that six companies distributed the vast majority of the pain pills. **McKesson Corp., Cardinal Health, Walgreens, AmerisourceBergen, CVS and Walmart accounted for 76 percent of the oxycodone and hydrocodone pills that were shipped between 2006 and 2014**



... Three manufacturers still accounted for 85 percent of the pills: SpecGx, a subsidiary of Mallinckrodt; Actavis Pharma; and Par Pharmaceutical, a subsidiary of Endo Pharmaceuticals.”

**-- The White House’s secret plan to divert \$7.2 billion in Pentagon funding for Trump’s border wall drew bipartisan criticism. [Paul](#)**

**[Sonne, Jeff Stein and Nick Miroff](#) report:** “Senior Republicans grumbled about the plan but mostly put the blame on Democrats, who agreed to provide \$1.4 billion in border barrier funding this year — far less than the \$5 billion Trump requested. ‘I wish they’d get the money somewhere else, instead of defense,’ said Sen. Richard C. Shelby (R-Ala.), chairman of the Senate Appropriations Committee. ‘But I do support building the wall.’ ... ‘I think it’s outrageous,’ said Sen. Jack Reed (D-R.I.), the top Democrat on the armed services committee, who called it ‘a slap to the military as well as a slap to Congress’ ... Defense Secretary Mark T. Esper, asked Tuesday if he supports the continued diverting of Defense Department money to fund the border wall, said that one of the Pentagon’s missions is supporting homeland defense. ‘If that’s what it takes, we are prepared to support’ it, he said.”

**-- An appeals court temporarily halted the purge of more than 200,000 people from Wisconsin’s voter rolls. [Reis Thebault](#)**

**[reports:](#)** “The Tuesday order came one day after the state’s elections commission and its three Democratic members were found in contempt of court for not complying with a judge’s previous order to cancel the registrations of roughly 6 percent of its voters. The case is largely split along partisan lines. Republicans argue that thousands of people who have changed addresses have not updated their voter

registration status and should therefore be struck from the rolls to ensure election integrity, while Democrats and voting rights advocates say the move will unjustly disenfranchise swaths of the electorate ... The six-person election commission had been split evenly along partisan lines, the Republicans voting in favor of the purge and the Democrats voting against it. In a meeting on Tuesday, commissioners again disagreed — 3 to 3 — about how to respond. ... A Journal Sentinel analysis of the over 200,000 register voters targeted — all of whom were sent a letter in October seeking address confirmation — found that most lived in municipalities that supported Hillary Clinton in 2016.”

**-- The Trump administration’s push to restart federal executions after nearly two decades heads back to court today.** [Mark Berman and Ann E. Marimow report](#): “Justice Department lawyers are asking the U.S. Court of Appeals for the District of Columbia Circuit to reverse a judge’s order and allow the administration to move forward with four executions the administration had scheduled for December and January. U.S. District Judge Tanya S. Chutkan in November found that the government had probably exceeded its powers with the adoption of a new lethal-injection protocol to be used in those executions. The new protocol, she wrote, is inconsistent with a 1994 law that requires federal executions to be carried out ‘in the manner prescribed by the law of the State in which the sentence is imposed.’”

**-- The Supreme Court will hear arguments in the “Bridgegate” scandal that shook New Jersey politics. The case could heavily impact future public corruption prosecutions.** [Matt Zapotosky reports](#): “As former New Jersey governor Chris Christie (R) looked on,



the Supreme Court heard arguments Tuesday on whether to overturn the convictions against two of his ex-political allies in the 'Bridgegate' case, and the decision could have broad implications for how federal prosecutors pursue allegations of public corruption. The two former allies — Bridget Kelly and William E. Baroni Jr. — argue that the Justice Department reached too far in charging them with fraud for their roles in an alleged plot to back up traffic on the George Washington Bridge, the nation's busiest, as retaliation against a local mayor who declined to endorse Christie's reelection bid. ... The Justice Department counters that Kelly and Baroni are misstating what occurred and that the evidence was sufficient to support their convictions. The questioning Tuesday did not break down neatly along traditional ideological lines, and it was difficult to predict what the ultimate decision might be. Some justices who asked questions of the attorneys for Baroni and Kelly also seemed critical of some of the government's points. ... In filings to the Supreme Court, Kelly and Baroni argued that — even if they did exactly what prosecutors allege — it could not constitute a federal crime. They argued that they were essentially convicted of lying about their true political motive for a decision."

**-- Michael Avenatti, the former attorney for adult-film actress Stormy Daniels, was arrested by IRS agents for allegedly violating his bail terms a week before his federal trial. [Timothy Bella reports](#):** "Avenatti, who is accused of extorting Nike for up to \$25 million and stealing millions of dollars from his clients for his own interests among other charges, was arrested while appearing before the State Bar Court in Los Angeles, in the middle of a disciplinary hearing alleging that he stole about \$840,000 from a former client."

**-- Rep. Joe Kennedy III (D-Mass.) is rolling out 16 Democratic endorsements for his primary challenge against incumbent Sen. Ed Markey, including Reps. John Lewis (Ga.) and Joaquin Castro (Tex.).** [From Boston Magazine](#): “Also on the list was co-chair of the Congressional Progressive Caucus, Congressman Mark Pocan, and the Caucus’s chair emeriti, Congressman Raul Grijalva. ... Kennedy collected endorsements from several other key groups in the House, including the co-chairs of the LGBTQ Equality Caucus, ... members of the Congressional Black Caucus ... and several members of the Congressional Hispanic Caucus ... Kennedy is also now outpacing Markey when it comes to raising campaign cash. ... Kennedy raised more than \$2.4 million over the last three months of 2019, while Markey’s campaign reports raising only \$1.4 million.”

**-- Boeing’s new CEO pledged greater transparency in a message to employees still reeling from the two 737 Max jet crashes that killed hundreds in the last two years.** [Lori Aratani reports](#): “‘This is a crucial time for Boeing,’ [David Calhoun] wrote. ‘We have work to do to uphold our values and to build on our strengths. I see greatness in this company, but I also see opportunities to do better. Much better.’ Calhoun’s top priority will be convincing federal regulators that the 737 Max is safe to fly. The plane has been grounded worldwide since March. Boeing also is counting on Calhoun to rebuild relationships with customers, regulators and the public.”

**-- A Delta flight dumped jet fuel on a playground near Los Angeles, leaving dozens with minor injuries.** [Justin Wm. Moyer reports](#): “Los Angeles County Fire Department officials said they responded to an elementary school ... after the aircraft apparently

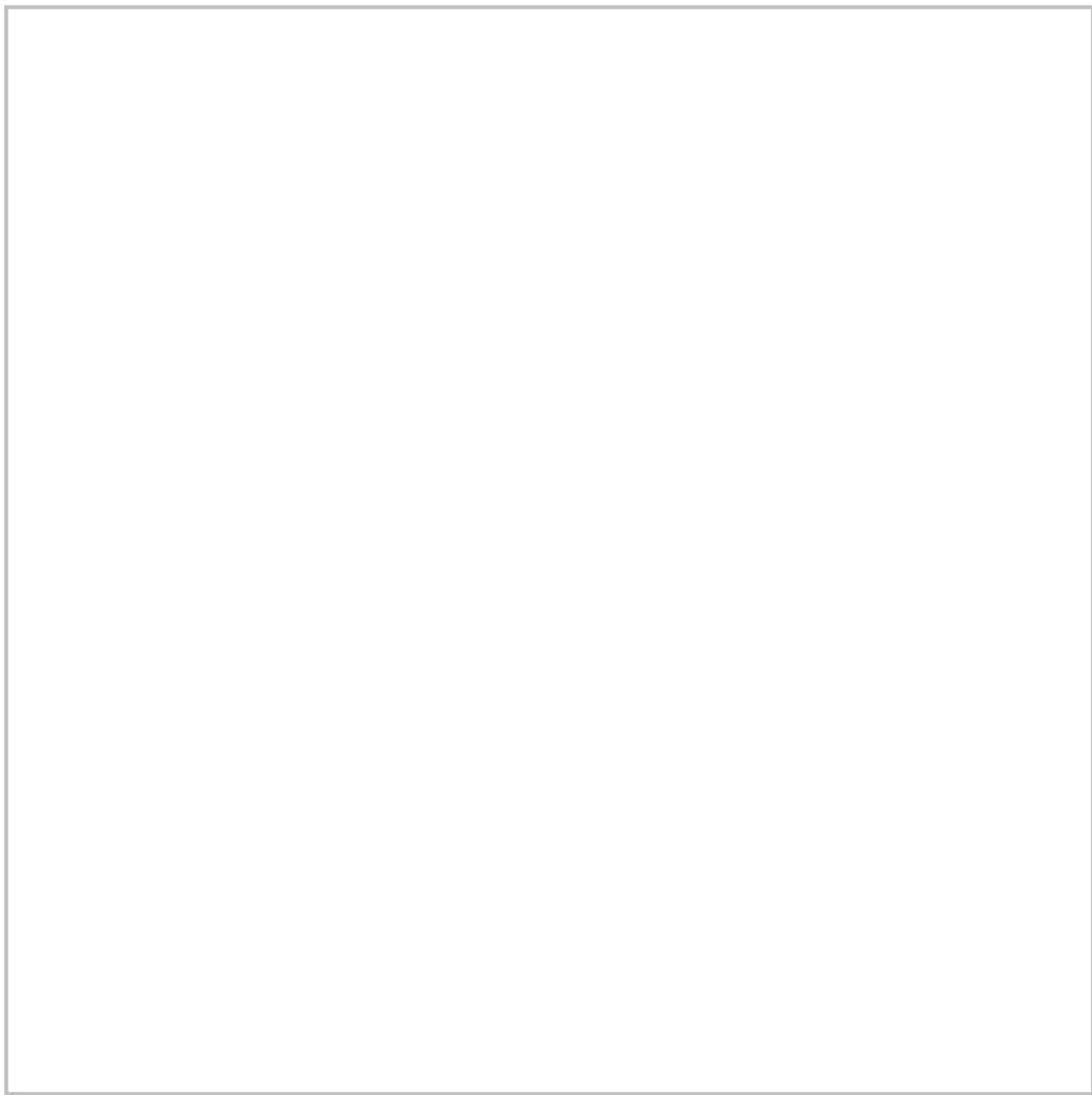


dumped the fuel while on a final approach to the airport. Twenty children and 11 adults complained of minor injuries, officials said. No one was taken to a hospital, officials said, and no evacuations were initiated. ... In a statement, Federal Aviation Administration spokesman Allen Kenitzer said Delta Air Lines Flight 89 declared an emergency after departing from the airport, then returned to the airport and 'landed without incident.'”

### **SOCIAL MEDIA SPEED READ:**

Here are the candidates most tweeted about during the debate:

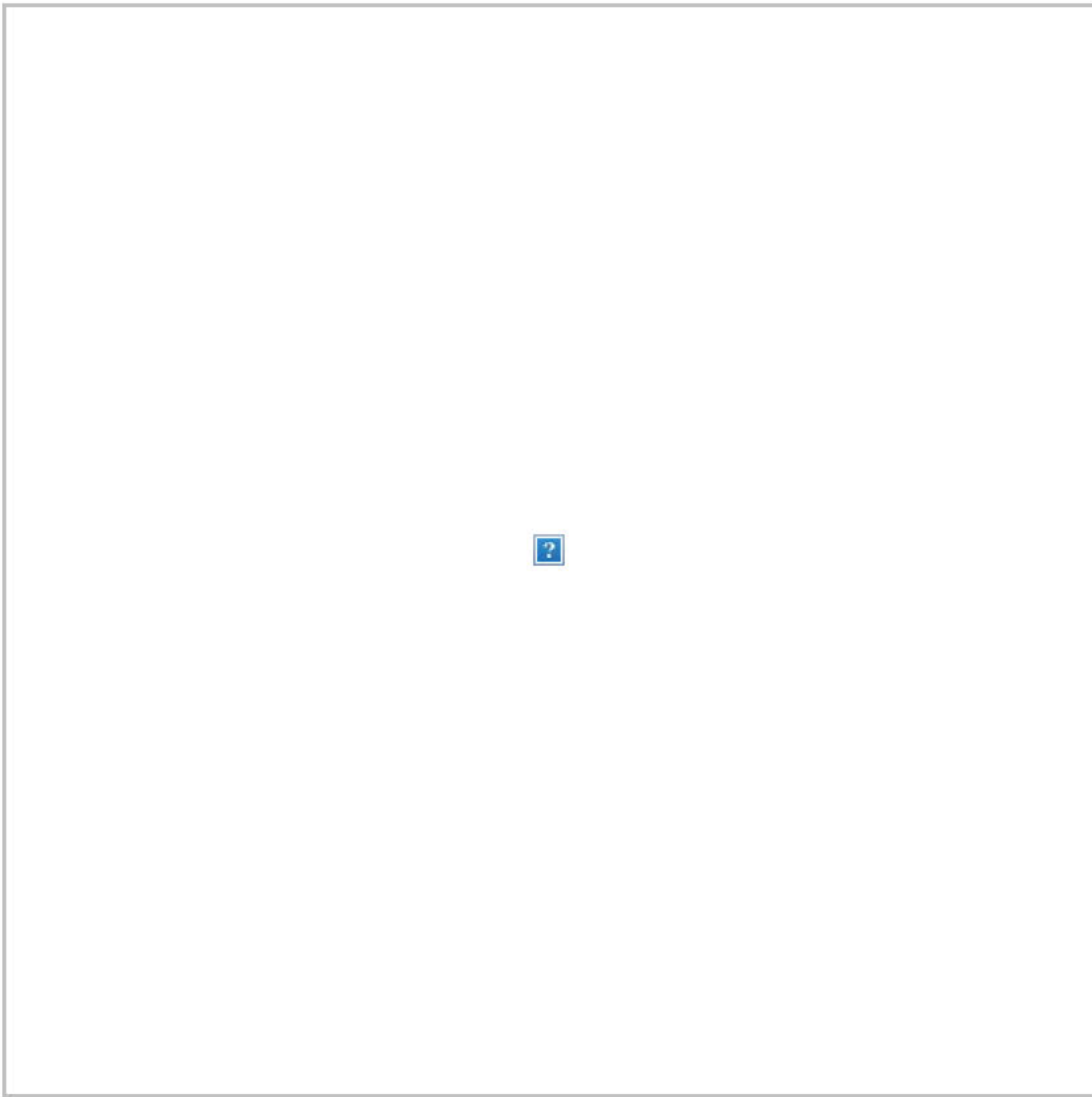




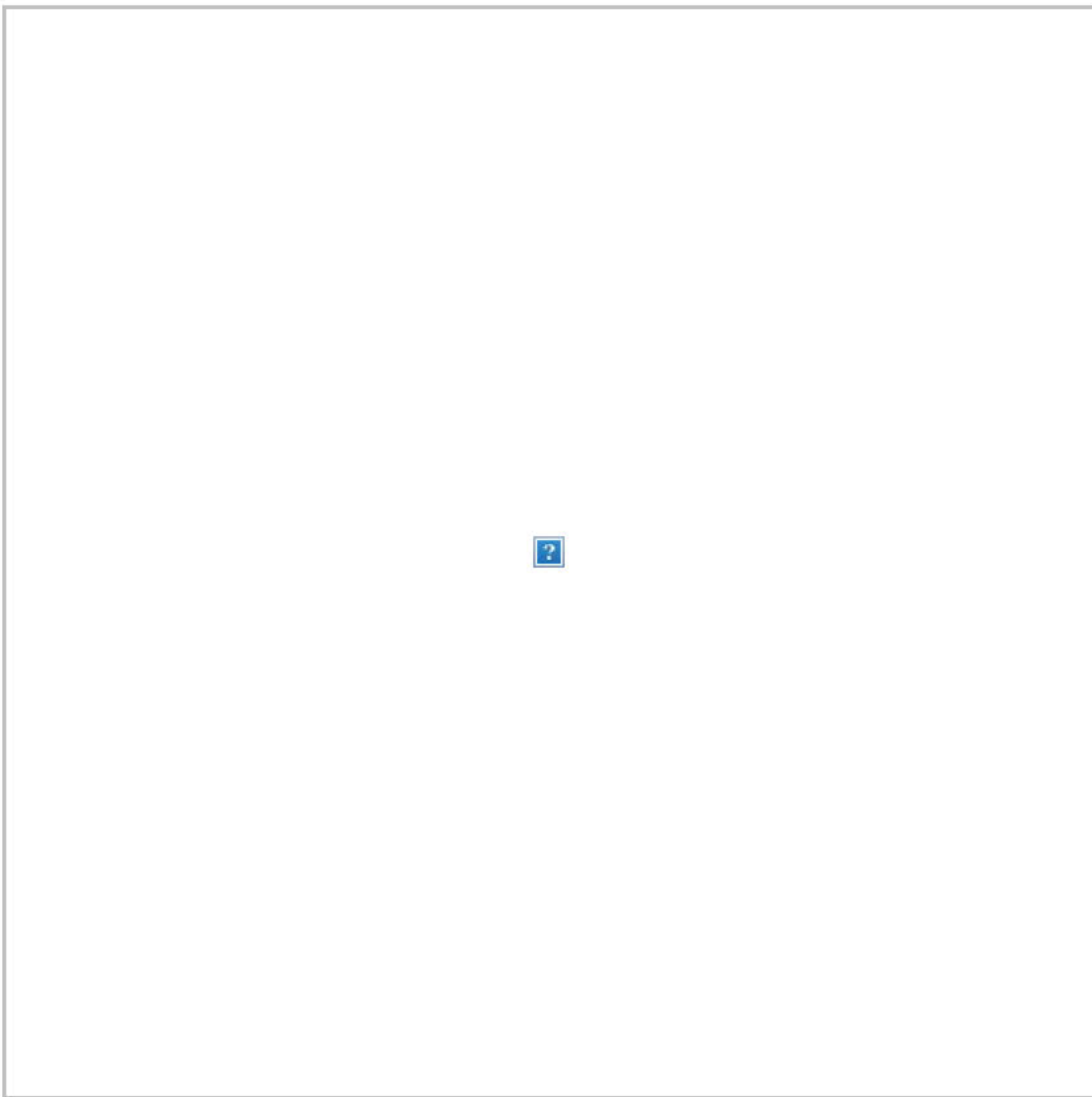
Klobuchar struggled during the debate to remember the name of the Democratic governor of Kansas who defeated Kris Kobach in 2018. The governor gamely replied:



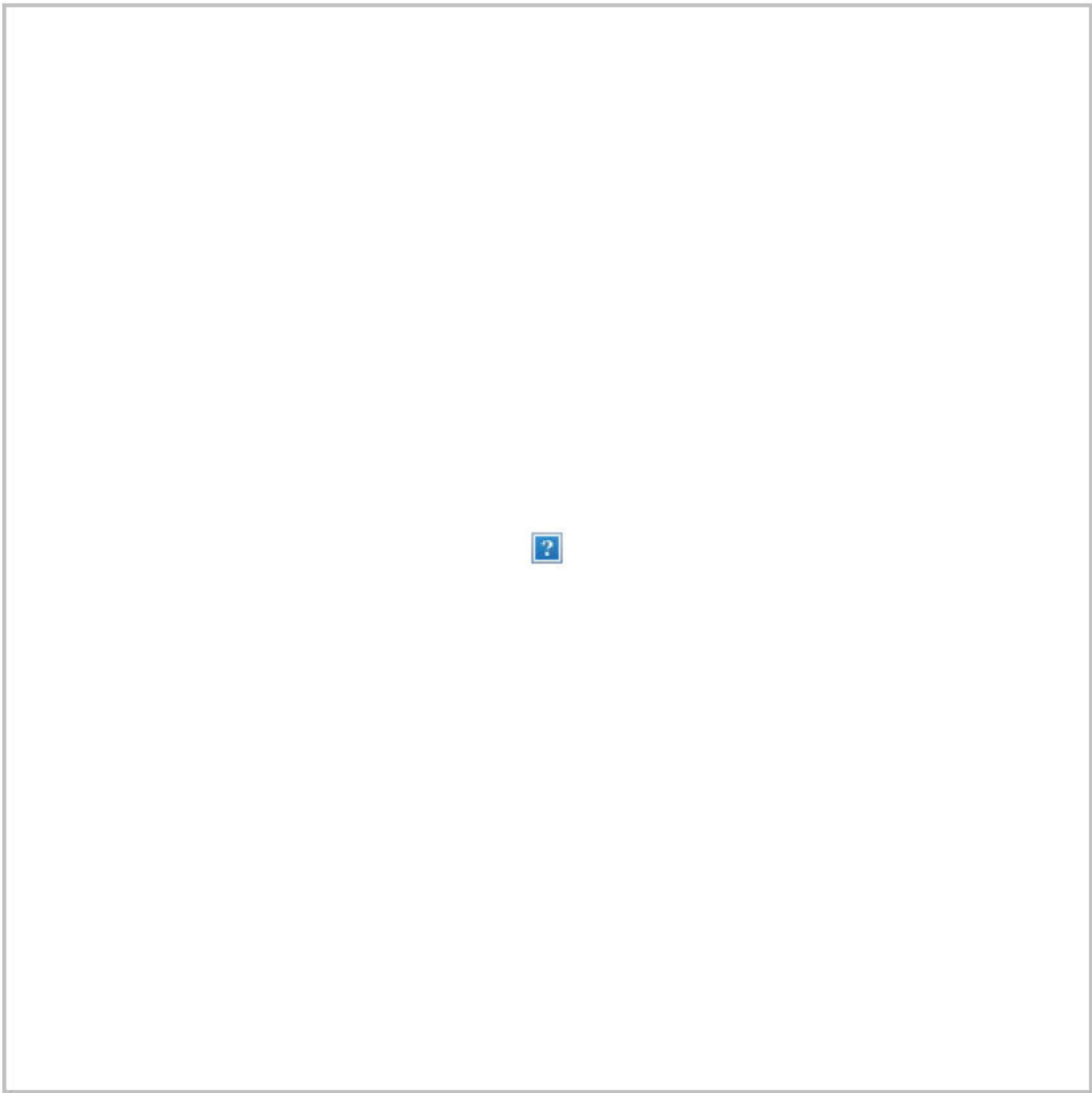
The former chief strategist for Obama noted that Sanders's 2016 clashes with Hillary Clinton created the backdrop to his back-and-forth with Warren over whether he said a woman cannot win. David Axelrod also makes the good point that Sanders is being much more explicit in saying he'll support the Democratic nominee than four years ago:



Biden raised eyebrows when he said during the debate that he had to get by as a single dad on a \$42,000 salary when he became a senator in 1973:

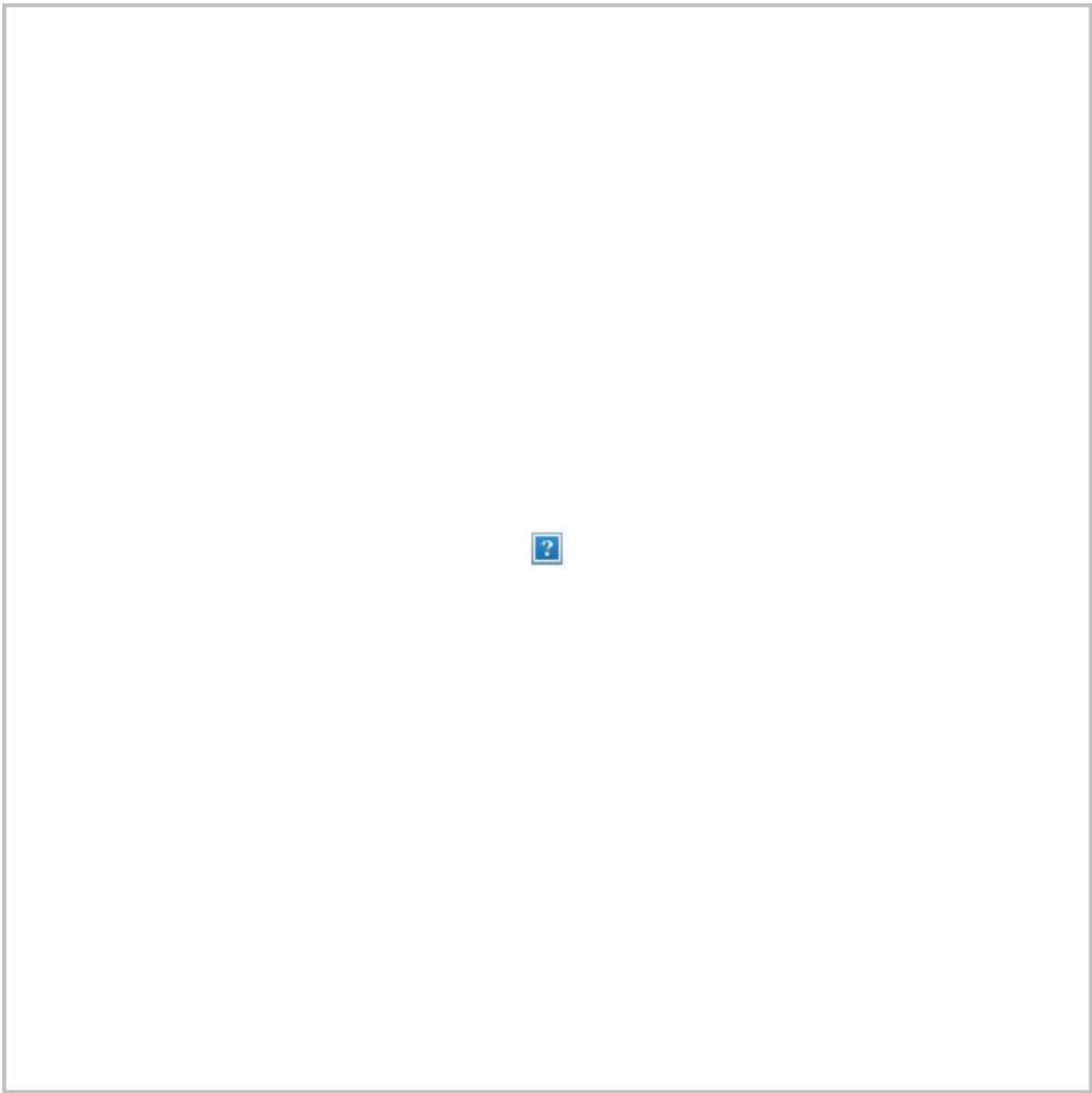


An organizational psychology professor at the Wharton School of Business suggested the Democratic candidates play a few board games instead of debating:

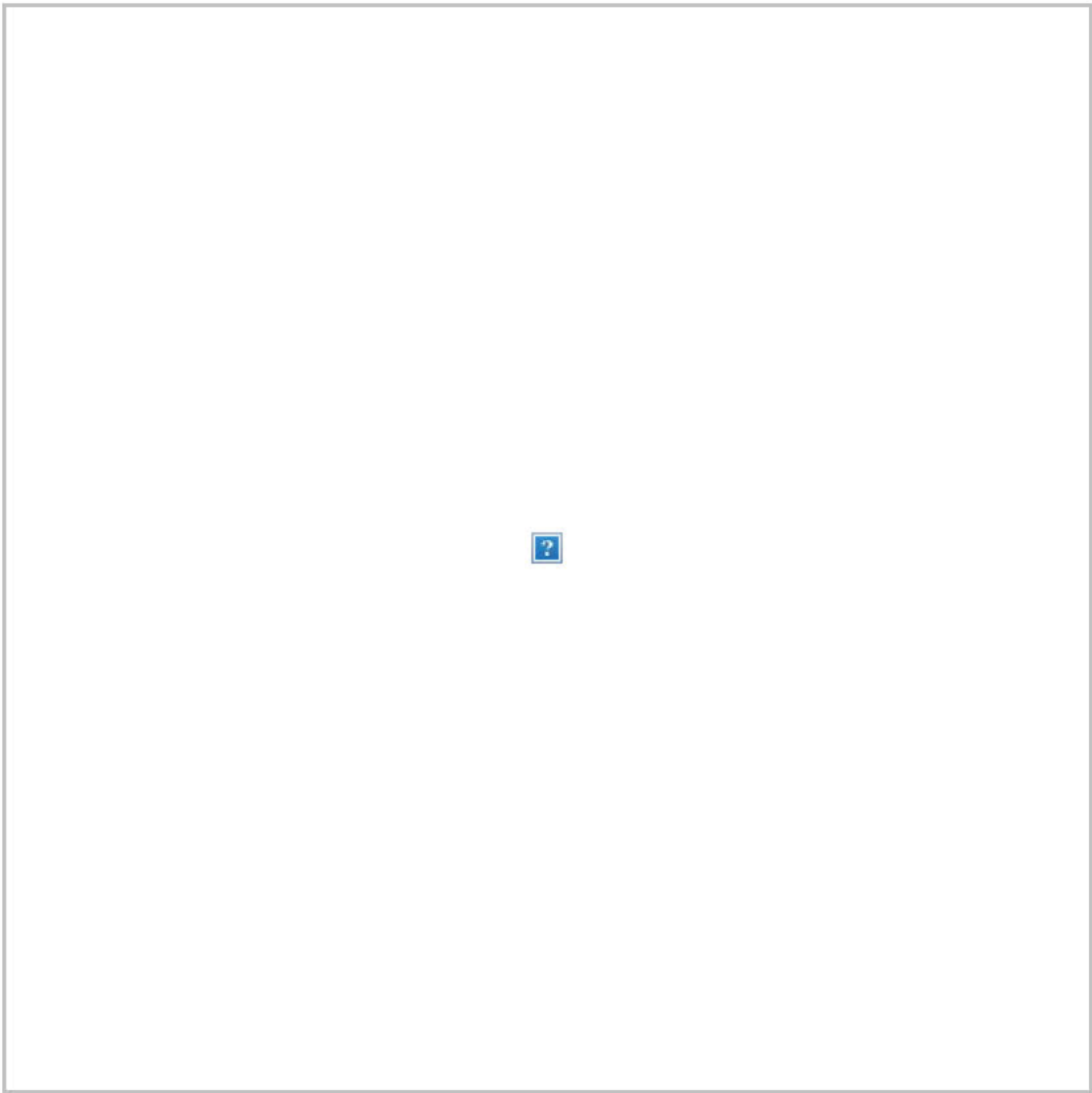


A Democratic congressman called out Mike Pompeo for talking to Fox News instead of showing up to a House hearing on Iran:

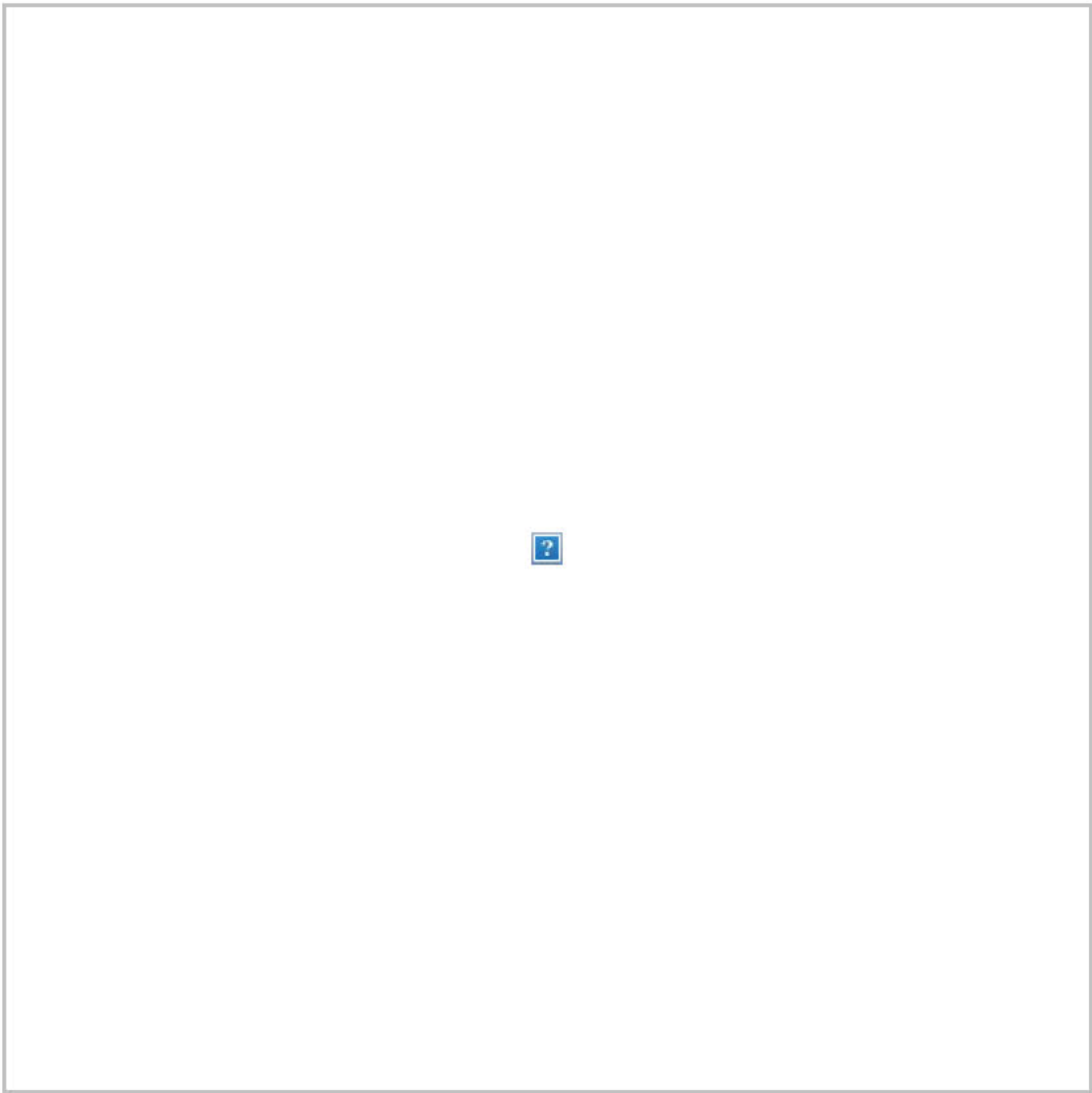




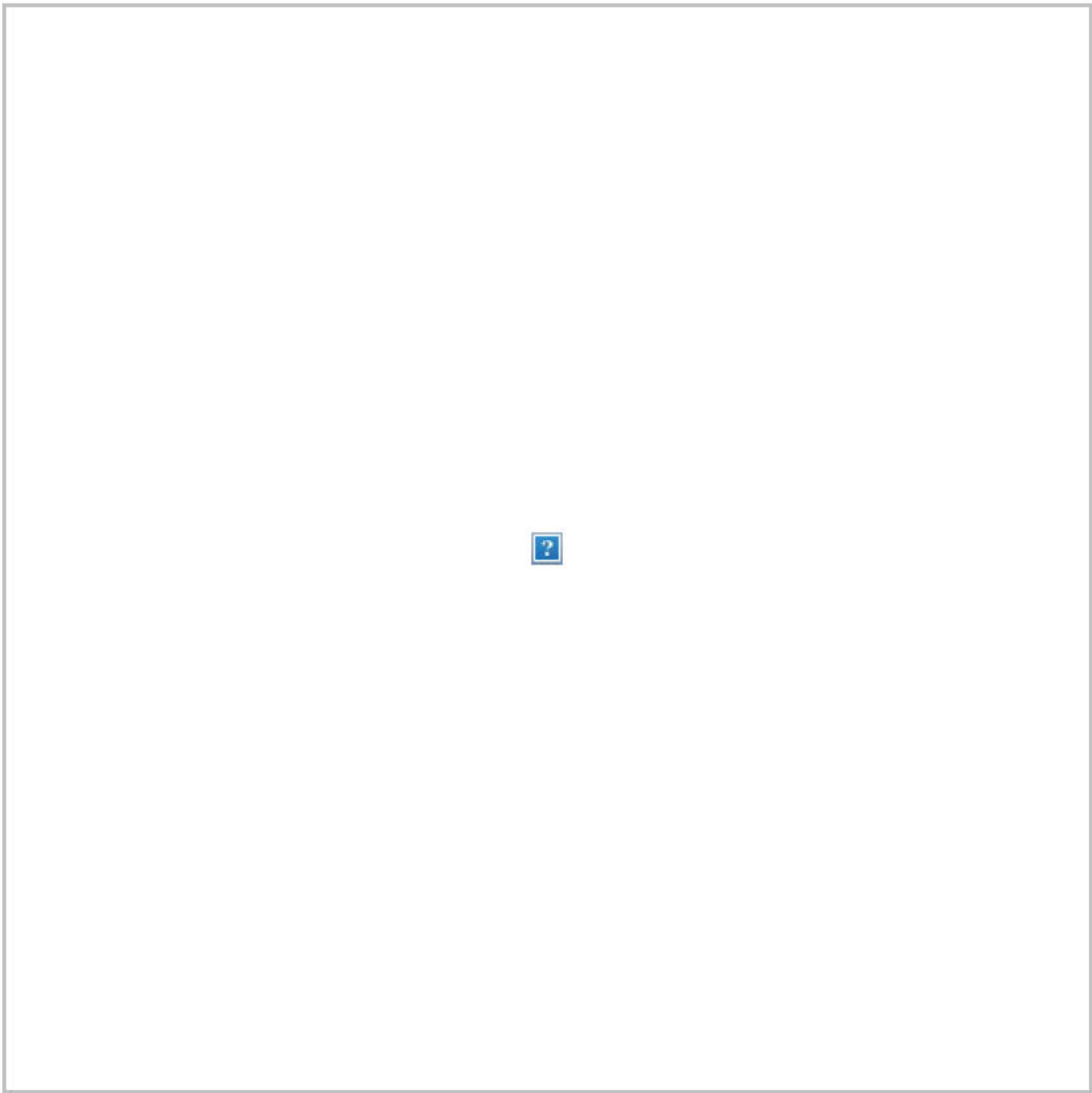
A Daily Beast reporter shared an image of Lev Parnas with Jared Kushner and Ivanka Trump:



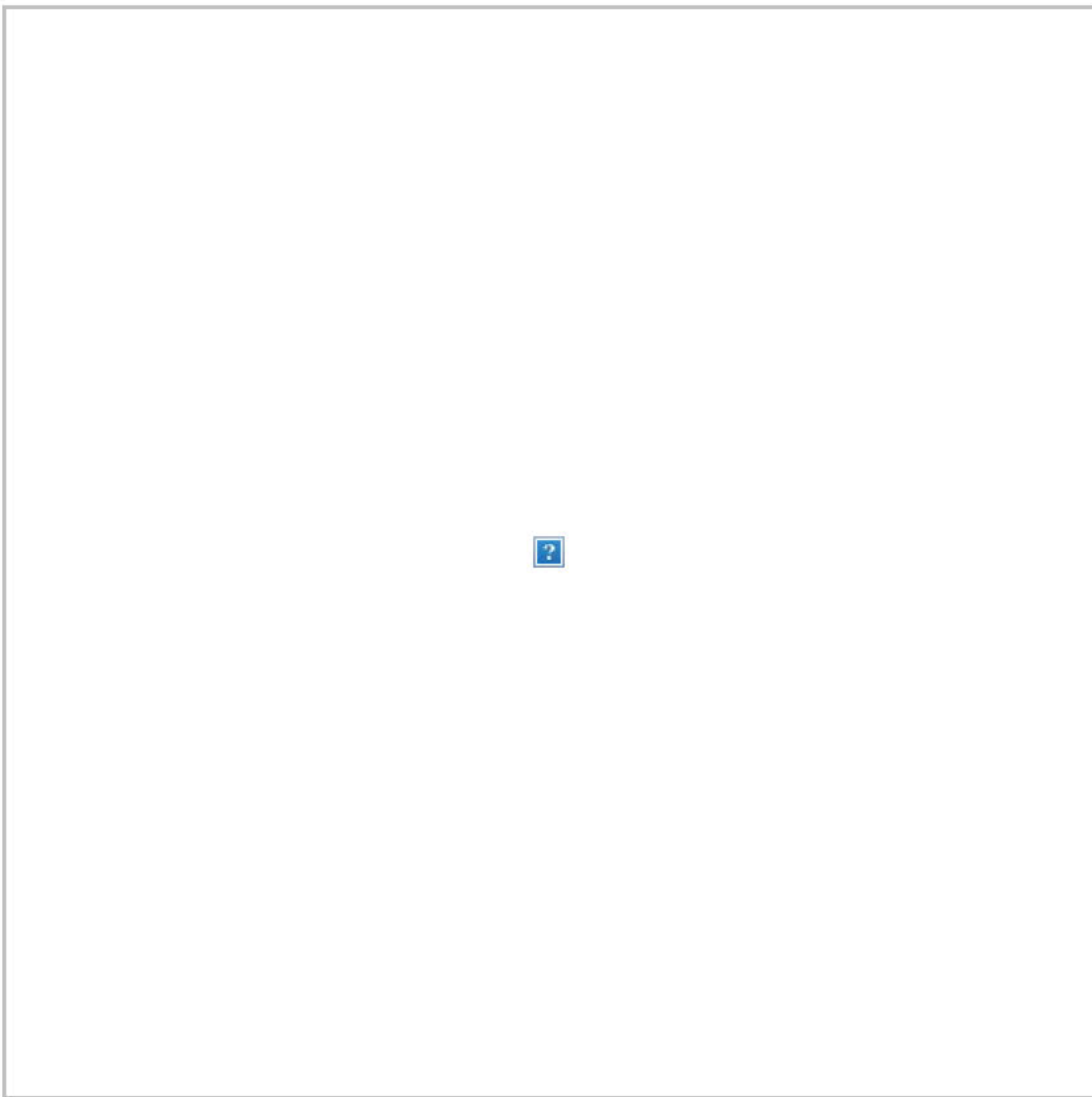
The documents Parnas turned in to Democratic investigators include this peculiar White House menu:



Other evidence in the hands of House Intelligence investigators includes this note:

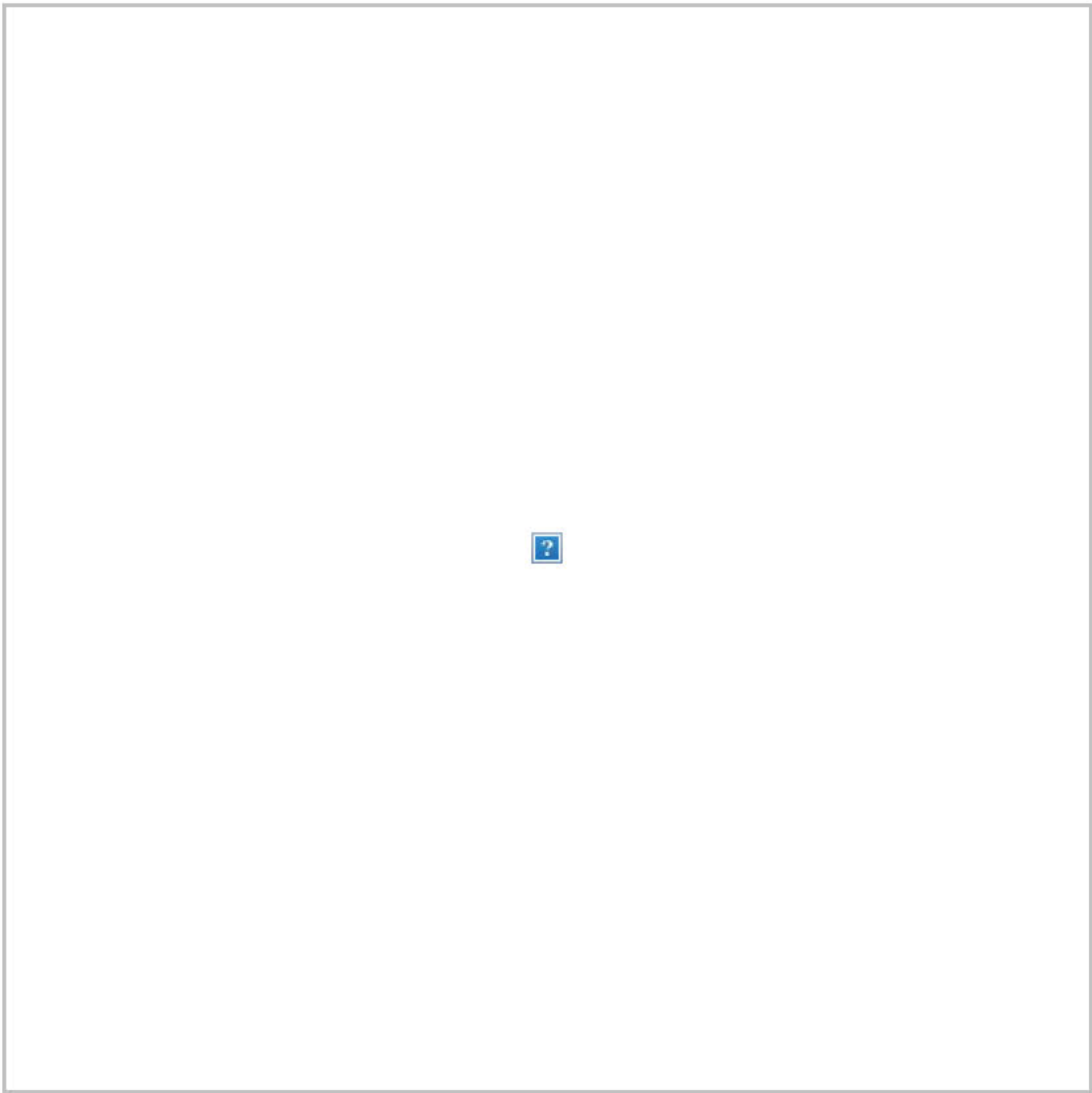


And this email:

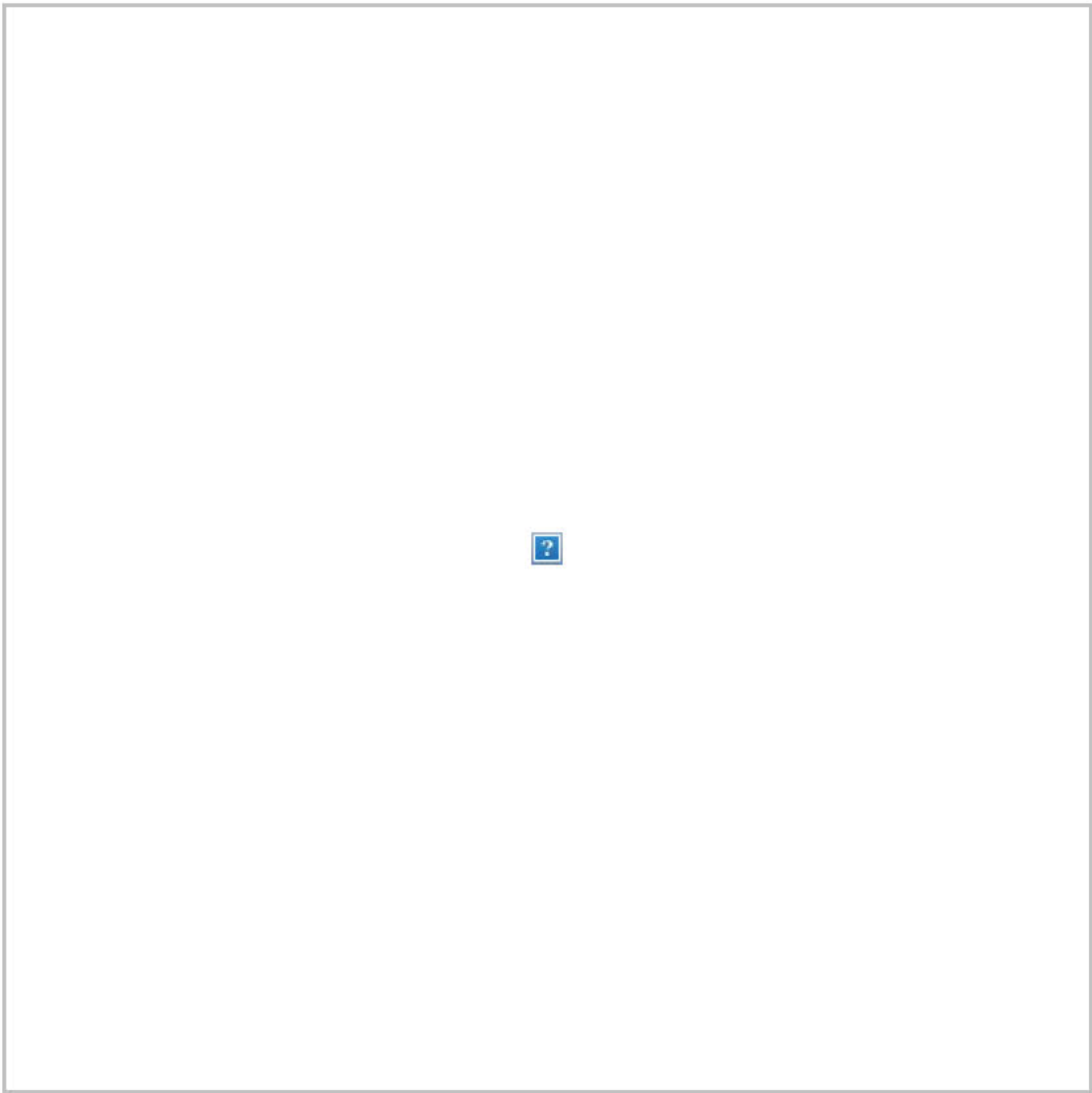


Conservative lawyer George Conway, husband of counselor to the president Kellyanne Conway, said Senate Republicans are restricting press access to the impeachment trial because they're scared and have something to hide:

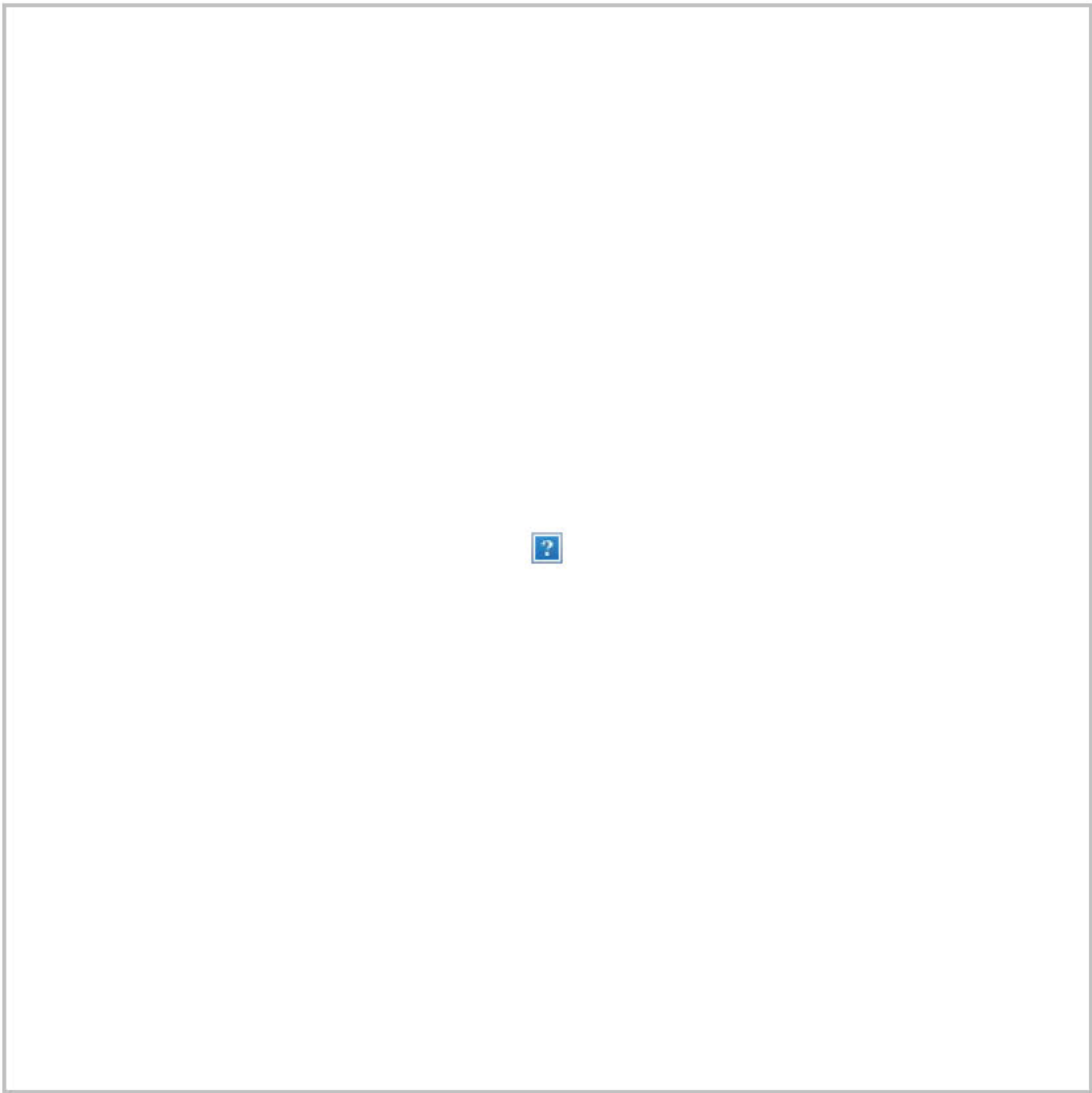




A Times photographer captured Trump wearing his reading glasses last night:



Warren's staff sent a pick-me-up to Cory Booker's team after the New Jersey senator dropped out of the presidential race:



And it finally rained in Melbourne:



Heavy rain, flash floods and severe thunderstorms swept over the Australian city. The very-welcome storm is expected to hit fire-affected parts of New South Wales and Victoria later this week, [the Guardian reports](#).

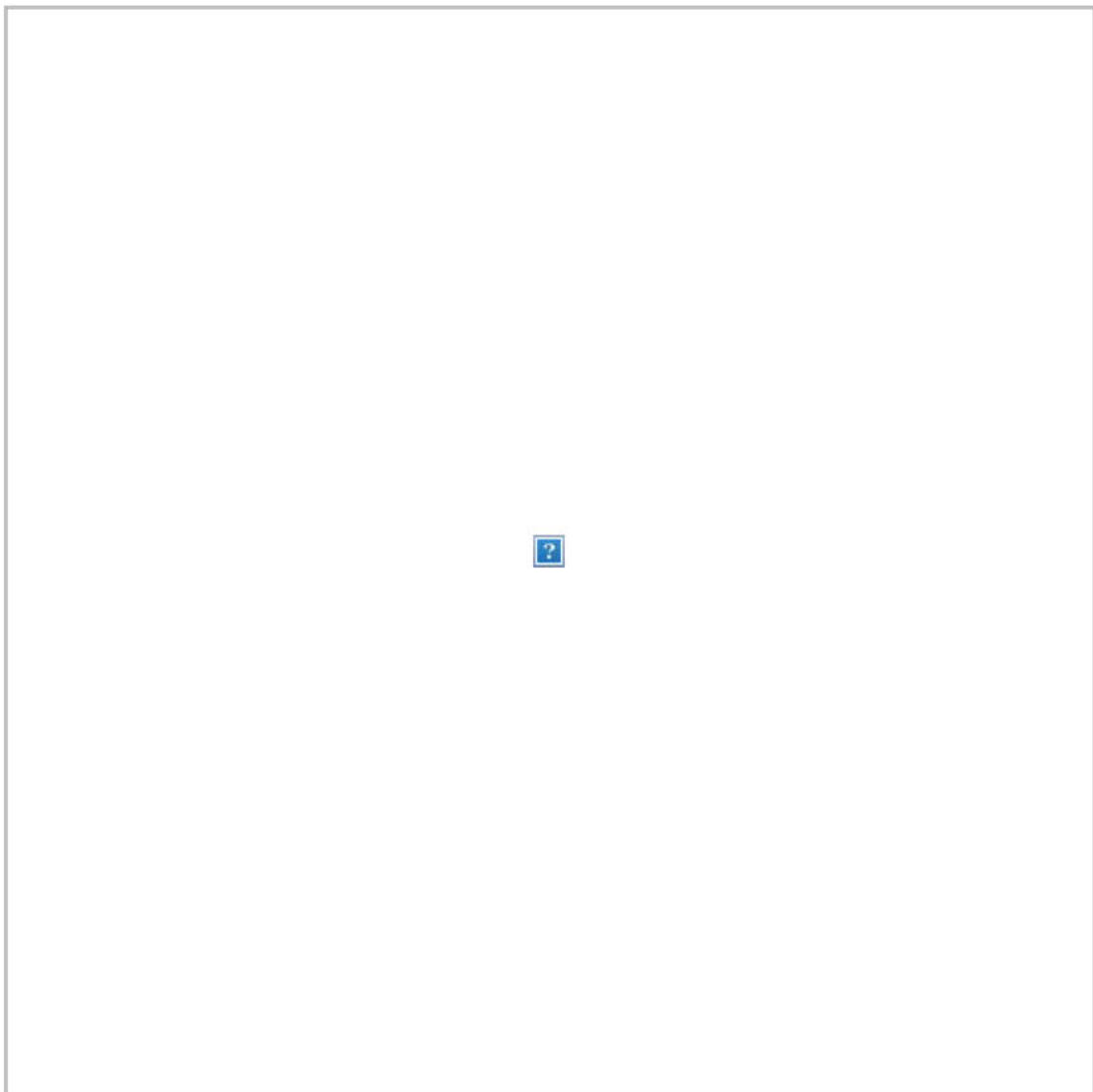
**QUOTE OF THE DAY:**

"Lyndon Johnson was sort of a tough guy. Can you imagine his phone calls? He's probably looking down, or looking up," Trump said during his rally in Wisconsin last night,

suggesting that LBJ may be in hell. ([HuffPost](#))

## **VIDEOS OF THE DAY:**

Stephen Colbert did his show live last night so he could cover the Democratic debate:



And then he wondered why Trump would talk about dishwashers during his rally in Milwaukee:





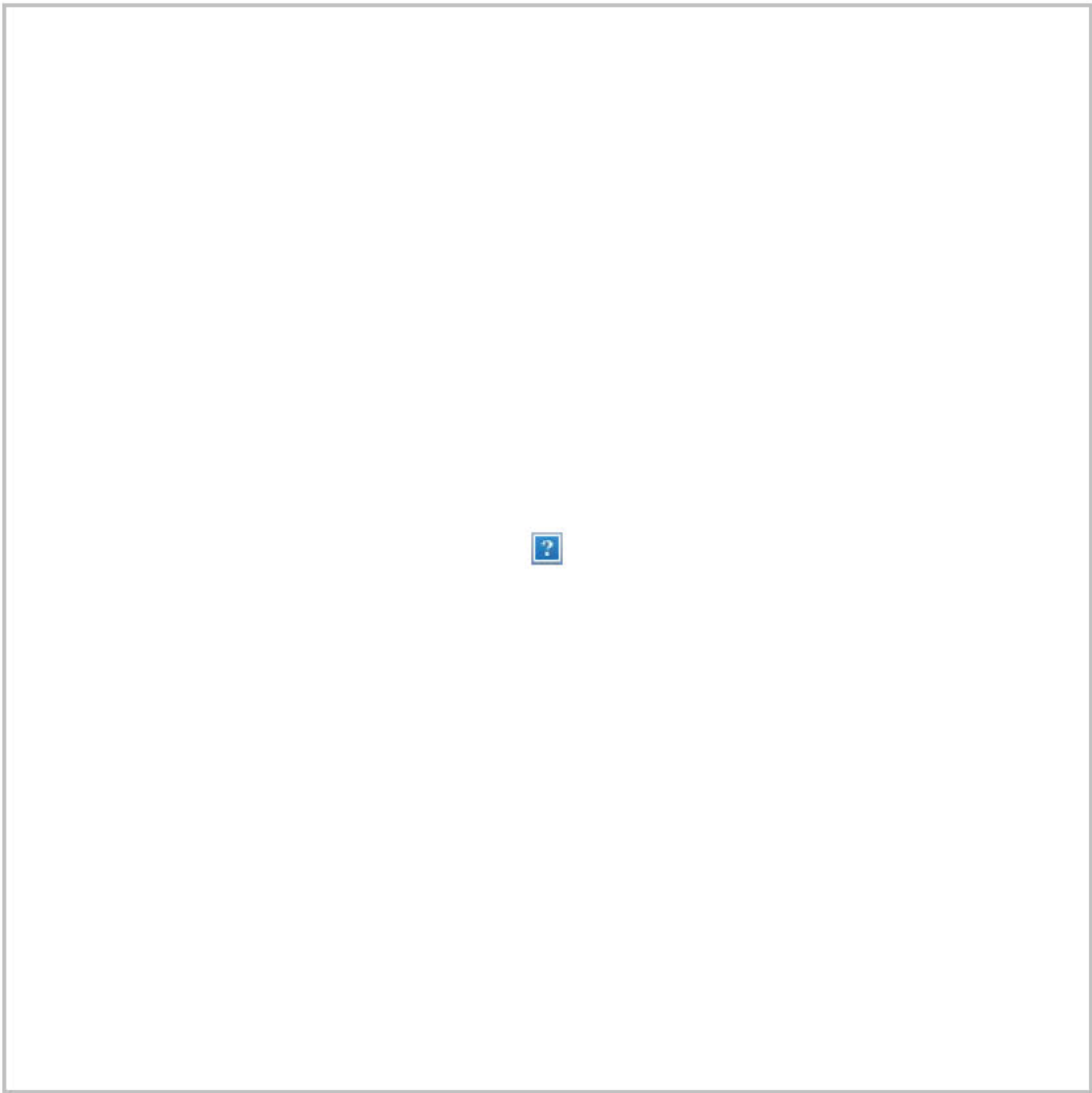
Trevor Noah opened his post-debate monologue by pointing out the demographics of the group of Democratic candidates who remain in the race:



Seth Meyers took a break from politics to introduce us all to some teen slang:



U.K. Prime Minister Boris Johnson wants Brits to pitch in and raise half a million pounds so that Big Ben can bong for Brexit:



You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)

---

©2020 The Washington Post | 1301 K St NW, Washington DC 20071



**From:** [The Washington Post](#)  
**To:** [achu@sunnyvale.ca.gov](mailto:achu@sunnyvale.ca.gov)  
**Subject:** The Daily 202: Democratic debate pits Bidenism vs. Bernieism – with the others staking out spaces in between  
**Date:** Wednesday, January 15, 2020 8:13:24 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you're having trouble reading this, [click here](#).

---

# The Daily 202



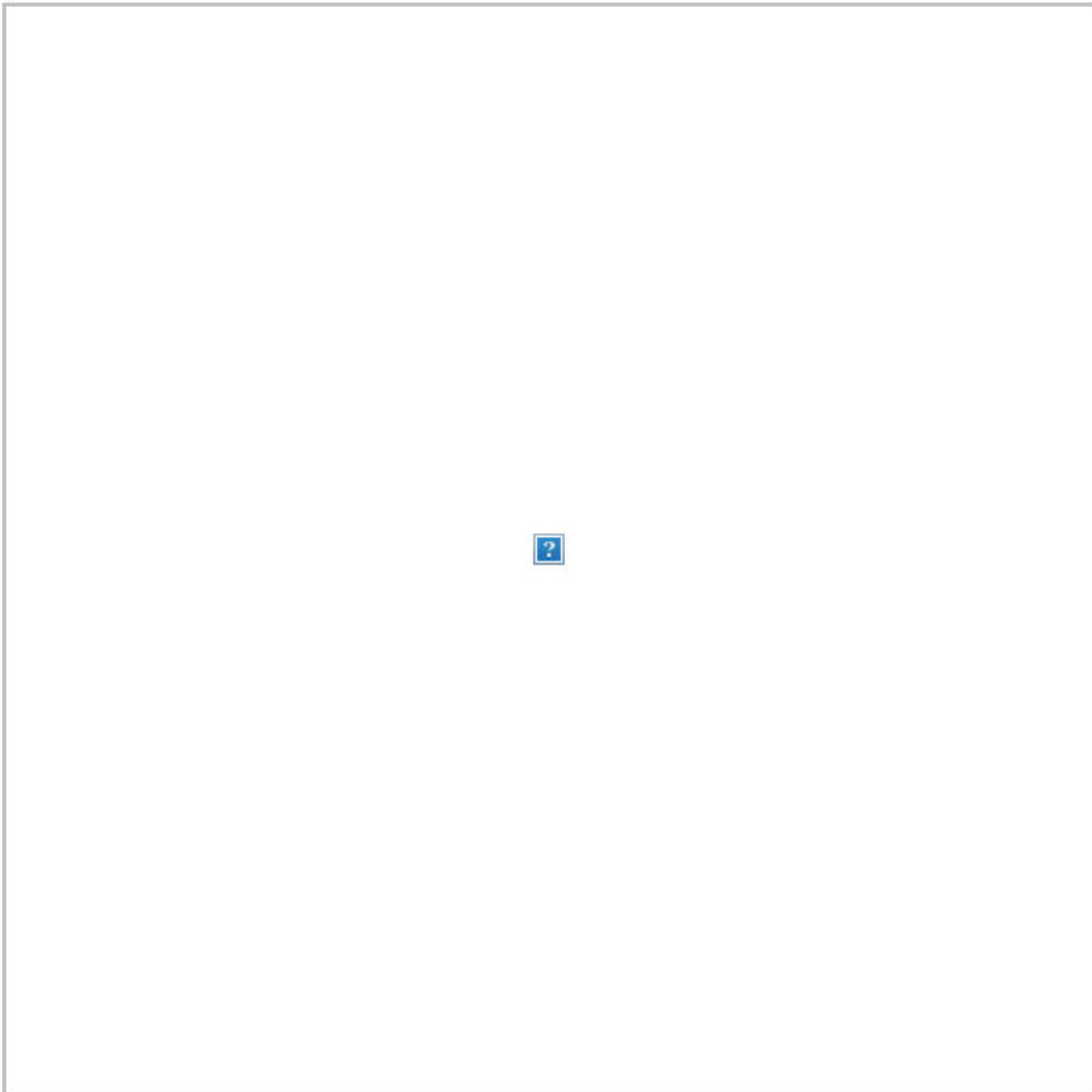


Share:  

 Listen to The Big Idea



## **Democratic debate pits Bidenism vs. Bernieism – with the others staking out spaces in between**



Elizabeth Warren and Bernie Sanders exchange words as Tom Steyer looks on after the debate. (Scott Olson/Getty Images)



**BY JAMES HOHMANN**

*with Mariana Alfaro*

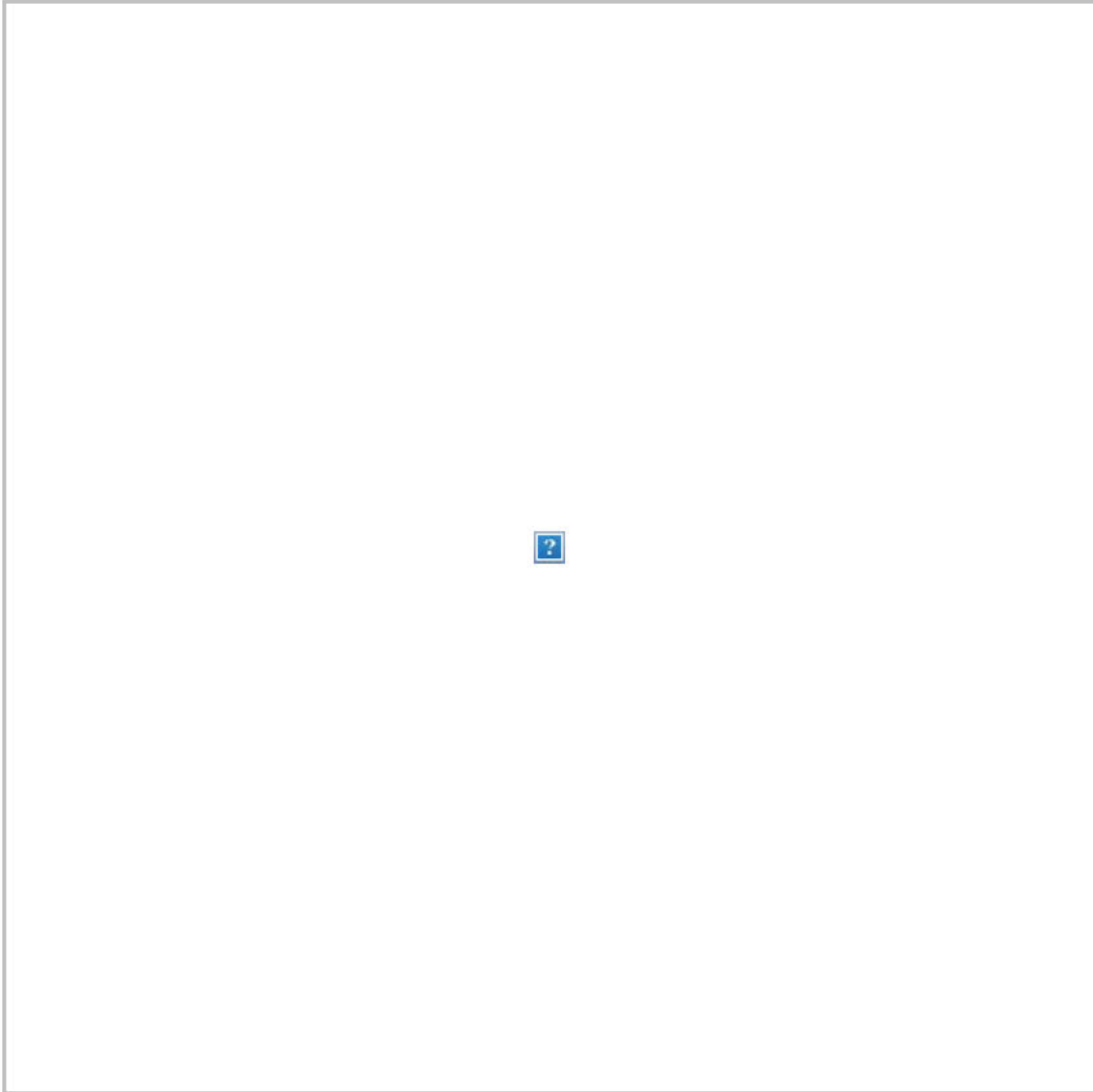
**THE BIG IDEA:** What people will remember from the final debate before the Iowa caucuses is Elizabeth Warren declining to shake Bernie Sanders's outstretched hand after their **brief onstage clash** over whether he really told her during a one-on-one dinner more than a year ago that a woman cannot get elected president. While that made for compelling television, it also distracted from a starker ideological choice that looms for Democratic voters in the weeks ahead.

The more substantive portions of the two-hour debate at Drake University in Des Moines put in stark relief the chasm between the approaches of Sanders and Joe Biden – the two leaders in Iowa and national polling – on the biggest issues that face a president, including foreign policy, health care and trade.

It also highlighted continuing tensions between the two men over experience vs. judgment, incrementalism vs. radicalism and whether Democrats are more likely to win in November by igniting the base or appealing to disenchanted moderates who defected to Donald Trump in 2016.

Whomever is coronated at the convention in Milwaukee six months from now will chart the future of the party as its standard-bearer. In Sanders's case, he has spent decades **proudly resisting pressure** to register as a Democrat. He remains an independent who caucuses with the Democrats in the Senate.

Iowa looks like a jump ball, with the latest polls showing no overwhelming favorite and many voters either undecided or willing to change their minds. The next three weeks would be an unpredictable free-for-all in the Hawkeye State anyway. But the impeachment trial threatens to strand a handful of senators in Washington for days at a time with only Sundays away from the chamber.



Joe Biden cracks a smile as Bernie Sanders attacks him during the Democratic debate at Drake University in Des Moines on Tuesday night. (Scott Olson/Getty Images)

**-- It is conceivable that neither Biden nor Sanders ultimately wins the Feb. 3 caucuses. Nevertheless, the two septuagenarians represent the ideological goalposts and the outer bounds – Sanders on the left and the Biden on the right (which, to be clear, is still left-of-center) – of what party regulars will abide.**

“Joe and I have a fundamental disagreement here, in case you haven't noticed,” Sanders said last night during the round on trade, a salient issue in a farm state where children are taught in school that Iowa is a net exporter. The line, though, can be applied to most every other flashpoint in Democratic politics.

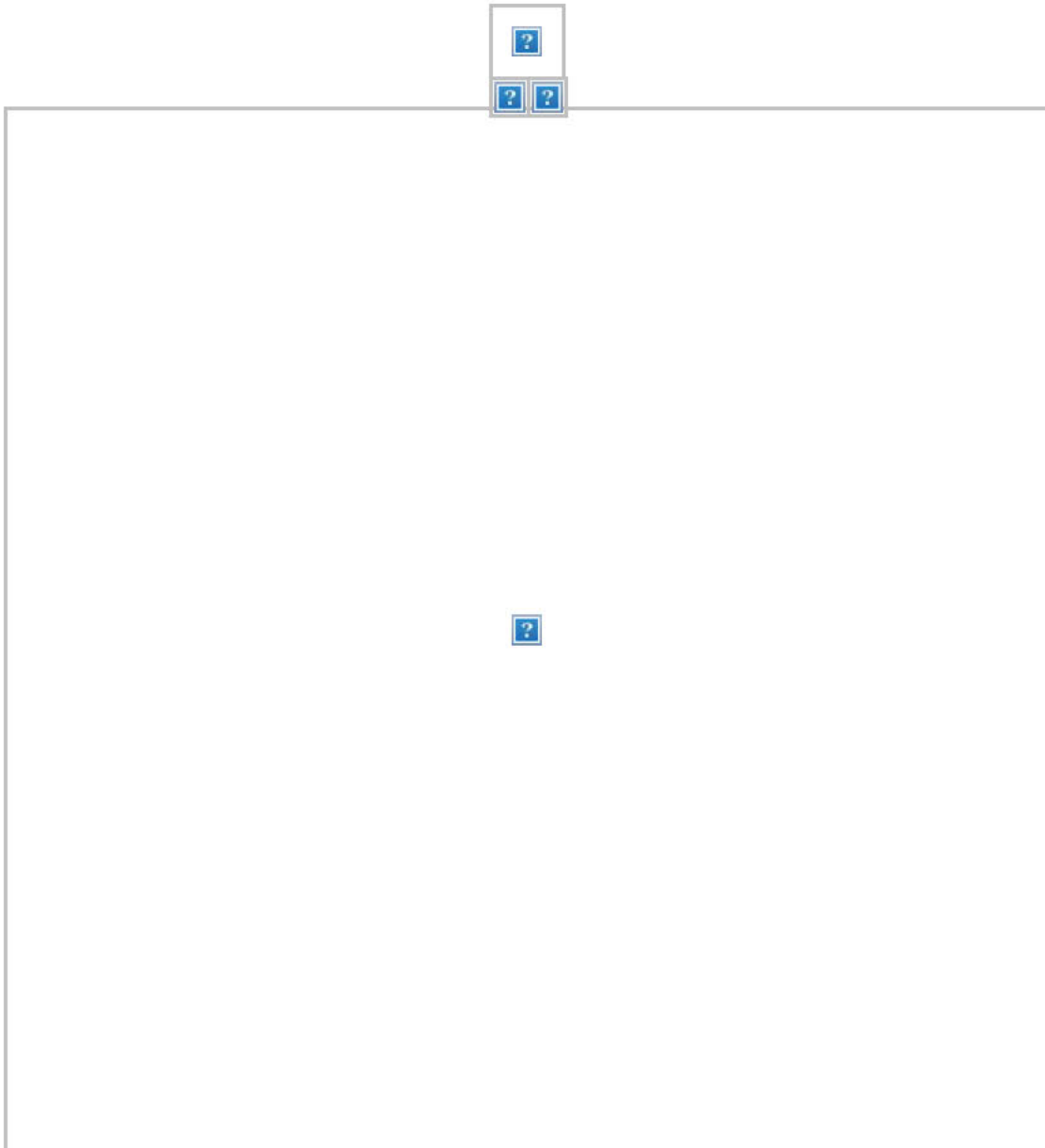
**Just as he opposed the North American Free Trade Agreement, which Biden voted for, Sanders now opposes its replacement, the U.S.-Mexico-Canada trade deal.** This iteration just passed the Democratic-controlled House and won the endorsement of the AFL-CIO. It's awaiting a vote in the Senate. “The answer is we could do much better than a Trump-led trade bill,” Sanders said. “If this is passed, I think it will set us back a number of years.”

**Biden, who supports the new deal, accused Sanders of knee-jerk opposition to everything.** “I don't know that there's any trade agreement that the senator would ever think made any sense, but the problem is that 95 percent of the customers are out there,” Biden said, referring to the rest of the world. “So we better figure out how we begin to write the rules of the road, not China.”

Sanders attacked Biden for voting to ratify multiple agreements over the years that he said have helped large multinational corporations at the expense of workers. Biden compared Sanders's approach to



“poking our finger in the eye of all of our friends and allies” by not trying to negotiate trade agreements with the rest of the world, which he argued empowers China.



Candidates take on foreign policy, trade, electability at seventh Democratic debate

**-- The trade clash was particularly interesting to watch because Sanders proudly stood alone onstage among the top-tier candidates in opposing the USMCA deal. Pete Buttigieg, Amy**



**Klobuchar and even Warren endorsed it.** Trying to show that she has a pragmatic streak, Warren called the deal imperfect but reasoned that “it will give some relief” to farmers and workers. “We get up the next day and fight for a better trade deal,” she said.

**It was a reminder of the extent to which the other candidates have all sought to position themselves somewhere between the poles of Sanders and Biden, and this played out repeatedly.** In theory, Biden and Sanders occupy separate “lanes,” to use the parlance of the operative class. But both men see the other as a direct threat. The Sanders team, in particular, has believed all election cycle that they’re competing for Biden voters just as much as Warren voters.

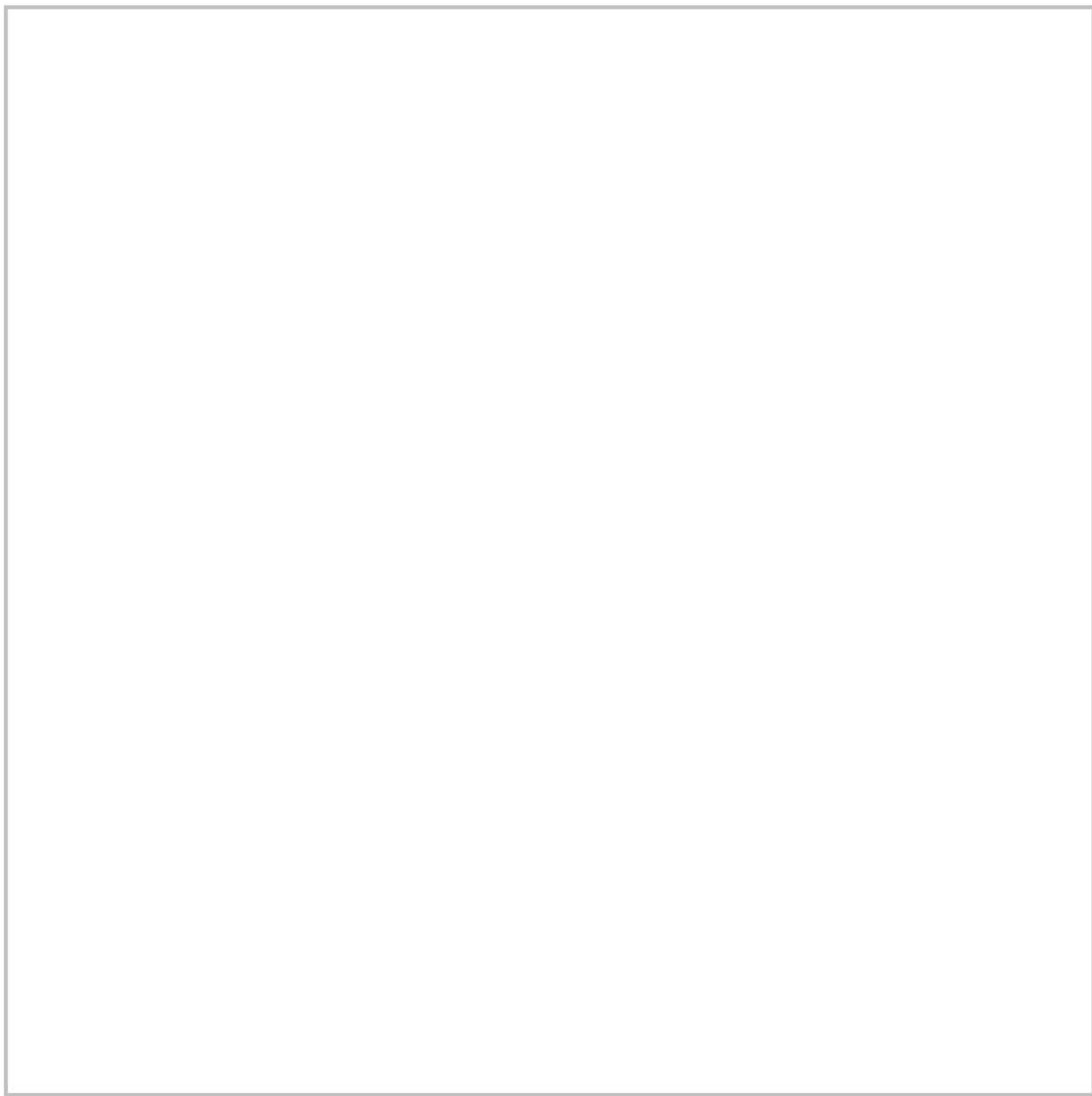
**Warren also tried to distinguish herself at one point by noting that she was the only candidate onstage who has defeated a Republican incumbent in the last 30 years.** She ousted Republican Scott Brown in 2012 to take back Ted Kennedy’s Senate seat in Massachusetts. Sanders chimed in to say that he defeated a GOP incumbent in Vermont to win a House seat in 1990. An amused Warren, once a high school debate state champion in Oklahoma, noted that this was why she specified 30 years. Then Biden added that he won a major upset in 1972 – 48 years ago – over a Republican incumbent to win his Senate seat.

**-- Biden often sounds like he’s promising a return to the pre-Trump status quo, when he was vice president.** “We can overcome four years of Donald Trump, but eight years of Donald Trump will be an absolute disaster and fundamentally change this nation,” he said. “We have to restore America’s soul, as I’ve said from the moment I

announced.”

**Sanders counters that “this is the moment when we have got to think big, not small”:** “This is the moment when we have got to have the courage to take on the 1 percent, take on the greed and take on the corruption of the corporate elite,” he said in his closing, “and create an economy and create a government that works for all of us, not just the 1 percent.”

**CNN’s Abby Phillip also noted that Sanders identifies as a democratic socialist and pointed to a poll that showed about two-thirds of Americans don’t like the idea of voting for a socialist.** She wondered, “Doesn’t that put your chances of beating Donald Trump at risk?” Sanders replied, “Nope, not at all.” He pivoted to attack Trump, displaying the moral certitude that his supporters love but Democratic establishmentarians loathe.



Iran takes center stage at Democratic debate

**-- The gulf between Sanders and Biden was apparent from the opening question of the debate.** The crisis in Iran has prompted the leading candidates to re-litigate the 2002 debate over whether to go to war with Iraq. "Joe and I listened to what Dick Cheney and George Bush and [Donald] Rumsfeld had to say," Sanders said. "I thought they were lying. I didn't believe them for a moment. I took to the floor. I did everything I could to prevent that war. Joe saw it differently."

**Biden emphasized his work bringing troops home from Iraq as**



**Barack Obama's vice president.** "It was a mistake to trust that they weren't going to go to war," he said, referring to the Bush administration. "They said they were not going to go to war. ... It was a mistake, and I acknowledge that."

**-- The well-trod debate over health care was similar, as Biden and Sanders went at it again over the price tag for Medicare-for-all and the other candidates staked out ground in between them.** Phillip, one of three moderators, asked Sanders about a study that said his policy proposals would double federal spending as a share of GDP to a level not seen since World War II. "No, my plan would not bankrupt the country," he answered. "I think you should show how you're going to pay for things, Bernie," replied Klobuchar.

**Warren sponsored Sanders's Medicare-for-all bill, but she moved away from it in the face of questions about how she'd implement it without raising taxes on the middle class or kicking people off their private insurance.** Warren ultimately proposed a three-year transition period to Medicare-for-all, but this only led to attacks from her left and right. Last night, Warren and Buttigieg bickered about who would get covered and how much it would cost.



Fact-Checking the January Democratic debate



-- Our Fact Checker team **calls out Biden and Sanders**, more than the other candidates, for making multiple misleading or false **statements**. For example, Biden did not provide an accurate description of what Bush said before the 2002 vote that allowed for war. Biden also boasted about getting troops out of Iraq under Obama without noting that this allowed for the emergence of the Islamic State,



which required the Obama-Biden administration to send combat troops back into the country. The Fact Checker team faults Sanders for claiming that Medicare-for-all will cost less than the status quo, for significantly exaggerating the number of people who go bankrupt because of medical bills and for incorrectly claiming that the United States spends twice as much per person on health care as “any other country.” It’s only true compared to the developed world.

**-- Warren, Buttigieg and Klobuchar are trying to varying degrees to position themselves as unity candidates between Sanders and Biden who can win support from both sides and therefore beat Trump.**

“It is easy to draw lines in the sand and sketch out grand ideological visions that will never see the light of day,” said Klobuchar. “What is hard is bringing people together and finding common ground instead of scorched earth. ... If you are tired of the extremes in our politics and the noise and the nonsense, you have a home with me.”

“We cannot take the risk with so much on the line of trying to confront this president with the same Washington mindset and political warfare that led us to this point,” said Buttigieg. “If you are watching this at home and you are exhausted by the spectacle of division and dysfunction, I’m asking you to join me to help turn the page on our politics.”



Sanders denies he told Warren a woman couldn't win the presidency

**-- Here's what you need to know about the Warren vs. Sanders kerfuffle: Sanders's campaign manager Faiz Shakir told The Post that Warren "came to raise a concern" with him after the debate.** "And he said let's talk about that later," Shakir said, declining to provide further details about the conversation captured in a viral video.

"Warren said Sanders disagreed with her view that a woman could win the presidential election. Sanders contends that he merely outlined what he said would be Trump's efforts to defeat another

female candidate, and in the debate, he said, ‘Of course a woman can win,’” [Annie Linskey and Sean Sullivan report](#). “The video ... shows Sanders extending his hand as Warren approaches him onstage. Rather than shaking it, Warren clasps her hands together and speaks to Sanders. He responds, as Tom Steyer walks toward them. ... Warren and Sanders then separate. Steyer and Sanders shake hands on one side of the stage. Nearby, Warren shakes hands with [Buttigieg]. ... Representatives for the Warren campaign declined to comment. After the debate, Steyer told MSNBC’s Chris Matthews that he did not know what Warren and Sanders said to each other.”

**-- Dan Balz notes that the Warren-Sanders clash was inevitable, and they remain on a collision course after last night:** “For the past few months, Warren found herself looking at Buttigieg as a more immediate threat in Iowa. She took a lead in a September Iowa poll by the Des Moines Register and CNN, only to see Buttigieg overtake her in the November poll. She and the mayor seemed to be competing in Iowa for the support of more-affluent voters with college degrees. Sanders’s campaign saw that as an opening and seized it.”

**New Hampshire could be even more consequential because Warren and Sanders both come from neighboring states and have invested heavily.** “That gives both of them a potential edge, and whoever finishes behind the other will have suffered a significant setback,” Dan notes.

**-- Warren spoke the most during the debate:**

(Dan Keating and Kevin Schaul)



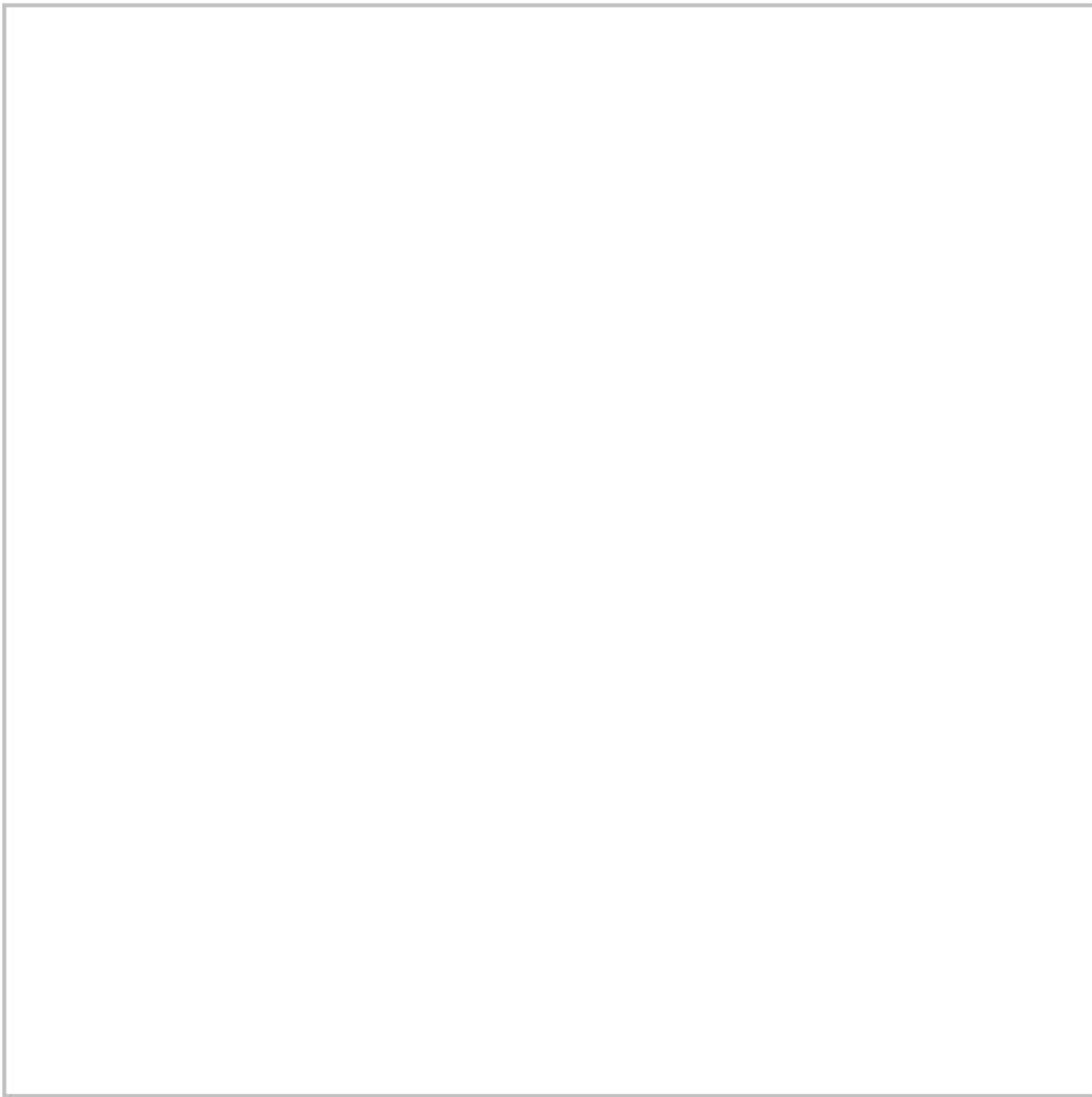
(Dan Keating and Kevin Schaul)

**-- The Post's opinion columnists largely focused on Warren vs. Sanders.** "Can a woman be elected president? Let's put that silly question behind us," wrote [Karen Tumulty](#). "Sanders vs. Warren shows the difference between identifying sexism and giving in to it," declared [Ruth Marcus](#). "There's a reason Bernie Sanders said Elizabeth Warren is lying," noted [David Von Drehle](#). "Democratic officials have reason to hope for a happy ending," said [Eugene Robinson](#). "The debate shows why."



-- Pundits are all over the place in their lists of winners and losers, suggesting that the muddled debate will do little to alter the trajectory of the race. [The Fix's Aaron Blake](#) considered Warren's sly attack on Sanders *and* Sanders's response winning moves. He said Buttigieg lost and Biden was "in the middle." [CNN's Chris Cillizza](#) thought Buttigieg, Warren and Klobuchar won, but Biden, Sanders and Steyer lost. But [Politico's campaign reporters](#) agreed with one another that Biden had the best night. [Fox News's Bret Baier](#) said Biden's performance was lackluster and Klobuchar "actually had a really good night" while Sanders "took a lot of incoming." [Vox](#) put Sanders and Buttigieg on its winners list and named Steyer as the losing candidate. Biden was on neither. [Jennifer Rubin](#) said Klobuchar and Biden shined. "The rest, not so much," she wrote.





Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



Pelosi announces impeachment managers

## **THE LATEST ON IMPEACHMENT:**

**-- Speaker Nancy Pelosi named the seven House Democrats who will serve as impeachment managers during the Senate trial:**

Intelligence Committee Chairman Adam Schiff (Calif.), Judiciary Committee Chairman Jerry Nadler (N.Y.), Hakeem Jeffries (N.Y.), Sylvia Garcia (Tex.), Val Demings (Fla.), Zoe Lofgren (Calif.) and Jason Crow (Colo.). Trump's defense team is expected to be led by White House counsel Pat Cipollone. Notably, Rep. Justin Amash, the

Republican-turned-independent who voted for impeachment, is not one of the managers. Lofgren worked on Richard Nixon's impeachment as a House staffer and was on the House Judiciary Committee during Bill Clinton's impeachment. ([We'll update our liveblog with more news all day.](#))



Rudy Giuliani, the president's personal lawyer, brought Lev Parnas, left, as his guest to the state funeral service for former president George H.W. Bush at the Washington National Cathedral in December 2018. (Al Drago/Bloomberg News)

**-- New materials released last night by House Democrats appear**

to show Ukraine's top prosecutor offering one of Rudy Giuliani's associates damaging information related to Joe Biden if the Trump administration recalled the U.S. ambassador to Ukraine. [Paul Sonne, Rosalind S. Helderman and Tom Hamburger report](#): "The text messages and documents provided to Congress by former Giuliani associate Lev Parnas also show that before the ambassador, Marie Yovanovitch, was removed from her post, a Parnas associate now running for Congress sent menacing text messages suggesting that he had Yovanovitch under surveillance in Ukraine. A lawyer for Yovanovitch said Tuesday that the episode should be investigated. ...

"Among the revelations in the documents released Tuesday: a message from Giuliani to Parnas saying he had involved a person he called "no 1" — possibly Trump himself — in an effort to lift a U.S. visa ban on a former Ukrainian prosecutor [who was planning to come to the United States](#) to make claims about Biden. The materials also include a letter Giuliani wrote to Ukraine's then-president-elect, Volodymyr Zelensky, requesting a May 14 meeting with the new leader in Giuliani's "capacity as personal counsel to President Trump and with his knowledge and consent." Giuliani scrapped his planned trip, and the meeting never took place. Another document released by the House investigators appears to show Parnas directly involved with efforts to get Zelensky to announce investigations related to Biden. In handwritten notes on a piece of stationery from the Ritz-Carlton Hotel in Vienna, Parnas wrote, 'get Zalenksy [sic] to Annouce [sic] that the Biden case will be Investigated.' ...



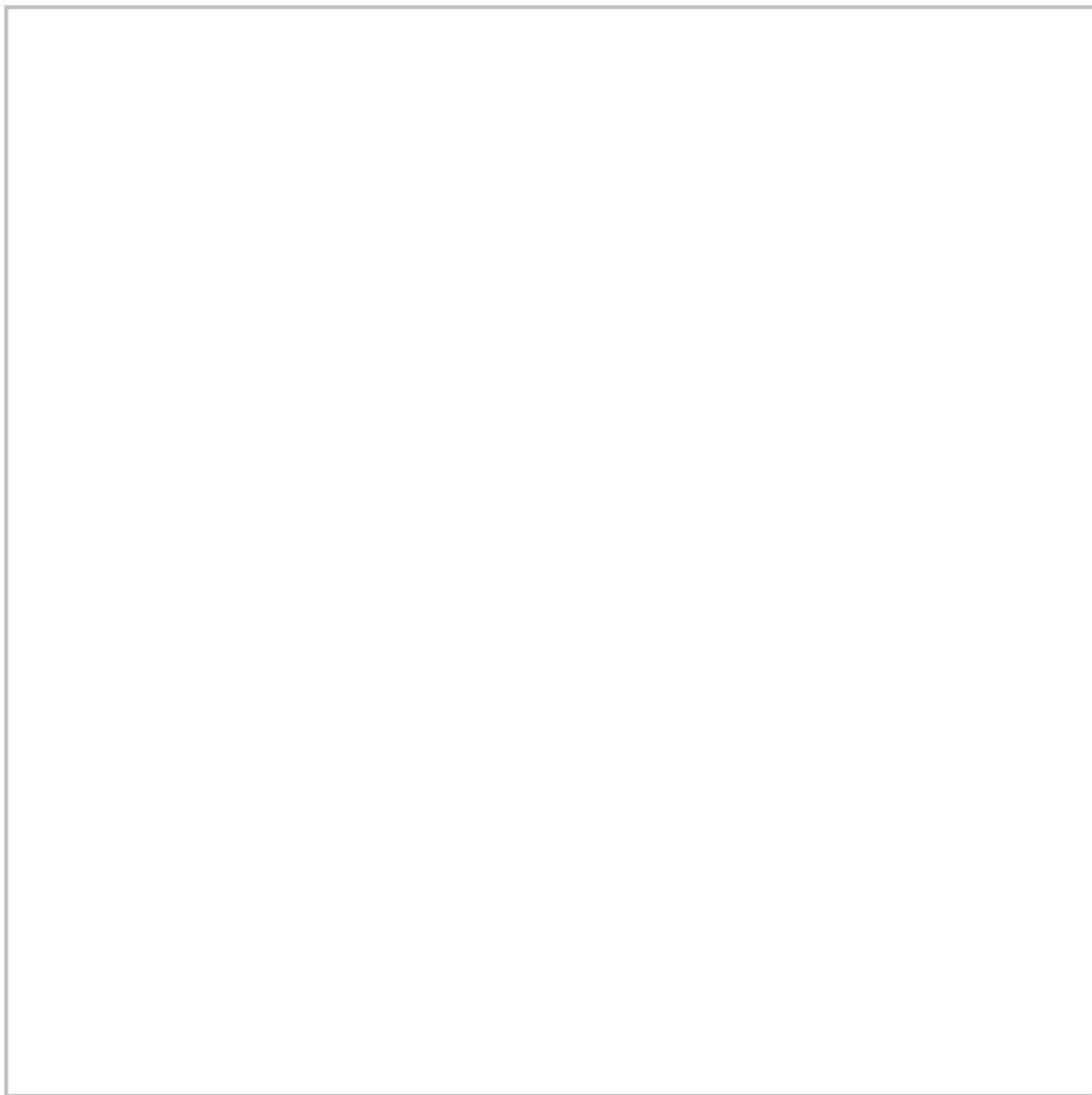
**"The materials show that Parnas, a Russian-speaker who helped coordinate Giuliani's outreach to Ukrainian sources, was directly communicating with an array of top Ukrainian officials.** Among them was Yuri Lutsenko, at the time Ukraine's top prosecutor and a close political ally of then-Ukrainian President Petro Poroshenko, who was running for reelection. Lutsenko wanted to get rid of Yovanovitch, the U.S. ambassador, in part because she had been critical of his office and supported a quasi-independent anti-corruption bureau he despised. The messages, written in Russian, show Lutsenko urging Parnas to force out Yovanovitch in exchange for cooperation regarding Biden. At one point, Lutsenko suggests he won't make any helpful public statements unless 'madam' is removed.

**"The new documents also introduced a new character in the drama over the ambassador's ouster: a Republican congressional candidate from Connecticut who asserted to Parnas in messages that he had Yovanovitch under physical and electronic surveillance.** 'Wow. Can't believe Trumo [sic] hasn't fired this b----,' Robert F. Hyde wrote in an encrypted message to Parnas on March 23. 'I'll get right [on] that.' Hyde described having contact with a 'private security' team located near the embassy that was apparently monitoring the ambassador's movements. 'She's talked to three people. Her phone is off. Computer is off,' he wrote in one message. 'They will let me know when she's on the move,' he said in another. Later, he alerted Parnas that he had been told Yovanovitch would not be moved to a 'special security unit.' 'They are willing to help if we/you would like a price,' he said in one note. 'Guess you can do anything in the Ukraine with money . . . what I was told.' Hyde did not explain how his team might 'help' Parnas, who responded only



with 'lol.' When asked for comment by The Washington Post in a text message, Hyde replied: 'Sorry I can't talk right now.' Hyde is one of three Republicans running to unseat an incumbent Democrat in the 5th Congressional District in Connecticut. He frequently tweets about his support for Trump and posted photos of himself with the president." ([Review the full cache of material for yourself here.](#))

**-- All the president's men, cont.: Former Trump national security adviser Michael Flynn asked a federal judge for permission to withdraw his guilty plea of lying to the FBI about this Russian contacts during special counsel Bob Mueller's probe.** [Spencer S. Hsu reports](#): "The stunning reversal — more than two years after Flynn pleaded guilty Dec. 1, 2017, and two weeks before he faces sentencing — threatens to sidetrack, if not derail, the prosecution of the highest-ranking Trump official charged and one of the first to cooperate with Mueller's office."



Russian Prime Minister Dmitry Medvedev holds a Russian-made weapon during a visit to the Promtehnologiya firearms company in Moscow in 2013. Medvedev resigned today as part of a shake-up orchestrated by Vladimir Putin. (Dmitry Astakhov/Sputnik/AFP via Getty Images)

**-- Russia's prime minister submitted his resignation today as part of a surprise government shake-up directed by President Vladimir Putin.** [Isabelle Khurshudyan reports from Moscow](#): "Putin accepted the resignation of the prime minister, Dmitry Medvedev, and asked the members of Medvedev's Cabinet to remain in place until a new government is formed ... The sweeping moves came shortly after

Putin gave his annual address to Russia's lower house of parliament and proposed constitutional changes to boost the powers of prime ministers and Cabinet members. ... Earlier, Putin proposed sweeping changes to the constitution Wednesday, including strengthening parliament and revamping the country's state council, possibly hinting at his plans for after he leaves power in 2024. In his annual address to lawmakers, Putin again suggested limiting presidential term limits to two, indicating that 20 years after he first became president, he won't attempt to seek a third consecutive term. But **Putin's plan to give constitutional status to the state council, a top advisory body to the president he created in 2000, and transfer more power to parliament, including naming the country's prime minister, could be a path for him to maintain significant influence in a different capacity once this presidential term is finished.** As the Russian constitution stands now, the president has the sole power to appoint the prime minister."



'There is little or no sentiment' among GOP for dismissing Senate trial, McConnell says

**-- Mitch McConnell is trying to balance the feuding factions within the Senate Republican Conference over whether to vote on calling witnesses.** [Seung Min Kim, Elise Viebeck and Robert Costa report](#): "On one end, a group of influential swing GOP senators — Sens. Susan Collins of Maine, Lisa Murkowski of Alaska, Mitt Romney of Utah and Lamar Alexander of Tennessee — are pushing to hold a vote on whether to call witnesses later in the proceedings. Democrats have vowed to exert pressure on the group to break with



their party on witnesses and other issues, such as obtaining documents. At the same time, the Senate's right flank is increasingly making the case to [McConnell] and other GOP leaders for a more aggressive posture in defense of Trump. In a private meeting with McConnell on Tuesday, Sen. Ted Cruz (Tex.) argued that if Democrats press the case for potentially damaging witnesses — such as former national security adviser John Bolton — the GOP should insist on incendiary witnesses of their own, such as Hunter Biden ... McConnell appeared receptive to Cruz's pitch ...

“Despite their role as potential swing GOP votes in a narrowly divided Senate, the group of moderates has yet to defect in any significant fashion from party leaders ... **In a nod to the moderates, there is expected to be a provision guaranteeing a vote on whether the Senate could consider subpoenaing witnesses**, according to two GOP officials familiar with the matter ... GOP leaders are confident that once voting begins to set the scope of the trial — called an organizing resolution — that no Republicans will defect, with the moderates placated by a guaranteed decision on witnesses later. That calculus could change once the Senate goes through the grind of opening arguments and a litany of questions, and if key GOP senators become dissatisfied that they hadn't gotten enough information from the trial proceedings.”

**-- Capitol Hill reporters are protesting unexpected restrictions on their access to the Senate during the impeachment trial.** [Derek Hawkins](#), [Felicia Sonmez](#) and [Fred Barbash](#) report: “The organization representing daily reporters on Capitol Hill is protesting restrictions expected to be imposed on the news media during the Senate



impeachment trial, saying the security crackdown will severely limit access to lawmakers and stifle coverage of the proceedings. ... Capitol security officials are [reportedly] considering measures that are all but certain to make it harder for journalists to report on the trial and question senators about their actions. A magnetometer in the Senate press gallery will require reporters to trickle into the chamber one at a time. Electronic devices will be banned, leaving reporters to scuttle in and out of the room to send tweets and emails. Reporters will be placed in pens, roping them off and restricting their ability to speak freely with senators as they enter and exit. ... Details about the nature and scope of the restrictions under consideration remained unclear, as neither the Senate sergeant at arms nor the Senate Committee on Rules and Administration, which are responsible for them, has issued a formal document.”

**-- Trump’s impeachment trial is a perilous duty for Chief Justice John Roberts because any signs of partisanship could further erode the Supreme Court's legitimacy. [From the New York Times](#):** “The chief justice’s responsibilities at the trial are fluid and ill-defined, and they will probably turn out to be largely ceremonial. ... The managers will march the articles over to the Senate chamber, touching off a series of steps that will initiate the trial. But before it can get underway Chief Justice **Roberts will be sworn in as the presiding officer and, in his first official act, administer an oath to senators in which they swear to do ‘impartial justice’ in the trial, with the real work not expected to begin until Tuesday.** ... Roberts has plenty on his plate already, much of it related to Mr. Trump. He is working on a Supreme Court docket crowded with divisive issues, including three cases on whether to allow release of Mr. Trump’s

financial records and one on Mr. Trump's efforts to withdraw protection from deportation for young immigrants. ... And Chief Justice Roberts has exchanged sharp remarks with Mr. Trump, laying bare a fundamental disagreement about the independence of federal judges."



Democrats have enough Republican votes to pass war resolution, says Kaine

## **THE IRAN CRISIS:**

**-- The Senate is poised to pass a resolution limiting Trump's**



**military authority on Iran, as four Republicans say they will vote with Democrats to assert Congress's war powers under the Constitution.** [Karoun Demirjian reports](#): “Congress cannot be sidelined on these important decisions,” said [Collins] who on Tuesday declared her support for the measure. She joins Sens. Todd C. Young (R-Ind.), Mike Lee (R-Utah) and Rand Paul (R-Ky.) and all 47 Democrats. A vote could come as soon as next week. ... The resolution is ‘privileged,’ meaning Republicans opposed to the measure cannot block it from coming to a vote once it is ‘ripe.’ It also means that supporters must secure only a simple majority of the Senate, 51 votes, for it to pass. **But it is almost certain that Trump will veto the measure and that Congress will not have the votes to override a veto.** ... Trump’s deputies and supporters said that such resolutions send a negative message to the troops and seemingly project support for the Iranian regime despite its sponsorship of terrorist activities that have led to the deaths of U.S. service members ... Supporters of the war powers measures have taken pains to say they believe [Iranian commander, Maj. Gen. Qasem] Soleimani was reprehensible as they argue that Trump cannot trample on Congress’s right to declare war.” (Kaine and Lee make the case for the resolution in [an op-ed in today’s newspaper](#).)

**-- [New video](#) shows two Iranian missiles hit the downed Ukrainian plane last week.** The [Times reports](#): “The missiles were launched from an Iranian military site around eight miles from the plane. The new video fills a gap about why the plane’s transponder stopped working, seconds before it was hit by a second missile. ... Neither strike downed the plane immediately. The new video shows the airliner on fire, circling back toward Tehran’s international airport.

Minutes later it exploded and crashed down, narrowly missing the village of Khalaj Abad ... The Times has confirmed that the new video was filmed by a camera on the roof of a building near the village of Bidkaneh, four miles from an Iranian military site. Amir Ali Hajizadeh, commander of the Islamic Revolutionary Guards Corps' airspace unit, said that missiles were launched from a base near there." ([Watch the video here.](#))

**-- The Iranian people, disturbed by the downing of the plane and the killing of Soleimani, have shown that it is possible to be angry at both their government and the United States at the same time.** [Erin Cunningham explains](#): "On Tuesday, student protesters at the University of Tehran chanted anti-government slogans as officials scrambled to find a way to quell the growing unrest. ... The efforts by senior officials to calm the public are in stark contrast to the defiant tones struck by Tehran amid an outpouring of grief this month for Soleimani at his funeral procession ... Iran is often presented 'as a monolith ... a country where all of its citizens move as one,' said Reza Akbari, a researcher of Iranian politics at the Institute for War and Peace Reporting in Washington. 'But Iranians are capable of condemning U.S. attacks against their sovereignty while protesting the gross negligence of their government,' he said. For many Iranians, Soleimani's killing in a U.S. drone strike in Baghdad was a national affront and came amid widespread resentment over harsh economic sanctions imposed on Iran by the Trump administration ... At the same time, the protests over the downed airliner, Akbari said, align with longer-term demands from the Iranian population for transparency, justice and accountability."

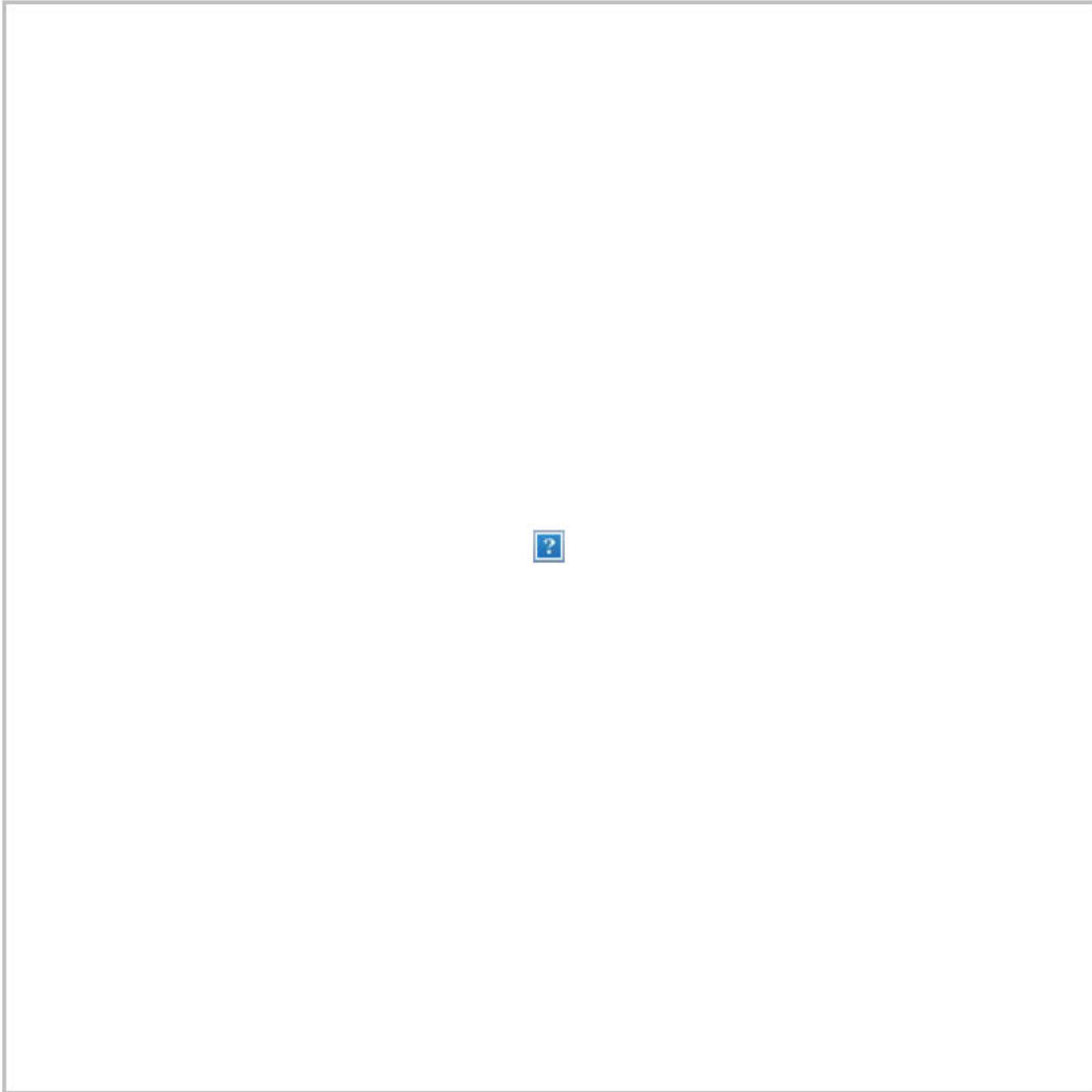


**-- The repressive Iranian regime arrested someone for recording a video of the missile strike that brought down the plane.** [From the Times](#): “The Islamic Revolutionary Guards Corps, a powerful arm of Iran’s military, said it had arrested a person it identified as having recorded a video ... which undercut the military’s initial denials that Iran was responsible. The arrest was announced by Iranian media outlets affiliated with the Guards. The contradictory messages from the president, who is elected, and the Guards, who answer to Iran’s clerical leaders, reflect the competing power centers in the Iranian government. ... In an apparent criticism of the military, [Hassan] Rouhani, a moderate, urged that an official inquiry be candid about its findings. But some hard-line lawmakers have lashed out at his administration, demanding resignations.”

**-- Officials at the State and Defense departments have discussed possible cuts of \$250 million in military aid to Iraq if U.S. troops are asked to leave,** [according to emails reviewed by the Wall Street Journal](#): “The emails indicate that the State Department’s Bureau of Near Eastern Affairs is working to cut all \$250 million in funds under the U.S. foreign military financing program for Iraq for the current fiscal year. The bureau also plans to ask the White House Office of Management and Budget whether it can eliminate the \$100 million request for fiscal year 2021, ‘due to current optics on the ground,’ according to the emails. ‘This does not preclude further congressional consideration of foreign assistance should the situation change in Iraq,’ one of the emails said. The emails assert that no final decision has been made, but top administration officials have ordered a review of what funds may be held or reallocated in the event Iraq requires the U.S. troops be removed. One of the emails said Secretary of State



Mike Pompeo directed that the 2020 foreign military financing funds be repurposed, or used elsewhere.”



Gun rights protesters hold signs at a meeting of the Virginia Senate Judiciary Committee in Richmond. (Steve Helber/AP)

## **DOMESTIC DEVELOPMENTS THAT SHOULDN'T BE OVERSHADOWED:**

-- Virginia Gov. Ralph Northam (D) will ban guns from the grounds of the state's capitol, at least temporarily. [Laura Vozzella and Gregory S. Schneider report](#): “The move comes just days after

newly empowered Democrats banned guns from the Capitol building and an adjacent legislative office building. And **it comes just ahead of a gun rights rally planned for Monday, which organizers say will draw tens of thousands to Capitol Square. The rally has drawn interest from militias and extremist groups across the country**, raising security concerns in Richmond. ... Security has been unusually tight during the General Assembly session that kicked off last week, as Democrats ... consider far-reaching gun-control legislation.”

**-- More than 100 billion doses of pain medication oxycodone and hydrocodone were shipped nationwide from 2006 through 2014, saturating the nation with 24 billion more doses than previously known to the public.** [Steven Rich, Scott Higham and Sari Horwitz report](#): “The Washington Post and the company that owns the Charleston Gazette-Mail in West Virginia first obtained the data, collected by the Drug Enforcement Administration, from 2006 through 2012 after waging a year-long legal fight. In July, The Post reported that the data revealed that the nation’s drug companies had manufactured and distributed more than 76 billion pain pills. The two additional years of information — 2013 and 2014 — was recently posted by a data analytics company managed by lawyers for the plaintiffs in a massive lawsuit against the opioid industry. ... The newly released data, which traces the path of pills from manufacturers and distributors to pharmacies across the country, confirms again that six companies distributed the vast majority of the pain pills. **McKesson Corp., Cardinal Health, Walgreens, AmerisourceBergen, CVS and Walmart accounted for 76 percent of the oxycodone and hydrocodone pills that were shipped between 2006 and 2014**

... Three manufacturers still accounted for 85 percent of the pills: SpecGx, a subsidiary of Mallinckrodt; Actavis Pharma; and Par Pharmaceutical, a subsidiary of Endo Pharmaceuticals.”

**-- The White House’s secret plan to divert \$7.2 billion in Pentagon funding for Trump’s border wall drew bipartisan criticism. [Paul](#)**

**[Sonne, Jeff Stein and Nick Miroff](#) report:** “Senior Republicans grumbled about the plan but mostly put the blame on Democrats, who agreed to provide \$1.4 billion in border barrier funding this year — far less than the \$5 billion Trump requested. ‘I wish they’d get the money somewhere else, instead of defense,’ said Sen. Richard C. Shelby (R-Ala.), chairman of the Senate Appropriations Committee. ‘But I do support building the wall.’ ... ‘I think it’s outrageous,’ said Sen. Jack Reed (D-R.I.), the top Democrat on the armed services committee, who called it ‘a slap to the military as well as a slap to Congress’ ... Defense Secretary Mark T. Esper, asked Tuesday if he supports the continued diverting of Defense Department money to fund the border wall, said that one of the Pentagon’s missions is supporting homeland defense. ‘If that’s what it takes, we are prepared to support’ it, he said.”

**-- An appeals court temporarily halted the purge of more than 200,000 people from Wisconsin’s voter rolls. [Reis Thebault](#)**

**[reports:](#)** “The Tuesday order came one day after the state’s elections commission and its three Democratic members were found in contempt of court for not complying with a judge’s previous order to cancel the registrations of roughly 6 percent of its voters. The case is largely split along partisan lines. Republicans argue that thousands of people who have changed addresses have not updated their voter



registration status and should therefore be struck from the rolls to ensure election integrity, while Democrats and voting rights advocates say the move will unjustly disenfranchise swaths of the electorate ... The six-person election commission had been split evenly along partisan lines, the Republicans voting in favor of the purge and the Democrats voting against it. In a meeting on Tuesday, commissioners again disagreed — 3 to 3 — about how to respond. ... A Journal Sentinel analysis of the over 200,000 register voters targeted — all of whom were sent a letter in October seeking address confirmation — found that most lived in municipalities that supported Hillary Clinton in 2016.”

**-- The Trump administration’s push to restart federal executions after nearly two decades heads back to court today.** [Mark Berman and Ann E. Marimow report](#): “Justice Department lawyers are asking the U.S. Court of Appeals for the District of Columbia Circuit to reverse a judge’s order and allow the administration to move forward with four executions the administration had scheduled for December and January. U.S. District Judge Tanya S. Chutkan in November found that the government had probably exceeded its powers with the adoption of a new lethal-injection protocol to be used in those executions. The new protocol, she wrote, is inconsistent with a 1994 law that requires federal executions to be carried out ‘in the manner prescribed by the law of the State in which the sentence is imposed.’”

**-- The Supreme Court will hear arguments in the “Bridgegate” scandal that shook New Jersey politics. The case could heavily impact future public corruption prosecutions.** [Matt Zapotosky reports](#): “As former New Jersey governor Chris Christie (R) looked on,

the Supreme Court heard arguments Tuesday on whether to overturn the convictions against two of his ex-political allies in the 'Bridgegate' case, and the decision could have broad implications for how federal prosecutors pursue allegations of public corruption. The two former allies — Bridget Kelly and William E. Baroni Jr. — argue that the Justice Department reached too far in charging them with fraud for their roles in an alleged plot to back up traffic on the George Washington Bridge, the nation's busiest, as retaliation against a local mayor who declined to endorse Christie's reelection bid. ... The Justice Department counters that Kelly and Baroni are misstating what occurred and that the evidence was sufficient to support their convictions. The questioning Tuesday did not break down neatly along traditional ideological lines, and it was difficult to predict what the ultimate decision might be. Some justices who asked questions of the attorneys for Baroni and Kelly also seemed critical of some of the government's points. ... In filings to the Supreme Court, Kelly and Baroni argued that — even if they did exactly what prosecutors allege — it could not constitute a federal crime. They argued that they were essentially convicted of lying about their true political motive for a decision."

**-- Michael Avenatti, the former attorney for adult-film actress Stormy Daniels, was arrested by IRS agents for allegedly violating his bail terms a week before his federal trial. [Timothy Bella reports](#):** "Avenatti, who is accused of extorting Nike for up to \$25 million and stealing millions of dollars from his clients for his own interests among other charges, was arrested while appearing before the State Bar Court in Los Angeles, in the middle of a disciplinary hearing alleging that he stole about \$840,000 from a former client."



**-- Rep. Joe Kennedy III (D-Mass.) is rolling out 16 Democratic endorsements for his primary challenge against incumbent Sen. Ed Markey, including Reps. John Lewis (Ga.) and Joaquin Castro (Tex.).** [From Boston Magazine](#): “Also on the list was co-chair of the Congressional Progressive Caucus, Congressman Mark Pocan, and the Caucus’s chair emeriti, Congressman Raul Grijalva. ... Kennedy collected endorsements from several other key groups in the House, including the co-chairs of the LGBTQ Equality Caucus, ... members of the Congressional Black Caucus ... and several members of the Congressional Hispanic Caucus ... Kennedy is also now outpacing Markey when it comes to raising campaign cash. ... Kennedy raised more than \$2.4 million over the last three months of 2019, while Markey’s campaign reports raising only \$1.4 million.”

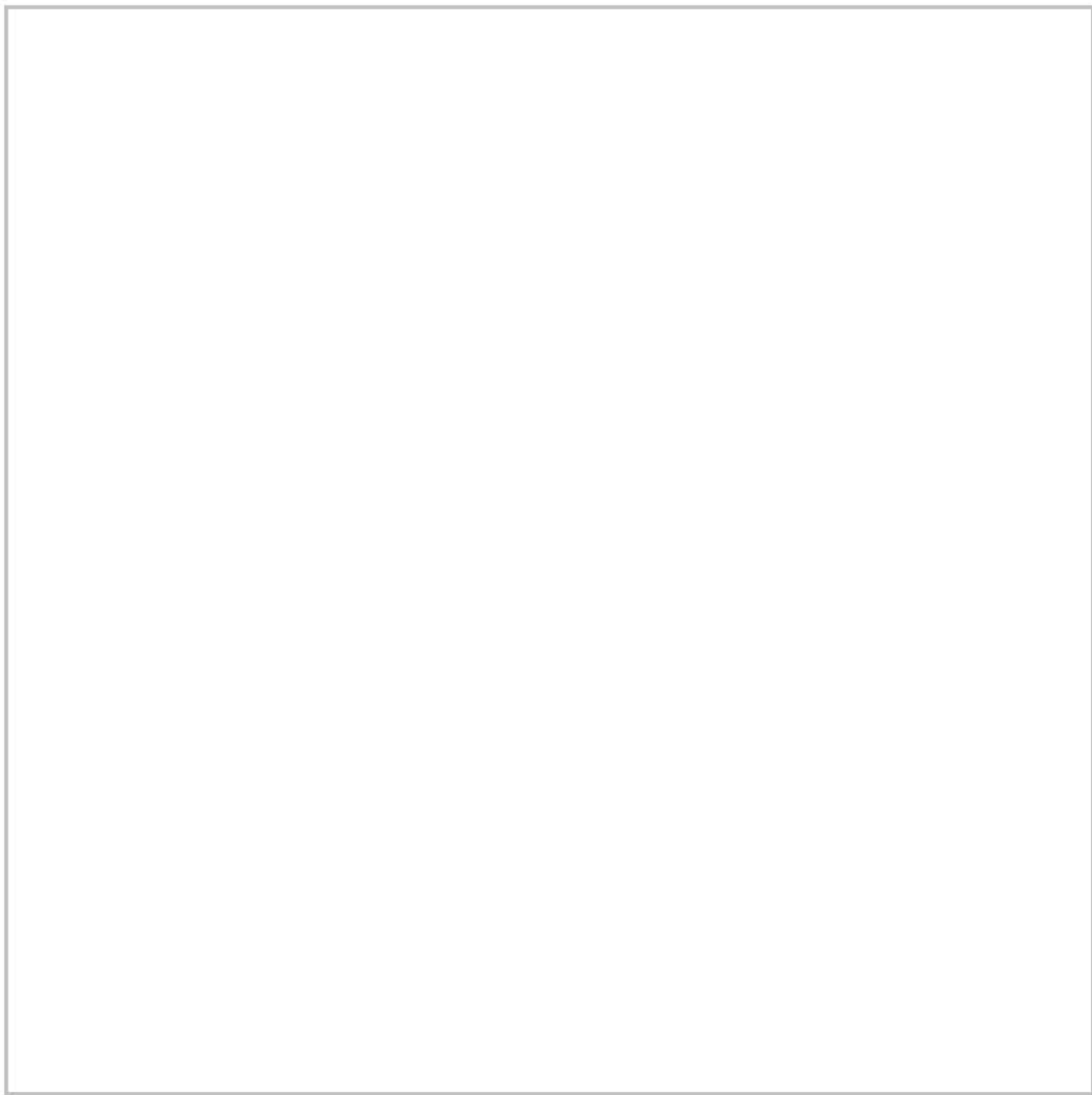
**-- Boeing’s new CEO pledged greater transparency in a message to employees still reeling from the two 737 Max jet crashes that killed hundreds in the last two years.** [Lori Aratani reports](#): “‘This is a crucial time for Boeing,’ [David Calhoun] wrote. ‘We have work to do to uphold our values and to build on our strengths. I see greatness in this company, but I also see opportunities to do better. Much better.’ Calhoun’s top priority will be convincing federal regulators that the 737 Max is safe to fly. The plane has been grounded worldwide since March. Boeing also is counting on Calhoun to rebuild relationships with customers, regulators and the public.”

**-- A Delta flight dumped jet fuel on a playground near Los Angeles, leaving dozens with minor injuries.** [Justin Wm. Moyer reports](#): “Los Angeles County Fire Department officials said they responded to an elementary school ... after the aircraft apparently

dumped the fuel while on a final approach to the airport. Twenty children and 11 adults complained of minor injuries, officials said. No one was taken to a hospital, officials said, and no evacuations were initiated. ... In a statement, Federal Aviation Administration spokesman Allen Kenitzer said Delta Air Lines Flight 89 declared an emergency after departing from the airport, then returned to the airport and 'landed without incident.'”

### **SOCIAL MEDIA SPEED READ:**

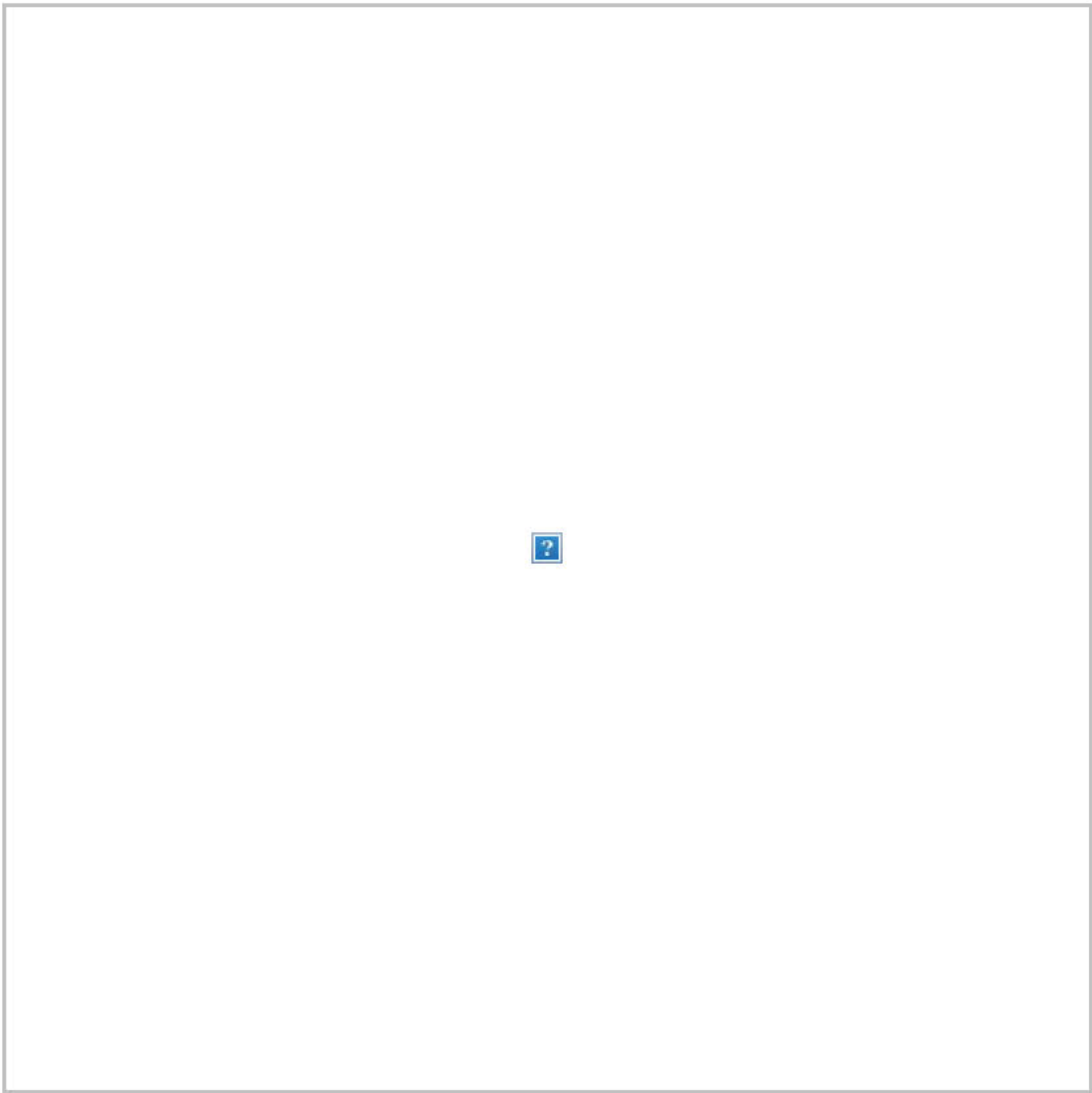
Here are the candidates most tweeted about during the debate:



Klobuchar struggled during the debate to remember the name of the Democratic governor of Kansas who defeated Kris Kobach in 2018. The governor gamely replied:

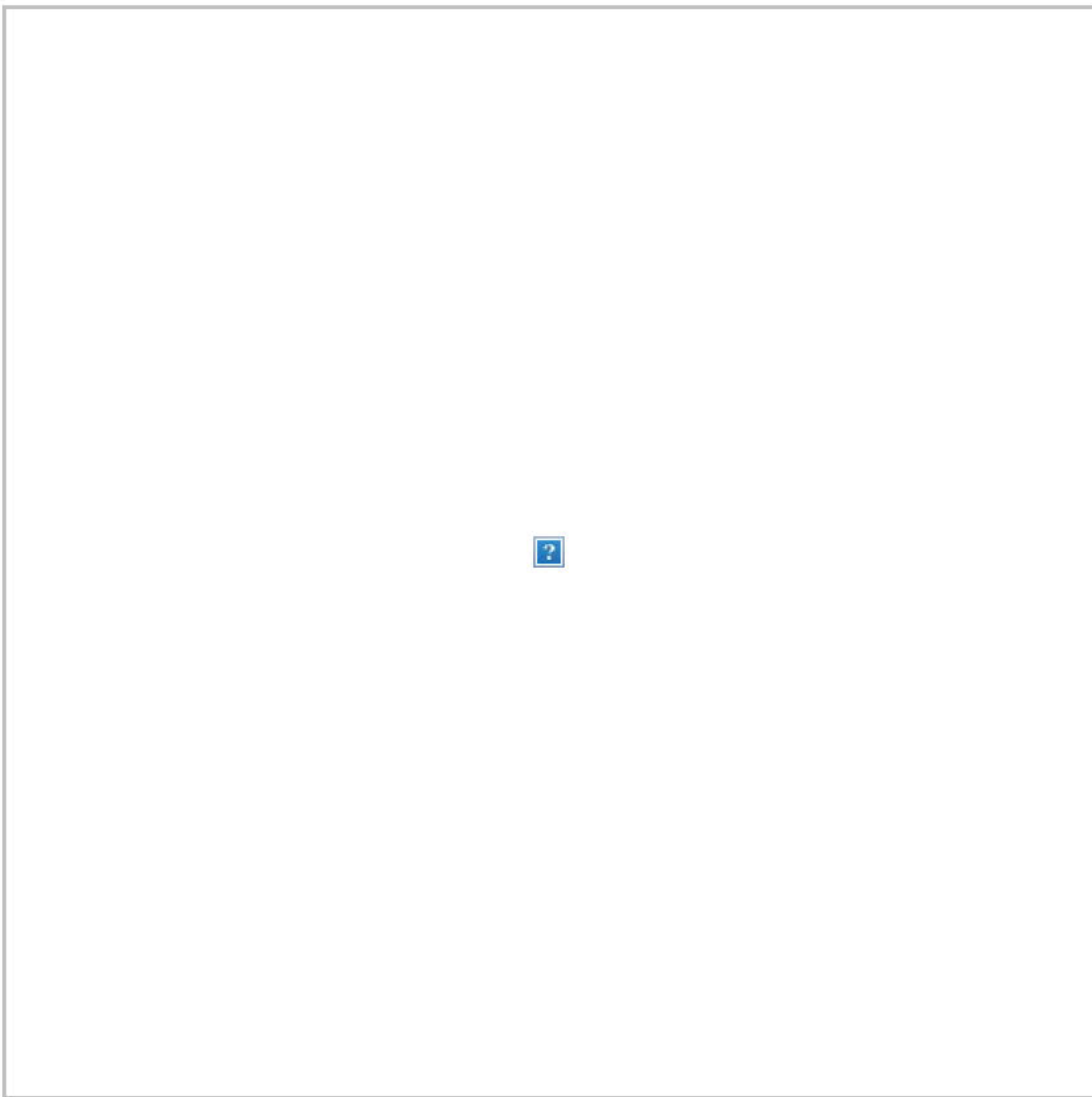


The former chief strategist for Obama noted that Sanders's 2016 clashes with Hillary Clinton created the backdrop to his back-and-forth with Warren over whether he said a woman cannot win. David Axelrod also makes the good point that Sanders is being much more explicit in saying he'll support the Democratic nominee than four years ago:

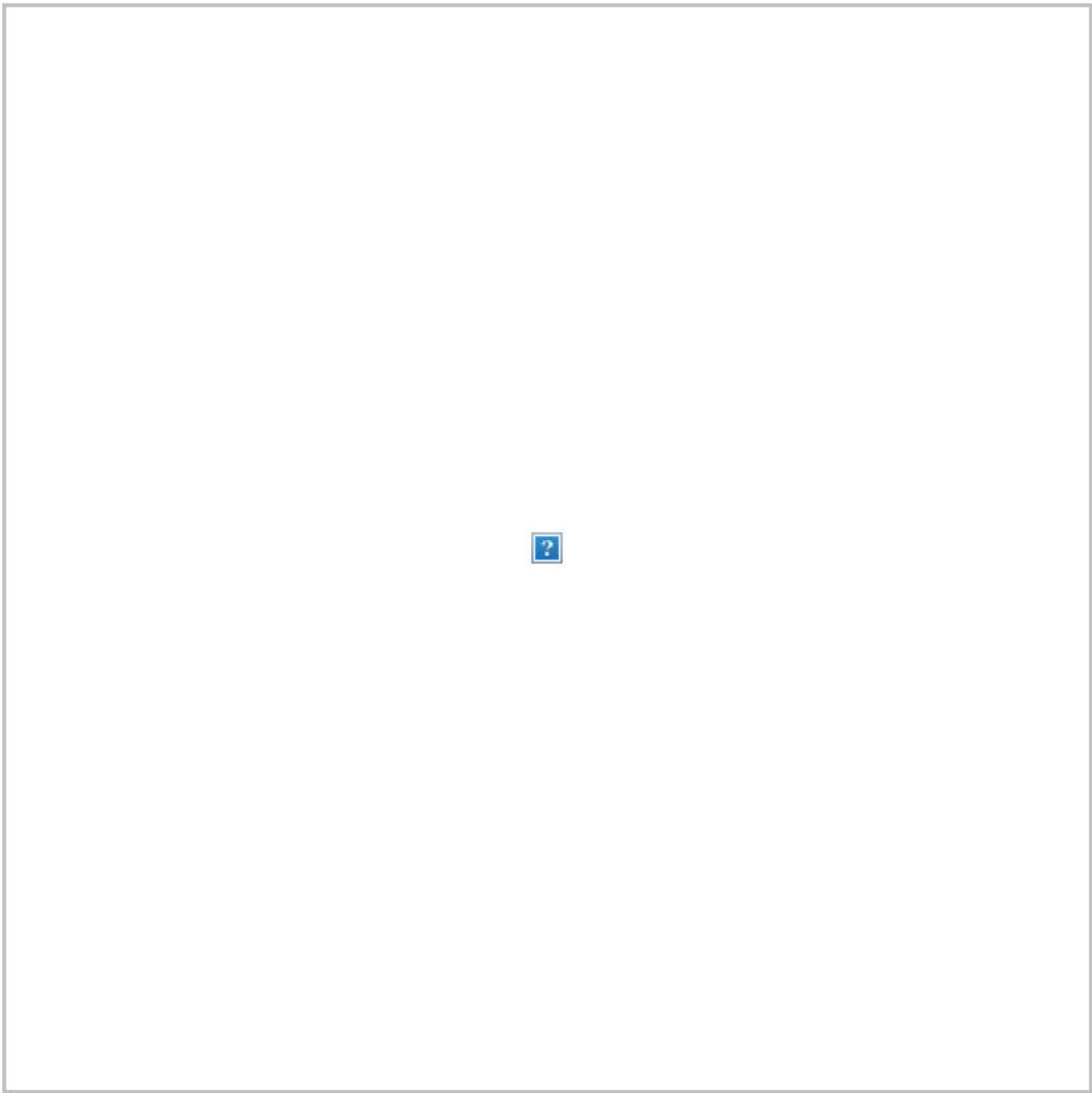


Biden raised eyebrows when he said during the debate that he had to get by as a single dad on a \$42,000 salary when he became a senator in 1973:

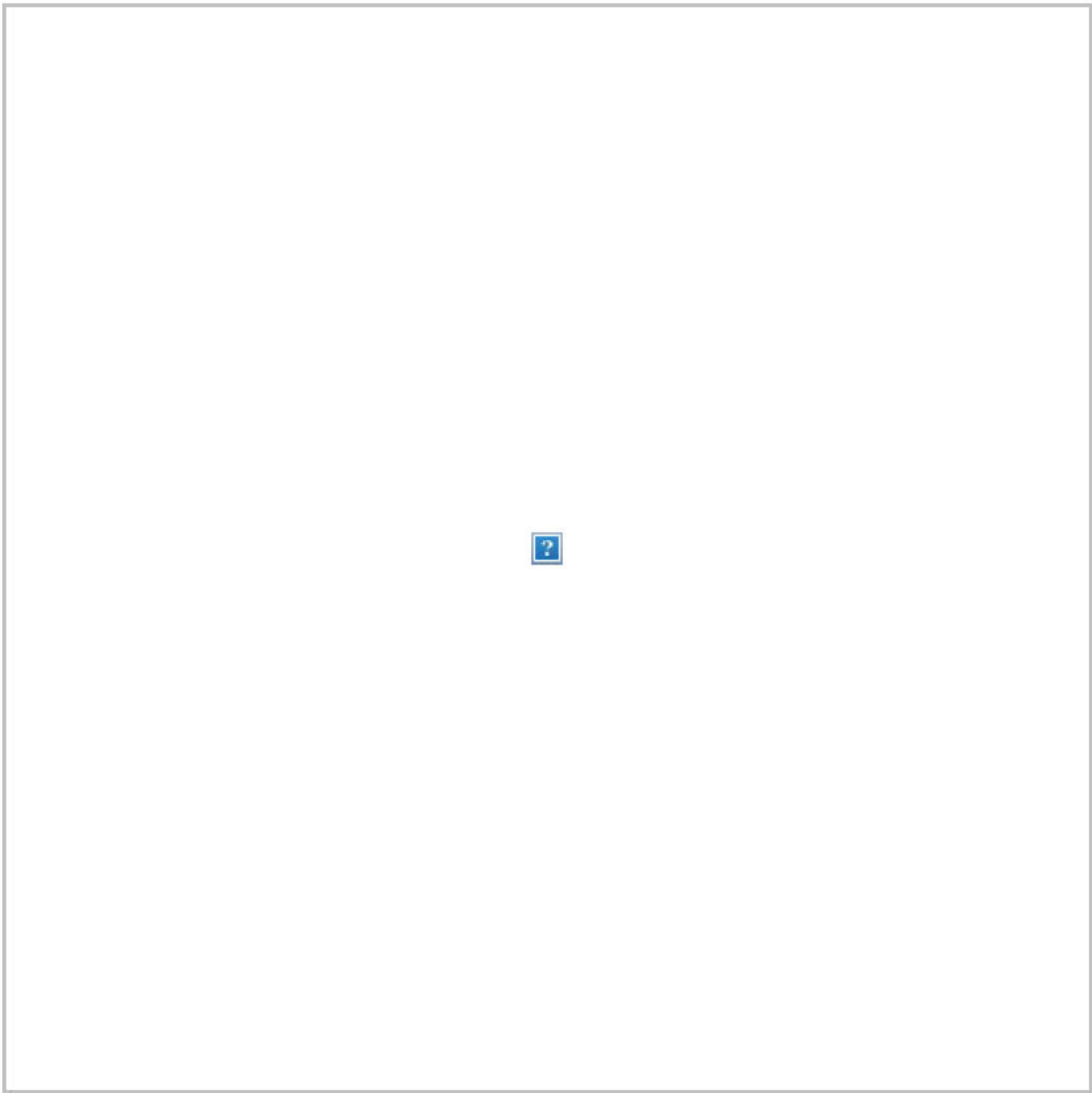




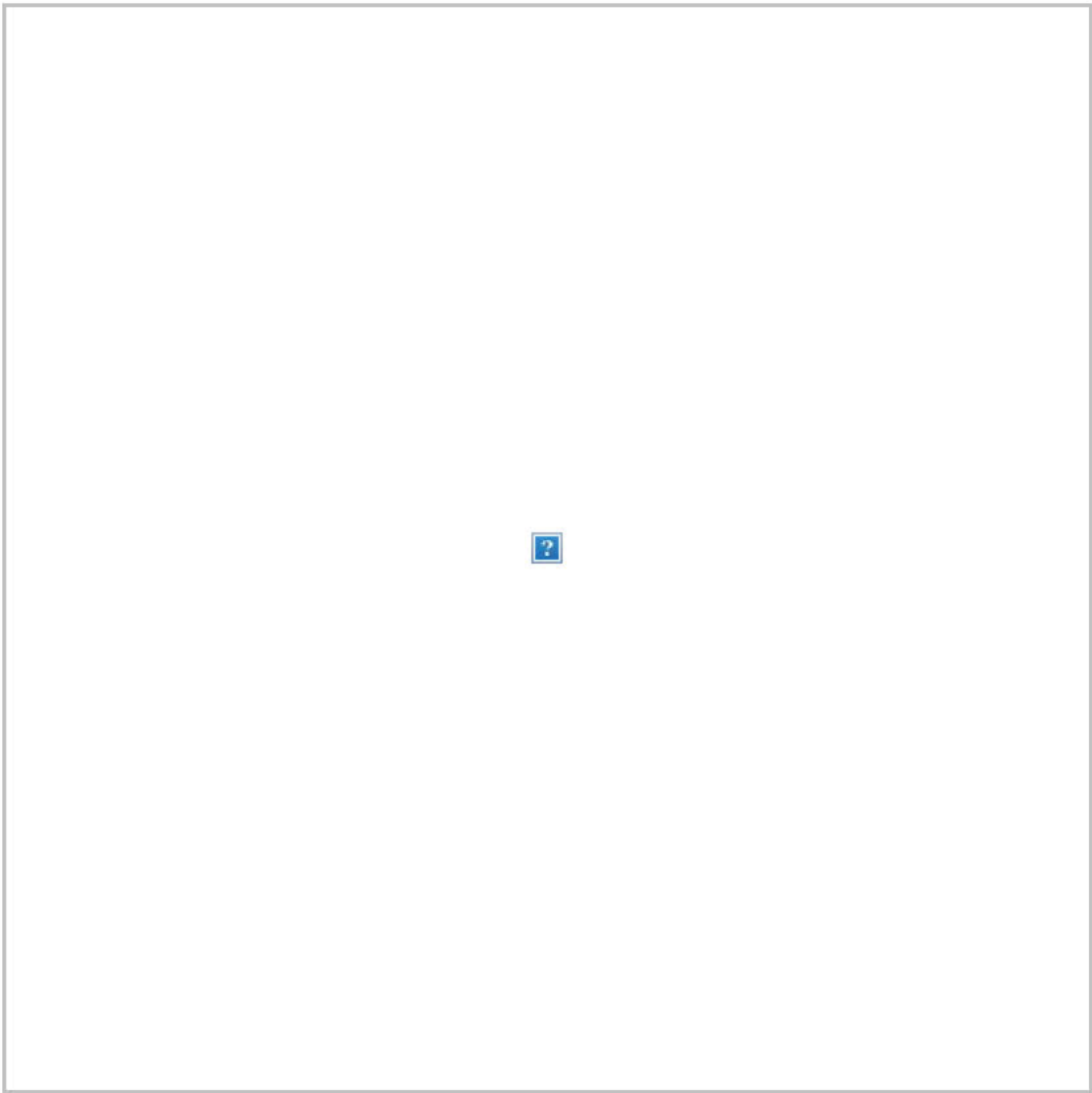
An organizational psychology professor at the Wharton School of Business suggested the Democratic candidates play a few board games instead of debating:



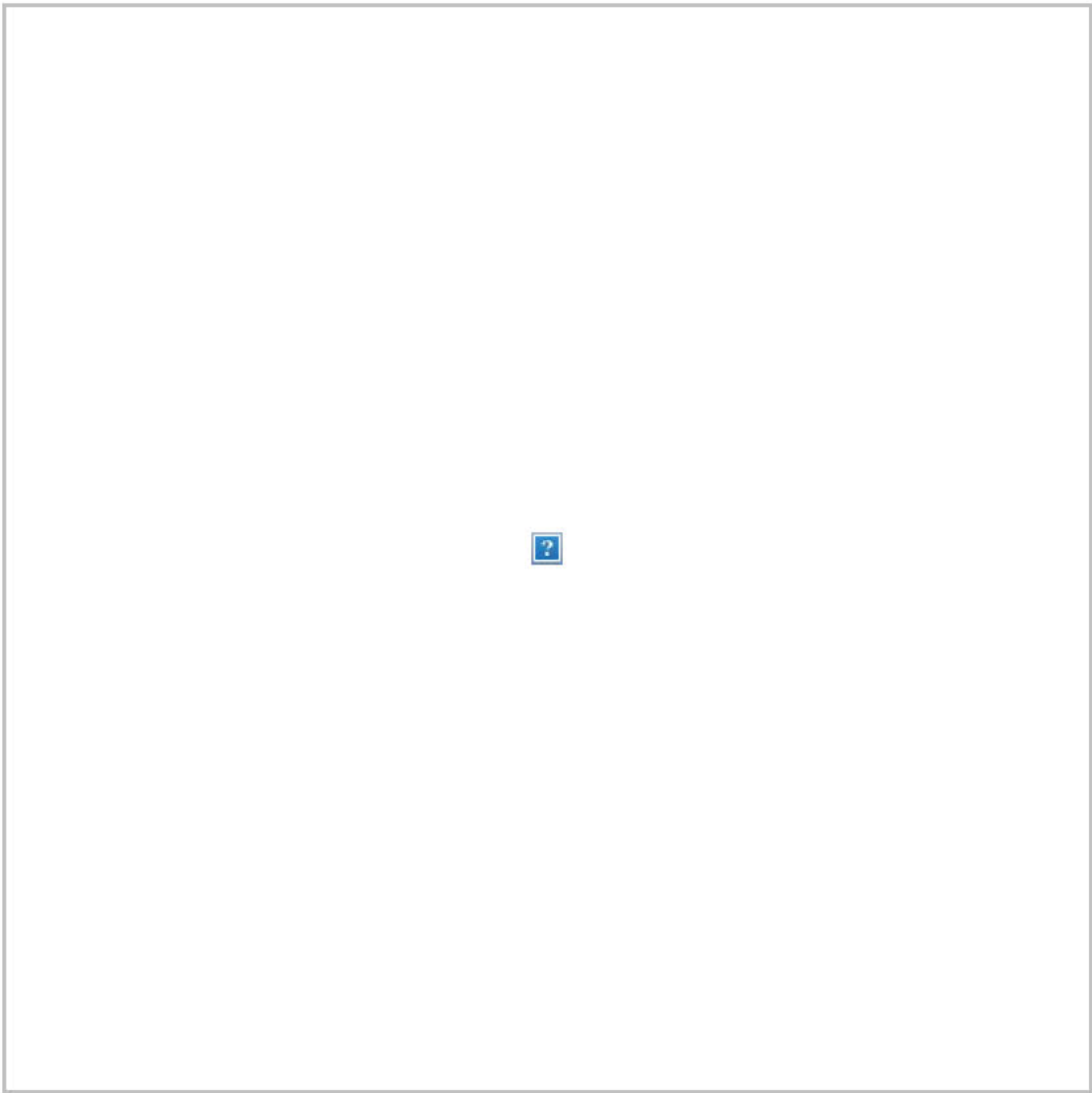
A Democratic congressman called out Mike Pompeo for talking to Fox News instead of showing up to a House hearing on Iran:



A Daily Beast reporter shared an image of Lev Parnas with Jared Kushner and Ivanka Trump:

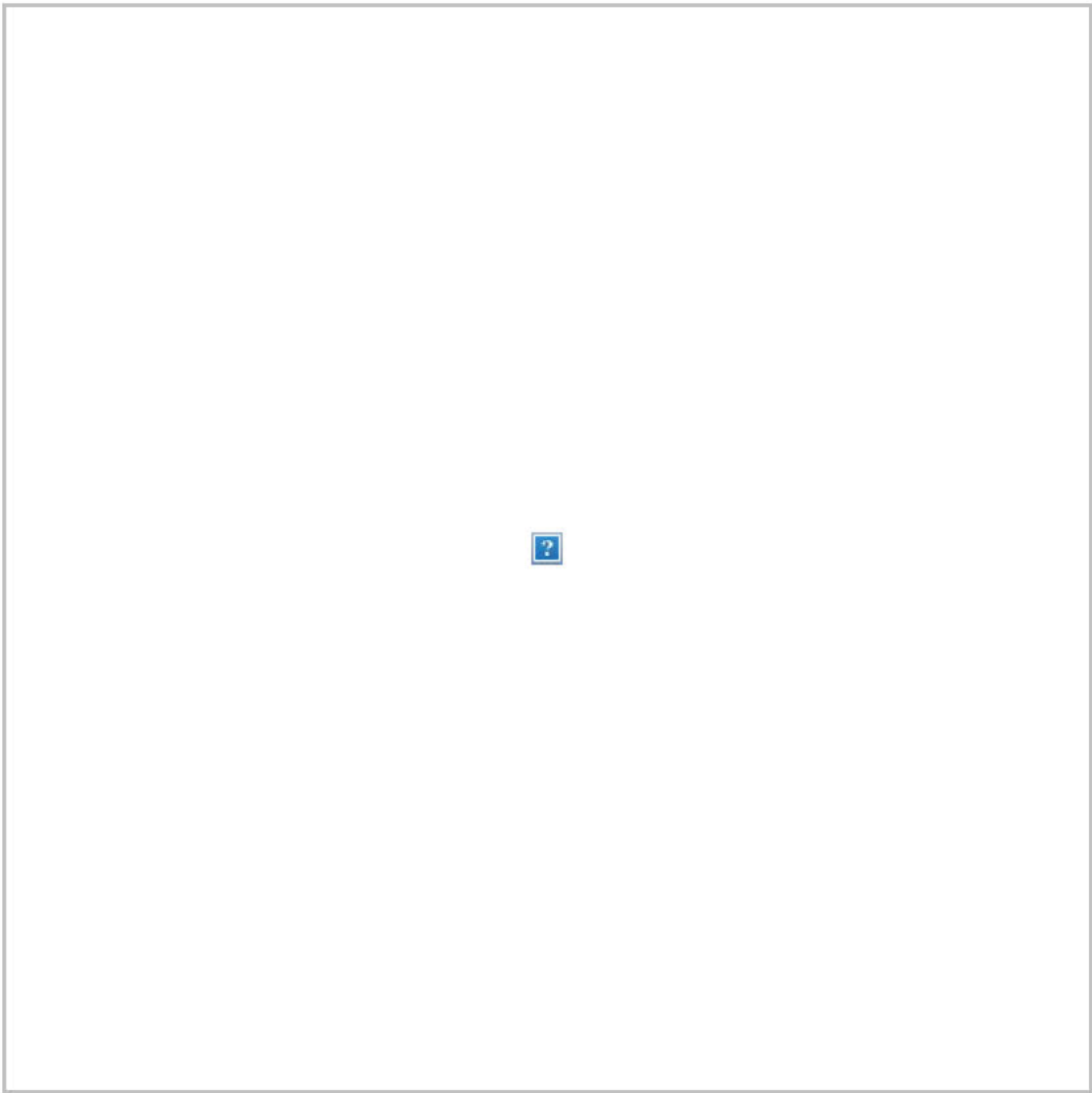


The documents Parnas turned in to Democratic investigators include this peculiar White House menu:

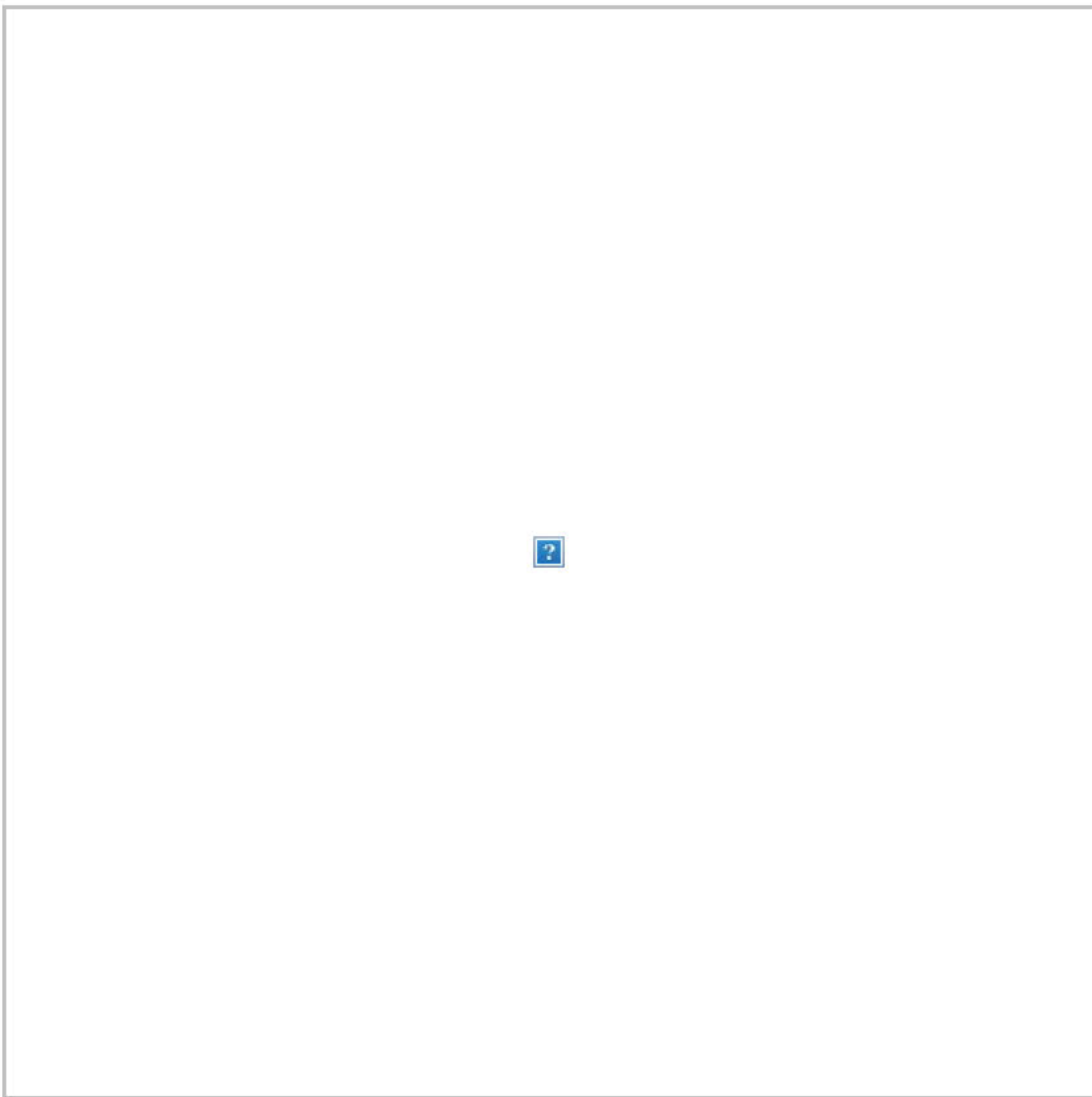


Other evidence in the hands of House Intelligence investigators includes this note:

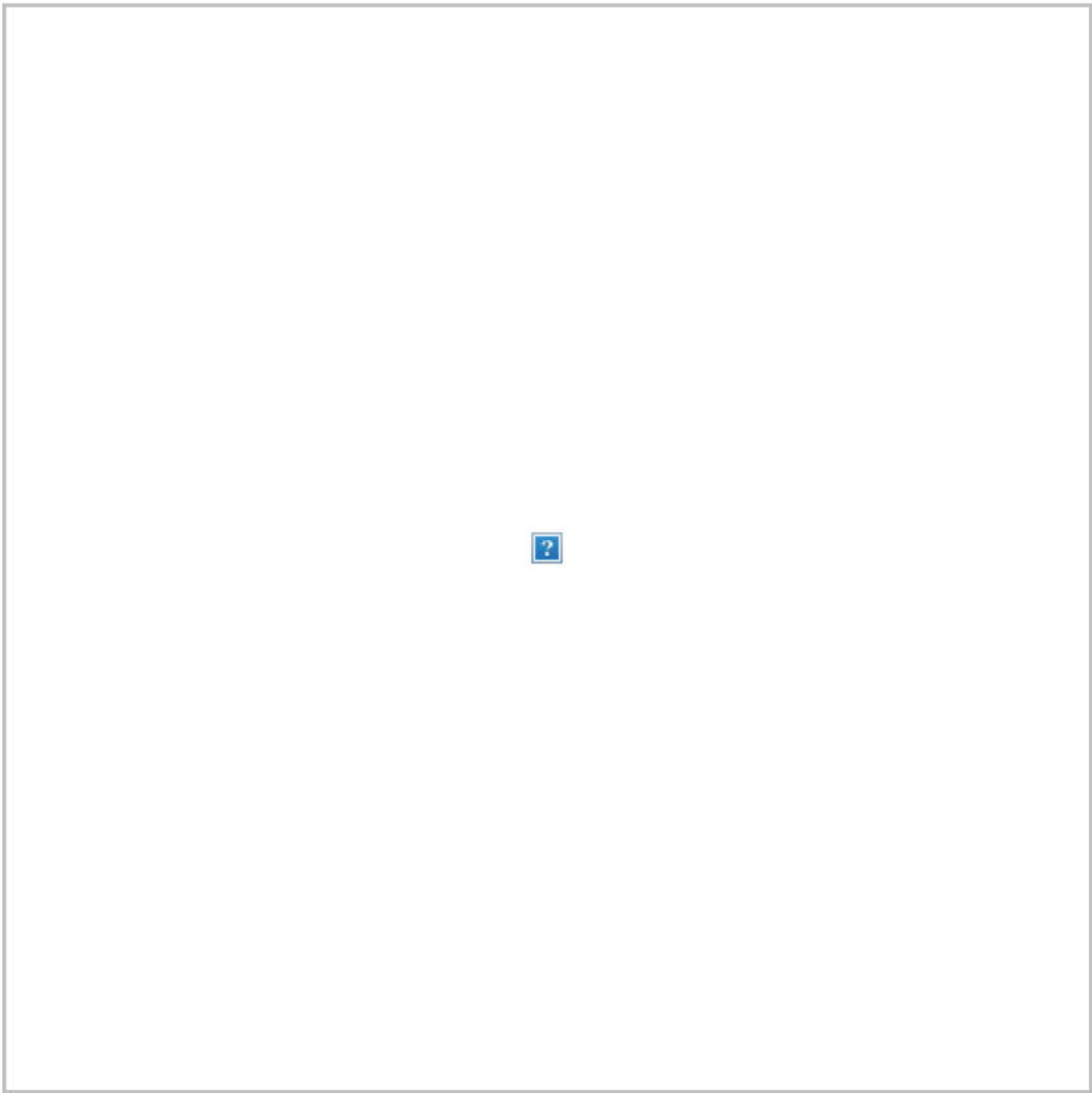




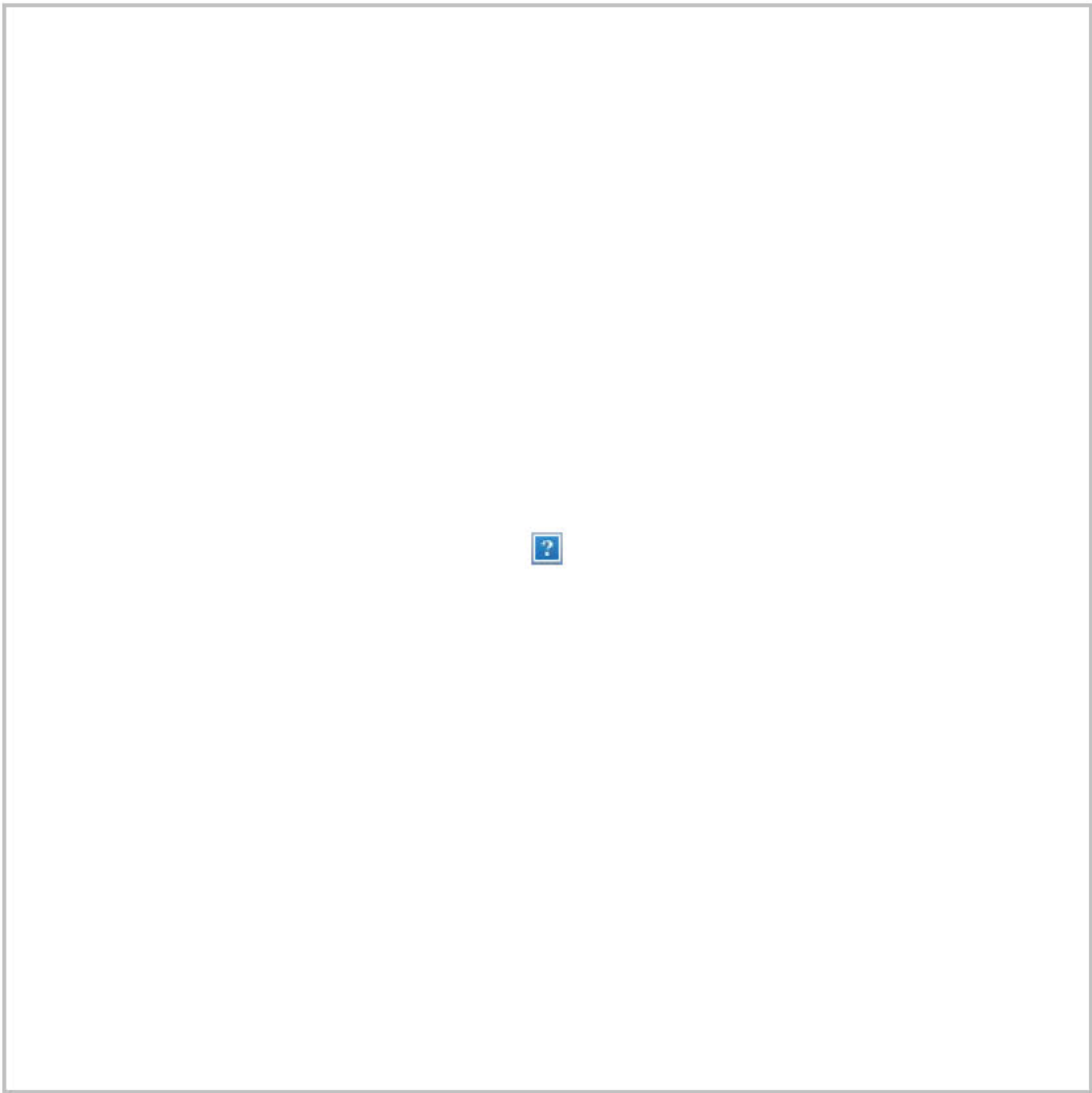
And this email:



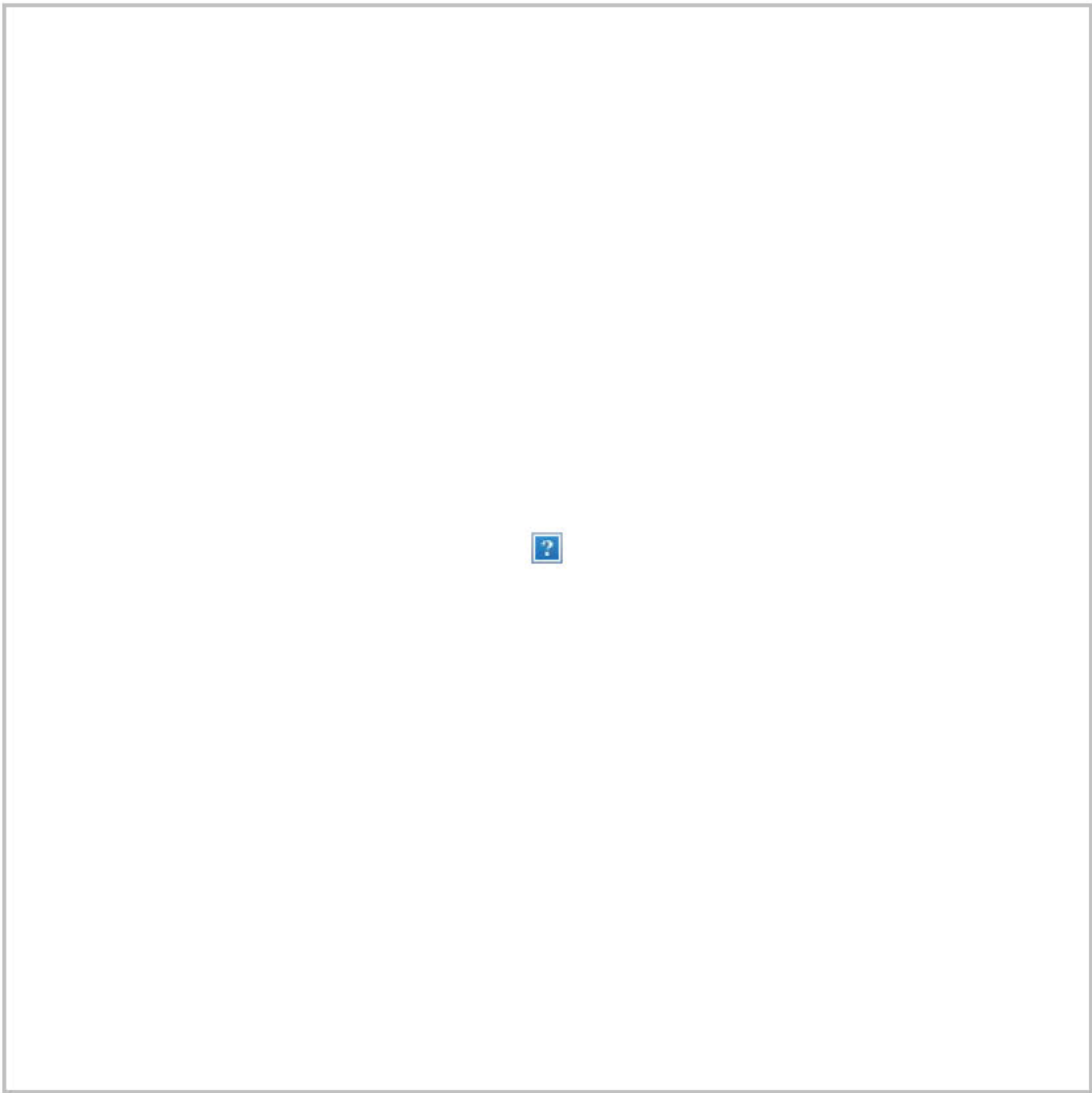
Conservative lawyer George Conway, husband of counselor to the president Kellyanne Conway, said Senate Republicans are restricting press access to the impeachment trial because they're scared and have something to hide:



A Times photographer captured Trump wearing his reading glasses last night:



Warren's staff sent a pick-me-up to Cory Booker's team after the New Jersey senator dropped out of the presidential race:



And it finally rained in Melbourne:





Heavy rain, flash floods and severe thunderstorms swept over the Australian city. The very-welcome storm is expected to hit fire-affected parts of New South Wales and Victoria later this week, [the Guardian reports](#).

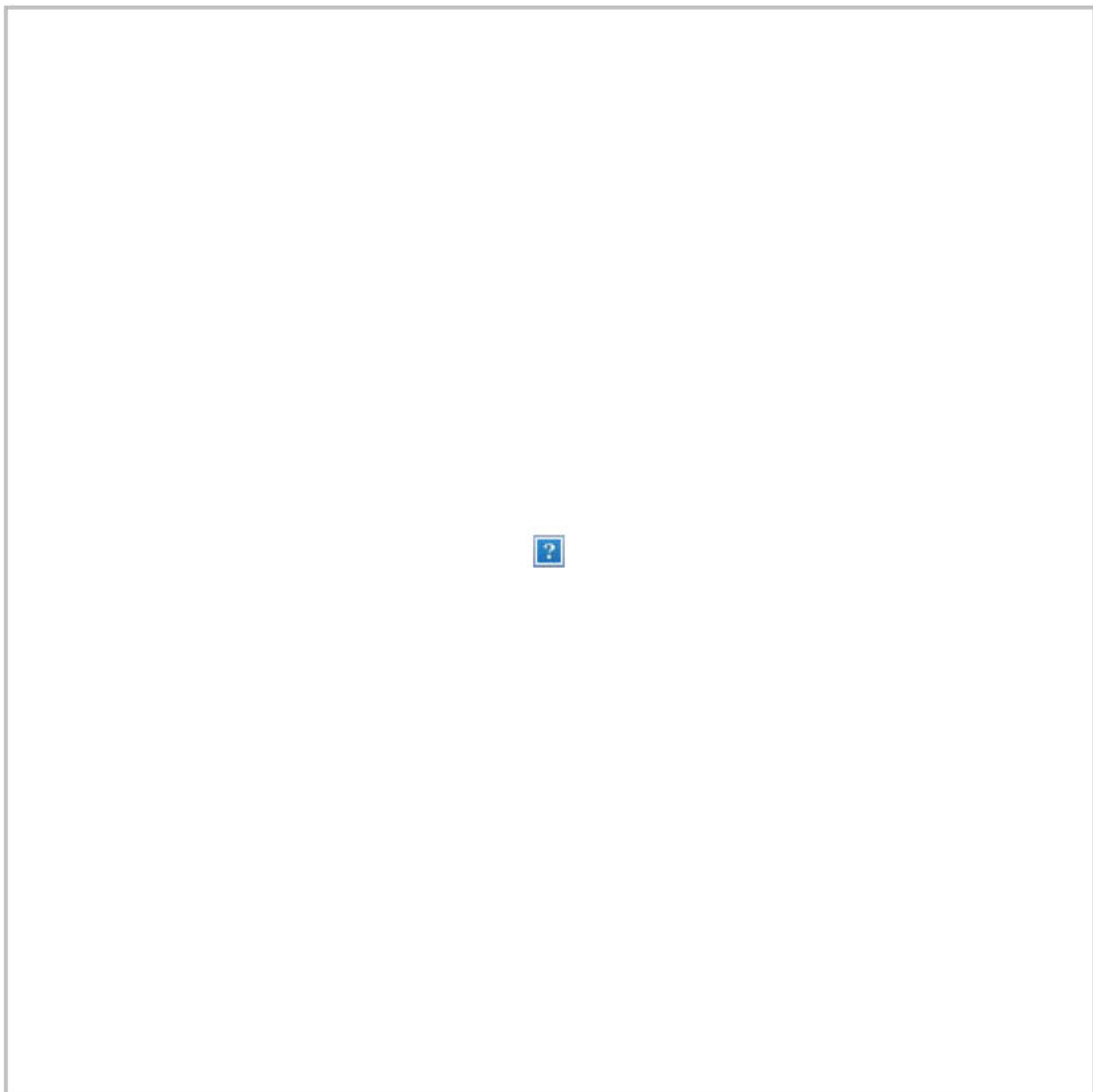
**QUOTE OF THE DAY:**

"Lyndon Johnson was sort of a tough guy. Can you imagine his phone calls? He's probably looking down, or looking up," Trump said during his rally in Wisconsin last night,

suggesting that LBJ may be in hell. ([HuffPost](#))

## **VIDEOS OF THE DAY:**

Stephen Colbert did his show live last night so he could cover the Democratic debate:



And then he wondered why Trump would talk about dishwashers during his rally in Milwaukee:



Trevor Noah opened his post-debate monologue by pointing out the demographics of the group of Democratic candidates who remain in the race:

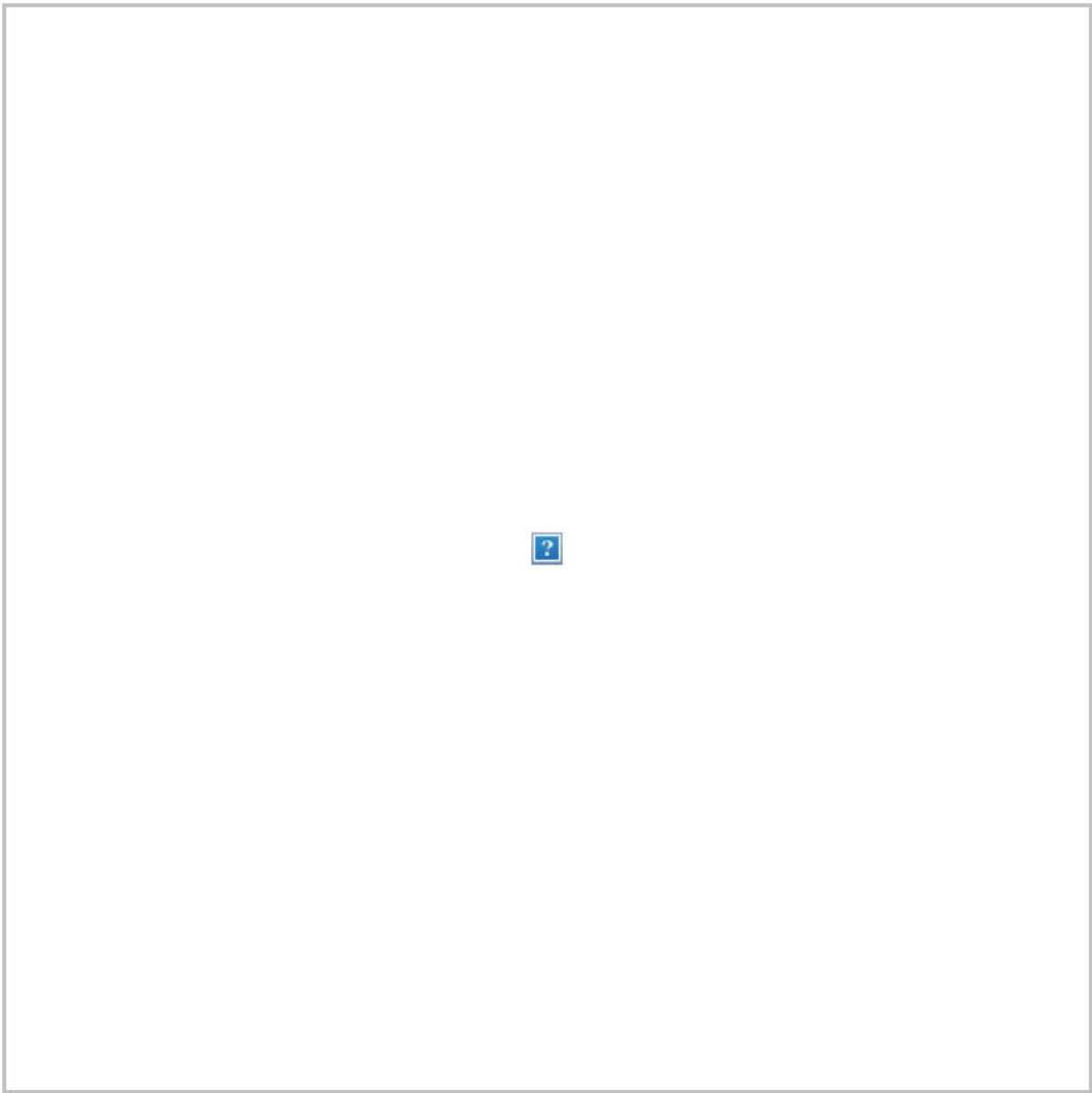


Seth Meyers took a break from politics to introduce us all to some teen slang:



U.K. Prime Minister Boris Johnson wants Brits to pitch in and raise half a million pounds so that Big Ben can bong for Brexit:





You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)

---

©2020 The Washington Post | 1301 K St NW, Washington DC 20071



**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of December 30, 2019  
**Date:** Monday, January 06, 2020 6:54:31 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of December 30, 2019](#)

01/06/2020 08:41 AM EST

Original release date: January 6, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
citrix -- application_delivery_controller	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	2019-12-27	<a href="#">7.5</a>	<a href="#">CVE-2019-19781</a> <a href="#">CONFIRM</a>
freeciv -- freeciv	A denial of service flaw was found in the way the server component of Freeciv before 2.3.4 processed certain packets. A remote attacker could send a specially-crafted packet that, when processed would lead to memory exhaustion or excessive CPU consumption.	2019-12-30	<a href="#">7.8</a>	<a href="#">CVE-2012-5645</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
magnolia_international	Magnolia CMS before 4.5.9 has multiple	2019-12-		<a href="#">CVE-2013-4621</a>

-- magnolia_cms &#xA0;	access bypass vulnerabilities	27	7.5	MISC MISC
open_dynamics -- collabtive	Collabtive 1.0 has incorrect access control	2019-12-27	7.5	CVE-2013-5027 MISC
php-shellcommand -- php-shellcommand	php-shellcommand versions before 1.6.1 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-30	10	CVE-2019-10774 MISC
senkas -- kolibri	Buffer overflow in Senkas Kolibri 2.0 allows remote attackers to execute arbitrary code via a long URI in a POST request.	2019-12-27	7.5	CVE-2014-5289 MISC BID XE
sqlite -- sqlite &#xA0;	selectExpander in select.c in SQLite 3.30.1 proceeds with WITH stack unwinding even after a parsing error.	2020-01-02	7.5	CVE-2019-20218 MISC
wordpress -- wordpress &#xA0;	wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript&colon; substring.	2019-12-27	7.5	CVE-2019-20041 MISC MISC
yandex -- clickhouse	In all versions of ClickHouse before 19.14, an OOB read, OOB write and integer underflow in decompression algorithms can be used to achieve RCE or DoS via native protocol.	2019-12-30	7.5	CVE-2019-16535 MISC

[Back to top](#)

&#xA0;

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bolt -- bolt &#xA0;	Bolt 3.6.4 has XSS via the slug, teaser, or title parameter to editcontent/pages, a related issue to CVE-2017-11128 and CVE-2018-19933.	2019-12-31	4.3	CVE-2019-9553 MISC MISC
genjxcms -- genjxcms &#xA0;	GeniXCMS 1.1.5 has XSS via the dbuser or dbhost parameter during step 1 of installation.	2019-12-31	4.3	CVE-2018-14476 MISC MISC
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_SPLINE_private in	2019-12-27	4.3	CVE-2019-20009 MISC MISC

	dwg.spec.			<a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. There is a use-after-free in resolve_objectref_vector in decode.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20010</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. There is a heap-based buffer over-read in decode_R13_R2000 in decode.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20011</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. There is a double-free in dwg_free in free.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20014</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_HATCH_private in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20012</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in decode_3dsolid in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20013</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_LWPOLYLINE_private in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20015</a> <a href="#">MISC</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function senc_Parse() in isomedia/box_code_drm.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20167</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_odf_avc_cfg_write_bs() in odf/descriptors.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20163</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the function trak_Read() in isomedia/box_code_base.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20169</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20168</a>

	function gf_isom_box_dump_ex() in isomedia/box_funcs.c.			<a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_dump() in isomedia/box_dump.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20166</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function ReadGF_IPMPX_WatermarkingInit() in odf/ipmpx_code.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20161</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a stack-based buffer overflow in the function av1_parse_tile_group() in media_tools/av_parsers.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20160</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function gf_isom_box_parse_ex() in isomedia/box_funcs.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20162</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_box_del() in isomedia/box_funcs.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20164</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function ilst_item_Read() in isomedia/box_code_apple.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20165</a> <a href="#">MISC</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 allows overly permissive cross-origin resource sharing which could allow an attacker to transfer private information. An attacker could exploit this vulnerability to access content that should be restricted. IBM X-Force ID: 161422.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-4343</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- mq	IBM MQ 9.1.0.0, 9.1.0.1, 9.1.0.2, 9.1.0.3, 9.1.1, 9.1.2, and 9.1.3 is vulnerable to a denial of service attack that would allow an authenticated user to reset client connections due to an error within the Data Conversion routine. IBM X-Force ID: 170966.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-4655</a> <a href="#">XF</a> <a href="#">CONFIRM</a>



ibm -- watson_studio_local &#xA0;	IBM Watson Studio Local 1.2.3 could disclose sensitive information over the network that an attacker could use in further attacks against the system. IBM X-Force ID: 145238.	2019-12-30	5	<a href="#">CVE-2018-1682</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
joomla! -- joomla! &#xA0;	Xorbin Analog Flash Clock 1.0 extension for Joomla has XSS	2019-12-27	4.3	<a href="#">CVE-2013-4692</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel_project -- libsixel	A memory leak was discovered in image_buffer_resize in fromsixel.c in libsixel 1.8.4.	2019-12-27	4.3	<a href="#">CVE-2019-20023</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An invalid memory address dereference was discovered in load_pnm in frompnm.c in libsixel before 1.8.3.	2019-12-27	4.3	<a href="#">CVE-2019-20022</a> <a href="#">MISC</a>
libsixel_project -- libsixel &#xA0;	An issue was discovered in libsixel 1.8.4. There is a heap-based buffer overflow in the function gif_init_frame at fromgif.c.	2019-12-30	6.8	<a href="#">CVE-2019-20094</a> <a href="#">MISC</a>
libsixel_project -- libsixel &#xA0;	A heap-based buffer overflow was discovered in image_buffer_resize in fromsixel.c in libsixel before 1.8.4.	2019-12-27	4.3	<a href="#">CVE-2019-20024</a> <a href="#">MISC</a>
livefyre -- livecomments	Cross-site scripting (XSS) vulnerability in Livefyre LiveComments 3.0 allows remote attackers to inject arbitrary web script or HTML via the name of an uploaded picture.	2019-12-27	4.3	<a href="#">CVE-2014-6420</a> <a href="#">MISC</a> <a href="#">XE</a>
luquidpixels -- liquifire_os	LuquidPixels LiquiFire OS 4.8.0 allows SSRF via the call%3Durl substring followed by a URL in square brackets.	2019-12-29	6.4	<a href="#">CVE-2019-20055</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi hostname parameter (Dynamic DNS Configuration).	2019-12-30	4.3	<a href="#">CVE-2019-20072</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi username parameter (DynDns settings of the Dynamic DNS Configuration).	2019-12-30	4.3	<a href="#">CVE-2019-20076</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the urlFQDN parameter to form2url.cgi (aka the Keyword field of the URL Blocking Configuration).	2019-12-30	4.3	<a href="#">CVE-2019-20070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, pingrtt_v6.html has XSS (Ping6 Diagnostic).	2019-12-30	4.3	<a href="#">CVE-2019-20075</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, any user role can view sensitive information, such as a user password or the FTP password, via the form2saveConf.cgi page.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-20074</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, CSRF exists via form2logaction.cgi to delete all logs.	2019-12-30	<a href="#">5.8</a>	<a href="#">CVE-2019-20071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, XSS exists via the form2userconfig.cgi username parameter (User Account Configuration).	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20073</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /search.htm searchtext parameter. NOTE: This product is discontinued.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-9207</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /public/login.htm errmsg or loginurl parameter. NOTE: This product is discontinued.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-9206</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5312</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/TiffDecode.c in Pillow before 6.2.2 has a TIFF decoding integer overflow, related to realloc.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5310</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/FliDecode.c in Pillow before 6.2.2 has an FLI buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5313</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/SgiRleDecode.c in Pillow before 6.2.2 has an SGI buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5311</a> <a href="#">MISC</a> <a href="#">MISC</a>
proxyman -- proxyman_for_macos	com.proxyman.NSProxy.HelperTool in Privileged Helper Tool in Proxyman for macOS 1.11.0 and earlier allows an attacker to change the System Proxy and redirect all traffic to an attacker-controlled computer, enabling MITM attacks.	2019-12-29	<a href="#">4.3</a>	<a href="#">CVE-2019-20057</a> <a href="#">MISC</a>
sencha_labs -- connect	Sencha Labs Connect has XSS with connect.methodOverride()	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4691</a> <a href="#">MISC</a>
spbas -- business_automation_software	SPBAS Business Automation Software 2012 has CSRF.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4665</a> <a href="#">MISC</a> <a href="#">MISC</a>

spbas-- business_automation_software	SPBAS Business Automation Software 2012 has XSS.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4664</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the search_id parameter in the search_incidents_advanced.php page is affected by XSS.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20220</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the Short Application Name and Application Name inputs in the config.php page are affected by XSS.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20222</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the Plugins input in the config.php page is affected by XSS. The XSS payload is, for example, executed on the about.php page.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20221</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the id parameter is affected by XSS on all endpoints that use this parameter, a related issue to CVE-2012-2235.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20223</a> <a href="#">MISC</a>
tbeu -- matio	A stack-based buffer over-read was discovered in ReadNextCell in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20018</a> <a href="#">MISC</a>
tbeu -- matio	A stack-based buffer over-read was discovered in Mat_VarReadNextInfo5 in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20017</a> <a href="#">MISC</a>
tbeu -- matio &#xA0;	A stack-based buffer over-read was discovered in ReadNextStructField in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20020</a> <a href="#">MISC</a>
tbeu -- matio &#xA0;	An attempted excessive memory allocation was discovered in Mat_VarRead5 in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20019</a> <a href="#">MISC</a>
toshiba -- configfree &#xA0;	Multiple stack-based buffer overflows in CFProfile.exe in Toshiba ConfigFree Utility 8.0.38 allow user-assisted attackers to execute arbitrary code.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2012-4980</a> <a href="#">BID</a> <a href="#">XE</a>
upx -- upx &#xA0;	A heap-based buffer over-read was discovered in canUnpack in p_mach.cpp in UPX 3.95 via a crafted Mach-O file.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20021</a> <a href="#">MISC</a>
winamp -- winamp &#xA0;	Winamp 5.63: Invalid Pointer Dereference leading to Arbitrary Code Execution	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2013-4695</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress Xorbin Digital Flash Clock 1.0 has XSS	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4693</a> <a href="#">MISC</a>
	WordPress before 5.3.1 allowed an			<a href="#">CVE-2019-20042</a>

wordpress -- wordpress	attacker to create a cross-site scripting attack (XSS) in well crafted links, because of an insufficient protection mechanism in wp_targeted_link_rel in wp-includes/formatting.php.	2019-12-27	<a href="#">4.3</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An XSS issue was discovered in the Laborator Neon theme 2.0 for WordPress via the data/autosuggest-remote.php q parameter.	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20141</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in the Conversador plugin 2.61 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the 'page' parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4519</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	WordPress before 5.3.1 allowed an unauthenticated user to make a post sticky through the REST API because of missing access control in wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php.	2019-12-27	<a href="#">5</a>	<a href="#">CVE-2019-20043</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in rss.class/scripts/magpie_debug.php in the WP-Planet plugin 0.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4592</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in the Easy Career Openings plugin 0.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4523</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in magpie/scripts/magpie_slashbox.php in the Ebay Feeds for WordPress plugin 1.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the rss_url parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4525</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in preview-shortcode-external.php in the Shortcode Ninja plugin 1.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the shortcode parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4550</a> <a href="#">MISC</a>
xnview -- xnview &#xA0;	Stack-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a crafted image layer in an XCF file.	2020-01-02	<a href="#">6.8</a>	<a href="#">CVE-2013-3246</a> <a href="#">MISC</a> <a href="#">MISC</a>
xnview -- xnview	Heap-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a	2020-01-	<a href="#">6.8</a>	<a href="#">CVE-2013-3247</a>

&#xA0;	crafted RLE compressed layer in an XCF file.	02		<a href="#">MISC</a> <a href="#">MISC</a>
--------	--	----	--	--

[Back to top](#)

&#xA0;

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_analytics &#xA0;	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 168924.	2019-12-30	<a href="#">3.5</a>	<a href="#">CVE-2019-4623</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- watson_studio_local &#xA0;	IBM Watson Studio Local 1.2.3 stores key files in the user's home directory which could be obtained by another local user. IBM X-Force ID: 161413.	2019-12-30	<a href="#">2.1</a>	<a href="#">CVE-2019-4335</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
nagios -- nagios_xi	In Nagios XI 5.6.9, XSS exists via the nocscreenapi.php host, hostgroup, or servicegroup parameter, or the schedulereport.php hour or frequency parameter. Any authenticated user can attack the admin user.	2019-12-30	<a href="#">3.5</a>	<a href="#">CVE-2019-20139</a> <a href="#">MISC</a>
tenable -- nessus &#xA0;	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would only potentially impact other admins. (Tenable ID 5198).	2019-12-27	<a href="#">3.5</a>	<a href="#">CVE-2016-1000028</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tenable -- nessus &#xA0;	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would potentially impact other admins (Tenable IDs 5218 and 5269).	2019-12-27	<a href="#">3.5</a>	<a href="#">CVE-2016-1000029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

&#xA0;

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
amazon -- blink_xt2_device	Blink XT2 Sync Module firmware prior to 2.13.11 allows remote attackers to execute arbitrary commands on the device due to improperly sanitized input	2019-12-31	not yet calculated	<a href="#">CVE-2019-3984</a>



	when the device retrieves updates scripts from the internet.			<a href="#">CONFIRM</a>
angular -- angular &#xA0;	There is a vulnerability in all angular versions before 1.5.0-beta.0, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14863</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
apache -- solr	Apache Solr 5.0.0 to Apache Solr 8.3.1 are vulnerable to a Remote Code Execution through the VelocityResponseWriter. A Velocity template can be provided through Velocity templates in a configset `velocity/` directory or as a parameter. A user defined configset could contain renderable, potentially malicious, templates. Parameter provided templates are disabled by default, but can be enabled by setting `params.resource.loader.enabled` by defining a response writer with that setting set to `true`. Defining a response writer requires configuration API access. Solr 8.4 removed the params resource loader entirely, and only enables the configset-provided template rendering when the configset is `trusted` (has been uploaded by an authenticated user).	2019-12-30	not yet calculated	<a href="#">CVE-2019-17558</a> <a href="#">MISC</a>
avira -- free_antivirus	Avira Free Antivirus 15.0.1907.1514 is prone to a local privilege escalation through the execution of kernel code from a restricted user.	2019-12-31	not yet calculated	<a href="#">CVE-2019-18568</a> <a href="#">CONFIRM</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a NULL pointer dereference in AP4_Descriptor::GetTag in mp42ts when called from AP4_EsDescriptor::GetDecoderConfigDescriptor in Ap4EsDescriptor.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20092</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a NULL pointer dereference in AP4_Descriptor::GetTag in mp42ts when called from AP4_DecoderConfigDescriptor::GetDecoderSpecificInfoDescriptor in Ap4DecoderConfigDescriptor.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20091</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a use-after-free in AP4_Sample::GetOffset in Core/Ap4Sample.h when called from Ap4LinearReader.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20090</a> <a href="#">MISC</a>
	Baidu Rust SGX SDK through 1.0.8 has			<a href="#">CVE-2020-</a>

baidu_x-lab -- rust_sgx_sdk	an enclave ID race. There are non-deterministic results in which, sometimes, two global IDs are the same.	2020-01-04	not yet calculated	<a href="#">CVE-2020-5499</a> <a href="#">MISC</a>
boltwire -- boltwire	Cross-site scripting (XSS) vulnerability in BoltWire 3.5 and earlier allows remote attackers to inject arbitrary web script or HTML via the fieldnames parameter.	2020-01-02	not yet calculated	<a href="#">CVE-2013-0737</a> <a href="#">MISC</a>
bombba -- bombba	The quaker function of a smart contract implementation for BOMBBA (BOMB), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19834</a> <a href="#">MISC</a>
bssys -- rbs_bs-client	Cross-site scripting (XSS) vulnerability in bsi.dll in Bank Soft Systems (BSS) RBS BS-Client 3.17.9 allows remote attackers to inject arbitrary web script or HTML via the colorstyle parameter.	2020-01-03	not yet calculated	<a href="#">CVE-2014-4196</a> <a href="#">MISC</a>
bssys -- rbs_bs-client	Multiple cross-site scripting (XSS) vulnerabilities in bsi.dll in Bank Soft Systems (BSS) RBS BS-Client. Private Client (aka RBS BS-Client. Retail Client) 2.5, 2.4, and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) DICTIONARY, (2) FILTERIDENT, (3) FROMSCHEME, (4) FromPoint, or (5) FName_0 parameter and a valid sid parameter value.	2020-01-03	not yet calculated	<a href="#">CVE-2014-10398</a> <a href="#">MISC</a>
bulb_security -- smartphone_pentest_framework	Bulb Security Smartphone Pentest Framework (SPF) before 0.1.3 allows remote attackers to execute arbitrary commands via shell metacharacters in the ipAddressTB parameter to (1) remoteAttack.pl or (2) guessPassword.pl in frameworkgui/; the filename parameter to (3) CSAttack.pl or (4) SEAttack.pl in frameworkgui/; the phNo2Attack parameter to (5) CSAttack.pl or (6) SEAttack.pl in frameworkgui/; the (7) phNo2Attack parameter to (7) frameworkgui/SEAttack.pl; the (8) agentURLPath or (9) agentControlKey parameter to frameworkgui/attach2agents.pl; or the (10) controlKey parameter to frameworkgui/attachMobileModem.pl. NOTE: The hostingPath parameter to CSAttack.pl and SEAttack.pl vectors and the appURLPath parameter to attachMobileModem.pl vector are covered by CVE-2012-5878.	2020-01-03	not yet calculated	<a href="#">CVE-2012-5693</a> <a href="#">MISC</a>
	Bulb Security Smartphone Pentest			

bulb_security -- smartphone_pentest_framework &#xA0;	Framework (SPF) 0.1.2 through 0.1.4 allows remote attackers to execute arbitrary commands via shell metacharacters in the hostingPath parameter to (1) SEAttack.pl or (2) CSAttack.pl in frameworkgui/ or the (3) appURLPath parameter to frameworkgui/attachMobileModem.pl.	2020-01-03	not yet calculated	<a href="#">CVE-2012-5878</a> <a href="#">MISC</a> <a href="#">MISC</a>
business_alliance_financial_circle -- business_alliance_financial_circle	The UBSexToken() function of a smart contract implementation for Business Alliance Financial Circle (BAFC), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function is public (by default) and does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19830</a> <a href="#">MISC</a>
chamilo -- chamilo_lms	Chamilo LMS through 1.9.10.2 allows a link_goto.php?link_url= open redirect, a related issue to CVE-2015-5503.	2020-01-04	not yet calculated	<a href="#">CVE-2015-9540</a> <a href="#">MISC</a>
clusterlabs -- fence-agents &#xA0;	In fence-agents before 4.0.17 does not verify remote SSL certificates in the fence_cisco_ucs.py script which can potentially allow for man-in-the-middle attackers to spoof SSL servers via arbitrary SSL certificates.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0104</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
comtech -- stampede_fx-1010_devices &#xA0;	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to execute arbitrary OS commands by navigating to the Diagnostics Ping page and entering shell metacharacters in the Target IP address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.)	2020-01-02	not yet calculated	<a href="#">CVE-2020-5179</a> <a href="#">MISC</a>
craftcms -- craft_cms	In the 3.1.12 Pro version of Craft CMS, XSS has been discovered in the header insertion field when adding source code at an s/admin/entries/news/new URI.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9554</a> <a href="#">MISC</a> <a href="#">MISC</a>
cryptobond_network -- cryptobond_network	The ToOwner() function of a smart contract implementation for Cryptbond Network (CBN), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19831</a> <a href="#">MISC</a>
cumin -- cumin &#xA0;	An import error was introduced in Cumin in the code refactoring in r5310. Server certificate validation is always disabled when connecting to Aviary servers, even if the installed packages on a system support it.	2019-12-30	not yet calculated	<a href="#">CVE-2013-0264</a> <a href="#">MISC</a> <a href="#">MISC</a>

d-link -- dgs-1510_series_switches	A security vulnerability in D-Link DGS-1510-series switches with firmware 1.20.011, 1.30.007, 1.31.B003 and older that may allow a remote attacker to inject malicious scripts in the device and execute commands via browser that is configuring the unit.	2019-12-30	not yet calculated	<a href="#">CVE-2018-7859</a> <a href="#">CONFIRM</a>
d-link -- dir-859_routers &#xA0;	D-Link DIR-859 routers before v1.07b03_beta allow Unauthenticated Information Disclosure via the AUTHORIZED_GROUP=1%0a value, as demonstrated by vpnconfig.php.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20213</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-859_wi-fi_router &#xA0;	The UPnP endpoint URL /gena.cgi in the D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01 allows an Unauthenticated remote attacker to execute system commands as root, by sending a specially crafted HTTP SUBSCRIBE request to the UPnP service when connecting to the local network.	2019-12-30	not yet calculated	<a href="#">CVE-2019-17621</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
ddq -- ddq &#xA0;	The owned function of a smart contract implementation for DDQ, an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19833</a> <a href="#">MISC</a>
docker -- docker &#xA0;	An issue was found in Docker before 1.6.0. Some programs and scripts in Docker are downloaded via HTTP and then executed or used in unsafe ways.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0048</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ds_data_systems -- konakart	Cross-site request forgery (CSRF) vulnerability in the Storefront Application in DS Data Systems KonaKart before 7.3.0.0 allows remote attackers to hijack the authentication of administrators for requests that change a user email address via an unspecified GET request.	2020-01-03	not yet calculated	<a href="#">CVE-2014-5516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
easy_xml_editor -- easy_xml_editor	Easy XML Editor through v1.7.8 is affected by: XML External Entity Injection. The impact is: Arbitrary File Read and DoS by consuming resources. The component is: XML Parsing. The attack vector is: Specially crafted XML payload.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19031</a> <a href="#">MISC</a>
ecstatic -- ecstatic	ecstatic have a denial of service vulnerability. Successful exploitation could lead to crash of an application.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10775</a> <a href="#">MISC</a>

embedded_glibc -- embedded_glibc	The eglibc package before 2.14 incorrectly handled the getaddrinfo() function. An attacker could use this issue to cause a denial of service.	2019-12-31	not yet calculated	<a href="#">CVE-2013-4357</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ezxml -- ezxml	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_ent_ok() mishandles recursion, leading to stack consumption for a crafted XML file.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20198</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The ezxml_parse_* functions mishandle XML entities, leading to an infinite loop in which memory allocations occur.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20201</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_decode, while parsing crafted a XML file, performs incorrect memory handling, leading to a heap-based buffer over-read in the "normalize line endings" feature.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20200</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_decode, while parsing a crafted XML file, performs incorrect memory handling, leading to NULL pointer dereference while running strlen() on a NULL pointer.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20199</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_char_content() tries to use realloc on a block that was not allocated, leading to an invalid free and segmentation fault.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20202</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.	2020-01-03	not yet calculated	<a href="#">CVE-2019-20330</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2013-4161</a>



fhdk -- gksu-polkit &#xA0;	gksu-polkit-0.0.3-6.fc18 was reported as fixing the issue in CVE-2012-5617 but the patch was improperly applied and it did not fixed the security issue.	2019-12-31	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fiberhome -- an5506-04-f_rp_2669_devices	FiberHome an5506-04-f RP2669 devices have XSS.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9556</a> <a href="#">MISC</a> <a href="#">MISC</a>
fontforge -- fontforge	FontForge 20190801 has a use-after-free in SFD_GetFontMetaData in sfd.c.	2020-01-03	not yet calculated	<a href="#">CVE-2020-5395</a> <a href="#">MISC</a>
fontforge -- fontforge	FontForge 20190801 has a heap-based buffer overflow in the Type2NotDefSplines() function in splinesave.c.	2020-01-03	not yet calculated	<a href="#">CVE-2020-5496</a> <a href="#">MISC</a>
ftp -- ftp	An issue was discovered in rovinbhandari FTP through 2012-03-28. receive_file in file_transfer_functions.c allows remote attackers to cause a denial of service (daemon crash) via a 0xffff datalen field value.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9668</a> <a href="#">MISC</a>
fusionforge -- fusionforge	FusionForge before 5.3.2 use scripts that run under the shared Apache user, which is also used by project homepages by default. If project webpages are hosted on the same server than FusionForge, it can allow users to incorrectly access on-disk private data in FusionForge.	2020-01-02	not yet calculated	<a href="#">CVE-2014-6275</a> <a href="#">MISC</a> <a href="#">MISC</a>
generalitat_de_catalunya -- accesuniversitat.gencat.cat &#xA0;	The Java API in Generalitat de Catalunya accesuniversitat.gencat.cat 1.7.5 allows remote attackers to get personal information of all registered students via several API endpoints, given that the attacker is authenticated as a student: 1) https://accesuniversitat.gencat.cat/accesuniversitat/AppJava/api/v1/estudiants/{student_id}/ 2) https://accesuniversitat.gencat.cat/accesuniversitat/accesuniversitat-rs/AppJava/api/v1/estudiants/?page={page}.	2019-12-31	not yet calculated	<a href="#">CVE-2019-12837</a> <a href="#">MISC</a>
getsimple_cms -- getsimple_cms &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in GetSimple CMS before 3.2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter to backup-edit.php; (2) title or (3) menu parameter to edit.php; or (4) path or (5) returnid parameter to filebrowser.php in admin/. NOTE: the path parameter in admin/upload.php vector is already covered by CVE-2012-6621.	2020-01-02	not yet calculated	<a href="#">CVE-2013-1420</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	Information Exposure.			<a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20494</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20498</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition 11.2.x through 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20496</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows SSRF.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20497</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 8.2 and later through 12.5 has Insecure Permissions.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19263</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 12.3 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19255</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 11.9 and later through 12.5 has Insecure Permissions.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19262</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 2 of 2).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19087</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 8.90 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19309</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) 11.3 through 12.4.2 allows Directory Traversal.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19088</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 6.7 and later through 12.5 allows SSRF.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19261</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-</a>

gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 1 of 2).	2020-01-03	not yet calculated	<a href="#">19086</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab Enterprise Edition 11.3.x and 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20491</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 11.3 and later through 12.5 allows an Insecure Direct Object Reference (IDOR).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19259</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 10.8 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19258</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.14 through 12.5, 12.4.3, and 12.3.6 allows XSS in group and profile fields.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19311</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 12.2 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19256</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 9.0 and later through 12.5 allows Information Disclosure.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19310</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gonicus -- gosa	The GOsa_Filter_Settings cookie in GONICUS GOsa 2.7.5.2 is vulnerable to PHP objection injection, which allows a remote authenticated attacker to perform file deletions (in the context of the user account that runs the web server) via a crafted cookie value, because unserialize is used to restore filter settings from a cookie.	2019-12-31	not yet calculated	<a href="#">CVE-2019-14466</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5845</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use-after-free in content delivery manager in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-13765</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially	2020-01-03	not yet calculated	<a href="#">CVE-2019-5846</a> <a href="#">MISC</a>

	exploit heap corruption via a crafted HTML page.			<a href="#">MISC</a>
google -- chrome &#xA0;	Use-after-free in accessibility in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-13766</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome &#xA0;	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5844</a> <a href="#">MISC</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GetPayload in GPMF_mp4reader.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20088</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GPMF_Next in GPMF_parser.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20086</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has an heap-based buffer over-read in GPMF_SeekToSamples in GPMF_parse.c for the size calculation.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20089</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GPMF_seekToSamples in GPMF-parse.c for the "matching tags" feature.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20087</a> <a href="#">MISC</a>
goscript -- goscript &#xA0;	go.cgi in GoScript 2.0 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) query string or (2) artarchive parameter.	2019-12-31	not yet calculated	<a href="#">CVE-2004-2776</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is an invalid pointer dereference in the function GF_IPMPX_AUTH_Delete() in odf/ipmpx_code.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20170</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There are memory leaks in metx_New in isomedia/box_code_base.c and abst_Read in isomedia/box_code_adobe.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20171</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a memory leak in dinf_New() in isomedia/box_code_base.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20159</a> <a href="#">MISC</a>
gpac -- gpac	dimC_Read in isomedia/box_code_3gpp.c in GPAC 0.8.0 has a stack-based buffer overflow.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20208</a> <a href="#">MISC</a>
	Unrestricted file upload vulnerability in			



helpdez -- helpdez	includes/classes/uploadify-v2.1.4/uploadify.php in HelpDEZk 1.0.1 and earlier allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in the directory specified by the folder parameter.	2020-01-03	not yet calculated	<a href="#">CVE-2014-8337</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp --multiple_products &#xA0;	A security vulnerability has been identified in HPE SimpliVity 380 Gen 9, HPE SimpliVity 380 Gen 10, HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen 10, SimpliVity OmniCube, SimpliVity OmniStack for Cisco, SimpliVity OmniStack for Lenovo and SimpliVity OmniStack for Dell nodes. An API is used to execute a command manifest file during upgrade does not correctly prevent directory traversal and so can be used to execute manifest files in arbitrary locations on the node. The API does not require user authentication and is accessible over the management network, resulting in the potential for unauthenticated remote execution of manifest files. For all customers running HPE OmniStack version 3.7.9 and earlier. HPE recommends upgrading the OmniStack software to version 3.7.10 or later, which contains a permanent resolution. Customers and partners who can upgrade to 3.7.10 should upgrade at the earliest convenience. For all customers and partners unable to upgrade their environments to the recommended version 3.7.10, HPE has created a Temporary Workaround <a href="https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061901&amp;withFrame">https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061901&amp;withFrame</a> for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.	2020-01-03	not yet calculated	<a href="#">CVE-2019-11994</a> <a href="#">MISC</a>
	A security vulnerability has been identified in HPE SimpliVity 380 Gen 9, HPE SimpliVity 380 Gen 10, HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen 10, SimpliVity OmniCube, SimpliVity OmniStack for Cisco, SimpliVity OmniStack for Lenovo and SimpliVity OmniStack for Dell nodes. Two now deprecated APIs run as root, accept a file name path, and can be used to create or			

hp -- multiple_products &#xA0;	delete arbitrary files on the nodes. These APIs do not require user authentication and are accessible over the management network, resulting in remote availability and integrity vulnerabilities For all customers running HPE OmniStack version 3.7.9 and earlier. HPE recommends upgrading the OmniStack software to version 3.7.10 or later, which contains a permanent resolution. Customers and partners who can upgrade to 3.7.10 should upgrade at the earliest convenience. For all customers and partners unable to upgrade their environments to the recommended version 3.7.10, HPE has created a Temporary Workaround <a href="https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061675&amp;withFrame">https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061675&amp;withFrame</a> for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.	2020-01-03	not yet calculated	<a href="#">CVE-2019-11993</a> <a href="#">MISC</a>
huawei -- multiple_products &#xA0;	Some Huawei products have a buffer error vulnerability. An unauthenticated, remote attacker could send specific MPLS Echo Request messages to the target products. Due to insufficient input validation of some parameters in the messages, successful exploit may cause the device to reset.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5304</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	Mate 10 Pro;Honor V10;Honor 10;Nova 4 smartphones have a denial of service vulnerability. The system does not properly check the status of certain module during certain operations, an attacker should trick the user into installing a malicious application, successful exploit could cause reboot of the smartphone.	2020-01-03	not yet calculated	<a href="#">CVE-2020-1785</a> <a href="#">MISC</a>
huawei -- p30_smartphones &#xA0;	HUAWEI P30 smart phones with versions earlier than 10.0.0.166(C00E66R1P11) have an information leak vulnerability. An attacker could send specific command in the local area network (LAN) to exploit this vulnerability. Successful exploitation may cause information leak.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19441</a> <a href="#">MISC</a>
huawei --	USG9500 with software of V500R001C30SPC100; V500R001C30SPC200; V500R001C30SPC600; V500R001C60SPC500; V500R005C00SPC100;			<a href="#">CVE-2020-</a>

usg9500_devices &#xA0;	V500R005C00SPC200 have an improper credentials management vulnerability. The software does not properly manage certain credentials. Successful exploit could cause information disclosure or damage, and impact the confidentiality or integrity.	2020-01-03	not yet calculated	<a href="#">1871</a> <a href="#">MISC</a>
infinispan -- infinispan &#xA0;	A flaw was found in Infinispan through version 9.4.14.Final. An improper implementation of the session fixation protection in the Spring Session integration can result in incorrect session handling.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10158</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	Heap-based buffer overflow in the MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via a levels header.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3946</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	Stack-based buffer overflow in the MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via an IMAGE tag.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3944</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	The MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via a nband tag.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3945</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
it-novum -- openitcockpit	openITCOCKPIT before 3.7.1 has reflected XSS in the 404-not-found component.	2019-12-31	not yet calculated	<a href="#">CVE-2019-10227</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
joomla! -- joomla! &#xA0;	Cross-site scripting (XSS) vulnerability in the Jomres (com_jomres) component before 7.3.1 for Joomla! allows remote authenticated users with the "Business Manager" permission to inject arbitrary web script or HTML via the property_name parameter, related to editing property details.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3931</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla! &#xA0;	SQL injection vulnerability in the Jomres (com_jomres) component before 7.3.1 for Joomla! allows remote authenticated users with the "Business Manager" permission to execute arbitrary SQL commands via the id parameter in an editProfile action to administrator/index.php.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3932</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
kind-of -- kind-of	ctorName in index.js in kind-of v6.0.2 allows external user input to overwrite certain internal attributes via a conflicting name, as demonstrated by 'constructor':	2019-12-	not yet	<a href="#">CVE-2019-20149</a>

	{'name':'Symbol'}. Hence, a crafted payload can overwrite this builtin attribute to manipulate the type detection result.	30	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
knockout -- knockout	There is a vulnerability in knockout before version 3.5.0-beta, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14862</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libmysofa -- libmysofa &#xA0;	hdf/dataobject.c in libmysofa before 0.8 has an uninitialized use of memory, as demonstrated by mysofa2json.	2019-12-29	not yet calculated	<a href="#">CVE-2019-20063</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel_project -- libsixel	libsixel 1.8.4 has an integer overflow in sixel_frame_resize in frame.c.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20205</a> <a href="#">MISC</a>
libsixel_project -- libsixel	stb_image.h (aka the stb image loader) 2.23, as used in libsixel and other products, has an assertion failure in stbi__shiftsigned.	2019-12-29	not yet calculated	<a href="#">CVE-2019-20056</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An issue was discovered in libsixel 1.8.4. There is a heap-based buffer overflow in the function gif_out_code at fromgif.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20140</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.0-rc7 (as distributed in ubuntu/linux.git on kernel.ubuntu.com), mounting a crafted f2fs filesystem image and performing some operations can lead to slab-out-of-bounds read access in ttm_put_pages in drivers/gpu/drm/ttm/ttm_page_alloc.c. This is related to the vmwgfx or ttm module.	2019-12-31	not yet calculated	<a href="#">CVE-2019-19927</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	mwifiex_tm_cmd in drivers/net/wireless/marvell/mwifiex/cfg80211.c in the Linux kernel before 5.1.6 has some error-handling cases that did not free allocated hostcmd memory, aka CID-003b686ace82. This will cause a memory leak and denial of service.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20095</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel &#xA0;	In the Linux kernel before 5.1, there is a memory leak in __feat_register_sp() in net/dccp/feat.c, which may cause denial of service, aka CID-1d3ff0950e2b.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20096</a> <a href="#">MISC</a> <a href="#">MISC</a>
loaded_commerce -- loaded_commerce	The bindReplace function in the query factory in includes/classes/database.php in Loaded Commerce 7 does not properly handle : (colon) characters, which allows remote authenticated users to conduct SQL injection attacks via the First name and Last name fields in the address book.	2020-01-03	not yet calculated	<a href="#">CVE-2014-5140</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

mailstore -- mailstore_server_and_authentication_engine does not	An issue was discovered in MailStore Server (and Service Provider Edition) 9.x through 11.x before 11.2.2. When the directory service (for synchronizing and authenticating users) is set to Generic LDAP, an attacker is able to login as an existing user with an arbitrary password on the second login attempt.	2019-12-31	not yet calculated	<a href="#">CVE-2019-10229</a> <a href="#">CONFIRM</a>
mfscripts -- yetishare	class.userpeer.php in MFScripts YetiShare 3.5.2 through 4.5.3 uses an insecure method of creating password reset hashes (based only on microtime), which allows an attacker to guess the hash and set the password within a few hours by bruteforcing.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19735</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the Secure flag on session cookies, allowing the cookie to be sent over cleartext channels.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19739</a> <a href="#">MISC</a>
mfscripts -- yetishare	translation_manage_text.ajax.php and various *_manage.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 directly insert values from the aSortDir_0 and/or sSortDir_0 parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19732</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the HttpOnly flag on session cookies, allowing the cookie to be read by script, which can potentially be used by attackers to obtain the cookie via cross-site scripting.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19736</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the SameSite flag on session cookies, allowing the cookie to be sent in cross-site requests and potentially be used in cross-site request forgery attacks.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19737</a> <a href="#">MISC</a>
mfscripts -- yetishare	log_file_viewer.php in MFScripts YetiShare 3.5.2 through 4.5.3 does not sanitize or encode the output from the IFile parameter on the page, which would allow an attacker to input HTML or execute scripts on the site, aka XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19738</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_account_move_file_in_folder.ajax.php in MFScripts YetiShare 3.5.2 directly inserts values from the filelds parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the	2019-12-30	not yet calculated	<a href="#">CVE-2019-19734</a> <a href="#">MISC</a> <a href="#">MISC</a>



	database, aka SQL Injection.			
mfscripts -- yetishare &#xA0;	_account_forgot_password.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 takes a different amount of time to return depending on whether an email address is configured for the account name provided. This can be used by an attacker to enumerate accounts by guessing email addresses.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19805</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_get_all_file_server_paths.ajax.php (aka get_all_file_server_paths.ajax.php) in MFScripts YetiShare 3.5.2 through 4.5.3 does not sanitize or encode the output from the filelds parameter on the page, which would allow an attacker to input HTML or execute scripts on the site, aka XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19733</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_account_forgot_password.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 displays a message indicating whether an email address is configured for the account name provided. This can be used by an attacker to enumerate accounts by guessing email addresses.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19806</a> <a href="#">MISC</a>
miniupnp -- ngiflib	ngiflib 0.4 has a heap-based buffer over-read in GifIndexToTrueColor in ngiflib.c.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20219</a> <a href="#">MISC</a>
mitreid_connect -- mitreid_connect	The OpenID Connect reference implementation for MITREid Connect through 1.3.3 allows XSS due to userInfoJson being included in the page unsanitized. This is related to header.tag. The issue can be exploited to execute arbitrary JavaScript.	2020-01-04	not yet calculated	<a href="#">CVE-2020-5497</a> <a href="#">MISC</a>
monitorix -- monitorix	The handle_request function in lib/HTTPServer.pm in Monitorix before 3.3.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the URI.	2019-12-31	not yet calculated	<a href="#">CVE-2013-7070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
monitorix -- monitorix	Cross-site scripting (XSS) vulnerability in the handle_request function in lib/HTTPServer.pm in Monitorix before 3.4.0 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2019-12-31	not yet calculated	<a href="#">CVE-2013-7071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mybb -- mybb	MyBB before 1.8.22 allows an open redirect on login.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20225</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In Nagios XI 5.6.9, an authenticated user is able to execute arbitrary OS commands	2019-12-	not yet	<a href="#">CVE-2019-</a>

nagios -- nagios_xi	via shell metacharacters in the id parameter to schedulereport.php, in the context of the web-server user account.	31	calculated	<a href="#">20197</a> <a href="#">MISC</a>
nasm -- netwide_assembler	In Netwide Assembler (NASM) 2.14.02, stack consumption occurs in expr# functions in asm/eval.c. This potentially affects the relationships among expr0, expr1, expr2, expr3, expr4, expr5, and expr6 (and stdscan in asm/stdscan.c). This is similar to CVE-2019-6290 and CVE-2019-6291.	2020-01-04	not yet calculated	<a href="#">CVE-2019-20334</a> <a href="#">MISC</a> <a href="#">MISC</a>
newinteltechmedia -- newinteltechmedia	The NETM() function of a smart contract implementation for NewIntelTechMedia (NETM), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19832</a> <a href="#">MISC</a>
nim -- nim	The HTTP Authentication library before 2019-12-27 for Nim has weak password hashing because the default algorithm for libsodium's crypto_pwhash_str is not used.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20138</a> <a href="#">MISC</a>
obs-server -- obs-server	obs-server before 1.7.7 allows logins by 'unconfirmed' accounts due to a bug in the REST api implementation.	2020-01-02	not yet calculated	<a href="#">CVE-2010-3782</a> <a href="#">MISC</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev27 and 7.4.x before 7.4.0-rev20 allows remote attackers to inject arbitrary web script or HTML via the body of an email. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7486</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">SECTRAK</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev26 and 7.4.x before 7.4.0-rev16 allows remote attackers to inject arbitrary web script or HTML via the publication name, which is not properly handled in an error message. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7485</a> <a href="#">OSVDB</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a> <a href="#">SECTRAK</a> <a href="#">XF</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the frontend in Open-Xchange (OX) AppSuite 6.22.3 before 6.22.3-rev5 and 6.22.4 before 6.22.4-rev12 allows remote attackers to inject arbitrary web script or HTML via the subject of an email. NOTE: the vulnerabilities related to the body of	2020-01-02	not yet calculated	<a href="#">CVE-2013-6242</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	the email and the publication name were SPLIT from this CVE ID because they affect different sets of versions.			<a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV 4.1.0. A specially crafted XML file can cause a buffer overflow, resulting in multiple heap corruptions and potential code execution. An attacker can provide a specially crafted file to trigger this vulnerability.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5063</a> <a href="#">MISC</a>
opencv -- opencv	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV, version 4.1.0. A specially crafted JSON file can cause a buffer overflow, resulting in multiple heap corruptions and potentially code execution. An attacker can provide a specially crafted file to trigger this vulnerability.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5064</a> <a href="#">MISC</a>
openlambda -- openlambda	OpenLambda 2019-09-10 allows DNS rebinding attacks against the OL server for the REST API on TCP port 5000.	2020-01-03	not yet calculated	<a href="#">CVE-2019-20329</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openldap -- openldap &#xA0;	An off-by-one error leading to a crash was discovered in openldap 2.4 when processing DNS SRV messages. If slapd was configured to use the dnssrv backend, an attacker could crash the service with crafted DNS responses.	2020-01-02	not yet calculated	<a href="#">CVE-2014-8182</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opsview -- opsview_and_opsview_core	Multiple cross-site scripting (XSS) vulnerabilities in Opsview before 4.4.1 and Opsview Core before 20130522 allow remote attackers to inject arbitrary web script or HTML.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3936</a> <a href="#">MISC</a> <a href="#">MISC</a>
opsview -- opsview_and_opsview_core	Cross-site request forgery (CSRF) vulnerability in Opsview before 4.4.1 and Opsview Core before 20130522 allows remote attackers to hijack the authentication of administrators for requests that change the administrator password via unspecified vectors.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3935</a> <a href="#">MISC</a> <a href="#">MISC</a>
outsystems -- platform	OutSystems Platform 10 through 11 allows ImageResourceDetail.aspx CSRF for content modifications and file uploads. NOTE: the product is self-hosted by the customer, even though it has a *.outsystemsenterprise.com domain name.)	2019-12-31	not yet calculated	<a href="#">CVE-2019-12273</a> <a href="#">MISC</a>



	host's qemu address space and thus increase their privileges on the host.			<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu &#xA0;	Qemu 1.1.2+dfsg to 2.1+dfsg suffers from a buffer overrun which could potentially result in arbitrary code execution on the host with the privileges of the QEMU process.	2020-01-02	not yet calculated	<a href="#">CVE-2013-4532</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
quixplorer -- quixplorer &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in QuiXplorer before 2.5.5 allow remote attackers to inject arbitrary web script or HTML via the (1) dir, (2) item, (3) order, (4) searchitem, (5) selitems[], or (6) srt parameter to index.php or (7) the QUERY_STRING to index.php.	2020-01-02	not yet calculated	<a href="#">CVE-2013-1642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible	Ansible, versions 2.9.x before 2.9.1, 2.8.x before 2.8.7 and Ansible versions 2.7.x before 2.7.15, is not respecting the flag no_log set it to True when Sumologic and Splunk callback plugins are used send tasks results events to collectors. This would discloses and collects any sensitive data.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14864</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_enterprise_application_platform &#xA0;	In JBoss EAP 6 a security domain is configured to use a cache that is shared between all applications that are in the security domain. This could allow an authenticated user in one application to access protected resources in another application without proper authorization. Although this is an intended functionality, it was not clearly documented which can mislead users into thinking that a security domain cache is isolated to a single application.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0169</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_portal &#xA0;	It was found that the implementation of the GTNSubjectCreatingInterceptor class in gatein-wsrp was not thread safe. For a specific WSRP endpoint, under high-concurrency scenarios or scenarios where SOAP messages take long to execute, it was possible for an unauthenticated remote attacker to gain privileged information if WS-Security is enabled for the WSRP Consumer, and the endpoint in question is being used by a privileged user. This affects JBoss Portal 6.2.0.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0245</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



red_hat -- openshift_enterprise &#xA0;	A CSRF issue was found in OpenShift Enterprise 1.2. The web console is using 'Basic authentication' and the REST API has no CSRF attack protection mechanism. This can allow an attacker to obtain the credential and the Authorization: header when requesting the REST API via web browser.	2019-12-30	not yet calculated	<a href="#">CVE-2013-0196</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openstack_essex_release	Within the RHOS Essex Preview (2012.2) of the OpenStack dashboard package, the file /etc/quantum/quantum.conf is world readable which exposes the admin password and token value.	2019-12-30	not yet calculated	<a href="#">CVE-2012-5476</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openstack_platform_and_essex_release &#xA0;	The file /etc/openstack-dashboard/local_settings within Red Hat OpenStack Platform 2.0 and RHOS Essex Release (python-openstack-dashboard before 2012.1.1) is world readable and exposes the secret key value.	2019-12-30	not yet calculated	<a href="#">CVE-2012-5474</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- quay	A flaw was found in the way Red Hat Quay stores robot account tokens in plain text. An attacker able to perform database queries in the Red Hat Quay database could use the tokens to read or write container images stored in the registry.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10205</a> <a href="#">CONFIRM</a>
red_hat -- satellite_6	Versions of Foreman as shipped with Red Hat Satellite 6 does not check for a correct CSRF token in the logout action. Therefore, an attacker can log out a user by having them view specially crafted content.	2020-01-02	not yet calculated	<a href="#">CVE-2014-3590</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- subscription_asset_manager	Versions of Katello as shipped with Red Hat Subscription Asset Manager 1.4 are vulnerable to a XSS via HTML in the systems name when registering.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0183</a> <a href="#">MISC</a> <a href="#">MISC</a>
ricoh -- marcomcentral &#xA0;	A directory traversal and local file inclusion vulnerability in FPProducerInternetServer.exe in Ricoh MarcomCentral, formerly PTI Marketing, FusionPro VDP before 10.0 allows a remote attacker to list or enumerate sensitive contents of files. Furthermore, this could allow for privilege escalation by dumping the local machine's SAM and SYSTEM database files, and possibly remote code execution.	2019-12-31	not yet calculated	<a href="#">CVE-2019-7751</a> <a href="#">MISC</a> <a href="#">MISC</a>
ros -- ros &#xA0;	An issue was discovered in the ROS communications-related packages (aka ros_comm or ros-melodic-ros-comm) through 1.14.3. parseOptions() in tools/rosbag/src/record.cpp has an	2019-12-30	not yet calculated	<a href="#">CVE-2019-13445</a> <a href="#">MISC</a>

	integer overflow when a crafted split option can be entered on the command line.			<a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ros -- ros &#xA0;	An issue was discovered in the ROS communications-related packages (aka ros_comm or ros-melodic-ros-comm) through 1.14.3. ROS_ASSERT_MSG only works when ROS_ASSERT_ENABLED is defined. This leads to a problem in the remove() function in clients/roscpp/src/libros/spinner.cpp. When ROS_ASSERT_ENABLED is not defined, the iterator loop will run out of the scope of the array, and cause denial of service for other components (that depend on the communication-related functions of this package).	2019-12-30	not yet calculated	<a href="#">CVE-2019-13465</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
rsa -- authentication_manager	RSA Authentication Manager versions prior to 8.4 P7 contain an XML Entity Injection Vulnerability. A remote authenticated malicious user could potentially exploit this vulnerability to cause information disclosure of local system files by supplying specially crafted XML message.	2020-01-03	not yet calculated	<a href="#">CVE-2019-3768</a> <a href="#">MISC</a>
samba -- samba &#xA0;	Multiple race conditions in the (1) mount.cifs and (2) umount.cifs programs in Samba 3.6 allow local users to cause a denial of service (mounting outage) via a SIGKILL signal during a time window when the /etc/mtab~ file exists.	2019-12-31	not yet calculated	<a href="#">CVE-2011-3585</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
serenityos -- serenityos &#xA0;	Kernel/VM/MemoryManager.cpp in SerenityOS before 2019-12-30 does not reject syscalls with pointers into the kernel-only virtual address space, which allows local users to gain privileges by overwriting a return address that was found on the kernel stack.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20172</a> <a href="#">MISC</a> <a href="#">MISC</a>
shaarli -- shaarli &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Shaarli allow remote attackers to inject arbitrary web script or HTML via the URL to the (1) showRSS, (2) showATOM, or (3) showDailyRSS function; a (4) file name to the importFile function; or (5) vectors related to bookmarks.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7351</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
sonicwall -- global_management_system	A vulnerability in GMS allow unauthenticated user to SQL injection in Webservice module. This vulnerability affected GMS versions GMS 8.4, 8.5, 8.6,	2019-12-31	not yet calculated	<a href="#">CVE-2019-7478</a> <a href="#">CONFIRM</a>

	8.7, 9.0 and 9.1.			
sonicwall -- sonicos &#xA0;	A vulnerability in SonicOS allow authenticated read-only admin can elevate permissions to configuration mode. This vulnerability affected SonicOS Gen 5 version 5.9.1.12-4o and earlier, Gen 6 version 6.2.7.4-32n, 6.5.1.4-4n, 6.5.2.3-4n, 6.5.3.3-3n, 6.2.7.10-3n, 6.4.1.0-3n, 6.5.3.3-3n, 6.5.1.9-4n and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V).	2019-12-31	not yet calculated	<a href="#">CVE-2019-7479</a> <a href="#">CONFIRM</a>
sqlite -- sqlite &#xA0;	ext/misc/zipfile.c in SQLite 3.30.1 mishandles certain uses of INSERT INTO in situations involving embedded '' characters in filenames, leading to a memory-management error that can be detected by (for example) valgrind.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19959</a> <a href="#">MISC</a> <a href="#">MISC</a>
supermicro -- x9_and_x8_generation &#xA0;	Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before SMT_X9_317 and firmware for Supermicro X8 generation motherboards before SMT X8 312 contain hardcoded private encryption keys for the (1) Lighttpd web server SSL interface and the (2) Dropbear SSH daemon.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3619</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
supermicro -- x9_and_x8_generation &#xA0;	Hardcoded WSMAN credentials in Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before 3.15 (SMT_X9_315) and firmware for Supermicro X8 generation motherboards before SMT X8 312.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3620</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
sylius -- sylius &#xA0;	An issue was discovered in Sylius products. Missing input sanitization in sylius/sylius 1.0.x through 1.0.18, 1.1.x through 1.1.17, 1.2.x through 1.2.16, 1.3.x through 1.3.11, and 1.4.x through 1.4.3 and sylius/grid 1.0.x through 1.0.18, 1.1.x through 1.1.18, 1.2.x through 1.2.17, 1.3.x through 1.3.12, 1.4.x through 1.4.4, and 1.5.0 allows an attacker (an admin in the sylius/sylius case) to perform XSS by injecting malicious code into a field displayed in a grid with the "string" field type. The contents are an object, with malicious code returned by the toString() method of that object.	2019-12-31	not yet calculated	<a href="#">CVE-2019-12186</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2013-4752</a>

symfony -- symfony &#xA0;	Symfony 2.0.X before 2.0.24, 2.1.X before 2.1.12, 2.2.X before 2.2.5, and 2.3.X before 2.3.3 have an issue in the HttpFoundation component. The Host header can be manipulated by an attacker when the framework is generating an absolute URL. A remote attacker could exploit this vulnerability to inject malicious content into the Web application page and conduct various attacks.	2020-01-02	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
telos -- automated_message_handling_system	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the LDAP cbURL parameter of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9538</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uploaditem.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9537</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Information Exposure vulnerability in itemlookup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9541</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in itemlookup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9542</a> <a href="#">CERT-VN</a>
	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in prefs.asp of			

telos -- automated_message_handling_system &#xA0;	Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9540</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ModalWindowPopup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9539</a> <a href="#">CERT-VN</a>
textproc/isearch -- textproc/isearch &#xA0;	The isearch package (textproc/isearch) before 1.47.01nb1 uses the tempnam() function to create insecure temporary files into a publicly-writable area (/tmp).	2019-12-30	not yet calculated	<a href="#">CVE-2012-5663</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tigervnc -- tigervnc &#xA0;	Multiple heap-based buffer overflows in the ZRLE_DECODE function in common/rfb/zrleDecode.h in TigerVNC before 1.3.1, when NDEBUB is enabled, allow remote VNC servers to cause a denial of service (vncviewer crash) and possibly execute arbitrary code via vectors related to screen image rendering.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0011</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tiny_file_manager -- tiny_file_manager &#xA0;	In Tiny File Manager before 2.3.9, there is a remote code execution via Upload from URL and Edit/Rename files. Only authenticated users are impacted.	2019-12-30	not yet calculated	<a href="#">CVE-2019-16790</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tinywall -- tinywall	An attacker who has already compromised the local system could use TinyWall Controller to gain additional privileges by attaching a debugger to the running process and modifying the code in memory. Vulnerability fixed in version 2.1.13.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19470</a> <a href="#">MISC</a>
tvb -- nvms-1000_devices	TVT NVMS-1000 devices allow GET /.. Directory Traversal	2019-12-30	not yet calculated	<a href="#">CVE-2019-20085</a> <a href="#">MISC</a>
unity_technologies -- editor &#xA0;	The com.unity3d.kharma protocol handler in Unity Editor 2018.3 allows remote attackers to execute arbitrary code.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9197</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vim -- vim	The autocmd feature in window.c in Vim	2019-12-	not yet	<a href="#">CVE-2019-20079</a>



&#xA0;	before 8.1.2136 accesses freed memory.	30	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
visual_mining -- netcharts_server &#xA0;	Unrestricted file upload vulnerability in Visual Mining NetCharts Server allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via unspecified vectors.	2020-01-03	not yet calculated	<a href="#">CVE-2014-8516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	Cross-site Scripting (XSS) in the spreadshirt-rss-3d-cube-flash-gallery plugin 2014 for WordPress allows remote attackers to execute arbitrary web script or HTML via unspecified parameters.	2020-01-02	not yet calculated	<a href="#">CVE-2014-4553</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	The Postie plugin 1.9.40 for WordPress allows XSS, as demonstrated by a certain payload with jaVaScRipt:/* at the beginning and a crafted SVG element.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20204</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	The Authorized Addresses feature in the Postie plugin 1.9.40 for WordPress allows remote attackers to publish posts by spoofing the From information of an email message.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20203</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
xmlblueprint -- xmlblueprint	XMLBlueprint through 16.191112 is affected by XML External Entity Injection. The impact is: Arbitrary File Read when an XML File is validated. The component is: XML Validate function. The attack vector is: Specially crafted XML payload.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19032</a> <a href="#">MISC</a>
xnview -- xnview	xnview.exe in XnView before 2.13 does not properly handle RLE strip lengths during processing of RGB files, which allows remote attackers to execute arbitrary code via the RLE strip size field in a RGB file, which leads to an unexpected sign extension error and a heap-based buffer overflow.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3939</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
xnview -- xnview	Heap-based buffer overflow in xnview.exe in XnView before 2.13 allows remote attackers to execute arbitrary code via the biBitCount field in a BMP file.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3937</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
xnview -- xnview &#xA0;	Xjp2.dll in XnView before 2.13 allows remote attackers to execute arbitrary code via (1) the Csiz parameter in a SIZ marker, which triggers an incorrect memory allocation, or (2) the lqcd field in a QCD marker in a crafted JPEG2000 file, which leads to a heap-based buffer	2020-01-02	not yet calculated	<a href="#">CVE-2013-3941</a> <a href="#">MISC</a> <a href="#">MISC</a>

	overflow.			
yandex -- clickhouse	In all versions of ClickHouse before 19.14.3, an attacker having write access to ZooKeeper and who is able to run a custom server available from the network where ClickHouse runs, can create a custom-built malicious server that will act as a ClickHouse replica and register it in ZooKeeper. When another replica will fetch data part from the malicious replica, it can force clickhouse-server to write to arbitrary path on filesystem.	2019-12-30	not yet calculated	<a href="#">CVE-2019-15024</a> <a href="#">MISC</a>
zend_framework -- zend_framework	Multiple cross-site scripting (XSS) vulnerabilities in Zend Framework 2.0.x before 2.0.1 allow remote attackers to inject arbitrary web script or HTML via unspecified input to (1) Debug, (2) Feed\PubSubHubbub, (3) Log\Formatter\Xml, (4) Tag\Cloud\Decorator, (5) Uri, (6) View\Helper\HeadStyle, (7) View\Helper\Navigation\Sitemap, or (8) View\Helper\Placeholder\Container\AbstractStandalone, related to Escaper.	2020-01-03	not yet calculated	<a href="#">CVE-2012-4451</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	SQL injection vulnerability in Zenphoto before 1.4.9 allow remote administrators to execute arbitrary SQL commands.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Cross-site request forgery (CSRF) vulnerability in admin.php in Zenphoto before 1.4.9 allows remote attackers to hijack the authentication of admin users for requests that may cause a denial of service (resource consumption).	2019-12-31	not yet calculated	<a href="#">CVE-2015-5595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Incomplete blacklist in sanitize_string in Zenphoto before 1.4.9 allows remote attackers to conduct cross-site scripting (XSS) attacks.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5592</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	The sanitize_string function in Zenphoto before 1.4.9 does not properly sanitize HTML tags, which allows remote attackers to perform a cross-site scripting (XSS) attack by wrapping a payload in "<<script></script>script>payload<script></script></script>", or in an image tag, with the payload as the onerror event.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in Zoho ManageEngine ADSelfService Plus 5.6			

zoho_manageengine - - adselfservice_plus	Build 5607. An exposed service allows an unauthenticated person to retrieve internal information from the system and modify the product installation.	2019-12-31	not yet calculated	<a href="#">CVE-2019-7162</a> <a href="#">MISC</a>
---	---	------------	--------------------	---

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [edigiovanna@sunnyvale.ca.gov](mailto:edigiovanna@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of December 30, 2019  
**Date:** Monday, January 06, 2020 6:47:43 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of December 30, 2019](#)

01/06/2020 08:41 AM EST

Original release date: January 6, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
citrix -- application_delivery_controller	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5, 11.1, 12.0, 12.1, and 13.0. They allow Directory Traversal.	2019-12-27	<a href="#">7.5</a>	<a href="#">CVE-2019-19781</a> <a href="#">CONFIRM</a>
freeciv -- freeciv	A denial of service flaw was found in the way the server component of Freeciv before 2.3.4 processed certain packets. A remote attacker could send a specially-crafted packet that, when processed would lead to memory exhaustion or excessive CPU consumption.	2019-12-30	<a href="#">7.8</a>	<a href="#">CVE-2012-5645</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
magnolia_international	Magnolia CMS before 4.5.9 has multiple	2019-12-		<a href="#">CVE-2013-4621</a>

-- magnolia_cms &#xA0;	access bypass vulnerabilities	27	7.5	MISC MISC
open_dynamics -- collabtive	Collabtive 1.0 has incorrect access control	2019-12-27	7.5	CVE-2013-5027 MISC
php-shellcommand -- php-shellcommand	php-shellcommand versions before 1.6.1 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-30	10	CVE-2019-10774 MISC
senkas -- kolibri	Buffer overflow in Senkas Kolibri 2.0 allows remote attackers to execute arbitrary code via a long URI in a POST request.	2019-12-27	7.5	CVE-2014-5289 MISC BID XE
sqlite -- sqlite &#xA0;	selectExpander in select.c in SQLite 3.30.1 proceeds with WITH stack unwinding even after a parsing error.	2020-01-02	7.5	CVE-2019-20218 MISC
wordpress -- wordpress &#xA0;	wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript&colon; substring.	2019-12-27	7.5	CVE-2019-20041 MISC MISC
yandex -- clickhouse	In all versions of ClickHouse before 19.14, an OOB read, OOB write and integer underflow in decompression algorithms can be used to achieve RCE or DoS via native protocol.	2019-12-30	7.5	CVE-2019-16535 MISC

[Back to top](#)

&#xA0;

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bolt -- bolt &#xA0;	Bolt 3.6.4 has XSS via the slug, teaser, or title parameter to editcontent/pages, a related issue to CVE-2017-11128 and CVE-2018-19933.	2019-12-31	4.3	CVE-2019-9553 MISC MISC
genjxcms -- genjxcms &#xA0;	GeniXCMS 1.1.5 has XSS via the dbuser or dbhost parameter during step 1 of installation.	2019-12-31	4.3	CVE-2018-14476 MISC MISC
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_SPLINE_private in	2019-12-27	4.3	CVE-2019-20009 MISC MISC



	dwg.spec.			<a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. There is a use-after-free in resolve_objectref_vector in decode.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20010</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. There is a heap-based buffer over-read in decode_R13_R2000 in decode.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20011</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. There is a double-free in dwg_free in free.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20014</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_HATCH_private in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20012</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in decode_3dsolid in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20013</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_LWPOLYLINE_private in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20015</a> <a href="#">MISC</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function senc_Parse() in isomedia/box_code_drm.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20167</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_odf_avc_cfg_write_bs() in odf/descriptors.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20163</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the function trak_Read() in isomedia/box_code_base.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20169</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20168</a>

	function gf_isom_box_dump_ex() in isomedia/box_funcs.c.			<a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_dump() in isomedia/box_dump.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20166</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function ReadGF_IPMPX_WatermarkingInit() in odg/ipmpx_code.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20161</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a stack-based buffer overflow in the function av1_parse_tile_group() in media_tools/av_parsers.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20160</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function gf_isom_box_parse_ex() in isomedia/box_funcs.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20162</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_box_del() in isomedia/box_funcs.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20164</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function ilst_item_Read() in isomedia/box_code_apple.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20165</a> <a href="#">MISC</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 allows overly permissive cross-origin resource sharing which could allow an attacker to transfer private information. An attacker could exploit this vulnerability to access content that should be restricted. IBM X-Force ID: 161422.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-4343</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- mq	IBM MQ 9.1.0.0, 9.1.0.1, 9.1.0.2, 9.1.0.3, 9.1.1, 9.1.2, and 9.1.3 is vulnerable to a denial of service attack that would allow an authenticated user to reset client connections due to an error within the Data Conversion routine. IBM X-Force ID: 170966.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-4655</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

ibm -- watson_studio_local &#xA0;	IBM Watson Studio Local 1.2.3 could disclose sensitive information over the network that an attacker could use in further attacks against the system. IBM X-Force ID: 145238.	2019-12-30	5	<a href="#">CVE-2018-1682</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
joomla! -- joomla! &#xA0;	Xorbin Analog Flash Clock 1.0 extension for Joomla has XSS	2019-12-27	4.3	<a href="#">CVE-2013-4692</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel_project -- libsixel	A memory leak was discovered in image_buffer_resize in fromsixel.c in libsixel 1.8.4.	2019-12-27	4.3	<a href="#">CVE-2019-20023</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An invalid memory address dereference was discovered in load_pnm in frompnm.c in libsixel before 1.8.3.	2019-12-27	4.3	<a href="#">CVE-2019-20022</a> <a href="#">MISC</a>
libsixel_project -- libsixel &#xA0;	An issue was discovered in libsixel 1.8.4. There is a heap-based buffer overflow in the function gif_init_frame at fromgif.c.	2019-12-30	6.8	<a href="#">CVE-2019-20094</a> <a href="#">MISC</a>
libsixel_project -- libsixel &#xA0;	A heap-based buffer overflow was discovered in image_buffer_resize in fromsixel.c in libsixel before 1.8.4.	2019-12-27	4.3	<a href="#">CVE-2019-20024</a> <a href="#">MISC</a>
livefyre -- livecomments	Cross-site scripting (XSS) vulnerability in Livefyre LiveComments 3.0 allows remote attackers to inject arbitrary web script or HTML via the name of an uploaded picture.	2019-12-27	4.3	<a href="#">CVE-2014-6420</a> <a href="#">MISC</a> <a href="#">XE</a>
luquidpixels -- liquifire_os	LuquidPixels LiquiFire OS 4.8.0 allows SSRF via the call%3Durl substring followed by a URL in square brackets.	2019-12-29	6.4	<a href="#">CVE-2019-20055</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi hostname parameter (Dynamic DNS Configuration).	2019-12-30	4.3	<a href="#">CVE-2019-20072</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi username parameter (DynDns settings of the Dynamic DNS Configuration).	2019-12-30	4.3	<a href="#">CVE-2019-20076</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the urlFQDN parameter to form2url.cgi (aka the Keyword field of the URL Blocking Configuration).	2019-12-30	4.3	<a href="#">CVE-2019-20070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, pingrtt_v6.html has XSS (Ping6 Diagnostic).	2019-12-30	4.3	<a href="#">CVE-2019-20075</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, any user role can view sensitive information, such as a user password or the FTP password, via the form2saveConf.cgi page.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-20074</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, CSRF exists via form2logaction.cgi to delete all logs.	2019-12-30	<a href="#">5.8</a>	<a href="#">CVE-2019-20071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, XSS exists via the form2userconfig.cgi username parameter (User Account Configuration).	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20073</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /search.htm searchtext parameter. NOTE: This product is discontinued.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-9207</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /public/login.htm errmsg or loginurl parameter. NOTE: This product is discontinued.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-9206</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5312</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/TiffDecode.c in Pillow before 6.2.2 has a TIFF decoding integer overflow, related to realloc.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5310</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/FliDecode.c in Pillow before 6.2.2 has an FLI buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5313</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/SgiRleDecode.c in Pillow before 6.2.2 has an SGI buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5311</a> <a href="#">MISC</a> <a href="#">MISC</a>
proxyman -- proxyman_for_macos	com.proxyman.NSProxy.HelperTool in Privileged Helper Tool in Proxyman for macOS 1.11.0 and earlier allows an attacker to change the System Proxy and redirect all traffic to an attacker-controlled computer, enabling MITM attacks.	2019-12-29	<a href="#">4.3</a>	<a href="#">CVE-2019-20057</a> <a href="#">MISC</a>
sencha_labs -- connect	Sencha Labs Connect has XSS with connect.methodOverride()	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4691</a> <a href="#">MISC</a>
spbas -- business_automation_software	SPBAS Business Automation Software 2012 has CSRF.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4665</a> <a href="#">MISC</a> <a href="#">MISC</a>

spbas-- business_automation_software	SPBAS Business Automation Software 2012 has XSS.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4664</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the search_id parameter in the search_incidents_advanced.php page is affected by XSS.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20220</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the Short Application Name and Application Name inputs in the config.php page are affected by XSS.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20222</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the Plugins input in the config.php page is affected by XSS. The XSS payload is, for example, executed on the about.php page.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20221</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the id parameter is affected by XSS on all endpoints that use this parameter, a related issue to CVE-2012-2235.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20223</a> <a href="#">MISC</a>
tbeu -- matio	A stack-based buffer over-read was discovered in ReadNextCell in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20018</a> <a href="#">MISC</a>
tbeu -- matio	A stack-based buffer over-read was discovered in Mat_VarReadNextInfo5 in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20017</a> <a href="#">MISC</a>
tbeu -- matio &#xA0;	A stack-based buffer over-read was discovered in ReadNextStructField in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20020</a> <a href="#">MISC</a>
tbeu -- matio &#xA0;	An attempted excessive memory allocation was discovered in Mat_VarRead5 in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20019</a> <a href="#">MISC</a>
toshiba -- configfree &#xA0;	Multiple stack-based buffer overflows in CFProfile.exe in Toshiba ConfigFree Utility 8.0.38 allow user-assisted attackers to execute arbitrary code.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2012-4980</a> <a href="#">BID</a> <a href="#">XE</a>
upx -- upx &#xA0;	A heap-based buffer over-read was discovered in canUnpack in p_mach.cpp in UPX 3.95 via a crafted Mach-O file.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20021</a> <a href="#">MISC</a>
winamp -- winamp &#xA0;	Winamp 5.63: Invalid Pointer Dereference leading to Arbitrary Code Execution	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2013-4695</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress Xorbin Digital Flash Clock 1.0 has XSS	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4693</a> <a href="#">MISC</a>
	WordPress before 5.3.1 allowed an			<a href="#">CVE-2019-20042</a>



wordpress -- wordpress	attacker to create a cross-site scripting attack (XSS) in well crafted links, because of an insufficient protection mechanism in wp_targeted_link_rel in wp-includes/formatting.php.	2019-12-27	<a href="#">4.3</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An XSS issue was discovered in the Laborator Neon theme 2.0 for WordPress via the data/autosuggest-remote.php q parameter.	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20141</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in the Conversador plugin 2.61 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the 'page' parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4519</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	WordPress before 5.3.1 allowed an unauthenticated user to make a post sticky through the REST API because of missing access control in wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php.	2019-12-27	<a href="#">5</a>	<a href="#">CVE-2019-20043</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in rss.class/scripts/magpie_debug.php in the WP-Planet plugin 0.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4592</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in the Easy Career Openings plugin 0.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4523</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in magpie/scripts/magpie_slashbox.php in the Ebay Feeds for WordPress plugin 1.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the rss_url parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4525</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in preview-shortcode-external.php in the Shortcode Ninja plugin 1.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the shortcode parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4550</a> <a href="#">MISC</a>
xnview -- xnview &#xA0;	Stack-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a crafted image layer in an XCF file.	2020-01-02	<a href="#">6.8</a>	<a href="#">CVE-2013-3246</a> <a href="#">MISC</a> <a href="#">MISC</a>
xnview -- xnview	Heap-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a	2020-01-	<a href="#">6.8</a>	<a href="#">CVE-2013-3247</a>

crafted RLE compressed layer in an XCF file.	02	<a href="#">MISC</a> <a href="#">MISC</a>
--	----	--

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 168924.	2019-12-30	<a href="#">3.5</a>	<a href="#">CVE-2019-4623</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- watson_studio_local	IBM Watson Studio Local 1.2.3 stores key files in the user's home directory which could be obtained by another local user. IBM X-Force ID: 161413.	2019-12-30	<a href="#">2.1</a>	<a href="#">CVE-2019-4335</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
nagios -- nagios_xi	In Nagios XI 5.6.9, XSS exists via the nocscreenapi.php host, hostgroup, or servicegroup parameter, or the schedulereport.php hour or frequency parameter. Any authenticated user can attack the admin user.	2019-12-30	<a href="#">3.5</a>	<a href="#">CVE-2019-20139</a> <a href="#">MISC</a>
tenable -- nessus	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would only potentially impact other admins. (Tenable ID 5198).	2019-12-27	<a href="#">3.5</a>	<a href="#">CVE-2016-1000028</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tenable -- nessus	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would potentially impact other admins (Tenable IDs 5218 and 5269).	2019-12-27	<a href="#">3.5</a>	<a href="#">CVE-2016-1000029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
amazon -- blink_xt2_device	Blink XT2 Sync Module firmware prior to 2.13.11 allows remote attackers to execute arbitrary commands on the device due to improperly sanitized input	2019-12-31	not yet calculated	<a href="#">CVE-2019-3984</a>

	when the device retrieves updates scripts from the internet.			<a href="#">CONFIRM</a>
angular -- angular &#xA0;	There is a vulnerability in all angular versions before 1.5.0-beta.0, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14863</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
apache -- solr	Apache Solr 5.0.0 to Apache Solr 8.3.1 are vulnerable to a Remote Code Execution through the VelocityResponseWriter. A Velocity template can be provided through Velocity templates in a configset `velocity/` directory or as a parameter. A user defined configset could contain renderable, potentially malicious, templates. Parameter provided templates are disabled by default, but can be enabled by setting `params.resource.loader.enabled` by defining a response writer with that setting set to `true`. Defining a response writer requires configuration API access. Solr 8.4 removed the params resource loader entirely, and only enables the configset-provided template rendering when the configset is `trusted` (has been uploaded by an authenticated user).	2019-12-30	not yet calculated	<a href="#">CVE-2019-17558</a> <a href="#">MISC</a>
avira -- free_antivirus	Avira Free Antivirus 15.0.1907.1514 is prone to a local privilege escalation through the execution of kernel code from a restricted user.	2019-12-31	not yet calculated	<a href="#">CVE-2019-18568</a> <a href="#">CONFIRM</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a NULL pointer dereference in AP4_Descriptor::GetTag in mp42ts when called from AP4_EsDescriptor::GetDecoderConfigDescriptor in Ap4EsDescriptor.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20092</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a NULL pointer dereference in AP4_Descriptor::GetTag in mp42ts when called from AP4_DecoderConfigDescriptor::GetDecoderSpecificInfoDescriptor in Ap4DecoderConfigDescriptor.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20091</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a use-after-free in AP4_Sample::GetOffset in Core/Ap4Sample.h when called from Ap4LinearReader.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20090</a> <a href="#">MISC</a>
	Baidu Rust SGX SDK through 1.0.8 has			<a href="#">CVE-2020-</a>

baidu_x-lab -- rust_sgx_sdk	an enclave ID race. There are non-deterministic results in which, sometimes, two global IDs are the same.	2020-01-04	not yet calculated	<a href="#">CVE-2020-5499</a> <a href="#">MISC</a>
boltwire -- boltwire	Cross-site scripting (XSS) vulnerability in BoltWire 3.5 and earlier allows remote attackers to inject arbitrary web script or HTML via the fieldnames parameter.	2020-01-02	not yet calculated	<a href="#">CVE-2013-0737</a> <a href="#">MISC</a>
bombba -- bombba	The quaker function of a smart contract implementation for BOMBBA (BOMB), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19834</a> <a href="#">MISC</a>
bssys -- rbs_bs-client	Cross-site scripting (XSS) vulnerability in bsi.dll in Bank Soft Systems (BSS) RBS BS-Client 3.17.9 allows remote attackers to inject arbitrary web script or HTML via the colorstyle parameter.	2020-01-03	not yet calculated	<a href="#">CVE-2014-4196</a> <a href="#">MISC</a>
bssys -- rbs_bs-client	Multiple cross-site scripting (XSS) vulnerabilities in bsi.dll in Bank Soft Systems (BSS) RBS BS-Client. Private Client (aka RBS BS-Client. Retail Client) 2.5, 2.4, and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) DICTIONARY, (2) FILTERIDENT, (3) FROMSCHEME, (4) FromPoint, or (5) FName_0 parameter and a valid sid parameter value.	2020-01-03	not yet calculated	<a href="#">CVE-2014-10398</a> <a href="#">MISC</a>
bulb_security -- smartphone_pentest_framework	Bulb Security Smartphone Pentest Framework (SPF) before 0.1.3 allows remote attackers to execute arbitrary commands via shell metacharacters in the ipAddressTB parameter to (1) remoteAttack.pl or (2) guessPassword.pl in frameworkgui/; the filename parameter to (3) CSAttack.pl or (4) SEAttack.pl in frameworkgui/; the phNo2Attack parameter to (5) CSAttack.pl or (6) SEAttack.pl in frameworkgui/; the (7) phNo2Attack parameter to (7) frameworkgui/SEAttack.pl; the (8) agentURLPath or (9) agentControlKey parameter to frameworkgui/attach2agents.pl; or the (10) controlKey parameter to frameworkgui/attachMobileModem.pl. NOTE: The hostingPath parameter to CSAttack.pl and SEAttack.pl vectors and the appURLPath parameter to attachMobileModem.pl vector are covered by CVE-2012-5878.	2020-01-03	not yet calculated	<a href="#">CVE-2012-5693</a> <a href="#">MISC</a>
	Bulb Security Smartphone Pentest			

bulb_security -- smartphone_pentest_framework &#xA0;	Framework (SPF) 0.1.2 through 0.1.4 allows remote attackers to execute arbitrary commands via shell metacharacters in the hostingPath parameter to (1) SEAttack.pl or (2) CSAttack.pl in frameworkgui/ or the (3) appURLPath parameter to frameworkgui/attachMobileModem.pl.	2020-01-03	not yet calculated	<a href="#">CVE-2012-5878</a> <a href="#">MISC</a> <a href="#">MISC</a>
business_alliance_financial_circle -- business_alliance_financial_circle	The UBSexToken() function of a smart contract implementation for Business Alliance Financial Circle (BAFC), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function is public (by default) and does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19830</a> <a href="#">MISC</a>
chamilo -- chamilo_lms	Chamilo LMS through 1.9.10.2 allows a link_goto.php?link_url= open redirect, a related issue to CVE-2015-5503.	2020-01-04	not yet calculated	<a href="#">CVE-2015-9540</a> <a href="#">MISC</a>
clusterlabs -- fence-agents &#xA0;	In fence-agents before 4.0.17 does not verify remote SSL certificates in the fence_cisco_ucs.py script which can potentially allow for man-in-the-middle attackers to spoof SSL servers via arbitrary SSL certificates.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0104</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
comtech -- stampede_fx-1010_devices &#xA0;	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to execute arbitrary OS commands by navigating to the Diagnostics Ping page and entering shell metacharacters in the Target IP address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.)	2020-01-02	not yet calculated	<a href="#">CVE-2020-5179</a> <a href="#">MISC</a>
craftcms -- craft_cms	In the 3.1.12 Pro version of Craft CMS, XSS has been discovered in the header insertion field when adding source code at an s/admin/entries/news/new URL.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9554</a> <a href="#">MISC</a> <a href="#">MISC</a>
cryptobond_network -- cryptobond_network	The ToOwner() function of a smart contract implementation for Cryptbond Network (CBN), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19831</a> <a href="#">MISC</a>
cumin -- cumint &#xA0;	An import error was introduced in Cumin in the code refactoring in r5310. Server certificate validation is always disabled when connecting to Aviary servers, even if the installed packages on a system support it.	2019-12-30	not yet calculated	<a href="#">CVE-2013-0264</a> <a href="#">MISC</a> <a href="#">MISC</a>



d-link -- dgs-1510_series_switches	A security vulnerability in D-Link DGS-1510-series switches with firmware 1.20.011, 1.30.007, 1.31.B003 and older that may allow a remote attacker to inject malicious scripts in the device and execute commands via browser that is configuring the unit.	2019-12-30	not yet calculated	<a href="#">CVE-2018-7859</a> <a href="#">CONFIRM</a>
d-link -- dir-859_routers &#xA0;	D-Link DIR-859 routers before v1.07b03_beta allow Unauthenticated Information Disclosure via the AUTHORIZED_GROUP=1%0a value, as demonstrated by vpnconfig.php.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20213</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-859_wi-fi_router &#xA0;	The UPnP endpoint URL /gena.cgi in the D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01 allows an Unauthenticated remote attacker to execute system commands as root, by sending a specially crafted HTTP SUBSCRIBE request to the UPnP service when connecting to the local network.	2019-12-30	not yet calculated	<a href="#">CVE-2019-17621</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
ddq -- ddq &#xA0;	The owned function of a smart contract implementation for DDQ, an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19833</a> <a href="#">MISC</a>
docker -- docker &#xA0;	An issue was found in Docker before 1.6.0. Some programs and scripts in Docker are downloaded via HTTP and then executed or used in unsafe ways.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0048</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ds_data_systems -- konakart	Cross-site request forgery (CSRF) vulnerability in the Storefront Application in DS Data Systems KonaKart before 7.3.0.0 allows remote attackers to hijack the authentication of administrators for requests that change a user email address via an unspecified GET request.	2020-01-03	not yet calculated	<a href="#">CVE-2014-5516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
easy_xml_editor -- easy_xml_editor	Easy XML Editor through v1.7.8 is affected by: XML External Entity Injection. The impact is: Arbitrary File Read and DoS by consuming resources. The component is: XML Parsing. The attack vector is: Specially crafted XML payload.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19031</a> <a href="#">MISC</a>
ecstatic -- ecstatic	ecstatic have a denial of service vulnerability. Successful exploitation could lead to crash of an application.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10775</a> <a href="#">MISC</a>

embedded_glibc -- embedded_glibc	The eglibc package before 2.14 incorrectly handled the getaddrinfo() function. An attacker could use this issue to cause a denial of service.	2019-12-31	not yet calculated	<a href="#">CVE-2013-4357</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ezxml -- ezxml	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_ent_ok() mishandles recursion, leading to stack consumption for a crafted XML file.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20198</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The ezxml_parse_* functions mishandle XML entities, leading to an infinite loop in which memory allocations occur.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20201</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_decode, while parsing crafted a XML file, performs incorrect memory handling, leading to a heap-based buffer over-read in the "normalize line endings" feature.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20200</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_decode, while parsing a crafted XML file, performs incorrect memory handling, leading to NULL pointer dereference while running strlen() on a NULL pointer.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20199</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_char_content() tries to use realloc on a block that was not allocated, leading to an invalid free and segmentation fault.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20202</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.	2020-01-03	not yet calculated	<a href="#">CVE-2019-20330</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2013-4161</a>

fhdk -- gksu-polkit &#xA0;	gksu-polkit-0.0.3-6.fc18 was reported as fixing the issue in CVE-2012-5617 but the patch was improperly applied and it did not fixed the security issue.	2019-12-31	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fiberhome -- an5506-04-f_rp_2669_devices	FiberHome an5506-04-f RP2669 devices have XSS.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9556</a> <a href="#">MISC</a> <a href="#">MISC</a>
fontforge -- fontforge	FontForge 20190801 has a use-after-free in SFD_GetFontMetaData in sfd.c.	2020-01-03	not yet calculated	<a href="#">CVE-2020-5395</a> <a href="#">MISC</a>
fontforge -- fontforge	FontForge 20190801 has a heap-based buffer overflow in the Type2NotDefSplines() function in splinesave.c.	2020-01-03	not yet calculated	<a href="#">CVE-2020-5496</a> <a href="#">MISC</a>
ftp -- ftp	An issue was discovered in rovinbhandari FTP through 2012-03-28. receive_file in file_transfer_functions.c allows remote attackers to cause a denial of service (daemon crash) via a 0xffff datalen field value.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9668</a> <a href="#">MISC</a>
fusionforge -- fusionforge	FusionForge before 5.3.2 use scripts that run under the shared Apache user, which is also used by project homepages by default. If project webpages are hosted on the same server than FusionForge, it can allow users to incorrectly access on-disk private data in FusionForge.	2020-01-02	not yet calculated	<a href="#">CVE-2014-6275</a> <a href="#">MISC</a> <a href="#">MISC</a>
generalitat_de_catalunya -- accesuniversitat.gencat.cat &#xA0;	The Java API in Generalitat de Catalunya accesuniversitat.gencat.cat 1.7.5 allows remote attackers to get personal information of all registered students via several API endpoints, given that the attacker is authenticated as a student: 1) https://accesuniversitat.gencat.cat/accesuniversitat/AppJava/api/v1/estudiants/{student_id}/ 2) https://accesuniversitat.gencat.cat/accesuniversitat/AppJava/api/v1/estudiants/?page={page}.	2019-12-31	not yet calculated	<a href="#">CVE-2019-12837</a> <a href="#">MISC</a>
getsimple_cms -- getsimple_cms &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in GetSimple CMS before 3.2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter to backup-edit.php; (2) title or (3) menu parameter to edit.php; or (4) path or (5) returnid parameter to filebrowser.php in admin/. NOTE: the path parameter in admin/upload.php vector is already covered by CVE-2012-6621.	2020-01-02	not yet calculated	<a href="#">CVE-2013-1420</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	Information Exposure.			<a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20494</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20498</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition 11.2.x through 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20496</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows SSRF.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20497</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 8.2 and later through 12.5 has Insecure Permissions.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19263</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 12.3 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19255</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 11.9 and later through 12.5 has Insecure Permissions.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19262</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 2 of 2).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19087</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 8.90 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19309</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) 11.3 through 12.4.2 allows Directory Traversal.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19088</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 6.7 and later through 12.5 allows SSRF.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19261</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-</a>



gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 1 of 2).	2020-01-03	not yet calculated	<a href="#">19086</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	An issue was discovered in GitLab Enterprise Edition 11.3.x and 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20491</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 11.3 and later through 12.5 allows an Insecure Direct Object Reference (IDOR).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19259</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 10.8 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19258</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab EE 8.14 through 12.5, 12.4.3, and 12.3.6 allows XSS in group and profile fields.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19311</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 12.2 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19256</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 9.0 and later through 12.5 allows Information Disclosure.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19310</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gonicus -- gosa	The GOsa_Filter_Settings cookie in GONICUS GOsa 2.7.5.2 is vulnerable to PHP objection injection, which allows a remote authenticated attacker to perform file deletions (in the context of the user account that runs the web server) via a crafted cookie value, because unserialize is used to restore filter settings from a cookie.	2019-12-31	not yet calculated	<a href="#">CVE-2019-14466</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5845</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use-after-free in content delivery manager in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-13765</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially	2020-01-03	not yet calculated	<a href="#">CVE-2019-5846</a> <a href="#">MISC</a>

	exploit heap corruption via a crafted HTML page.			<a href="#">MISC</a>
google -- chrome &#xA0;	Use-after-free in accessibility in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-13766</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome &#xA0;	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5844</a> <a href="#">MISC</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GetPayload in GPMF_mp4reader.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20088</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GPMF_Next in GPMF_parser.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20086</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has an heap-based buffer over-read in GPMF_SeekToSamples in GPMF_parse.c for the size calculation.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20089</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GPMF_seekToSamples in GPMF-parse.c for the "matching tags" feature.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20087</a> <a href="#">MISC</a>
goscript -- goscript &#xA0;	go.cgi in GoScript 2.0 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) query string or (2) artarchive parameter.	2019-12-31	not yet calculated	<a href="#">CVE-2004-2776</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is an invalid pointer dereference in the function GF_IPMPX_AUTH_Delete() in odf/ipmpx_code.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20170</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There are memory leaks in metx_New in isomedia/box_code_base.c and abst_Read in isomedia/box_code_adobe.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20171</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a memory leak in dinf_New() in isomedia/box_code_base.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20159</a> <a href="#">MISC</a>
gpac -- gpac	dimC_Read in isomedia/box_code_3gpp.c in GPAC 0.8.0 has a stack-based buffer overflow.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20208</a> <a href="#">MISC</a>
	Unrestricted file upload vulnerability in			

helpdez -- helpdez	includes/classes/uploadify-v2.1.4/uploadify.php in HelpDEZk 1.0.1 and earlier allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in the directory specified by the folder parameter.	2020-01-03	not yet calculated	<a href="#">CVE-2014-8337</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp --multiple_products &#xA0;	A security vulnerability has been identified in HPE SimpliVity 380 Gen 9, HPE SimpliVity 380 Gen 10, HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen 10, SimpliVity OmniCube, SimpliVity OmniStack for Cisco, SimpliVity OmniStack for Lenovo and SimpliVity OmniStack for Dell nodes. An API is used to execute a command manifest file during upgrade does not correctly prevent directory traversal and so can be used to execute manifest files in arbitrary locations on the node. The API does not require user authentication and is accessible over the management network, resulting in the potential for unauthenticated remote execution of manifest files. For all customers running HPE OmniStack version 3.7.9 and earlier. HPE recommends upgrading the OmniStack software to version 3.7.10 or later, which contains a permanent resolution. Customers and partners who can upgrade to 3.7.10 should upgrade at the earliest convenience. For all customers and partners unable to upgrade their environments to the recommended version 3.7.10, HPE has created a Temporary Workaround <a href="https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061901&amp;withFrame">https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061901&amp;withFrame</a> for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.	2020-01-03	not yet calculated	<a href="#">CVE-2019-11994</a> <a href="#">MISC</a>
	A security vulnerability has been identified in HPE SimpliVity 380 Gen 9, HPE SimpliVity 380 Gen 10, HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen 10, SimpliVity OmniCube, SimpliVity OmniStack for Cisco, SimpliVity OmniStack for Lenovo and SimpliVity OmniStack for Dell nodes. Two now deprecated APIs run as root, accept a file name path, and can be used to create or			

hp -- multiple_products &#xA0;	delete arbitrary files on the nodes. These APIs do not require user authentication and are accessible over the management network, resulting in remote availability and integrity vulnerabilities For all customers running HPE OmniStack version 3.7.9 and earlier. HPE recommends upgrading the OmniStack software to version 3.7.10 or later, which contains a permanent resolution. Customers and partners who can upgrade to 3.7.10 should upgrade at the earliest convenience. For all customers and partners unable to upgrade their environments to the recommended version 3.7.10, HPE has created a Temporary Workaround <a href="https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061675&amp;withFrame">https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061675&amp;withFrame</a> for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.	2020-01-03	not yet calculated	<a href="#">CVE-2019-11993</a> <a href="#">MISC</a>
huawei -- multiple_products &#xA0;	Some Huawei products have a buffer error vulnerability. An unauthenticated, remote attacker could send specific MPLS Echo Request messages to the target products. Due to insufficient input validation of some parameters in the messages, successful exploit may cause the device to reset.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5304</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	Mate 10 Pro;Honor V10;Honor 10;Nova 4 smartphones have a denial of service vulnerability. The system does not properly check the status of certain module during certain operations, an attacker should trick the user into installing a malicious application, successful exploit could cause reboot of the smartphone.	2020-01-03	not yet calculated	<a href="#">CVE-2020-1785</a> <a href="#">MISC</a>
huawei -- p30_smartphones &#xA0;	HUAWEI P30 smart phones with versions earlier than 10.0.0.166(C00E66R1P11) have an information leak vulnerability. An attacker could send specific command in the local area network (LAN) to exploit this vulnerability. Successful exploitation may cause information leak.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19441</a> <a href="#">MISC</a>
huawei --	USG9500 with software of V500R001C30SPC100; V500R001C30SPC200; V500R001C30SPC600; V500R001C60SPC500; V500R005C00SPC100;			<a href="#">CVE-2020-</a>

usg9500_devices &#xA0;	V500R005C00SPC200 have an improper credentials management vulnerability. The software does not properly manage certain credentials. Successful exploit could cause information disclosure or damage, and impact the confidentiality or integrity.	2020-01-03	not yet calculated	<a href="#">1871</a> <a href="#">MISC</a>
infinispan -- infinispan &#xA0;	A flaw was found in Infinispan through version 9.4.14.Final. An improper implementation of the session fixation protection in the Spring Session integration can result in incorrect session handling.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10158</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	Heap-based buffer overflow in the MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via a levels header.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3946</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	Stack-based buffer overflow in the MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via an IMAGE tag.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3944</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	The MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via a nband tag.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3945</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
it-novum -- openitcockpit	openITCOCKPIT before 3.7.1 has reflected XSS in the 404-not-found component.	2019-12-31	not yet calculated	<a href="#">CVE-2019-10227</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
joomla! -- joomla! &#xA0;	Cross-site scripting (XSS) vulnerability in the Jomres (com_jomres) component before 7.3.1 for Joomla! allows remote authenticated users with the "Business Manager" permission to inject arbitrary web script or HTML via the property_name parameter, related to editing property details.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3931</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla! &#xA0;	SQL injection vulnerability in the Jomres (com_jomres) component before 7.3.1 for Joomla! allows remote authenticated users with the "Business Manager" permission to execute arbitrary SQL commands via the id parameter in an editProfile action to administrator/index.php.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3932</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
kind-of -- kind-of	ctorName in index.js in kind-of v6.0.2 allows external user input to overwrite certain internal attributes via a conflicting name, as demonstrated by 'constructor':	2019-12-	not yet	<a href="#">CVE-2019-20149</a>



	{'name':'Symbol'}. Hence, a crafted payload can overwrite this builtin attribute to manipulate the type detection result.	30	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
knockout -- knockout	There is a vulnerability in knockout before version 3.5.0-beta, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14862</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libmysofa -- libmysofa &#xA0;	hdf/dataobject.c in libmysofa before 0.8 has an uninitialized use of memory, as demonstrated by mysofa2json.	2019-12-29	not yet calculated	<a href="#">CVE-2019-20063</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel_project -- libsixel	libsixel 1.8.4 has an integer overflow in sixel_frame_resize in frame.c.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20205</a> <a href="#">MISC</a>
libsixel_project -- libsixel	stb_image.h (aka the stb image loader) 2.23, as used in libsixel and other products, has an assertion failure in stbi__shiftsigned.	2019-12-29	not yet calculated	<a href="#">CVE-2019-20056</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An issue was discovered in libsixel 1.8.4. There is a heap-based buffer overflow in the function gif_out_code at fromgif.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20140</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.0-rc7 (as distributed in ubuntu/linux.git on kernel.ubuntu.com), mounting a crafted f2fs filesystem image and performing some operations can lead to slab-out-of-bounds read access in ttm_put_pages in drivers/gpu/drm/ttm/ttm_page_alloc.c. This is related to the vmwgfx or ttm module.	2019-12-31	not yet calculated	<a href="#">CVE-2019-19927</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	mwifiex_tm_cmd in drivers/net/wireless/marvell/mwifiex/cfg80211.c in the Linux kernel before 5.1.6 has some error-handling cases that did not free allocated hostcmd memory, aka CID-003b686ace82. This will cause a memory leak and denial of service.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20095</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel &#xA0;	In the Linux kernel before 5.1, there is a memory leak in __feat_register_sp() in net/dccp/feat.c, which may cause denial of service, aka CID-1d3ff0950e2b.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20096</a> <a href="#">MISC</a> <a href="#">MISC</a>
loaded_commerce -- loaded_commerce	The bindReplace function in the query factory in includes/classes/database.php in Loaded Commerce 7 does not properly handle : (colon) characters, which allows remote authenticated users to conduct SQL injection attacks via the First name and Last name fields in the address book.	2020-01-03	not yet calculated	<a href="#">CVE-2014-5140</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

mailstore -- mailstore_server_and_authentication_options	An issue was discovered in MailStore Server (and Service Provider Edition) 9.x through 11.x before 11.2.2. When the directory service (for synchronizing and authenticating users) is set to Generic LDAP, an attacker is able to login as an existing user with an arbitrary password on the second login attempt.	2019-12-31	not yet calculated	<a href="#">CVE-2019-10229</a> <a href="#">CONFIRM</a>
mfscripts -- yetishare	class.userpeer.php in MFScripts YetiShare 3.5.2 through 4.5.3 uses an insecure method of creating password reset hashes (based only on microtime), which allows an attacker to guess the hash and set the password within a few hours by bruteforcing.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19735</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the Secure flag on session cookies, allowing the cookie to be sent over cleartext channels.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19739</a> <a href="#">MISC</a>
mfscripts -- yetishare	translation_manage_text.ajax.php and various *_manage.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 directly insert values from the aSortDir_0 and/or sSortDir_0 parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19732</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the HttpOnly flag on session cookies, allowing the cookie to be read by script, which can potentially be used by attackers to obtain the cookie via cross-site scripting.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19736</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the SameSite flag on session cookies, allowing the cookie to be sent in cross-site requests and potentially be used in cross-site request forgery attacks.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19737</a> <a href="#">MISC</a>
mfscripts -- yetishare	log_file_viewer.php in MFScripts YetiShare 3.5.2 through 4.5.3 does not sanitize or encode the output from the IFile parameter on the page, which would allow an attacker to input HTML or execute scripts on the site, aka XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19738</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_account_move_file_in_folder.ajax.php in MFScripts YetiShare 3.5.2 directly inserts values from the filelds parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the	2019-12-30	not yet calculated	<a href="#">CVE-2019-19734</a> <a href="#">MISC</a> <a href="#">MISC</a>

	database, aka SQL Injection.			
mfscripts -- yetishare &#xA0;	_account_forgot_password.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 takes a different amount of time to return depending on whether an email address is configured for the account name provided. This can be used by an attacker to enumerate accounts by guessing email addresses.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19805</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_get_all_file_server_paths.ajax.php (aka get_all_file_server_paths.ajax.php) in MFScripts YetiShare 3.5.2 through 4.5.3 does not sanitize or encode the output from the filelds parameter on the page, which would allow an attacker to input HTML or execute scripts on the site, aka XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19733</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_account_forgot_password.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 displays a message indicating whether an email address is configured for the account name provided. This can be used by an attacker to enumerate accounts by guessing email addresses.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19806</a> <a href="#">MISC</a>
miniupnp -- ngiflib	ngiflib 0.4 has a heap-based buffer over-read in GifIndexToTrueColor in ngiflib.c.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20219</a> <a href="#">MISC</a>
mitreid_connect -- mitreid_connect	The OpenID Connect reference implementation for MITREid Connect through 1.3.3 allows XSS due to userInfoJson being included in the page unsanitized. This is related to header.tag. The issue can be exploited to execute arbitrary JavaScript.	2020-01-04	not yet calculated	<a href="#">CVE-2020-5497</a> <a href="#">MISC</a>
monitorix -- monitorix	The handle_request function in lib/HTTPServer.pm in Monitorix before 3.3.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the URI.	2019-12-31	not yet calculated	<a href="#">CVE-2013-7070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
monitorix -- monitorix	Cross-site scripting (XSS) vulnerability in the handle_request function in lib/HTTPServer.pm in Monitorix before 3.4.0 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2019-12-31	not yet calculated	<a href="#">CVE-2013-7071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mybb -- mybb	MyBB before 1.8.22 allows an open redirect on login.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20225</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In Nagios XI 5.6.9, an authenticated user is able to execute arbitrary OS commands	2019-12-	not yet	<a href="#">CVE-2019-</a>

nagios -- nagios_xi	via shell metacharacters in the id parameter to schedulereport.php, in the context of the web-server user account.	31	calculated	<a href="#">20197</a> <a href="#">MISC</a>
nasm -- netwide_assembler	In Netwide Assembler (NASM) 2.14.02, stack consumption occurs in expr# functions in asm/eval.c. This potentially affects the relationships among expr0, expr1, expr2, expr3, expr4, expr5, and expr6 (and stdscan in asm/stdscan.c). This is similar to CVE-2019-6290 and CVE-2019-6291.	2020-01-04	not yet calculated	<a href="#">CVE-2019-20334</a> <a href="#">MISC</a> <a href="#">MISC</a>
newinteltechmedia -- newinteltechmedia	The NETM() function of a smart contract implementation for NewIntelTechMedia (NETM), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19832</a> <a href="#">MISC</a>
nim -- nim	The HTTP Authentication library before 2019-12-27 for Nim has weak password hashing because the default algorithm for libsodium's crypto_pwhash_str is not used.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20138</a> <a href="#">MISC</a>
obs-server -- obs-server	obs-server before 1.7.7 allows logins by 'unconfirmed' accounts due to a bug in the REST api implementation.	2020-01-02	not yet calculated	<a href="#">CVE-2010-3782</a> <a href="#">MISC</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev27 and 7.4.x before 7.4.0-rev20 allows remote attackers to inject arbitrary web script or HTML via the body of an email. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7486</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">SECTRAK</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev26 and 7.4.x before 7.4.0-rev16 allows remote attackers to inject arbitrary web script or HTML via the publication name, which is not properly handled in an error message. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7485</a> <a href="#">OSVDB</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a> <a href="#">SECTRAK</a> <a href="#">XF</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the frontend in Open-Xchange (OX) AppSuite 6.22.3 before 6.22.3-rev5 and 6.22.4 before 6.22.4-rev12 allows remote attackers to inject arbitrary web script or HTML via the subject of an email. NOTE: the vulnerabilities related to the body of	2020-01-02	not yet calculated	<a href="#">CVE-2013-6242</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	the email and the publication name were SPLIT from this CVE ID because they affect different sets of versions.			<a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV 4.1.0. A specially crafted XML file can cause a buffer overflow, resulting in multiple heap corruptions and potential code execution. An attacker can provide a specially crafted file to trigger this vulnerability.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5063</a> <a href="#">MISC</a>
opencv -- opencv	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV, version 4.1.0. A specially crafted JSON file can cause a buffer overflow, resulting in multiple heap corruptions and potentially code execution. An attacker can provide a specially crafted file to trigger this vulnerability.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5064</a> <a href="#">MISC</a>
openlambda -- openlambda	OpenLambda 2019-09-10 allows DNS rebinding attacks against the OL server for the REST API on TCP port 5000.	2020-01-03	not yet calculated	<a href="#">CVE-2019-20329</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openldap -- openldap &#xA0;	An off-by-one error leading to a crash was discovered in openldap 2.4 when processing DNS SRV messages. If slapd was configured to use the dnssrv backend, an attacker could crash the service with crafted DNS responses.	2020-01-02	not yet calculated	<a href="#">CVE-2014-8182</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opsview -- opsview_and_opsview_core	Multiple cross-site scripting (XSS) vulnerabilities in Opsview before 4.4.1 and Opsview Core before 20130522 allow remote attackers to inject arbitrary web script or HTML.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3936</a> <a href="#">MISC</a> <a href="#">MISC</a>
opsview -- opsview_and_opsview_core	Cross-site request forgery (CSRF) vulnerability in Opsview before 4.4.1 and Opsview Core before 20130522 allows remote attackers to hijack the authentication of administrators for requests that change the administrator password via unspecified vectors.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3935</a> <a href="#">MISC</a> <a href="#">MISC</a>
outsystems -- platform	OutSystems Platform 10 through 11 allows ImageResourceDetail.aspx CSRF for content modifications and file uploads. NOTE: the product is self-hosted by the customer, even though it has a *.outsystemsenterprise.com domain name.)	2019-12-31	not yet calculated	<a href="#">CVE-2019-12273</a> <a href="#">MISC</a>





	host's qemu address space and thus increase their privileges on the host.			<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu &#xA0;	Qemu 1.1.2+dfsg to 2.1+dfsg suffers from a buffer overrun which could potentially result in arbitrary code execution on the host with the privileges of the QEMU process.	2020-01-02	not yet calculated	<a href="#">CVE-2013-4532</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
quixplorer -- quixplorer &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in QuiXplorer before 2.5.5 allow remote attackers to inject arbitrary web script or HTML via the (1) dir, (2) item, (3) order, (4) searchitem, (5) selitems[], or (6) srt parameter to index.php or (7) the QUERY_STRING to index.php.	2020-01-02	not yet calculated	<a href="#">CVE-2013-1642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible	Ansible, versions 2.9.x before 2.9.1, 2.8.x before 2.8.7 and Ansible versions 2.7.x before 2.7.15, is not respecting the flag no_log set it to True when Sumologic and Splunk callback plugins are used send tasks results events to collectors. This would discloses and collects any sensitive data.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14864</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_enterprise_application_platform &#xA0;	In JBoss EAP 6 a security domain is configured to use a cache that is shared between all applications that are in the security domain. This could allow an authenticated user in one application to access protected resources in another application without proper authorization. Although this is an intended functionality, it was not clearly documented which can mislead users into thinking that a security domain cache is isolated to a single application.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0169</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_portal &#xA0;	It was found that the implementation of the GTNSubjectCreatingInterceptor class in gatein-wsrp was not thread safe. For a specific WSRP endpoint, under high-concurrency scenarios or scenarios where SOAP messages take long to execute, it was possible for an unauthenticated remote attacker to gain privileged information if WS-Security is enabled for the WSRP Consumer, and the endpoint in question is being used by a privileged user. This affects JBoss Portal 6.2.0.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0245</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

red_hat -- openshift_enterprise &#xA0;	A CSRF issue was found in OpenShift Enterprise 1.2. The web console is using 'Basic authentication' and the REST API has no CSRF attack protection mechanism. This can allow an attacker to obtain the credential and the Authorization: header when requesting the REST API via web browser.	2019-12-30	not yet calculated	<a href="#">CVE-2013-0196</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openstack_essex_release	Within the RHOS Essex Preview (2012.2) of the OpenStack dashboard package, the file /etc/quantum/quantum.conf is world readable which exposes the admin password and token value.	2019-12-30	not yet calculated	<a href="#">CVE-2012-5476</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openstack_platform_and_essex_release &#xA0;	The file /etc/openstack-dashboard/local_settings within Red Hat OpenStack Platform 2.0 and RHOS Essex Release (python-openstack-dashboard before 2012.1.1) is world readable and exposes the secret key value.	2019-12-30	not yet calculated	<a href="#">CVE-2012-5474</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- quay	A flaw was found in the way Red Hat Quay stores robot account tokens in plain text. An attacker able to perform database queries in the Red Hat Quay database could use the tokens to read or write container images stored in the registry.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10205</a> <a href="#">CONFIRM</a>
red_hat -- satellite_6	Versions of Foreman as shipped with Red Hat Satellite 6 does not check for a correct CSRF token in the logout action. Therefore, an attacker can log out a user by having them view specially crafted content.	2020-01-02	not yet calculated	<a href="#">CVE-2014-3590</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- subscription_asset_manager	Versions of Katello as shipped with Red Hat Subscription Asset Manager 1.4 are vulnerable to a XSS via HTML in the systems name when registering.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0183</a> <a href="#">MISC</a> <a href="#">MISC</a>
ricoh -- marcomcentral &#xA0;	A directory traversal and local file inclusion vulnerability in FPProducerInternetServer.exe in Ricoh MarcomCentral, formerly PTI Marketing, FusionPro VDP before 10.0 allows a remote attacker to list or enumerate sensitive contents of files. Furthermore, this could allow for privilege escalation by dumping the local machine's SAM and SYSTEM database files, and possibly remote code execution.	2019-12-31	not yet calculated	<a href="#">CVE-2019-7751</a> <a href="#">MISC</a> <a href="#">MISC</a>
ros -- ros &#xA0;	An issue was discovered in the ROS communications-related packages (aka ros_comm or ros-melodic-ros-comm) through 1.14.3. parseOptions() in tools/rosbag/src/record.cpp has an	2019-12-30	not yet calculated	<a href="#">CVE-2019-13445</a> <a href="#">MISC</a>

	integer overflow when a crafted split option can be entered on the command line.			<a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ros -- ros &#xA0;	An issue was discovered in the ROS communications-related packages (aka ros_comm or ros-melodic-ros-comm) through 1.14.3. ROS_ASSERT_MSG only works when ROS_ASSERT_ENABLED is defined. This leads to a problem in the remove() function in clients/roscpp/src/libros/spinner.cpp. When ROS_ASSERT_ENABLED is not defined, the iterator loop will run out of the scope of the array, and cause denial of service for other components (that depend on the communication-related functions of this package).	2019-12-30	not yet calculated	<a href="#">CVE-2019-13465</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
rsa -- authentication_manager	RSA Authentication Manager versions prior to 8.4 P7 contain an XML Entity Injection Vulnerability. A remote authenticated malicious user could potentially exploit this vulnerability to cause information disclosure of local system files by supplying specially crafted XML message.	2020-01-03	not yet calculated	<a href="#">CVE-2019-3768</a> <a href="#">MISC</a>
samba -- samba &#xA0;	Multiple race conditions in the (1) mount.cifs and (2) umount.cifs programs in Samba 3.6 allow local users to cause a denial of service (mounting outage) via a SIGKILL signal during a time window when the /etc/mtab~ file exists.	2019-12-31	not yet calculated	<a href="#">CVE-2011-3585</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
serenityos -- serenityos &#xA0;	Kernel/VM/MemoryManager.cpp in SerenityOS before 2019-12-30 does not reject syscalls with pointers into the kernel-only virtual address space, which allows local users to gain privileges by overwriting a return address that was found on the kernel stack.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20172</a> <a href="#">MISC</a> <a href="#">MISC</a>
shaarli -- shaarli &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Shaarli allow remote attackers to inject arbitrary web script or HTML via the URL to the (1) showRSS, (2) showATOM, or (3) showDailyRSS function; a (4) file name to the importFile function; or (5) vectors related to bookmarks.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7351</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
sonicwall -- global_management_system	A vulnerability in GMS allow unauthenticated user to SQL injection in Webservice module. This vulnerability affected GMS versions GMS 8.4, 8.5, 8.6,	2019-12-31	not yet calculated	<a href="#">CVE-2019-7478</a> <a href="#">CONFIRM</a>

	8.7, 9.0 and 9.1.			
sonicwall -- sonicos &#xA0;	A vulnerability in SonicOS allow authenticated read-only admin can elevate permissions to configuration mode. This vulnerability affected SonicOS Gen 5 version 5.9.1.12-4o and earlier, Gen 6 version 6.2.7.4-32n, 6.5.1.4-4n, 6.5.2.3-4n, 6.5.3.3-3n, 6.2.7.10-3n, 6.4.1.0-3n, 6.5.3.3-3n, 6.5.1.9-4n and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V).	2019-12-31	not yet calculated	<a href="#">CVE-2019-7479</a> <a href="#">CONFIRM</a>
sqlite -- sqlite &#xA0;	ext/misc/zipfile.c in SQLite 3.30.1 mishandles certain uses of INSERT INTO in situations involving embedded '' characters in filenames, leading to a memory-management error that can be detected by (for example) valgrind.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19959</a> <a href="#">MISC</a> <a href="#">MISC</a>
supermicro -- x9_and_x8_generation &#xA0;	Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before SMT_X9_317 and firmware for Supermicro X8 generation motherboards before SMT X8 312 contain hardcoded private encryption keys for the (1) Lighttpd web server SSL interface and the (2) Dropbear SSH daemon.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3619</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
supermicro -- x9_and_x8_generation &#xA0;	Hardcoded WSMAN credentials in Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before 3.15 (SMT_X9_315) and firmware for Supermicro X8 generation motherboards before SMT X8 312.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3620</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
sylius -- sylius &#xA0;	An issue was discovered in Sylius products. Missing input sanitization in sylius/sylius 1.0.x through 1.0.18, 1.1.x through 1.1.17, 1.2.x through 1.2.16, 1.3.x through 1.3.11, and 1.4.x through 1.4.3 and sylius/grid 1.0.x through 1.0.18, 1.1.x through 1.1.18, 1.2.x through 1.2.17, 1.3.x through 1.3.12, 1.4.x through 1.4.4, and 1.5.0 allows an attacker (an admin in the sylius/sylius case) to perform XSS by injecting malicious code into a field displayed in a grid with the "string" field type. The contents are an object, with malicious code returned by the toString() method of that object.	2019-12-31	not yet calculated	<a href="#">CVE-2019-12186</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2013-4752</a>



symfony -- symfony &#xA0;	Symfony 2.0.X before 2.0.24, 2.1.X before 2.1.12, 2.2.X before 2.2.5, and 2.3.X before 2.3.3 have an issue in the HttpFoundation component. The Host header can be manipulated by an attacker when the framework is generating an absolute URL. A remote attacker could exploit this vulnerability to inject malicious content into the Web application page and conduct various attacks.	2020-01-02	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
telos -- automated_message_handling_system	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the LDAP cbURL parameter of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9538</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uploaditem.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9537</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Information Exposure vulnerability in itemlookup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9541</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in itemlookup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9542</a> <a href="#">CERT-VN</a>
	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in prefs.asp of			

telos -- automated_message_handling_system &#xA0;	Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9540</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ModalWindowPopup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9539</a> <a href="#">CERT-VN</a>
textproc/isearch -- textproc/isearch &#xA0;	The isearch package (textproc/isearch) before 1.47.01nb1 uses the tempnam() function to create insecure temporary files into a publicly-writable area (/tmp).	2019-12-30	not yet calculated	<a href="#">CVE-2012-5663</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tigervnc -- tigervnc &#xA0;	Multiple heap-based buffer overflows in the ZRLE_DECODE function in common/rfb/zrleDecode.h in TigerVNC before 1.3.1, when NDEBUB is enabled, allow remote VNC servers to cause a denial of service (vncviewer crash) and possibly execute arbitrary code via vectors related to screen image rendering.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0011</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tiny_file_manager -- tiny_file_manager &#xA0;	In Tiny File Manager before 2.3.9, there is a remote code execution via Upload from URL and Edit/Rename files. Only authenticated users are impacted.	2019-12-30	not yet calculated	<a href="#">CVE-2019-16790</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tinywall -- tinywall	An attacker who has already compromised the local system could use TinyWall Controller to gain additional privileges by attaching a debugger to the running process and modifying the code in memory. Vulnerability fixed in version 2.1.13.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19470</a> <a href="#">MISC</a>
tvf -- nvms-1000_devices	TVF NVMS-1000 devices allow GET /.. Directory Traversal	2019-12-30	not yet calculated	<a href="#">CVE-2019-20085</a> <a href="#">MISC</a>
unity_technologies -- editor &#xA0;	The com.unity3d.kharma protocol handler in Unity Editor 2018.3 allows remote attackers to execute arbitrary code.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9197</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vim -- vim	The autocmd feature in window.c in Vim	2019-12-	not yet	<a href="#">CVE-2019-20079</a>

&#xA0;	before 8.1.2136 accesses freed memory.	30	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
visual_mining -- netcharts_server &#xA0;	Unrestricted file upload vulnerability in Visual Mining NetCharts Server allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via unspecified vectors.	2020-01-03	not yet calculated	<a href="#">CVE-2014-8516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	Cross-site Scripting (XSS) in the spreadshirt-rss-3d-cube-flash-gallery plugin 2014 for WordPress allows remote attackers to execute arbitrary web script or HTML via unspecified parameters.	2020-01-02	not yet calculated	<a href="#">CVE-2014-4553</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	The Postie plugin 1.9.40 for WordPress allows XSS, as demonstrated by a certain payload with jaVaScRipt:/* at the beginning and a crafted SVG element.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20204</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	The Authorized Addresses feature in the Postie plugin 1.9.40 for WordPress allows remote attackers to publish posts by spoofing the From information of an email message.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20203</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
xmlblueprint -- xmlblueprint	XMLBlueprint through 16.191112 is affected by XML External Entity Injection. The impact is: Arbitrary File Read when an XML File is validated. The component is: XML Validate function. The attack vector is: Specially crafted XML payload.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19032</a> <a href="#">MISC</a>
xnview -- xnview	xnview.exe in XnView before 2.13 does not properly handle RLE strip lengths during processing of RGB files, which allows remote attackers to execute arbitrary code via the RLE strip size field in a RGB file, which leads to an unexpected sign extension error and a heap-based buffer overflow.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3939</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
xnview -- xnview	Heap-based buffer overflow in xnview.exe in XnView before 2.13 allows remote attackers to execute arbitrary code via the biBitCount field in a BMP file.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3937</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
xnview -- xnview &#xA0;	Xjp2.dll in XnView before 2.13 allows remote attackers to execute arbitrary code via (1) the Csiz parameter in a SIZ marker, which triggers an incorrect memory allocation, or (2) the lqcd field in a QCD marker in a crafted JPEG2000 file, which leads to a heap-based buffer	2020-01-02	not yet calculated	<a href="#">CVE-2013-3941</a> <a href="#">MISC</a> <a href="#">MISC</a>

	overflow.			
yandex -- clickhouse	In all versions of ClickHouse before 19.14.3, an attacker having write access to ZooKeeper and who is able to run a custom server available from the network where ClickHouse runs, can create a custom-built malicious server that will act as a ClickHouse replica and register it in ZooKeeper. When another replica will fetch data part from the malicious replica, it can force clickhouse-server to write to arbitrary path on filesystem.	2019-12-30	not yet calculated	<a href="#">CVE-2019-15024</a> <a href="#">MISC</a>
zend_framework -- zend_framework	Multiple cross-site scripting (XSS) vulnerabilities in Zend Framework 2.0.x before 2.0.1 allow remote attackers to inject arbitrary web script or HTML via unspecified input to (1) Debug, (2) Feed\PubSubHubbub, (3) Log\Formatter\Xml, (4) Tag\CloudDecorator, (5) Uri, (6) View\Helper\HeadStyle, (7) View\Helper\Navigation\Sitemap, or (8) View\Helper\Placeholder\Container\AbstractStandalone, related to Escaper.	2020-01-03	not yet calculated	<a href="#">CVE-2012-4451</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	SQL injection vulnerability in Zenphoto before 1.4.9 allow remote administrators to execute arbitrary SQL commands.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Cross-site request forgery (CSRF) vulnerability in admin.php in Zenphoto before 1.4.9 allows remote attackers to hijack the authentication of admin users for requests that may cause a denial of service (resource consumption).	2019-12-31	not yet calculated	<a href="#">CVE-2015-5595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Incomplete blacklist in sanitize_string in Zenphoto before 1.4.9 allows remote attackers to conduct cross-site scripting (XSS) attacks.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5592</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	The sanitize_string function in Zenphoto before 1.4.9 does not properly sanitize HTML tags, which allows remote attackers to perform a cross-site scripting (XSS) attack by wrapping a payload in "<<script></script>script>payload<script></script></script>", or in an image tag, with the payload as the onerror event.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in Zoho ManageEngine ADSelfService Plus 5.6			

zoho_manageengine - - adselfservice_plus	Build 5607. An exposed service allows an unauthenticated person to retrieve internal information from the system and modify the product installation.	2019-12-31	not yet calculated	<a href="#">CVE-2019-7162</a> <a href="#">MISC</a>
---	---	------------	--------------------	---

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to edigiovanna@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870





**From:** [US-CERT](#)  
**To:** [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of December 30, 2019  
**Date:** Monday, January 06, 2020 6:42:50 PM



National Cyber Awareness System:

## [Vulnerability Summary for the Week of December 30, 2019](#)

01/06/2020 08:41 AM EST

Original release date: January 6, 2020

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
citrix -- application_delivery_controller	An issue was discovered in Citrix Application Delivery Controller (ADC) and Gateway 10.5 and 11.0. They allow Directory Traversal.	2019-12-27	7.5	<a href="#">CVE-2019-19781</a> <a href="#">CONFIRM</a>
freeciv -- freeciv	A denial of service flaw was found in the way the server component of Freeciv before 2.3.4 processed certain packets. A remote attacker could send a specially-crafted packet that, when processed would lead to memory exhaustion or excessive CPU consumption.	2019-12-30	7.8	<a href="#">CVE-2012-5645</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
magnolia_international -- magnolia_cms	Magnolia CMS before 4.5.9 has multiple access bypass vulnerabilities	2019-12-27	7.5	<a href="#">CVE-2013-4621</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2013-</a>

open_dynamics -- collabtive	Collabtive 1.0 has incorrect access control	2019-12-27	<a href="#">7.5</a>	<a href="#">5027 MISC</a>
php-shellcommand -- php-shellcommand	php-shellcommand versions before 1.6.1 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-30	<a href="#">10</a>	<a href="#">CVE-2019-10774 MISC</a>
senkas -- kolibri	Buffer overflow in Senkas Kolibri 2.0 allows remote attackers to execute arbitrary code via a long URI in a POST request.	2019-12-27	<a href="#">7.5</a>	<a href="#">CVE-2014-5289 MISC BID XE</a>
sqlite -- sqlite	selectExpander in select.c in SQLite 3.30.1 proceeds with WITH stack unwinding even after a parsing error.	2020-01-02	<a href="#">7.5</a>	<a href="#">CVE-2019-20218 MISC</a>
wordpress -- wordpress	wp_kses_bad_protocol in wp-includes/kses.php in WordPress before 5.3.1 mishandles the HTML5 colon named entity, allowing attackers to bypass input sanitization, as demonstrated by the javascript&colon; substring.	2019-12-27	<a href="#">7.5</a>	<a href="#">CVE-2019-20041 MISC MISC</a>
yandex -- clickhouse	In all versions of ClickHouse before 19.14, an OOB read, OOB write and integer underflow in decompression algorithms can be used to achieve RCE or DoS via native protocol.	2019-12-30	<a href="#">7.5</a>	<a href="#">CVE-2019-16535 MISC</a>

[Back to top](#)

&#xA0;

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bolt -- bolt	Bolt 3.6.4 has XSS via the slug, teaser, or title parameter to editcontent/pages, a related issue to CVE-2017-11128 and CVE-2018-19933.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-9553 MISC MISC</a>
genjxcms -- genjxcms	GeniXCMS 1.1.5 has XSS via the dbuser or dbhost parameter during step 1 of installation.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2018-14476 MISC MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_SPLINE_private in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20009 MISC MISC MISC</a>
gnu -- libredwg	An issue was discovered in GNU	2019-12-		<a href="#">CVE-2019-20010</a>

&#xA0;	LibreDWG 0.92. There is a use-after-free in resolve_objectref_vector in decode.c.	27	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. There is a heap-based buffer over-read in decode_R13_R2000 in decode.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20011</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. There is a double-free in dwg_free in free.c.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2019-20014</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_HATCH_private in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20012</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG before 0.93. Crafted input will lead to an attempted excessive memory allocation in decode_3dsolid in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20013</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg &#xA0;	An issue was discovered in GNU LibreDWG 0.92. Crafted input will lead to an attempted excessive memory allocation in dwg_decode_LWPOLYLINE_private in dwg.spec.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20015</a> <a href="#">MISC</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function senc_Parse() in isomedia/box_code_drm.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20167</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_odf_avc_cfg_write_bs() in odf/descriptors.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20163</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the function trak_Read() in isomedia/box_code_base.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20169</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a use-after-free in the function gf_isom_box_dump_ex() in isomedia/box_funcs.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20168</a> <a href="#">MISC</a>
	An issue was discovered in GPAC			

gpac -- gpac	version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_dump() in isomedia/box_dump.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20166</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function ReadGF_IPMPX_WatermarkingInit() in odf/ipmpx_code.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20161</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a stack-based buffer overflow in the function av1_parse_tile_group() in media_tools/av_parsers.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20160</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is heap-based buffer overflow in the function gf_isom_box_parse_ex() in isomedia/box_funcs.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20162</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function gf_isom_box_del() in isomedia/box_funcs.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20164</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a NULL pointer dereference in the function ilst_item_Read() in isomedia/box_code_apple.c.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-20165</a> <a href="#">MISC</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.1 allows overly permissive cross-origin resource sharing which could allow an attacker to transfer private information. An attacker could exploit this vulnerability to access content that should be restricted. IBM X-Force ID: 161422.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-4343</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- mq	IBM MQ 9.1.0.0, 9.1.0.1, 9.1.0.2, 9.1.0.3, 9.1.1, 9.1.2, and 9.1.3 is vulnerable to a denial of service attack that would allow an authenticated user to reset client connections due to an error within the Data Conversion routine. IBM X-Force ID: 170966.	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-4655</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- watson_studio_local	IBM Watson Studio Local 1.2.3 could disclose sensitive information over the network that an attacker could use in	2019-12-30	<a href="#">5</a>	<a href="#">CVE-2018-1682</a> <a href="#">XF</a>

&#xA0;	further attacks against the system. IBM X-Force ID: 145238.			<a href="#">CONFIRM</a>
joomla! -- joomla! &#xA0;	Xorbin Analog Flash Clock 1.0 extension for Joomla has XSS	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4692</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel_project -- libsixel	A memory leak was discovered in image_buffer_resize in fromsixel.c in libsixel 1.8.4.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20023</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An invalid memory address dereference was discovered in load_pnm in frompnm.c in libsixel before 1.8.3.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20022</a> <a href="#">MISC</a>
libsixel_project -- libsixel &#xA0;	An issue was discovered in libsixel 1.8.4. There is a heap-based buffer overflow in the function gif_init_frame at fromgif.c.	2019-12-30	<a href="#">6.8</a>	<a href="#">CVE-2019-20094</a> <a href="#">MISC</a>
libsixel_project -- libsixel &#xA0;	A heap-based buffer overflow was discovered in image_buffer_resize in fromsixel.c in libsixel before 1.8.4.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20024</a> <a href="#">MISC</a>
livefyre -- livecomments	Cross-site scripting (XSS) vulnerability in Livefyre LiveComments 3.0 allows remote attackers to inject arbitrary web script or HTML via the name of an uploaded picture.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-6420</a> <a href="#">MISC</a> <a href="#">XE</a>
luquidpixels -- liquifire_os	LuquidPixels LiquiFire OS 4.8.0 allows SSRF via the call%3Durl substring followed by a URL in square brackets.	2019-12-29	<a href="#">6.4</a>	<a href="#">CVE-2019-20055</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi hostname parameter (Dynamic DNS Configuration).	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20072</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the form2Ddns.cgi username parameter (DynDns settings of the Dynamic DNS Configuration).	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20076</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices	On Netis DL4323 devices, XSS exists via the urlFQDN parameter to form2url.cgi (aka the Keyword field of the URL Blocking Configuration).	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, pingrtt_v6.html has XSS (Ping6 Diagnostic).	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20075</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, any user role can view sensitive information, such as a user password or the FTP password, via	2019-12-30	<a href="#">4</a>	<a href="#">CVE-2019-20074</a> <a href="#">MISC</a>



	the form2saveConf.cgi page.			<a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, CSRF exists via form2logaction.cgi to delete all logs.	2019-12-30	<a href="#">5.8</a>	<a href="#">CVE-2019-20071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
netis -- dl4323_devices &#xA0;	On Netis DL4323 devices, XSS exists via the form2userconfig.cgi username parameter (User Account Configuration).	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20073</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /search.htm searchtext parameter. NOTE: This product is discontinued.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-9207</a> <a href="#">MISC</a> <a href="#">MISC</a>
paessler -- prtg_network_monitor	PRTG Network Monitor v7.1.3.3378 allows XSS via the /public/login.htm errmsg or loginurl parameter. NOTE: This product is discontinued.	2019-12-31	<a href="#">4.3</a>	<a href="#">CVE-2019-9206</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5312</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/TiffDecode.c in Pillow before 6.2.2 has a TIFF decoding integer overflow, related to realloc.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5310</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/FliDecode.c in Pillow before 6.2.2 has an FLI buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5313</a> <a href="#">MISC</a> <a href="#">MISC</a>
pillow -- pillow &#xA0;	libImaging/SgiRleDecode.c in Pillow before 6.2.2 has an SGI buffer overflow.	2020-01-03	<a href="#">6.8</a>	<a href="#">CVE-2020-5311</a> <a href="#">MISC</a> <a href="#">MISC</a>
proxyman -- proxyman_for_macos	com.proxyman.NSProxy.HelperTool in Privileged Helper Tool in Proxyman for macOS 1.11.0 and earlier allows an attacker to change the System Proxy and redirect all traffic to an attacker-controlled computer, enabling MITM attacks.	2019-12-29	<a href="#">4.3</a>	<a href="#">CVE-2019-20057</a> <a href="#">MISC</a>
sencha_labs -- connect	Sencha Labs Connect has XSS with connect.methodOverride()	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4691</a> <a href="#">MISC</a>
spbas -- business_automation_software	SPBAS Business Automation Software 2012 has CSRF.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4665</a> <a href="#">MISC</a> <a href="#">MISC</a>
spbas--	SPBAS Business Automation Software	2019-12-		<a href="#">CVE-2013-4664</a>

business_automation_software	2012 has XSS.	27	<a href="#">4.3</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the search_id parameter in the search_incidents_advanced.php page is affected by XSS.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20220</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the Short Application Name and Application Name inputs in the config.php page are affected by XSS.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20222</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the Plugins input in the config.php page is affected by XSS. The XSS payload is, for example, executed on the about.php page.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20221</a> <a href="#">MISC</a>
support_incident_tracker -- support_incident_tracker	In Support Incident Tracker (SiT!) 3.67, the id parameter is affected by XSS on all endpoints that use this parameter, a related issue to CVE-2012-2235.	2020-01-02	<a href="#">4.3</a>	<a href="#">CVE-2019-20223</a> <a href="#">MISC</a>
tbeu -- matio	A stack-based buffer over-read was discovered in ReadNextCell in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20018</a> <a href="#">MISC</a>
tbeu -- matio	A stack-based buffer over-read was discovered in Mat_VarReadNextInfo5 in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20017</a> <a href="#">MISC</a>
tbeu -- matio &#xA0;	A stack-based buffer over-read was discovered in ReadNextStructField in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20020</a> <a href="#">MISC</a>
tbeu -- matio &#xA0;	An attempted excessive memory allocation was discovered in Mat_VarRead5 in mat5.c in matio 1.5.17.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20019</a> <a href="#">MISC</a>
toshiba -- configfree &#xA0;	Multiple stack-based buffer overflows in CFProfile.exe in Toshiba ConfigFree Utility 8.0.38 allow user-assisted attackers to execute arbitrary code.	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2012-4980</a> <a href="#">BID</a> <a href="#">XE</a>
upx -- upx &#xA0;	A heap-based buffer over-read was discovered in canUnpack in p_mach.cpp in UPX 3.95 via a crafted Mach-O file.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2019-20021</a> <a href="#">MISC</a>
winamp -- winamp &#xA0;	Winamp 5.63: Invalid Pointer Dereference leading to Arbitrary Code Execution	2019-12-27	<a href="#">6.8</a>	<a href="#">CVE-2013-4695</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress Xorbin Digital Flash Clock 1.0 has XSS	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2013-4693</a> <a href="#">MISC</a>
wordpress --	WordPress before 5.3.1 allowed an attacker to create a cross-site scripting attack (XSS) in well crafted links, because	2019-12-	<a href="#">4.3</a>	<a href="#">CVE-2019-20042</a> <a href="#">MISC</a> <a href="#">MISC</a>

wordpress	of an insufficient protection mechanism in wp_targeted_link_rel in wp-includes/formatting.php.	27		<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An XSS issue was discovered in the Laborator Neon theme 2.0 for WordPress via the data/autosuggest-remote.php q parameter.	2019-12-30	<a href="#">4.3</a>	<a href="#">CVE-2019-20141</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in the Conversador plugin 2.61 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the 'page' parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4519</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	WordPress before 5.3.1 allowed an unauthenticated user to make a post sticky through the REST API because of missing access control in wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php.	2019-12-27	<a href="#">5</a>	<a href="#">CVE-2019-20043</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in rss.class/scripts/magpie_debug.php in the WP-Planet plugin 0.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4592</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in the Easy Career Openings plugin 0.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4523</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in magpie/scripts/magpie_slashbox.php in the Ebay Feeds for WordPress plugin 1.1 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the rss_url parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4525</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress &#xA0;	Cross-site scripting (XSS) vulnerability in preview-shortcode-external.php in the Shortcode Ninja plugin 1.4 and earlier for WordPress allows remote attackers to inject arbitrary web script or HTML via the shortcode parameter.	2019-12-27	<a href="#">4.3</a>	<a href="#">CVE-2014-4550</a> <a href="#">MISC</a>
xnview -- xnview &#xA0;	Stack-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a crafted image layer in an XCF file.	2020-01-02	<a href="#">6.8</a>	<a href="#">CVE-2013-3246</a> <a href="#">MISC</a> <a href="#">MISC</a>
xnview -- xnview &#xA0;	Heap-based buffer overflow in xnview.exe in XnView before 2.03 allows remote attackers to execute arbitrary code via a crafted RLE compressed layer in an XCF file.	2020-01-02	<a href="#">6.8</a>	<a href="#">CVE-2013-3247</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

&#xA0;

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cognos_analytics &#xA0;	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 168924.	2019-12-30	<a href="#">3.5</a>	<a href="#">CVE-2019-4623</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- watson_studio_local &#xA0;	IBM Watson Studio Local 1.2.3 stores key files in the user's home directory which could be obtained by another local user. IBM X-Force ID: 161413.	2019-12-30	<a href="#">2.1</a>	<a href="#">CVE-2019-4335</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
nagios -- nagios_xi	In Nagios XI 5.6.9, XSS exists via the nocscreenapi.php host, hostgroup, or servicegroup parameter, or the schedulereport.php hour or frequency parameter. Any authenticated user can attack the admin user.	2019-12-30	<a href="#">3.5</a>	<a href="#">CVE-2019-20139</a> <a href="#">MISC</a>
tenable -- nessus &#xA0;	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would only potentially impact other admins. (Tenable ID 5198).	2019-12-27	<a href="#">3.5</a>	<a href="#">CVE-2016-1000028</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tenable -- nessus &#xA0;	Tenable Nessus before 6.8 has a stored XSS issue that requires admin-level authentication to the Nessus UI, and would potentially impact other admins (Tenable IDs 5218 and 5269).	2019-12-27	<a href="#">3.5</a>	<a href="#">CVE-2016-1000029</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

&#xA0;

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
amazon -- blink_xt2_device	Blink XT2 Sync Module firmware prior to 2.13.11 allows remote attackers to execute arbitrary commands on the device due to improperly sanitized input when the device retrieves updates scripts from the internet.	2019-12-31	not yet calculated	<a href="#">CVE-2019-3984</a> <a href="#">CONFIRM</a>

angular -- angular &#xA0;	There is a vulnerability in all angular versions before 1.5.0-beta.0, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14863</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
apache -- solr	Apache Solr 5.0.0 to Apache Solr 8.3.1 are vulnerable to a Remote Code Execution through the VelocityResponseWriter. A Velocity template can be provided through Velocity templates in a configset `velocity/` directory or as a parameter. A user defined configset could contain renderable, potentially malicious, templates. Parameter provided templates are disabled by default, but can be enabled by setting `params.resource.loader.enabled` by defining a response writer with that setting set to `true`. Defining a response writer requires configuration API access. Solr 8.4 removed the params resource loader entirely, and only enables the configset-provided template rendering when the configset is `trusted` (has been uploaded by an authenticated user).	2019-12-30	not yet calculated	<a href="#">CVE-2019-17558</a> <a href="#">MISC</a>
avira -- free_antivirus	Avira Free Antivirus 15.0.1907.1514 is prone to a local privilege escalation through the execution of kernel code from a restricted user.	2019-12-31	not yet calculated	<a href="#">CVE-2019-18568</a> <a href="#">CONFIRM</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a NULL pointer dereference in AP4_Descriptor::GetTag in mp42ts when called from AP4_EsDescriptor::GetDecoderConfigDescriptor in Ap4EsDescriptor.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20092</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a NULL pointer dereference in AP4_Descriptor::GetTag in mp42ts when called from AP4_DecoderConfigDescriptor::GetDecoderSpecificInfoDescriptor in Ap4DecoderConfigDescriptor.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20091</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a use-after-free in AP4_Sample::GetOffset in Core/Ap4Sample.h when called from Ap4LinearReader.cpp.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20090</a> <a href="#">MISC</a>
baidu_x-lab -- rust_sgx_sdk	Baidu Rust SGX SDK through 1.0.8 has an enclave ID race. There are non-deterministic results in which, sometimes, two global IDs are the same.	2020-01-04	not yet calculated	<a href="#">CVE-2020-5499</a> <a href="#">MISC</a>



boltwire -- boltwire &#xA0;	Cross-site scripting (XSS) vulnerability in BoltWire 3.5 and earlier allows remote attackers to inject arbitrary web script or HTML via the fieldnames parameter.	2020-01-02	not yet calculated	<a href="#">CVE-2013-0737</a> <a href="#">MISC</a>
bombba -- bombba	The quaker function of a smart contract implementation for BOMBBA (BOMB), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19834</a> <a href="#">MISC</a>
bssys -- rbs_bs-client	Cross-site scripting (XSS) vulnerability in bsi.dll in Bank Soft Systems (BSS) RBS BS-Client 3.17.9 allows remote attackers to inject arbitrary web script or HTML via the colorstyle parameter.	2020-01-03	not yet calculated	<a href="#">CVE-2014-4196</a> <a href="#">MISC</a>
bssys -- rbs_bs-client &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in bsi.dll in Bank Soft Systems (BSS) RBS BS-Client. Private Client (aka RBS BS-Client. Retail Client) 2.5, 2.4, and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) DICTIONARY, (2) FILTERIDENT, (3) FROMSCHEME, (4) FromPoint, or (5) FName_0 parameter and a valid sid parameter value.	2020-01-03	not yet calculated	<a href="#">CVE-2014-10398</a> <a href="#">MISC</a>
bulb_security -- smartphone_pentest_framework &#xA0;	Bulb Security Smartphone Pentest Framework (SPF) before 0.1.3 allows remote attackers to execute arbitrary commands via shell metacharacters in the ipAddressTB parameter to (1) remoteAttack.pl or (2) guessPassword.pl in frameworkgui/; the filename parameter to (3) CSAttack.pl or (4) SEAttack.pl in frameworkgui/; the phNo2Attack parameter to (5) CSAttack.pl or (6) SEAttack.pl in frameworkgui/; the (7) platformDD2 parameter to frameworkgui/SEAttack.pl; the (8) agentURLPath or (9) agentControlKey parameter to frameworkgui/attach2agents.pl; or the (10) controlKey parameter to frameworkgui/attachMobileModem.pl. NOTE: The hostingPath parameter to CSAttack.pl and SEAttack.pl vectors and the appURLPath parameter to attachMobileModem.pl vector are covered by CVE-2012-5878.	2020-01-03	not yet calculated	<a href="#">CVE-2012-5693</a> <a href="#">MISC</a>
bulb_security --	Bulb Security Smartphone Pentest Framework (SPF) 0.1.2 through 0.1.4 allows remote attackers to execute arbitrary commands via shell	2020-01-	not yet	<a href="#">CVE-2012-5878</a>

smartphone_pentest_framework -- metacharacters in the hostingPath parameter to (1) SEAttack.pl or (2) CSAttack.pl in frameworkgui/ or the (3) appURLPath parameter to frameworkgui/attachMobileModem.pl.	03	calculated	<a href="#">MISC</a> <a href="#">MISC</a>	
business_alliance_financial_circle -- business_alliance_financial_circle	The UBSexToken() function of a smart contract implementation for Business Alliance Financial Circle (BAFC), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function is public (by default) and does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19830</a> <a href="#">MISC</a>
chamilo -- chamilo_lms	Chamilo LMS through 1.9.10.2 allows a link_goto.php?link_url= open redirect, a related issue to CVE-2015-5503.	2020-01-04	not yet calculated	<a href="#">CVE-2015-9540</a> <a href="#">MISC</a>
clusterlabs -- fence-agents	In fence-agents before 4.0.17 does not verify remote SSL certificates in the fence_cisco_ucs.py script which can potentially allow for man-in-the-middle attackers to spoof SSL servers via arbitrary SSL certificates.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0104</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
comtech -- stampede_fx-1010_devices	Comtech Stampede FX-1010 7.4.3 devices allow remote authenticated administrators to execute arbitrary OS commands by navigating to the Diagnostics Ping page and entering shell metacharacters in the Target IP address field. (In some cases, authentication can be achieved with the comtech password for the comtech account.)	2020-01-02	not yet calculated	<a href="#">CVE-2020-5179</a> <a href="#">MISC</a>
craftcms -- craft_cms	In the 3.1.12 Pro version of Craft CMS, XSS has been discovered in the header insertion field when adding source code at an s/admin/entries/news/new URI.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9554</a> <a href="#">MISC</a> <a href="#">MISC</a>
cryptobond_network -- cryptobond_network	The ToOwner() function of a smart contract implementation for Cryptbond Network (CBN), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19831</a> <a href="#">MISC</a>
cumin -- cumin	An import error was introduced in Cumin in the code refactoring in r5310. Server certificate validation is always disabled when connecting to Aviary servers, even if the installed packages on a system support it.	2019-12-30	not yet calculated	<a href="#">CVE-2013-0264</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dgs-	A security vulnerability in D-Link DGS-1510-series switches with firmware 1.20.011, 1.30.007, 1.31.B003 and older	2019-12-	not yet	<a href="#">CVE-2018-</a>

1510_series_switches	that may allow a remote attacker to inject malicious scripts in the device and execute commands via browser that is configuring the unit.	30	calculated	<a href="#">7859</a> <a href="#">CONFIRM</a>
d-link -- dir-859_routers	D-Link DIR-859 routers before v1.07b03_beta allow Unauthenticated Information Disclosure via the AUTHORIZED_GROUP=1%0a value, as demonstrated by vpnconfig.php.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20213</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-859_wi-fi_router	The UPnP endpoint URL /gena.cgi in the D-Link DIR-859 Wi-Fi router 1.05 and 1.06B01 Beta01 allows an Unauthenticated remote attacker to execute system commands as root, by sending a specially crafted HTTP SUBSCRIBE request to the UPnP service when connecting to the local network.	2019-12-30	not yet calculated	<a href="#">CVE-2019-17621</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
ddq -- ddq	The owned function of a smart contract implementation for DDQ, an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19833</a> <a href="#">MISC</a>
docker -- docker	An issue was found in Docker before 1.6.0. Some programs and scripts in Docker are downloaded via HTTP and then executed or used in unsafe ways.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0048</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ds_data_systems -- konakart	Cross-site request forgery (CSRF) vulnerability in the Storefront Application in DS Data Systems KonaKart before 7.3.0.0 allows remote attackers to hijack the authentication of administrators for requests that change a user email address via an unspecified GET request.	2020-01-03	not yet calculated	<a href="#">CVE-2014-5516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
easy_xml_editor -- easy_xml_editor	Easy XML Editor through v1.7.8 is affected by: XML External Entity Injection. The impact is: Arbitrary File Read and DoS by consuming resources. The component is: XML Parsing. The attack vector is: Specially crafted XML payload.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19031</a> <a href="#">MISC</a>
ecstatic -- ecstatic	ecstatic have a denial of service vulnerability. Successful exploitation could lead to crash of an application.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10775</a> <a href="#">MISC</a>
				<a href="#">CVE-2013-4357</a>

embedded_glibc -- embedded_glibc	The eglibc package before 2.14 incorrectly handled the getaddrinfo() function. An attacker could use this issue to cause a denial of service.	2019-12-31	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ezxml -- ezxml	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_ent_ok() mishandles recursion, leading to stack consumption for a crafted XML file.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20198</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The ezxml_parse_* functions mishandle XML entities, leading to an infinite loop in which memory allocations occur.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20201</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_decode, while parsing crafted a XML file, performs incorrect memory handling, leading to a heap-based buffer over-read in the "normalize line endings" feature.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20200</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_decode, while parsing a crafted XML file, performs incorrect memory handling, leading to NULL pointer dereference while running strlen() on a NULL pointer.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20199</a> <a href="#">MISC</a>
ezxml -- ezxml &#xA0;	An issue was discovered in ezXML 0.8.3 through 0.8.6. The function ezxml_char_content() tries to use realloc on a block that was not allocated, leading to an invalid free and segmentation fault.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20202</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.	2020-01-03	not yet calculated	<a href="#">CVE-2019-20330</a> <a href="#">MISC</a> <a href="#">MISC</a>
fhdk -- gksu-polkit	gksu-polkit-0.0.3-6.fc18 was reported as fixing the issue in CVE-2012-5617 but the	2019-12-	not yet	<a href="#">CVE-2013-4161</a> <a href="#">MISC</a> <a href="#">MISC</a>

&#xA0;	patch was improperly applied and it did not fixed the security issue.	31	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fiberhome -- an5506-04-f_rp_2669_devices	FiberHome an5506-04-f RP2669 devices have XSS.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9556</a> <a href="#">MISC</a> <a href="#">MISC</a>
fontforge -- fontforge	FontForge 20190801 has a use-after-free in SFD_GetFontMetaData in sfd.c.	2020-01-03	not yet calculated	<a href="#">CVE-2020-5395</a> <a href="#">MISC</a>
fontforge -- fontforge	FontForge 20190801 has a heap-based buffer overflow in the Type2NotDefSplines() function in splinesave.c.	2020-01-03	not yet calculated	<a href="#">CVE-2020-5496</a> <a href="#">MISC</a>
ftp -- ftp	An issue was discovered in rovinbhandari FTP through 2012-03-28. receive_file in file_transfer_functions.c allows remote attackers to cause a denial of service (daemon crash) via a 0xffff datalen field value.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9668</a> <a href="#">MISC</a>
fusionforge -- fusionforge	FusionForge before 5.3.2 use scripts that run under the shared Apache user, which is also used by project homepages by default. If project webpages are hosted on the same server than FusionForge, it can allow users to incorrectly access on-disk private data in FusionForge.	2020-01-02	not yet calculated	<a href="#">CVE-2014-6275</a> <a href="#">MISC</a> <a href="#">MISC</a>
generalitat_de_catalunya -- accesuniversitat.gencat.cat &#xA0;	The Java API in Generalitat de Catalunya accesuniversitat.gencat.cat 1.7.5 allows remote attackers to get personal information of all registered students via several API endpoints, given that the attacker is authenticated as a student: 1) <a href="https://accesuniversitat.gencat.cat/accesuniversitat/AppJava/api/v1/estudiants/{student_id}/">https://accesuniversitat.gencat.cat/accesuniversitat/AppJava/api/v1/estudiants/{student_id}/</a> 2) <a href="https://accesuniversitat.gencat.cat/accesuniversitat/AppJava/api/v1/estudiants/?page={page}">https://accesuniversitat.gencat.cat/accesuniversitat/AppJava/api/v1/estudiants/?page={page}</a> .	2019-12-31	not yet calculated	<a href="#">CVE-2019-12837</a> <a href="#">MISC</a>
getsimple_cms -- getsimple_cms &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in GetSimple CMS before 3.2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) id parameter to backup-edit.php; (2) title or (3) menu parameter to edit.php; or (4) path or (5) returnid parameter to filebrowser.php in admin/. NOTE: the path parameter in admin/upload.php vector is already covered by CVE-2012-6621.	2020-01-02	not yet calculated	<a href="#">CVE-2013-1420</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in GitLab Enterprise Edition 11.2.x through 11.4.x			<a href="#">CVE-2018-</a>



gitlab -- enterprise_edition	before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">20507</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition 11.2.x through 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20490</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and enterprise_edition	GitLab Community Edition (CE) and Enterprise Edition (EE). 9.6 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19254</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20489</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows Information Exposure.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20488</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20493</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and enterprise_edition	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows SSRF.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20499</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and enterprise_edition	GitLab Community Edition (CE) and Enterprise Edition (EE) through 12.5 has Incorrect Access Control (issue 1 of 2).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19257</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and enterprise_edition	GitLab Community Edition (CE) and Enterprise Edition (EE) through 12.5 has Incorrect Access Control (issue 2 of 2).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19260</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and enterprise_edition &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20501</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and enterprise_edition &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition 11.3.x and 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows Information Exposure.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20495</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20494</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It has Incorrect Access Control.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20498</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition 11.2.x through 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20496</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_community_and &#xA0;	An issue was discovered in GitLab Community and Enterprise Edition before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows SSRF.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20497</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 8.2 and later through 12.5 has Insecure Permissions.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19263</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 12.3 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19255</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 11.9 and later through 12.5 has Insecure Permissions.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19262</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 2 of 2).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19087</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 8.90 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19309</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) 11.3 through 12.4.2 allows Directory Traversal.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19088</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	GitLab Enterprise Edition (EE) 6.7 and later through 12.5 allows SSRF.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19261</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition	Gitlab Enterprise Edition (EE) before 12.5.1 has Insecure Permissions (issue 1	2020-01-03	not yet calculated	<a href="#">CVE-2019-19086</a> <a href="#">CONFIRM</a>

	of 2).			<a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition &#xA0;	An issue was discovered in GitLab Enterprise Edition 11.3.x and 11.4.x before 11.4.13, 11.5.x before 11.5.6, and 11.6.x before 11.6.1. It allows XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2018-20491</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gitlab -- gitlab_enterprise_edition &#xA0;	GitLab Enterprise Edition (EE) 11.3 and later through 12.5 allows an Insecure Direct Object Reference (IDOR).	2020-01-03	not yet calculated	<a href="#">CVE-2019-19259</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition &#xA0;	GitLab Enterprise Edition (EE) 10.8 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19258</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition &#xA0;	GitLab EE 8.14 through 12.5, 12.4.3, and 12.3.6 allows XSS in group and profile fields.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19311</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition &#xA0;	GitLab Enterprise Edition (EE) 12.2 and later through 12.5 has Incorrect Access Control.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19256</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gitlab -- gitlab_enterprise_edition &#xA0;	GitLab Enterprise Edition (EE) 9.0 and later through 12.5 allows Information Disclosure.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19310</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
gonicus -- gosa	The GOsa_Filter_Settings cookie in GONICUS GOsa 2.7.5.2 is vulnerable to PHP objection injection, which allows a remote authenticated attacker to perform file deletions (in the context of the user account that runs the web server) via a crafted cookie value, because unserialize is used to restore filter settings from a cookie.	2019-12-31	not yet calculated	<a href="#">CVE-2019-14466</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5845</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome	Use-after-free in content delivery manager in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-13765</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome &#xA0;	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5846</a> <a href="#">MISC</a> <a href="#">MISC</a>

google -- chrome &#xA0;	Use-after-free in accessibility in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-13766</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- chrome &#xA0;	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5844</a> <a href="#">MISC</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GetPayload in GPMF_mp4reader.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20088</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GPMF_Next in GPMF_parser.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20086</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has an heap-based buffer over-read in GPMF_SeekToSamples in GPMF_parse.c for the size calculation.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20089</a> <a href="#">MISC</a>
gopro -- gpmf-parser	GoPro GPMF-parser 1.2.3 has a heap-based buffer over-read in GPMF_seekToSamples in GPMF-parse.c for the "matching tags" feature.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20087</a> <a href="#">MISC</a>
goscript -- goscript &#xA0;	go.cgi in GoScript 2.0 allows remote attackers to execute arbitrary commands via shell metacharacters in the (1) query string or (2) artarchive parameter.	2019-12-31	not yet calculated	<a href="#">CVE-2004-2776</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is an invalid pointer dereference in the function GF_IPMPX_AUTH_Delete() in odf/ipmpx_code.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20170</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There are memory leaks in metx_New in isomedia/box_code_base.c and abst_Read in isomedia/box_code_adobe.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20171</a> <a href="#">MISC</a>
gpac -- gpac	An issue was discovered in GPAC version 0.8.0 and 0.9.0-development-20191109. There is a memory leak in dinf_New() in isomedia/box_code_base.c.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20159</a> <a href="#">MISC</a>
gpac -- gpac	dimC_Read in isomedia/box_code_3gpp.c in GPAC 0.8.0 has a stack-based buffer overflow.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20208</a> <a href="#">MISC</a>
	Unrestricted file upload vulnerability in includes/classes/uploadify-v2.1.4/uploadify.php in HelpDEZk 1.0.1 and earlier allows remote attackers to			<a href="#">CVE-2014-</a>

helpdez k -- helpdez k	execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in the directory specified by the folder parameter.	2020-01-03	not yet calculated	<a href="#">8337</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- multiple_products &#xA0;	A security vulnerability has been identified in HPE SimpliVity 380 Gen 9, HPE SimpliVity 380 Gen 10, HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen 10, SimpliVity OmniCube, SimpliVity OmniStack for Cisco, SimpliVity OmniStack for Lenovo and SimpliVity OmniStack for Dell nodes. An API is used to execute a command manifest file during upgrade does not correctly prevent directory traversal and so can be used to execute manifest files in arbitrary locations on the node. The API does not require user authentication and is accessible over the management network, resulting in the potential for unauthenticated remote execution of manifest files. For all customers running HPE OmniStack version 3.7.9 and earlier. HPE recommends upgrading the OmniStack software to version 3.7.10 or later, which contains a permanent resolution. Customers and partners who can upgrade to 3.7.10 should upgrade at the earliest convenience. For all customers and partners unable to upgrade their environments to the recommended version 3.7.10, HPE has created a Temporary Workaround <a href="https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061901&amp;withFrame">https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061901&amp;withFrame</a> for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.	2020-01-03	not yet calculated	<a href="#">CVE-2019-11994</a> <a href="#">MISC</a>
	A security vulnerability has been identified in HPE SimpliVity 380 Gen 9, HPE SimpliVity 380 Gen 10, HPE SimpliVity 380 Gen 10 G, HPE SimpliVity 2600 Gen 10, SimpliVity OmniCube, SimpliVity OmniStack for Cisco, SimpliVity OmniStack for Lenovo and SimpliVity OmniStack for Dell nodes. Two now deprecated APIs run as root, accept a file name path, and can be used to create or delete arbitrary files on the nodes. These APIs do not require user authentication and are accessible over the management			



hp -- multiple_products &#xA0;	network, resulting in remote availability and integrity vulnerabilities For all customers running HPE OmniStack version 3.7.9 and earlier. HPE recommends upgrading the OmniStack software to version 3.7.10 or later, which contains a permanent resolution. Customers and partners who can upgrade to 3.7.10 should upgrade at the earliest convenience. For all customers and partners unable to upgrade their environments to the recommended version 3.7.10, HPE has created a Temporary Workaround <a href="https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061675&amp;withFrame">https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=mmr_sf-EN_US000061675&amp;withFrame</a> for you to implement. All customer should upgrade to the recommended 3.7.10 or later version at the earliest convenience.	2020-01-03	not yet calculated	<a href="#">CVE-2019-11993</a> <a href="#">MISC</a>
huawei -- multiple_products &#xA0;	Some Huawei products have a buffer error vulnerability. An unauthenticated, remote attacker could send specific MPLS Echo Request messages to the target products. Due to insufficient input validation of some parameters in the messages, successful exploit may cause the device to reset.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5304</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	Mate 10 Pro;Honor V10;Honor 10;Nova 4 smartphones have a denial of service vulnerability. The system does not properly check the status of certain module during certain operations, an attacker should trick the user into installing a malicious application, successful exploit could cause reboot of the smartphone.	2020-01-03	not yet calculated	<a href="#">CVE-2020-1785</a> <a href="#">MISC</a>
huawei -- p30_smartphones &#xA0;	HUAWEI P30 smart phones with versions earlier than 10.0.0.166(C00E66R1P11) have an information leak vulnerability. An attacker could send specific command in the local area network (LAN) to exploit this vulnerability. Successful exploitation may cause information leak.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19441</a> <a href="#">MISC</a>
huawei -- usg9500_devices &#xA0;	USG9500 with software of V500R001C30SPC100; V500R001C30SPC200; V500R001C30SPC600; V500R001C60SPC500; V500R005C00SPC100; V500R005C00SPC200 have an improper credentials management vulnerability. The software does not properly manage	2020-01-03	not yet calculated	<a href="#">CVE-2020-1871</a> <a href="#">MISC</a>

	certain credentials. Successful exploit could cause information disclosure or damage, and impact the confidentiality or integrity.			
infinispan -- infinisp &#xA0;	A flaw was found in Infinispan through version 9.4.14.Final. An improper implementation of the session fixation protection in the Spring Session integration can result in incorrect session handling.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10158</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	Heap-based buffer overflow in the MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via a levels header.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3946</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	Stack-based buffer overflow in the MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via an IMAGE tag.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3944</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
irfanview -- irfanview &#xA0;	The MrSID plugin (MrSID.dll) before 4.37 for IrfanView allows remote attackers to execute arbitrary code via a nband tag.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3945</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
it-novum -- openitcockpit	openITCOCKPIT before 3.7.1 has reflected XSS in the 404-not-found component.	2019-12-31	not yet calculated	<a href="#">CVE-2019-10227</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
joomla! -- joomla! &#xA0;	Cross-site scripting (XSS) vulnerability in the Jomres (com_jomres) component before 7.3.1 for Joomla! allows remote authenticated users with the "Business Manager" permission to inject arbitrary web script or HTML via the property_name parameter, related to editing property details.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3931</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla! -- joomla! &#xA0;	SQL injection vulnerability in the Jomres (com_jomres) component before 7.3.1 for Joomla! allows remote authenticated users with the "Business Manager" permission to execute arbitrary SQL commands via the id parameter in an editProfile action to administrator/index.php.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3932</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
kind-of -- kind-of	ctorName in index.js in kind-of v6.0.2 allows external user input to overwrite certain internal attributes via a conflicting name, as demonstrated by 'constructor': {'name':'Symbol'}. Hence, a crafted payload can overwrite this builtin attribute to manipulate the type detection result.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20149</a> <a href="#">MISC</a> <a href="#">MISC</a>

knockout -- knockout	There is a vulnerability in knockout before version 3.5.0-beta, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14862</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libmysofa -- libmysofa &#xA0;	hdf/dataobject.c in libmysofa before 0.8 has an uninitialized use of memory, as demonstrated by mysofa2json.	2019-12-29	not yet calculated	<a href="#">CVE-2019-20063</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel_project -- libsixel	libsixel 1.8.4 has an integer overflow in sixel_frame_resize in frame.c.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20205</a> <a href="#">MISC</a>
libsixel_project -- libsixel	stb_image.h (aka the stb image loader) 2.23, as used in libsixel and other products, has an assertion failure in stbi__shiftsigned.	2019-12-29	not yet calculated	<a href="#">CVE-2019-20056</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An issue was discovered in libsixel 1.8.4. There is a heap-based buffer overflow in the function gif_out_code at fromgif.c.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20140</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.0-rc7 (as distributed in ubuntu/linux.git on kernel.ubuntu.com), mounting a crafted f2fs filesystem image and performing some operations can lead to slab-out-of-bounds read access in ttm_put_pages in drivers/gpu/drm/ttm/ttm_page_alloc.c. This is related to the vmwgfx or ttm module.	2019-12-31	not yet calculated	<a href="#">CVE-2019-19927</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	mwifiex_tm_cmd in drivers/net/wireless/marvell/mwifiex/cfg80211.c in the Linux kernel before 5.1.6 has some error-handling cases that did not free allocated hostcmd memory, aka CID-003b686ace82. This will cause a memory leak and denial of service.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20095</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel &#xA0;	In the Linux kernel before 5.1, there is a memory leak in __feat_register_sp() in net/dccp/feat.c, which may cause denial of service, aka CID-1d3ff0950e2b.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20096</a> <a href="#">MISC</a> <a href="#">MISC</a>
loaded_commerce -- loaded_commerce	The bindReplace function in the query factory in includes/classes/database.php in Loaded Commerce 7 does not properly handle : (colon) characters, which allows remote authenticated users to conduct SQL injection attacks via the First name and Last name fields in the address book.	2020-01-03	not yet calculated	<a href="#">CVE-2014-5140</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mailstore --	An issue was discovered in MailStore Server (and Service Provider Edition) 9.x through 11.x before 11.2.2. When the directory service (for synchronizing and	2019-12-	not yet	<a href="#">CVE-2019-10229</a>

mailstore_server_and_authentication.php	mailstore_server_and_authentication.php does not set to Generic LDAP, an attacker is able to login as an existing user with an arbitrary password on the second login attempt.	31	calculated	<a href="#">CONFIRM</a>
mfscripts -- yetishare	class.userpeer.php in MFScripts YetiShare 3.5.2 through 4.5.3 uses an insecure method of creating password reset hashes (based only on microtime), which allows an attacker to guess the hash and set the password within a few hours by bruteforcing.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19735</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the Secure flag on session cookies, allowing the cookie to be sent over cleartext channels.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19739</a> <a href="#">MISC</a>
mfscripts -- yetishare	translation_manage_text.ajax.php and various *_manage.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 directly insert values from the aSortDir_0 and/or sSortDir_0 parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19732</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the HttpOnly flag on session cookies, allowing the cookie to be read by script, which can potentially be used by attackers to obtain the cookie via cross-site scripting.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19736</a> <a href="#">MISC</a>
mfscripts -- yetishare	MFScripts YetiShare 3.5.2 through 4.5.3 does not set the SameSite flag on session cookies, allowing the cookie to be sent in cross-site requests and potentially be used in cross-site request forgery attacks.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19737</a> <a href="#">MISC</a>
mfscripts -- yetishare	log_file_viewer.php in MFScripts YetiShare 3.5.2 through 4.5.3 does not sanitize or encode the output from the lFile parameter on the page, which would allow an attacker to input HTML or execute scripts on the site, aka XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19738</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_account_move_file_in_folder.ajax.php in MFScripts YetiShare 3.5.2 directly inserts values from the filelds parameter into a SQL string. This allows an attacker to inject their own SQL and manipulate the query, typically extracting data from the database, aka SQL Injection.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19734</a> <a href="#">MISC</a> <a href="#">MISC</a>
	_account_forgot_password.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3			

mfscripts -- yetishare &#xA0;	takes a different amount of time to return depending on whether an email address is configured for the account name provided. This can be used by an attacker to enumerate accounts by guessing email addresses.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19805</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_get_all_file_server_paths.ajax.php (aka get_all_file_server_paths.ajax.php) in MFScripts YetiShare 3.5.2 through 4.5.3 does not sanitize or encode the output from the filelds parameter on the page, which would allow an attacker to input HTML or execute scripts on the site, aka XSS.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19733</a> <a href="#">MISC</a> <a href="#">MISC</a>
mfscripts -- yetishare &#xA0;	_account_forgot_password.ajax.php in MFScripts YetiShare 3.5.2 through 4.5.3 displays a message indicating whether an email address is configured for the account name provided. This can be used by an attacker to enumerate accounts by guessing email addresses.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19806</a> <a href="#">MISC</a>
miniupnp -- ngiflib	ngiflib 0.4 has a heap-based buffer over-read in GifIndexToTrueColor in ngiflib.c.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20219</a> <a href="#">MISC</a>
mitreid_connect -- mitreid_connect	The OpenID Connect reference implementation for MITREid Connect through 1.3.3 allows XSS due to userInfoJson being included in the page unsanitized. This is related to header.tag. The issue can be exploited to execute arbitrary JavaScript.	2020-01-04	not yet calculated	<a href="#">CVE-2020-5497</a> <a href="#">MISC</a>
monitorix -- monitorix	The handle_request function in lib/HTTPServer.pm in Monitorix before 3.3.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the URI.	2019-12-31	not yet calculated	<a href="#">CVE-2013-7070</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
monitorix -- monitorix	Cross-site scripting (XSS) vulnerability in the handle_request function in lib/HTTPServer.pm in Monitorix before 3.4.0 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2019-12-31	not yet calculated	<a href="#">CVE-2013-7071</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mybb -- mybb	MyBB before 1.8.22 allows an open redirect on login.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20225</a> <a href="#">MISC</a> <a href="#">MISC</a>
nagios -- nagios_xi	In Nagios XI 5.6.9, an authenticated user is able to execute arbitrary OS commands via shell metacharacters in the id parameter to schedulereport.php, in the context of the web-server user account.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20197</a> <a href="#">MISC</a>



nasm -- netwide_assembler	In Netwide Assembler (NASM) 2.14.02, stack consumption occurs in expr# functions in asm/eval.c. This potentially affects the relationships among expr0, expr1, expr2, expr3, expr4, expr5, and expr6 (and stdscan in asm/stdscan.c). This is similar to CVE-2019-6290 and CVE-2019-6291.	2020-01-04	not yet calculated	<a href="#">CVE-2019-20334</a> <a href="#">MISC</a> <a href="#">MISC</a>
newinteltechmedia -- newinteltechmedia	The NETM() function of a smart contract implementation for NewIntelTechMedia (NETM), an tradable Ethereum ERC20 token, allows attackers to change the owner of the contract, because the function does not check the caller's identity.	2019-12-31	not yet calculated	<a href="#">CVE-2018-19832</a> <a href="#">MISC</a>
nim -- nim	The HTTP Authentication library before 2019-12-27 for Nim has weak password hashing because the default algorithm for libsodium's crypto_pwhash_str is not used.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20138</a> <a href="#">MISC</a>
obs-server -- obs-server	obs-server before 1.7.7 allows logins by 'unconfirmed' accounts due to a bug in the REST api implementation.	2020-01-02	not yet calculated	<a href="#">CVE-2010-3782</a> <a href="#">MISC</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev27 and 7.4.x before 7.4.0-rev20 allows remote attackers to inject arbitrary web script or HTML via the body of an email. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7486</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">SECTRAK</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the backend in Open-Xchange (OX) AppSuite 7.2.x before 7.2.2-rev26 and 7.4.x before 7.4.0-rev16 allows remote attackers to inject arbitrary web script or HTML via the publication name, which is not properly handled in an error message. NOTE: this vulnerability was SPLIT from CVE-2013-6242 because it affects different sets of versions.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7485</a> <a href="#">OSVDB</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a> <a href="#">SECTRAK</a> <a href="#">XF</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
open-xchange -- appsuite &#xA0;	Cross-site scripting (XSS) vulnerability in the frontend in Open-Xchange (OX) AppSuite 6.22.3 before 6.22.3-rev5 and 6.22.4 before 6.22.4-rev12 allows remote attackers to inject arbitrary web script or HTML via the subject of an email. NOTE: the vulnerabilities related to the body of the email and the publication name were SPLIT from this CVE ID because they affect different sets of versions.	2020-01-02	not yet calculated	<a href="#">CVE-2013-6242</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

opencv -- opencv	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV 4.1.0. A specially crafted XML file can cause a buffer overflow, resulting in multiple heap corruptions and potential code execution. An attacker can provide a specially crafted file to trigger this vulnerability.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5063</a> <a href="#">MISC</a>
opencv -- opencv	An exploitable heap buffer overflow vulnerability exists in the data structure persistence functionality of OpenCV, version 4.1.0. A specially crafted JSON file can cause a buffer overflow, resulting in multiple heap corruptions and potentially code execution. An attacker can provide a specially crafted file to trigger this vulnerability.	2020-01-03	not yet calculated	<a href="#">CVE-2019-5064</a> <a href="#">MISC</a>
openlambda -- openlambda	OpenLambda 2019-09-10 allows DNS rebinding attacks against the OL server for the REST API on TCP port 5000.	2020-01-03	not yet calculated	<a href="#">CVE-2019-20329</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openldap -- openldap &#xA0;	An off-by-one error leading to a crash was discovered in openldap 2.4 when processing DNS SRV messages. If slapd was configured to use the dnssrv backend, an attacker could crash the service with crafted DNS responses.	2020-01-02	not yet calculated	<a href="#">CVE-2014-8182</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opsview -- opsview_and_opsview_core	Multiple cross-site scripting (XSS) vulnerabilities in Opsview before 4.4.1 and Opsview Core before 20130522 allow remote attackers to inject arbitrary web script or HTML.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3936</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opsview -- opsview_and_opsview_core	Cross-site request forgery (CSRF) vulnerability in Opsview before 4.4.1 and Opsview Core before 20130522 allows remote attackers to hijack the authentication of administrators for requests that change the administrator password via unspecified vectors.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3935</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
outsystems -- platform	OutSystems Platform 10 through 11 allows ImageResourceDetail.aspx CSRF for content modifications and file uploads. NOTE: the product is self-hosted by the customer, even though it has a *.outsystemsenterprise.com domain name.)	2019-12-31	not yet calculated	<a href="#">CVE-2019-12273</a> <a href="#">MISC</a>
ovirt-engine-sdk-	ovirt-engine-sdk-python before 3.4.0.7 and 3.5.0.4 does not verify that the hostname of the remote endpoint matches the Common Name (CN) or			<a href="#">CVE-2014-</a>

[illegible]

qemu -- qemu &#xA0;	Qemu 1.1.2+dfsg to 2.1+dfsg suffers from a buffer overrun which could potentially result in arbitrary code execution on the host with the privileges of the QEMU process.	2020-01-02	not yet calculated	<a href="#">CVE-2013-4532</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
quixplorer -- quixplorer &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in QuiXplorer before 2.5.5 allow remote attackers to inject arbitrary web script or HTML via the (1) dir, (2) item, (3) order, (4) searchitem, (5) selitems[], or (6) srt parameter to index.php or (7) the QUERY_STRING to index.php.	2020-01-02	not yet calculated	<a href="#">CVE-2013-1642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- ansible	Ansible, versions 2.9.x before 2.9.1, 2.8.x before 2.8.7 and Ansible versions 2.7.x before 2.7.15, is not respecting the flag no_log set it to True when Sumologic and Splunk callback plugins are used send tasks results events to collectors. This would discloses and collects any sensitive data.	2020-01-02	not yet calculated	<a href="#">CVE-2019-14864</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_enterprise_application_platform &#xA0;	In JBoss EAP 6 a security domain is configured to use a cache that is shared between all applications that are in the security domain. This could allow an authenticated user in one application to access protected resources in another application without proper authorization. Although this is an intended functionality, it was not clearly documented which can mislead users into thinking that a security domain cache is isolated to a single application.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0169</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_portal &#xA0;	It was found that the implementation of the GTNSubjectCreatingInterceptor class in gatein-wsrp was not thread safe. For a specific WSRP endpoint, under high-concurrency scenarios or scenarios where SOAP messages take long to execute, it was possible for an unauthenticated remote attacker to gain privileged information if WS-Security is enabled for the WSRP Consumer, and the endpoint in question is being used by a privileged user. This affects JBoss Portal 6.2.0.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0245</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat --	A CSRF issue was found in OpenShift Enterprise 1.2. The web console is using 'Basic authentication' and the REST API			<a href="#">CVE-2013-</a>

openshift_enterprise &#xA0;	has no CSRF attack protection mechanism. This can allow an attacker to obtain the credential and the Authorization: header when requesting the REST API via web browser.	2019-12-30	not yet calculated	<a href="#">0196</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openstack_essex_release	Within the RHOS Essex Preview (2012.2) of the OpenStack dashboard package, the file /etc/quantum/quantum.conf is world readable which exposes the admin password and token value.	2019-12-30	not yet calculated	<a href="#">CVE-2012-5476</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openstack_platform_and_essex_release &#xA0;	The file /etc/openstack-dashboard/local_settings within Red Hat OpenStack Platform 2.0 and RHOS Essex Release (python-openstack-horizon package before 2012.1.1) is world readable and exposes the secret key value.	2019-12-30	not yet calculated	<a href="#">CVE-2012-5474</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- quay	A flaw was found in the way Red Hat Quay stores robot account tokens in plain text. An attacker able to perform database queries in the Red Hat Quay database could use the tokens to read or write container images stored in the registry.	2020-01-02	not yet calculated	<a href="#">CVE-2019-10205</a> <a href="#">CONFIRM</a>
red_hat -- satellite_6	Versions of Foreman as shipped with Red Hat Satellite 6 does not check for a correct CSRF token in the logout action. Therefore, an attacker can log out a user by having them view specially crafted content.	2020-01-02	not yet calculated	<a href="#">CVE-2014-3590</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- subscription_asset_manager	Versions of Katello as shipped with Red Hat Subscription Asset Manager 1.4 are vulnerable to a XSS via HTML in the systems name when registering.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0183</a> <a href="#">MISC</a> <a href="#">MISC</a>
ricoh -- marcomcentral &#xA0;	A directory traversal and local file inclusion vulnerability in FPProducerInternetServer.exe in Ricoh MarcomCentral, formerly PTI Marketing, FusionPro VDP before 10.0 allows a remote attacker to list or enumerate sensitive contents of files. Furthermore, this could allow for privilege escalation by dumping the local machine's SAM and SYSTEM database files, and possibly remote code execution.	2019-12-31	not yet calculated	<a href="#">CVE-2019-7751</a> <a href="#">MISC</a> <a href="#">MISC</a>
ros -- ros &#xA0;	An issue was discovered in the ROS communications-related packages (aka ros_comm or ros-melodic-ros-comm) through 1.14.3. parseOptions() in tools/rosbag/src/record.cpp has an integer overflow when a crafted split option can be entered on the command line.	2019-12-30	not yet calculated	<a href="#">CVE-2019-13445</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>



ros -- ros &#xA0;	An issue was discovered in the ROS communications-related packages (aka ros_comm or ros-melodic-ros-comm) through 1.14.3. ROS_ASSERT_MSG only works when ROS_ASSERT_ENABLED is defined. This leads to a problem in the remove() function in clients/roscpp/src/libros/spinner.cpp. When ROS_ASSERT_ENABLED is not defined, the iterator loop will run out of the scope of the array, and cause denial of service for other components (that depend on the communication-related functions of this package).	2019-12-30	not yet calculated	<a href="#">CVE-2019-13465</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
rsa -- authentication_manager	RSA Authentication Manager versions prior to 8.4 P7 contain an XML Entity Injection Vulnerability. A remote authenticated malicious user could potentially exploit this vulnerability to cause information disclosure of local system files by supplying specially crafted XML message.	2020-01-03	not yet calculated	<a href="#">CVE-2019-3768</a> <a href="#">MISC</a>
samba -- samba &#xA0;	Multiple race conditions in the (1) mount.cifs and (2) umount.cifs programs in Samba 3.6 allow local users to cause a denial of service (mounting outage) via a SIGKILL signal during a time window when the /etc/mtab~ file exists.	2019-12-31	not yet calculated	<a href="#">CVE-2011-3585</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
serenityos -- serenityos &#xA0;	Kernel/VM/MemoryManager.cpp in SerenityOS before 2019-12-30 does not reject syscalls with pointers into the kernel-only virtual address space, which allows local users to gain privileges by overwriting a return address that was found on the kernel stack.	2019-12-31	not yet calculated	<a href="#">CVE-2019-20172</a> <a href="#">MISC</a> <a href="#">MISC</a>
shaarli -- shaarli &#xA0;	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Shaarli allow remote attackers to inject arbitrary web script or HTML via the URL to the (1) showRSS, (2) showATOM, or (3) showDailyRSS function; a (4) file name to the importFile function; or (5) vectors related to bookmarks.	2020-01-02	not yet calculated	<a href="#">CVE-2013-7351</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
sonicwall -- global_management_system	A vulnerability in GMS allow unauthenticated user to SQL injection in Webservice module. This vulnerability affected GMS versions GMS 8.4, 8.5, 8.6, 8.7, 9.0 and 9.1.	2019-12-31	not yet calculated	<a href="#">CVE-2019-7478</a> <a href="#">CONFIRM</a>
	A vulnerability in SonicOS allow authenticated read-only admin can			

sonicwall -- sonicos &#xA0;	elevate permissions to configuration mode. This vulnerability affected SonicOS Gen 5 version 5.9.1.12-4o and earlier, Gen 6 version 6.2.7.4-32n, 6.5.1.4-4n, 6.5.2.3-4n, 6.5.3.3-3n, 6.2.7.10-3n, 6.4.1.0-3n, 6.5.3.3-3n, 6.5.1.9-4n and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V).	2019-12-31	not yet calculated	<a href="#">CVE-2019-7479</a> <a href="#">CONFIRM</a>
sqlite -- sqlite &#xA0;	ext/misc/zipfile.c in SQLite 3.30.1 mishandles certain uses of INSERT INTO in situations involving embedded '' characters in filenames, leading to a memory-management error that can be detected by (for example) valgrind.	2020-01-03	not yet calculated	<a href="#">CVE-2019-19959</a> <a href="#">MISC</a> <a href="#">MISC</a>
supermicro -- x9_and_x8_generation &#xA0;	Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before SMT_X9_317 and firmware for Supermicro X8 generation motherboards before SMT X8 312 contain hardcoded private encryption keys for the (1) Lighttpd web server SSL interface and the (2) Dropbear SSH daemon.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3619</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
supermicro -- x9_and_x8_generation &#xA0;	Hardcoded WSMAN credentials in Intelligent Platform Management Interface (IPMI) with firmware for Supermicro X9 generation motherboards before 3.15 (SMT_X9_315) and firmware for Supermicro X8 generation motherboards before SMT X8 312.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3620</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
sylius -- sylius &#xA0;	An issue was discovered in Sylius products. Missing input sanitization in sylius/sylius 1.0.x through 1.0.18, 1.1.x through 1.1.17, 1.2.x through 1.2.16, 1.3.x through 1.3.11, and 1.4.x through 1.4.3 and sylius/grid 1.0.x through 1.0.18, 1.1.x through 1.1.18, 1.2.x through 1.2.17, 1.3.x through 1.3.12, 1.4.x through 1.4.4, and 1.5.0 allows an attacker (an admin in the sylius/sylius case) to perform XSS by injecting malicious code into a field displayed in a grid with the "string" field type. The contents are an object, with malicious code returned by the toString() method of that object.	2019-12-31	not yet calculated	<a href="#">CVE-2019-12186</a> <a href="#">CONFIRM</a>
	Symfony 2.0.X before 2.0.24, 2.1.X before 2.1.12, 2.2.X before 2.2.5, and			<a href="#">CVE-2013-4752</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

symfony -- symfony &#xA0;	2.3.X before 2.3.3 have an issue in the HttpFoundation component. The Host header can be manipulated by an attacker when the framework is generating an absolute URL. A remote attacker could exploit this vulnerability to inject malicious content into the Web application page and conduct various attacks.	2020-01-02	not yet calculated	MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
telos -- automated_message_handling_system	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the LDAP cbURL parameter of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9538</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in uploaditem.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9537</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Information Exposure vulnerability in itemlookup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9541</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in itemlookup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9542</a> <a href="#">CERT-VN</a>
telos -- automated_message_handling_system &#xA0;	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in prefs.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9540</a> <a href="#">CERT-VN</a>

	This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.			
telos -- automated_message_handling &#xA0;	: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ModalWindowPopup.asp of Telos Automated Message Handling System allows a remote attacker to inject arbitrary script into an AMHS session. This issue affects: Telos Automated Message Handling System versions prior to 4.1.5.5.	2020-01-03	not yet calculated	<a href="#">CVE-2019-9539</a> <a href="#">CERT-VN</a>
textproc/isearch -- textproc/isearch &#xA0;	The isearch package (textproc/isearch) before 1.47.01nb1 uses the tempnam() function to create insecure temporary files into a publicly-writable area (/tmp).	2019-12-30	not yet calculated	<a href="#">CVE-2012-5663</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tigervnc -- tigervnc &#xA0;	Multiple heap-based buffer overflows in the ZRLE_DECODE function in common/rfb/zrleDecode.h in TigerVNC before 1.3.1, when NDEBUB is enabled, allow remote VNC servers to cause a denial of service (vncviewer crash) and possibly execute arbitrary code via vectors related to screen image rendering.	2020-01-02	not yet calculated	<a href="#">CVE-2014-0011</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tiny_file_manager -- tiny_file_manager &#xA0;	In Tiny File Manager before 2.3.9, there is a remote code execution via Upload from URL and Edit/Rename files. Only authenticated users are impacted.	2019-12-30	not yet calculated	<a href="#">CVE-2019-16790</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tinywall -- tinywall	An attacker who has already compromised the local system could use TinyWall Controller to gain additional privileges by attaching a debugger to the running process and modifying the code in memory. Vulnerability fixed in version 2.1.13.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19470</a> <a href="#">MISC</a>
tvb -- nvms-1000_devices	TVT NVMS-1000 devices allow GET /.. Directory Traversal	2019-12-30	not yet calculated	<a href="#">CVE-2019-20085</a> <a href="#">MISC</a>
unity_technologies -- editor &#xA0;	The com.unity3d.kharma protocol handler in Unity Editor 2018.3 allows remote attackers to execute arbitrary code.	2019-12-31	not yet calculated	<a href="#">CVE-2019-9197</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
vim -- vim &#xA0;	The autocmd feature in window.c in Vim before 8.1.2136 accesses freed memory.	2019-12-30	not yet calculated	<a href="#">CVE-2019-20079</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

visual_mining -- netcharts_server &#xA0;	Unrestricted file upload vulnerability in Visual Mining NetCharts Server allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via unspecified vectors.	2020-01-03	not yet calculated	<a href="#">CVE-2014-8516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	Cross-site Scripting (XSS) in the spreadshirt-rss-3d-cube-flash-gallery plugin 2014 for WordPress allows remote attackers to execute arbitrary web script or HTML via unspecified parameters.	2020-01-02	not yet calculated	<a href="#">CVE-2014-4553</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	The Postie plugin 1.9.40 for WordPress allows XSS, as demonstrated by a certain payload with jaVaScRipt:/* at the beginning and a crafted SVG element.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20204</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress &#xA0;	The Authorized Addresses feature in the Postie plugin 1.9.40 for WordPress allows remote attackers to publish posts by spoofing the From information of an email message.	2020-01-02	not yet calculated	<a href="#">CVE-2019-20203</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
xmlblueprint -- xmlblueprint	XMLBlueprint through 16.191112 is affected by XML External Entity Injection. The impact is: Arbitrary File Read when an XML File is validated. The component is: XML Validate function. The attack vector is: Specially crafted XML payload.	2019-12-30	not yet calculated	<a href="#">CVE-2019-19032</a> <a href="#">MISC</a>
xnview -- xnview	xnview.exe in XnView before 2.13 does not properly handle RLE strip lengths during processing of RGB files, which allows remote attackers to execute arbitrary code via the RLE strip size field in a RGB file, which leads to an unexpected sign extension error and a heap-based buffer overflow.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3939</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
xnview -- xnview	Heap-based buffer overflow in xnview.exe in XnView before 2.13 allows remote attackers to execute arbitrary code via the biBitCount field in a BMP file.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3937</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
xnview -- xnview &#xA0;	Xjp2.dll in XnView before 2.13 allows remote attackers to execute arbitrary code via (1) the Csiz parameter in a SIZ marker, which triggers an incorrect memory allocation, or (2) the lqcd field in a QCD marker in a crafted JPEG2000 file, which leads to a heap-based buffer overflow.	2020-01-02	not yet calculated	<a href="#">CVE-2013-3941</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In all versions of ClickHouse before 19.14.3, an attacker having write access			



yandex -- clickhouse &#xA0;	to ZooKeeper and who is able to run a custom server available from the network where ClickHouse runs, can create a custom-built malicious server that will act as a ClickHouse replica and register it in ZooKeeper. When another replica will fetch data part from the malicious replica, it can force clickhouse-server to write to arbitrary path on filesystem.	2019-12-30	not yet calculated	<a href="#">CVE-2019-15024</a> <a href="#">MISC</a>
zend_framework -- zend_framework	Multiple cross-site scripting (XSS) vulnerabilities in Zend Framework 2.0.x before 2.0.1 allow remote attackers to inject arbitrary web script or HTML via unspecified input to (1) Debug, (2) Feed\PubSubHubbub, (3) Log\Formatter\Xml, (4) Tag\Cloud\Decorator, (5) Uri, (6) View\Helper\HeadStyle, (7) View\Helper\Navigation\Sitemap, or (8) View\Helper\Placeholder\Container\AbstractStandalone, related to Escaper.	2020-01-03	not yet calculated	<a href="#">CVE-2012-4451</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	SQL injection vulnerability in Zenphoto before 1.4.9 allow remote administrators to execute arbitrary SQL commands.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto &#xA0;	Cross-site request forgery (CSRF) vulnerability in admin.php in Zenphoto before 1.4.9 allows remote attackers to hijack the authentication of admin users for requests that may cause a denial of service (resource consumption).	2019-12-31	not yet calculated	<a href="#">CVE-2015-5595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto &#xA0;	Incomplete blacklist in sanitize_string in Zenphoto before 1.4.9 allows remote attackers to conduct cross-site scripting (XSS) attacks.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5592</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto &#xA0;	The sanitize_string function in Zenphoto before 1.4.9 does not properly sanitize HTML tags, which allows remote attackers to perform a cross-site scripting (XSS) attack by wrapping a payload in "<<script></script>script>payload<script></script></script>", or in an image tag, with the payload as the onerror event.	2019-12-31	not yet calculated	<a href="#">CVE-2015-5593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine - adselfservice_plus	An issue was discovered in Zoho ManageEngine ADSelfService Plus 5.6 Build 5607. An exposed service allows an unauthenticated person to retrieve internal information from the system and	2019-12-31	not yet calculated	<a href="#">CVE-2019-7162</a> <a href="#">MISC</a>

modify the product installation.

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of December 16, 2019  
**Date:** Monday, December 23, 2019 1:38:34 PM

---



National Cyber Awareness System:

## **Vulnerability Summary for the Week of December 16, 2019**

12/23/2019 06:26 AM EST

Original release date: December 23, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- diaganywhere_server	In Advantech DiagAnywhere Server, Versions 3.07.11 and prior, multiple stack-based buffer overflow vulnerabilities exist in the file transfer service listening on the TCP port. Successful exploitation could allow an unauthenticated attacker to execute arbitrary code with the privileges of the user running DiagAnywhere Server.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-18257</a> <a href="#">MISC</a>
apple -- icloud_for_windows	A race condition existed during the installation of iTunes for Windows. This was addressed with improved state handling. This issue is fixed in iCloud for Windows 7.11. Running the iTunes installer in an untrusted directory may result in arbitrary code execution.	2019-12-18	<a href="#">7.6</a>	<a href="#">CVE-2019-6232</a> <a href="#">MISC</a>
apple -- icloud_for_windows	A race condition existed during the installation of iCloud for Windows. This was addressed with improved state handling. This issue is fixed in iCloud for Windows 7.11. Running the iCloud installer in an untrusted directory may	2019-12-18	<a href="#">7.6</a>	<a href="#">CVE-2019-6236</a> <a href="#">MISC</a>

	result in arbitrary code execution.			
apple -- macos_catalina	A validation issue was addressed with improved logic. This issue is fixed in macOS Catalina 10.15.1. A malicious application may be able to gain root privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8802 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8748 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8781 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8758 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8807 MISC</a>
apple -- macos_catalina_and_tvos	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15, tvOS 13. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8717 MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8694 MISC</a>
apple -- macos_mojave	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8590 MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8695 MISC</a>

	able to execute arbitrary code with system privileges.			
apple -- macos_mojave	This issue was addressed with improved checks. This issue is fixed in macOS Mojave 10.14.4. A local user may be able to execute arbitrary shell commands.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8513</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8629</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8635</a> <a href="#">MISC</a>
apple -- macos_mojave	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.6. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8661</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8697</a> <a href="#">MISC</a>
apple -- macos_mojave	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8555</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8616</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8604</a> <a href="#">MISC</a>
apple -- macos_mojave	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. Mounting a maliciously crafted NFS network share	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8508</a> <a href="#">MISC</a>





	execution.			<a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8815</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8688</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8669</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8684</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8689</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were addressed with improved memory			<a href="#">CVE-2019-8816</a>

apple -- multiple_products	handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8685</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8574</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8648</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8605</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.4, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8647</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8641</a> <a href="#">MISC</a> <a href="#">MISC</a>

	unexpected application termination or arbitrary code execution.			<a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. An attacker may be able to trigger a use-after-free in an application deserializing an untrusted NSDictionary.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8662</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to gain root privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8637</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8660</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8672</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- watchos	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8747</a> <a href="#">MISC</a>
apple -- watchos_and_icloud_for_windows	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Multiple issues in libxslt.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8750</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- xcode	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8723</a> <a href="#">MISC</a>
apple -- xcode	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without	2019-12-	<a href="#">9.3</a>	<a href="#">CVE-2019-8724</a>

	proper input validation could lead to arbitrary code execution with user privilege.	18		<a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below can be used as an HTTP GET request proxy when unauthenticated remote attackers send crafted HTTP POST requests.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-3996</a> <a href="#">MISC</a>
envoy_proxy -- envoy	An issue was discovered in Envoy 1.12.0. An untrusted remote client may send an HTTP header (such as Host) with whitespace after the header content. Envoy will treat "header-value " as a different string from "header-value" so for example with the Host header "example.com " one could bypass "example.com" matchers.	2019-12-13	<a href="#">7.5</a>	<a href="#">CVE-2019-18802</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
envoy_proxy -- envoy	An issue was discovered in Envoy 1.12.0. An untrusted remote client may send HTTP/2 requests that write to the heap outside of the request buffers when the upstream is HTTP/1. This may be used to corrupt nearby heap contents (leading to a query-of-death scenario) or may be used to bypass Envoy's access control mechanisms such as path based routing. An attacker can also modify requests from other users that happen to be proximal temporally and spatially.	2019-12-13	<a href="#">7.5</a>	<a href="#">CVE-2019-18801</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
fontforge -- libspiro	Libspiro through 20190731 has a stack-based buffer overflow in the spiro_to_bpath0() function in spiro.c.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-19847</a> <a href="#">MISC</a>
google -- tensorflow	In TensorFlow before 1.15, a heap buffer overflow in UnsortedSegmentSum can be produced when the Index template argument is int32. In this case data_size and num_segments fields are truncated from int64 to int32 and can produce negative numbers, resulting in accessing out of bounds heap memory. This is unlikely to be exploitable and was detected and fixed internally in TensorFlow 1.15 and 2.0.	2019-12-16	<a href="#">7.5</a>	<a href="#">CVE-2019-16778</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla -- joomla!	class.upload.php in verot.net class.upload through 1.0.3 and 2.x through 2.0.4, as used in the K2 extension for Joomla! and other products, omits .pht from the set of dangerous file extensions, a similar issue to CVE-2019-19576.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-19634</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomla -- joomla!	In Joomla! before 3.9.14, the lack of validation of configuration parameters used in SQL queries caused various SQL	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-19846</a> <a href="#">MISC</a>



	injection vectors.			
labf -- aceaxe_plus	The FTP client in AceaXe Plus 1.0 allows a buffer overflow via a long EHLO response from an FTP server.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-19782</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause a NULL pointer dereference in f2fs_recover_fsycn_data in fs/f2fs/recovery.c. This is related to F2FS_P_SB in fs/f2fs/f2fs.h.	2019-12-17	<a href="#">7.1</a>	<a href="#">CVE-2019-19815</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.	2019-12-17	<a href="#">9.3</a>	<a href="#">CVE-2019-19814</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.	2019-12-17	<a href="#">9.3</a>	<a href="#">CVE-2019-19816</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in __mutex_lock in kernel/locking/mutex.c. This is related to mutex_can_spin_on_owner in kernel/locking/mutex.c, __btrfs_qgroup_free_meta in fs/btrfs/qgroup.c, and btrfs_insert_delayed_items in fs/btrfs/delayed-inode.c.	2019-12-17	<a href="#">9.3</a>	<a href="#">CVE-2019-19813</a> <a href="#">MISC</a>
petwant_and_skymee -- pf-103_and_petalk_ai	The processCommandSetMac() function of libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16737</a> <a href="#">MISC</a>
petwant_and_skymee -- pf-103_and_petalk_ai	processCommandSetUid() in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16733</a> <a href="#">MISC</a>
petwant_and_skymee -- pf-103_and_petalk_ai	Unencrypted HTTP communications for firmware upgrades in Petalk AI and PF-103 allow man-in-the-middle attackers to	2019-12-13	<a href="#">9.3</a>	<a href="#">CVE-2019-16732</a> <a href="#">MISC</a>

	run arbitrary code as the root user.			
petwant_and_skymee -- pf- 103_and_petalk_ai	A stack-based buffer overflow in processCommandUploadLog in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to cause denial of service or run arbitrary code as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16735</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	processCommandUpgrade() in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16730</a> <a href="#">MISC</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	The processCommandUploadLog() function of libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-17364</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	A stack-based buffer overflow in processCommandUploadSnapshot in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to cause denial of service or run arbitrary code as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16736</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	Use of default credentials for the TELNET server in Petwant PF-103 firmware 4.3.2.50 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16734</a> <a href="#">MISC</a>
puppet -- mcollective	mcollective has a default password set at install	2019-12-13	<a href="#">7.5</a>	<a href="#">CVE-2014-0175</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
python-requests-kerberos -- python-requests-kerberos	python-requests-Kerberos through 0.5 does not handle mutual authentication	2019-12-15	<a href="#">7.5</a>	<a href="#">CVE-2014-8650</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial			

qualcomm -- multiple_snapdragon_products	IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2019-12-18	7.5	<a href="#">CVE-2019-10614</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24	2019-12-18	7.2	<a href="#">CVE-2019-10605</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2019-2304</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074,	2019-12-18	7.2	<a href="#">CVE-2019-10601</a> <a href="#">CONFIRM</a>

	MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150			
qualcomm -- multiple_snapdragon_products	When a fake broadcast/multicast 11w rmf without mmie received, since no proper length check in wma_process_bip, buffer overflow will happen in both cds_is_mmie_valid and qdf_nbuf_trim_tail in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8937, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDM630, SDM636, SDM660, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2018-11980</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2019-10480</a> <a href="#">CONFIRM</a>
	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon			

qualcomm -- multiple_snapdragon_products	Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130	2019-12-18	10	<a href="#">CVE-2019-2242</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2019-2274</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917,	2019-12-18	7.2	<a href="#">CVE-2019-10607</a> <a href="#">CONFIRM</a>



	MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130			
qualcomm -- multiple_snapdragon_products	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2019-10598</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24	2019-12-18	7.2	<a href="#">CVE-2019-10595</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150,	2019-12-	7.2	<a href="#">CVE-2019-10600</a>

	MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	18		<a href="#">CONFIRM</a>
red_hat -- edeploy	eDeploy has tmp file race condition flaws	2019-12-15	<a href="#">9.3</a>	<a href="#">CVE-2014-3701</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- edeploy	eDeploy has RCE via cPickle deserialization of untrusted data	2019-12-15	<a href="#">7.5</a>	<a href="#">CVE-2014-3699</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
xfig -- fig2dev	read_colordef in read.c in Xfig fig2dev 3.2.7b has an out-of-bounds write.	2019-12-15	<a href="#">7.5</a>	<a href="#">CVE-2019-19797</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- incubator_superset	In Apache Incubator Superset before 0.31 user could query database metadata information from a database he has no access to, by using a specially crafted complex query.	2019-12-16	<a href="#">5</a>	<a href="#">CVE-2019-12413</a> <a href="#">MISC</a>
apache -- incubator_superset	In Apache Incubator Superset before 0.32, a user can view database names that he has no access to on a dropdown list in SQLLab	2019-12-16	<a href="#">5</a>	<a href="#">CVE-2019-12414</a> <a href="#">MISC</a>
apple -- ios	A logic issue was addressed with improved state management. This issue is fixed in iOS 13. Visiting a malicious website may lead to address bar spoofing.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8727</a> <a href="#">MISC</a>
apple -- ios	A user privacy issue was addressed by removing the broadcast MAC address. This issue is fixed in iOS 12.2. A device may be passively tracked by its WiFi MAC	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8567</a> <a href="#">MISC</a>

	address.			
apple -- ios	A permissions issue existed in which execute permission was incorrectly granted. This issue was addressed with improved permission validation. This issue is fixed in iOS 13. Processing a maliciously crafted file may disclose user information.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8731</a> <a href="#">MISC</a>
apple -- ios	A logic issue existed with the display of notification previews. This issue was addressed with improved validation. This issue is fixed in iOS 13. Notification previews may show on Bluetooth accessories even when previews are disabled.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8711</a> <a href="#">MISC</a>
apple -- ios	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 12.3. A sandboxed process may be able to circumvent sandbox restrictions.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8617</a> <a href="#">MISC</a>
apple -- ios	A permissions issue existed in the handling of motion and orientation data. This issue was addressed with improved restrictions. This issue is fixed in iOS 12.2. A website may be able to access sensor information without user consent.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8554</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6. A remote attacker may be able to leak memory.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8663</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_safari	A logic issue was addressed with improved state management. This issue is fixed in iOS 13, Safari 13. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8674</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_tvos	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in iOS 12.4, tvOS 12.4. A malicious application may be able to restrict access to websites.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8698</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_watchos	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.4, watchOS 5.3. A remote attacker may cause an unexpected application termination.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8665</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_watchos	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, watchOS 5.2.1. Processing a maliciously crafted message	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8626</a> <a href="#">MISC</a> <a href="#">MISC</a>

	may lead to a denial of service.			
apple -- macos_catalina	"Clear History and Website Data" did not clear the history. The issue was addressed with improved data deletion. This issue is fixed in macOS Catalina 10.15. A user may be unable to delete browsing history items.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8768</a> <a href="#">MISC</a>
apple -- macos_catalina	The issue was addressed with improved permissions logic. This issue is fixed in macOS Catalina 10.15. A malicious application may be able to access recent documents.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8770</a> <a href="#">MISC</a>
apple -- macos_catalina	An issue existed in the handling of links in encrypted PDFs. This issue was addressed by adding a confirmation prompt. This issue is fixed in macOS Catalina 10.15. An attacker may be able to exfiltrate the contents of an encrypted PDF.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8772</a> <a href="#">MISC</a>
apple -- macos_catalina_and_tvos	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15, tvOS 13. Processing a maliciously crafted movie may result in the disclosure of process memory.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8705</a> <a href="#">MISC</a>
apple -- macos_mojave	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.6. The encryption status of a Time Machine backup may be incorrect.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8667</a> <a href="#">MISC</a>
apple -- macos_mojave	This issue was addressed with improved handling of file metadata. This issue is fixed in macOS Mojave 10.14.4. A malicious application may bypass Gatekeeper checks.	2019-12-18	<a href="#">4.6</a>	<a href="#">CVE-2019-6239</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.5. An application may be able to read restricted memory.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8603</a> <a href="#">MISC</a>
apple -- macos_mojave	An authentication issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.5. A user may be unexpectedly logged in to another user's account.	2019-12-18	<a href="#">6.5</a>	<a href="#">CVE-2019-8634</a> <a href="#">MISC</a>
apple -- macos_mojave	A logic issue was addressed with improved validation. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to elevate privileges.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8561</a> <a href="#">MISC</a>

apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8693</a> <a href="#">MISC</a>
apple -- macos_mojave	This issue was addressed with improved checks. This issue is fixed in macOS Mojave 10.14.5. A malicious application may bypass Gatekeeper checks.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8589</a> <a href="#">MISC</a>
apple -- macos_mojave_and_safari	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.6, Safari 12.1.2. Visiting a malicious website may lead to address bar spoofing.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8670</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8690</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A remote attacker may be able to leak memory.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8787</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8822</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8821</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2			<a href="#">CVE-2019-8820</a> <a href="#">MISC</a>



apple -- multiple_products	and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8819</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8812</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8678</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to cause unexpected system termination or read kernel memory.	2019-12-18	<a href="#">6.6</a>	<a href="#">CVE-2019-8576</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8763</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8625</a> <a href="#">MISC</a>

	for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting.			<a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted memory.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8598</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8597</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8735</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple --	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari	2019-12-		<a href="#">CVE-2019-8596</a> <a href="#">MISC</a> <a href="#">MISC</a>

multiple_products	12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	18	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8563</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8686</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8649</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8811</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to leak memory.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8646</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A user privacy issue was addressed by removing the broadcast MAC address. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A device may be passively tracked by its WiFi MAC	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8620</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	address.			
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8609</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8594</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8687</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to read restricted memory.	2019-12-18	4.3	<a href="#">CVE-2019-8560</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8823</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. Parsing a maliciously crafted office document may lead to an unexpected application termination or arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8657</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were			<a href="#">CVE-2019-8586</a>

apple -- multiple_products	addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8615</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8584</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8673</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows. A sandboxed process may be able to circumvent sandbox restrictions.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8562</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8608</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2,			<a href="#">CVE-2019-8559</a> <a href="#">MISC</a>



apple -- multiple_products	tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8558</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8556</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2. Clicking a malicious SMS link may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8553</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8571</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8813</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8719</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were addressed with improved memory			<a href="#">CVE-2019-8601</a>

apple -- multiple_products	handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8622</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8681</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8623</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8677</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously	2019-12-18	6.8	<a href="#">CVE-2019-8611</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	crafted web content may lead to arbitrary code execution.			MISC MISC MISC
apple -- multiple_products	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges.	2019-12-18	6.8	CVE-2019-8577 MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	CVE-2019-8683 MISC MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	CVE-2019-8610 MISC MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	CVE-2019-8680 MISC MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	CVE-2019-8628 MISC MISC MISC MISC MISC MISC MISC
	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4,			CVE-2019-8644 MISC

apple -- multiple_products	macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. Processing a maliciously crafted movie file may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8585</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8671</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8679</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8666</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- safari	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in Safari 13.0.1. Visiting a malicious website may lead to user interface spoofing.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8654</a> <a href="#">MISC</a>
apple -- safari	The issue was addressed with improved handling of service worker lifetime. This issue is fixed in Safari 13.0.1. Service workers may leak private browsing history.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8725</a> <a href="#">MISC</a>
apple -- watchos	This issue was addressed with improved checks. This issue is fixed in watchOS 5.3. Users removed from an iMessage	2019-12-	<a href="#">5</a>	<a href="#">CVE-2019-8659</a>

	conversation may still be able to alter state.	18		<a href="#">MISC</a>
apple -- watchos	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 5.3. A remote attacker may be able to leak memory.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8624</a> <a href="#">MISC</a>
apple -- watchos	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8765</a> <a href="#">MISC</a>
apple -- watchos	A logic issue was addressed with improved state management. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8764</a> <a href="#">MISC</a>
apple -- watchos	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8743</a> <a href="#">MISC</a>
apple -- watchos_and_icloud_for_windows	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8766</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira	The WorkflowResource class removeStatus method in Jira before version 7.13.12, from version 8.0.0 before version 8.4.3, and from version 8.5.0 before version 8.5.2 allows authenticated remote attackers who do not have project administration access to remove a configured issue status from a project via a missing authorisation check.	2019-12-18	<a href="#">4</a>	<a href="#">CVE-2019-15013</a> <a href="#">MISC</a>
atlassian -- multiple_products	An issue was discovered in the SAML Single Sign On (SSO) plugin for several Atlassian products affecting versions 3.1.0 through 3.2.2 for Jira and Confluence, versions 2.4.0 through 3.0.3 for Bitbucket, and versions 2.4.0 through 2.5.2 for Bamboo. It allows locally disabled users to reactivate their accounts just by browsing the affected Jira/Confluence/Bitbucket/Bamboo instance, even when the applicable configuration option of the plugin has been disabled ("Reactivate inactive	2019-12-13	<a href="#">6</a>	<a href="#">CVE-2019-13347</a> <a href="#">MISC</a> <a href="#">MISC</a>





dovecot -- dovecot	In Dovecot before 2.3.9.2, an attacker can crash a push-notification driver with a crafted email when push notifications are used, because of a NULL Pointer Dereference. The email must use a group address as either the sender or the recipient.	2019-12-13	5	<a href="#">CVE-2019-19722</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
duplicity -- duplicity	duplicity 0.6.24 has improper verification of SSL certificates	2019-12-13	5	<a href="#">CVE-2014-3495</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below is affected by an information disclosure vulnerability. A remote unauthenticated attacker can recover a user's password hash by sending a crafted HTTP POST request.	2019-12-17	5	<a href="#">CVE-2019-3993</a> <a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below is affected by a denial of service vulnerability due to a use after free. A remote unauthenticated attacker can crash the ELOG server by sending multiple HTTP POST requests which causes the ELOG function retrieve_url() to use a freed variable.	2019-12-17	5	<a href="#">CVE-2019-3994</a> <a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below is affected by a denial of service vulnerability due to a NULL pointer dereference. A remote unauthenticated attacker can crash the ELOG server by sending a crafted HTTP GET request.	2019-12-17	5	<a href="#">CVE-2019-3995</a> <a href="#">MISC</a>
elog-- elog	ELOG 3.1.4-57bea22 and below is affected by an information disclosure vulnerability. A remote unauthenticated attacker can access the server's configuration file by sending an HTTP GET request. Amongst the configuration data, the attacker may gain access to valid admin usernames and, in older versions of ELOG, passwords.	2019-12-17	5	<a href="#">CVE-2019-3992</a> <a href="#">MISC</a>
envoy_proxy -- envoy	An issue was discovered in Envoy 1.12.0. Upon receipt of a malformed HTTP request without a Host header, it sends an internally generated "Invalid request" response. This internally generated response is dispatched through the configured encoder filter chain before being sent to the client. An encoder filter that invokes route manager APIs that access a request's Host header causes a	2019-12-13	5	<a href="#">CVE-2019-18838</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	NULL pointer dereference, resulting in abnormal termination of the Envoy process.			
huawei -- campusinsight	There is an out-of-bounds read vulnerability in the Advanced Packages feature of the Gauss100 OLTP database in CampusInsight before V100R019C00SPC200. Attackers who gain the specific permission can use this vulnerability by sending elaborate SQL statements to the database. Successful exploit of this vulnerability may cause the database to crash.	2019-12-13	<a href="#">4</a>	<a href="#">CVE-2019-5278</a> <a href="#">MISC</a>
huawei -- cloudengine	CloudEngine 12800 has a DoS vulnerability. An attacker of a neighboring device sends a large number of specific packets. As a result, a memory leak occurs after the device uses the specific packet. As a result, the attacker can exploit this vulnerability to cause DoS attacks on the target device.	2019-12-13	<a href="#">6.1</a>	<a href="#">CVE-2019-5248</a> <a href="#">MISC</a>
huawei -- cloudusm-eua_product	Huawei CloudUSM-EUA V600R006C10;V600R019C00 have an information leak vulnerability. Due to improper configuration, the attacker may cause information leak by successful exploitation.	2019-12-13	<a href="#">5</a>	<a href="#">CVE-2019-5277</a> <a href="#">MISC</a>
huawei -- mate_20_pro_smartphones	Mate 20 Pro smartphones with versions earlier than 9.1.0.135(C00E133R3P1) have an improper authorization vulnerability. The software does not properly restrict certain operation of certain privilege, the attacker could trick the user into installing a malicious application before the user turns on student mode function. Successful exploit could allow the attacker to bypass the limit of student mode function.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-5250</a> <a href="#">MISC</a>
huawei -- multiple_products	There is a weak algorithm vulnerability in some Huawei products. The affected products use weak algorithms by default. Attackers may exploit the vulnerability to cause information leaks.	2019-12-13	<a href="#">5</a>	<a href="#">CVE-2019-19397</a> <a href="#">MISC</a>
huawei -- multiple_products	Some Huawei products have an insufficient verification of data authenticity vulnerability. A remote, unauthenticated attacker has to intercept specific packets between two devices, modify the packets, and send the modified packets to the peer device. Due to insufficient verification of some fields in the packets, an attacker may exploit the vulnerability to cause the	2019-12-13	<a href="#">4.3</a>	<a href="#">CVE-2019-5291</a> <a href="#">MISC</a>

	target device to be abnormal.			
huawei -- multiple_products	Certain Huawei products (AP2000;IPS Module;NGFW Module;NIP6300;NIP6600;NIP6800;S5700;SVN5600;SVN5800;SVN5800-C;SeMG9811;Secospace AntiDDoS8000;Secospace USG6300;Secospace USG6500;Secospace USG6600;USG6000V;eSpace U1981) have an out-of-bounds read vulnerability. An attacker who logs in to the board may send crafted messages from the internal network port or tamper with inter-process message packets to exploit this vulnerability. Due to insufficient validation of the message, successful exploit may cause the affected board to be abnormal.	2019-12-13	5	<a href="#">CVE-2019-5254</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	There is a path traversal vulnerability in several Huawei smartphones. The system does not sufficiently validate certain pathnames from the application. An attacker could trick the user into installing, backing up and restoring a malicious application. Successful exploit could cause information disclosure.	2019-12-13	4.3	<a href="#">CVE-2019-5251</a> <a href="#">MISC</a>
huawei -- s5700_and_s6700_devices	Huawei S5700 and S6700 have a DoS security vulnerability. Attackers with certain permissions perform specific operations on affected devices. Because the pointer in the program is not processed properly, the vulnerability can be exploited to cause the device to be abnormal.	2019-12-13	4	<a href="#">CVE-2019-5290</a> <a href="#">MISC</a>
huawei -- y9_2019_and_honor_v	Huawei smartphones HUAWEI Y9 2019 and Honor View 20 have a denial of service vulnerability. Due to insufficient input validation of specific value when parsing the messages, an attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices to exploit this vulnerability. Successful exploit may cause an infinite loop and the device to reboot.	2019-12-13	6.1	<a href="#">CVE-2019-5260</a> <a href="#">MISC</a>
ibm -- api_connect	IBM API Connect 2018.4.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 168510.	2019-12-18	5	<a href="#">CVE-2019-4609</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm --	IBM Financial Transaction Manager 3.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed			<a href="#">CVE-2019-</a>

financial_transaction_manager	arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 172882.	2019-12-20	4.3	<a href="#">4744</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- financial_transaction_manager	IBM Financial Transaction Manager 3.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 172880.	2019-12-20	4.3	<a href="#">CVE-2019-4743</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- mq_and_mq_appliance	IBM MQ and IBM MQ Appliance 9.1 CD, 9.1 LTS, 9.0 LTS, and 8.0 is vulnerable to a denial of service attack caused by channels processing poorly formatted messages. IBM X-Force ID: 166357.	2019-12-16	4	<a href="#">CVE-2019-4560</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	imagemagick 6.8.9.6 has remote DOS via infinite loop	2019-12-15	4.3	<a href="#">CVE-2014-8561</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
intel -- control_center-i	Unquoted service path in Control Center-I version 2.1.0.0 and earlier may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	4.6	<a href="#">CVE-2019-14599</a> <a href="#">MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Alauda DevOps Pipeline Plugin 2.3.2 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-12-17	4	<a href="#">CVE-2019-16574</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Team Concert Plugin 1.3.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-12-17	6.8	<a href="#">CVE-2019-16565</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Team Concert Plugin 1.3.0 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2019-12-17	4	<a href="#">CVE-2019-16567</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>



jenkins -- jenkins	A missing permission check in Jenkins RapidDeploy Plugin 4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified web server.	2019-12-17	4	<a href="#">CVE-2019-16571</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins WebSphere Deployer Plugin 1.6.1 and earlier allows users with Overall/Read access to disable SSL/TLS certificate and hostname validation for the entire Jenkins master JVM.	2019-12-17	5.5	<a href="#">CVE-2019-16561</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Alauda DevOps Pipeline Plugin 2.3.2 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-12-17	6.8	<a href="#">CVE-2019-16573</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins SCTMExecutor Plugin 2.2 and earlier transmits previously configured service credentials in plain text as part of the global configuration, as well as individual jobs' configurations.	2019-12-17	5	<a href="#">CVE-2019-16568</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Mantis Plugin 0.26 and earlier allows attackers to connect to an attacker-specified web server using attacker-specified credentials.	2019-12-17	4.3	<a href="#">CVE-2019-16569</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Alauda Kubernetes Suport Plugin 2.3.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing the Kubernetes service account token or credentials stored in Jenkins.	2019-12-17	4	<a href="#">CVE-2019-16576</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Alauda Kubernetes Suport Plugin 2.3.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing the Kubernetes service account token or credentials stored in Jenkins.	2019-12-17	6.8	<a href="#">CVE-2019-16575</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Team Concert Plugin 1.3.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-12-17	4	<a href="#">CVE-2019-16566</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins RapidDeploy Plugin 4.1 and earlier allows attackers to connect to an attacker-specified web server.	2019-12-17	<a href="#">6.8</a>	<a href="#">CVE-2019-16570</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jersey -- jersey	jersey: XXE via parameter entities not disabled by the jersey SAX parser	2019-12-15	<a href="#">5</a>	<a href="#">CVE-2014-3643</a> <a href="#">REDHAT</a> <a href="#">MISC</a>
joomla -- joomla!	In Joomla! before 3.9.14, a missing access check in framework files could lead to a path disclosure.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-19845</a> <a href="#">MISC</a>
knot-resolver -- knot-resolver	knot-resolver before version 4.3.0 is vulnerable to denial of service through high CPU utilization. DNS replies with very many resource records might be processed very inefficiently, in extreme cases taking even several CPU seconds for each such uncached message. For example, a few thousand A records can be squashed into one DNS message (limit is 64kB).	2019-12-16	<a href="#">5</a>	<a href="#">CVE-2019-19331</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libsixel_project -- libsixel	stb_image.h (aka the stb image loader) 2.23, as used in libsixel and other products, has a heap-based buffer over-read in stbi__load_main.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-19777</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An issue was discovered in libsixel 1.8.2. There is a heap-based buffer over-read in the function load_sixel at loader.c.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-19778</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.3.11, sound/core/timer.c has a use-after-free caused by erroneous code refactoring, aka CID-e7af6307a8a5. This is related to snd_timer_open and snd_timer_close_locked. The timeri variable was originally intended to be for a newly created timer instance, but was used for a different purpose after refactoring.	2019-12-15	<a href="#">4.9</a>	<a href="#">CVE-2019-19807</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.4.2, the io_uring feature leads to requests that inadvertently have UID 0 and full capabilities, aka CID-181e448d8709. This is related to fs/io-wq.c, fs/io_uring.c, and net/socket.c. For example, an attacker can bypass intended restrictions on adding an IPv4 address to the loopback interface. This occurs because IORING_OP_SENDMSG operations, although requested in the context of an unprivileged user, are sometimes performed by a kernel worker thread without considering that context.	2019-12-17	<a href="#">4.6</a>	<a href="#">CVE-2019-19241</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

lout -- lout	Lout 3.40 has a heap-based buffer overflow in the srcnext() function in z02.c.	2019-12-20	6.8	<a href="#">CVE-2019-19918</a> <a href="#">MISC</a>
lout -- lout	Lout 3.40 has a buffer overflow in the StringQuotedWord() function in z39.c.	2019-12-20	6.8	<a href="#">CVE-2019-19917</a> <a href="#">MISC</a>
mahara -- mahara	Multiple cross-site scripting (XSS) vulnerabilities in Mahara 1.4.x before 1.4.3 and 1.5.x before 1.5.2 allow remote attackers to inject arbitrary web script or HTML via vectors related to (1) javascript innerHTML as used when generating login forms, (2) links or (3) resources URLs, and (4) the Display name in a user profile.	2019-12-17	4.3	<a href="#">CVE-2012-2237</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
micro_focus -- arcsight_logger	Cross-Site Request Forgery vulnerability in all Micro Focus ArcSight Logger affecting all product versions below version 7.0. The vulnerability could be exploited to perform CSRF attack.	2019-12-17	6.8	<a href="#">CVE-2019-11657</a> <a href="#">MISC</a>
nitro -- nitro_free_pdf_reader	The JBIG2Decode library in npdf.dll in Nitro Free PDF Reader 12.0.0.112 has a CAPPDAnnotHandlerUtils::PDAnnotHandlerDestroyData Out-of-Bounds Read via crafted Unicode content.	2019-12-16	4.3	<a href="#">CVE-2019-19818</a> <a href="#">MISC</a> <a href="#">MISC</a>
npm -- cli	Versions of the npm CLI prior to 6.13.3 are vulnerable to an Arbitrary File Write. It fails to prevent access to folders outside of the intended node_modules folder through the bin field. A properly constructed entry in the package.json bin field would allow a package publisher to modify and/or gain access to arbitrary files on a user's system when the package is installed. This behavior is still possible through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option.	2019-12-13	5.5	<a href="#">CVE-2019-16776</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
npm -- cli	Versions of the npm CLI prior to 6.13.3 are vulnerable to an Arbitrary File Write. It is possible for packages to create symlinks to files outside of the node_modules folder through the bin field upon installation. A properly constructed entry in the package.json bin field would allow a package publisher to create a symlink pointing to arbitrary files on a user's system when the package is installed. This behavior is still possible through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option.	2019-12-13	4	<a href="#">CVE-2019-16775</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

npm -- cli	<p>Versions of the npm CLI prior to 6.13.4 are vulnerable to an Arbitrary File Overwrite. It fails to prevent existing globally-installed binaries to be overwritten by other package installations. For example, if a package was installed globally and created a serve binary, any subsequent installs of packages that also create a serve binary would overwrite the previous serve binary. This behavior is still allowed in local installations and also through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option.</p>	2019-12-13	5.5	<a href="#">CVE-2019-16777</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
owncloud -- owncloud	<p>Cross-site scripting (XSS) vulnerability in ownCloud 4.5.5, 4.0.10, and earlier allows remote attackers to inject arbitrary web script or HTML via the action parameter to core/ajax/sharing.php.</p>	2019-12-17	4.3	<a href="#">CVE-2013-0202</a> <a href="#">MISC</a> <a href="#">MISC</a>
pen -- pen	<p>Pen 0.18.0 has Insecure Temporary File Creation vulnerabilities</p>	2019-12-13	4.6	<a href="#">CVE-2014-2387</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
petwant_and_skymee -- pf-103_and_petalk_ai	<p>The udpServerSys service in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to initiate firmware upgrades and alter device settings.</p>	2019-12-13	5	<a href="#">CVE-2019-16731</a> <a href="#">MISC</a>
puppet -- puppet_agent	<p>Previous versions of Puppet Agent didn't verify the peer in the SSL connection prior to downloading the CRL. This issue is resolved in Puppet Agent 6.4.0.</p>	2019-12-16	5	<a href="#">CVE-2018-11751</a> <a href="#">MISC</a>
qpid-cpp -- qpid-cpp	<p>qpid-cpp: ACL policies only loaded if the acl-file option specified enabling DoS by consuming all available file descriptors</p>	2019-12-13	5	<a href="#">CVE-2014-0212</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qualcomm --	<p>Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,</p>			<a href="#">CVE-2019-</a>

multiple_snapdragon_products	APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2019-12-18	<a href="#">4.6</a>	<a href="#">10584</a> <a href="#">CONFIRM</a>
red_hat -- cloudforms_management_engine	CFME: CSRF protection vulnerability via permissive check of the referrer header	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2014-0197</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_keycloak	JBoss KeyCloak: Open redirect vulnerability via failure to validate the redirect URL.	2019-12-15	<a href="#">5.8</a>	<a href="#">CVE-2014-3652</a> <a href="#">MISC</a> <a href="#">MISC</a>
samurai -- samurai	samurai 0.7 has a heap-based buffer overflow in canonpath in util.c via a crafted build file.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-19795</a> <a href="#">MISC</a>
sap -- treasury_and_risk_management	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-12-17	<a href="#">6.5</a>	<a href="#">CVE-2019-0383</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- treasury_and_risk_management	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for functionalities that require user identity.	2019-12-17	<a href="#">6.5</a>	<a href="#">CVE-2019-0384</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
solarwinds -- serv-u_ftp_server	A CSV injection vulnerability exists in the web UI of SolarWinds Serv-U FTP Server v15.1.7.	2019-12-16	<a href="#">4</a>	<a href="#">CVE-2019-13181</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
sonicwall -- sma100_devices	Vulnerability in SonicWall SMA100 allow unauthenticated user to gain read-only access to unauthorized resources. This vulnerability impacted SMA100 version 9.0.0.3 and earlier.	2019-12-17	<a href="#">5</a>	<a href="#">CVE-2019-7481</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2019-</a>



spip -- spip	_core_/plugins/medias in SPIP 3.2.x before 3.2.7 allows remote authenticated authors to inject content into the database.	2019-12-17	4	<a href="#">19830 MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
sqlite -- sqlite	exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because constant integer values in ORDER BY clauses of window definitions are mishandled.	2019-12-18	5	<a href="#">CVE-2019-19880</a> <a href="#">MISC</a>
suphp -- suphp	suPHP before 0.7.2 source-highlighting feature allows security bypass which could lead to arbitrary code execution	2019-12-13	4.4	<a href="#">CVE-2014-1867</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tematres -- tematres	TemaTres 3.0 has reflected XSS via the replace_string or search_string parameter to the vocab/admin.php?doAdmin=bulkReplace URI.	2019-12-13	4.3	<a href="#">CVE-2019-14344</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco -- spotfire_analytics_platform	The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker to perform a reflected cross-site scripting (XSS) attack. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0.	2019-12-17	4.3	<a href="#">CVE-2019-17337</a> <a href="#">MISC</a> <a href="#">MISC</a>
typo3 -- typo3	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. Because escaping of user-submitted content is mishandled, the class QueryGenerator is vulnerable to SQL injection. Exploitation requires having the system extension ext:lowlevel installed, and a valid backend user who has administrator privileges.	2019-12-17	6.5	<a href="#">CVE-2019-19850</a> <a href="#">MISC</a> <a href="#">MISC</a>
veracrypt -- veracrypt	VeraCrypt 1.24 allows Local Privilege Escalation during execution of VeraCryptExpander.exe.	2019-12-13	4.6	<a href="#">CVE-2019-19501</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The quiz-master-next (aka Quiz And Survey Master) plugin before 6.3.5 for WordPress is affected by: Cross Site			

wordpress -- wordpress	Scripting (XSS). The impact is: Allows an attacker to execute arbitrary HTML and JavaScript code via the from or till parameter (and/or the quiz_id parameter). The component is: admin/quiz-options-page.php. The attack vector is: When the Administrator is logged in, a reflected XSS may execute upon a click on a malicious URL.	2019-12-13	4.3	<a href="#">CVE-2019-17599</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
yabasic -- yabasic	Yabasic 2.86.2 has a heap-based buffer overflow in myformat in function.c via a crafted BASIC source file.	2019-12-13	6.8	<a href="#">CVE-2019-19796</a> <a href="#">MISC</a>
zend_framework -- zend_framework	ZF2014-03 has a potential cross site scripting vector in multiple view helpers	2019-12-15	4.3	<a href="#">CVE-2014-4913</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zulip -- zulip_server	The image thumbnailing handler in Zulip Server versions 1.9.0 to before 2.0.8 allowed an open redirect that was visible to logged-in users.	2019-12-18	5.8	<a href="#">CVE-2019-19775</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
altn -- mdaemon_email_server	MDaemon Email Server 17.5.1 allows XSS via the filename of an attachment to an email message.	2019-12-17	3.5	<a href="#">CVE-2019-19497</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 12.3. A person with physical access to an iOS device may be able to see the email address used for iTunes.	2019-12-18	2.1	<a href="#">CVE-2019-8599</a> <a href="#">MISC</a>
apple -- ios	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 13. A person with physical access to an iOS device may be able to access contacts from the lock screen.	2019-12-18	2.1	<a href="#">CVE-2019-8742</a> <a href="#">MISC</a>
apple -- ios_and_watchos	The issue was addressed with improved UI handling. This issue is fixed in iOS 12.4, watchOS 5.3. A user may inadvertently complete an in-app purchase while on the lock screen.	2019-12-18	2.1	<a href="#">CVE-2019-8682</a> <a href="#">MISC</a> <a href="#">MISC</a>

apple -- macos_mojave	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.4. Processing malicious data may lead to unexpected application termination.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8507</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8691</a> <a href="#">MISC</a>
apple -- macos_mojave	An access issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.4. A local user may be able to view a user's locked notes.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8537</a> <a href="#">MISC</a>
apple -- macos_mojave	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to read restricted memory.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8520</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8692</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to modify protected parts of the file system.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8568</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8510</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-6207</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- tvos	An authentication issue was addressed with improved state management. This	2019-12-	<a href="#">2.1</a>	<a href="#">CVE-2019-8704</a>

	issue is fixed in tvOS 13. A local user may be able to leak sensitive user information.	18		<a href="#">MISC</a> <a href="#">MISC</a>
hammer_cli_foreman_gems -- hammer_cli_foreman_gems	ruby foreman on rails foreman: File /etc/hammer/cli.modules.d/foreman.yml world-readable on rails	2019-12-13	<a href="#">2.1</a>	<a href="#">CVE-2014-0241</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- api_connect	IBM API Connect 2018.1 through 2018.4.1.7 Developer Portal's user registration page does not disable password autocomplete. An attacker with access to the browser instance and local system credentials can steal the credentials used for registration. IBM X-Force ID: 163453.	2019-12-16	<a href="#">2.1</a>	<a href="#">CVE-2019-4444</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- case_builder_and_case_manager	The Case Builder component shipped with 18.0.0.1 through 19.0.0.2 and IBM Case Manager 5.1.1 through 5.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 162772.	2019-12-13	<a href="#">3.5</a>	<a href="#">CVE-2019-4426</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins buildgraph-view Plugin 1.8 and earlier does not escape the description of builds shown in its view, resulting in a stored XSS vulnerability exploitable by users able to change build descriptions.	2019-12-17	<a href="#">3.5</a>	<a href="#">CVE-2019-16562</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Weibo Plugin 1.0.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2019-12-17	<a href="#">2.1</a>	<a href="#">CVE-2019-16572</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Pipeline Aggregator View Plugin 1.8 and earlier does not escape information shown on its view, resulting in a stored XSS vulnerability exploitable by attackers able to affects view content such as job display name or pipeline stage names.	2019-12-17	<a href="#">3.5</a>	<a href="#">CVE-2019-16564</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Mission Control Plugin 0.9.16 and earlier does not escape job display names and build names shown on its view, resulting in a stored XSS vulnerability exploitable by attackers able to change these properties.	2019-12-17	<a href="#">3.5</a>	<a href="#">CVE-2019-16563</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
red_hat -- cloudforms_management	CFME (CloudForms Management Engine) 5: RHN account information is logged to /var/log/foreman/foreman.log during	2019-12-15	<a href="#">2.1</a>	<a href="#">CVE-2014-3536</a> <a href="#">MISC</a>

	registration			MISC
solarwinds -- serv-u_ftp_server	A stored cross-site scripting (XSS) vulnerability exists in the web UI of SolarWinds Serv-U FTP Server 15.1.7.	2019-12-16	3.5	<a href="#">CVE-2019-13182</a> MISC FULLDISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3s-smart - multiple_codesys_products	3S-Smart CODESYS SP Realtime NT before V2.3.7.28, CODESYS Runtime Toolkit 32 bit full before V2.4.7.54 and CODESYS PLCWinNT before V2.4.7.54 allow a NULL pointer dereference.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19789</a> CONFIRM MISC
abb -- pb610_panel_builder_600	The HMISimulator component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier fails to validate the content-length field for HTTP requests, exposing HMISimulator to denial of service via crafted HTTP requests manipulating the content-length setting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18995</a> MISC
	The HMISimulator component of ABB PB610 Panel Builder 600 uses the readFile/writeFile interface to			



abb -- pb610_panel_builder_600	manipulate the work file. Path configuration in PB610 HMISide_600 versions 2.8.0.424 and earlier potentially allows access to files outside of the working directory, thus potentially supporting unauthorized file access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18997</a> <a href="#">MISC</a>
abb -- pb610_panel_builder_600	Due to a lack of file length check, the HMISide component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier crashes when trying to load an empty *.JPR application file. An attacker with access to the file system might be able to cause application malfunction such as denial of service.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18994</a> <a href="#">MISC</a>
abb -- pb610_panel_builder_600	Path settings in HMISide component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier accept DLLs outside of the program directory, potentially allowing an attacker with access to the local file system the execution of code in the application's context.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18996</a> <a href="#">MISC</a>
	In the Quick Access Service			

acer -- quick_access	(QAAAdminAgent.exe) in Acer Quick Access V2.01.3000 through 2.01.3027 and V3.00.3000 through V3.00.3008, a REGULAR user can load an arbitrary unsigned DLL into the signed service's process, which is running as NT AUTHORITY\SYSTEM. This is a DLL Hijacking vulnerability (including search order hijacking, which searches for the missing DLL in the PATH environment variable), which is caused by an uncontrolled search path element for nvapi.dll, atiadlxx.dll, or atiadlxy.dll.	2019- 12- 17	not yet calculated	<a href="#">CVE-2019-18670</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
adobe -- coldfusion	ColdFusion versions Update 6 and earlier have an insecure inherited permissions of default installation directory vulnerability. Successful exploitation could lead to privilege escalation.	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-8256</a> <a href="#">CONFIRM</a>
	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version,	2019-		

adobe -- acrobat_reader	2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	12-19	not yet calculated	<a href="#">CVE-2019-16448 CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16457 CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16464 CONFIRM</a>
	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155			

adobe -- acrobat_reader	and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-16453</a> <a href="#">CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16452</a> <a href="#">CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16449</a> <a href="#">CONFIRM</a>
	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier,			

adobe -- acrobat_and	2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16465</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a binary planting (default folder privilege escalation) vulnerability. Successful exploitation could lead to privilege escalation.	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16444</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16445</a> <a href="#">CONFIRM</a>
	Adobe Acrobat and Reader versions ,			



adobe -- acrobat_and	2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16456 CONFIRM</a>
adobe -- acrobat_and	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16451 CONFIRM</a>
adobe -- acrobat_and	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16450 CONFIRM</a>
	Adobe Acrobat and			

adobe -- acrobat_and_reader	Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16463</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16459</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16461</a> <a href="#">CONFIRM</a>

	disclosure .			
adobe -- acrobat_ and reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16455</a> <a href="#">CONFIRM</a>
adobe -- acrobat_ and reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16454</a> <a href="#">CONFIRM</a>
adobe -- acrobat_ and reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful	2019-12-19	not yet calculated	<a href="#">CVE-2019-16458</a> <a href="#">CONFIRM</a>

	exploitation could lead to information disclosure .			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16462</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16446</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer	2019-12-19	not yet calculated	<a href="#">CVE-2019-16460</a> <a href="#">CONFIRM</a>

	dereference vulnerability. Successful exploitation could lead to arbitrary code execution .			
adobe -- brackets	Brackets versions 1.14 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-8255</a> <a href="#">CONFIRM</a>
adobe -- photoshop CC	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-8253</a> <a href="#">CONFIRM</a>
adobe -- photoshop CC	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-8254</a> <a href="#">CONFIRM</a>
apache -- http_server	A Path traversal exists in http_server which allows an attacker to read arbitrary system files.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15600</a> <a href="#">MISC</a>
	Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute	2019-		



apache -- log4j	arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.	12-20	not yet calculated	<a href="#">CVE-2019-17571</a> <a href="#">CONFIRM</a>
apache -- xerces-c	The Apache Xerces-C 3.0.0 to 3.2.2 XML parser contains a use-after-free error triggered during the scanning of external DTDs. This flaw has not been addressed in the maintained version of the library and has no current mitigation other than to disable DTD processing. This can be accomplished via the DOM using a standard parser feature, or via SAX using the XERCES_DISABLE_DTD environment variable.	2019-12-18	not yet calculated	<a href="#">CVE-2018-1311</a> <a href="#">CONFIRM</a>
apple -- macos_catalina	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Catalina 10.15.1. An application may be able to execute arbitrary code with	2019-12-18	not yet calculated	<a href="#">CVE-2019-8805</a> <a href="#">MISC</a>

	system privileges.			
apple -- macos_catalina	<p>A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Catalina 10.15.1. An application may be able to read restricted memory.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-8817</a> <a href="#">MISC</a>
apple -- macos_catalina	<p>A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with system privileges.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-8701</a> <a href="#">MISC</a>
apple -- icloud_for_windows	<p>Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-8710</a> <a href="#">MISC</a>
apple -- ios	<p>A logic issue existed in the handling of answering phone calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.4. The initiator of a phone call may be able to cause the recipient to answer a simultaneous Walkie-Talkie connection.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-8699</a> <a href="#">MISC</a>

apple -- ios	The issue was addressed with improved UI handling. This issue is fixed in iOS 12.3. The lock screen may show a locked icon after unlocking.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8630 MISC</a>
apple -- ios	This issue was addressed with improved checks. This issue is fixed in iOS 12.2. Processing a maliciously crafted mail message may lead to S/MIME signature spoofing.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7284 MISC</a>
apple -- ios	A consistency issue was addressed with improved state handling. This issue is fixed in iOS 12.2. A website may be able to access the microphone without the microphone use indicator being shown.	2019-12-18	not yet calculated	<a href="#">CVE-2019-6222 MISC</a>
apple -- ios	An API issue existed in the handling of microphone data. This issue was addressed with improved validation. This issue is fixed in iOS 12.2. A malicious application may be able to access the microphone without indication to the user.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8566 MISC</a>
	A memory corruption issue was addressed with improved			

apple -- ios	input validation. This issue is fixed in iOS 12.1.4. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7287</a> <a href="#">MISC</a>
apple -- ios	This issue was addressed with improved transparency. This issue is fixed in iOS 12.2. A user may authorize an enterprise administrator to remotely wipe their device without appropriate disclosure.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8512</a> <a href="#">MISC</a>
apple -- ios	This issue was addressed by improving Face ID machine learning models. This issue is fixed in iOS 13. A 3D model constructed to look like the enrolled user may authenticate via Face ID.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8760</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue applied the incorrect restrictions. This issue was addressed by updating the logic to apply the correct restrictions. This issue is fixed in iOS 13.1.1 and iPadOS 13.1.1. Third party app extensions may not receive the correct sandbox restrictions.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8779</a> <a href="#">MISC</a>
	The issue was addressed by restricting options offered on a locked			

apple -- ios_and_ipados	device. This issue is fixed in iOS 13.1 and iPadOS 13.1. A person with physical access to an iOS device may be able to access contacts from the lock screen.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8775</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A consistency issue existed in deciding when to show the screen recording indicator. The issue was resolved with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2. A local user may be able to record the screen without a visible screen recording indicator.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8793</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An inconsistency in Wi-Fi network configuration settings was addressed. This issue is fixed in iOS 13.2 and iPadOS 13.2. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8804</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the drawing of web page elements. The issue was addressed with improved logic. This issue is fixed in iOS 13.1, iPadOS 13.1, macOS Catalina 10.15. Visiting a maliciously crafted	2019-12-18	not yet calculated	<a href="#">CVE-2019-8769</a> <a href="#">MISC</a>



	website may reveal browsing history.			
apple -- ios_and_ipados_and_macos_catalina	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 12.2, iPadOS 13.2, macOS Catalina 10.15.1. Improper URL processing may lead to data exfiltration.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8788</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_ipados_and_macos_catalina	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Parsing a maliciously crafted iBooks file may lead to disclosure of user information.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8789</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_ipados_and_tvos	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8795</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple --	This issue was addressed with improved checks. This issue is fixed in iOS 12.2, macOS Mojave	2019-12-	not yet calculated	<a href="#">CVE-2019-8521</a> <a href="#">MISC</a>

ios_and_macos_mojave	10.14.4. A malicious application may be able to overwrite arbitrary files.	18		<a href="#">MISC</a>
apple -- ios_and_macos_mojave	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. A local user may be able to read kernel memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8504</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8529</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.4, macOS Mojave 10.14.3 Supplemental Update. An application may be able to gain elevated privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7286</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave_and_tvos	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4,	2019-12-18	not yet calculated	<a href="#">CVE-2019-8546</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	watchOS 5.2. A local user may be able to view sensitive user information.			
apple -- ios_and_macos_mojave_and_tvos	This issue was addressed with improved checks. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. A malicious application may be able to overwrite arbitrary files.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8530</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave_and_watchos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, watchOS 5.2. A malicious application may be able to elevate privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8511</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave_and_watchos	An issue existed in the pausing of FaceTime video. The issue was resolved with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, watchOS 5.2. A user's video may not be paused in a FaceTime call if they exit the FaceTime app while the call is ringing.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8550</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple --	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, Safari 12.1. Enabling the	2019-12-	not yet calculated	<a href="#">CVE-2019-8505</a> <a href="#">MISC</a>

ios_and_safari	Safari Reader feature on a maliciously crafted webpage may lead to universal cross site scripting.	18		<a href="#">MISC</a>
apple -- ios_and_safari	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, Safari 12.1. Enabling the Safari Reader feature on a maliciously crafted webpage may lead to universal cross site scripting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-6204</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_watchos	A privacy issue existed in motion sensor calibration. This issue was addressed with improved motion sensor processing. This issue is fixed in iOS 12.2, watchOS 5.2. A malicious app may be able to track users between installs.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8541</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_catalina	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15. A malicious application may be able to determine kernel memory layout.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8755</a> <a href="#">MISC</a>
apple --	A race condition existed when reading and writing user preferences. This was addressed with improved state handling. This	2019-		<a href="#">CVE-2019-8757</a>

macos_catalina	issue is fixed in macOS Catalina 10.15. The "Share Mac Analytics" setting may not be disabled when a user deselects the switch to share analytics.	12-18	not yet calculated	<a href="#">MISC</a>
apple -- macos_catalina	The contents of locked notes sometimes appeared in search results. This issue was addressed with improved data cleanup. This issue is fixed in macOS Catalina 10.15. A local user may be able to view a user's locked notes.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8730</a> <a href="#">MISC</a>
apple -- macos_catalina_and_itunes_for_windows	A dynamic library loading issue existed in iTunes setup. This was addressed with improved path searching. This issue is fixed in macOS Catalina 10.15.1, iTunes for Windows 12.10.2. Running the iTunes installer in an untrusted directory may result in arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8801</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_mojave	A lock handling issue was addressed with improved lock handling. This issue is fixed in macOS Mojave 10.14.4. A Mac may not lock when disconnecting from an external monitor.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8533</a> <a href="#">MISC</a>
	A logic issue was			



apple -- macos_mojave	addressed with improved state management. This issue is fixed in macOS Mojave 10.14.4. An encrypted volume may be unmounted and remounted by a different user without prompting for the password.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8522</a> <a href="#">MISC</a>
apple -- macos_mojave	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. An application may be able to read restricted memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8519</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Mojave 10.14.5. A local user may be able to load unsigned kernel extensions.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8606</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8540</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted string may lead to a denial of service.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An API issue existed in the handling of dictation requests. This issue was addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to initiate a Dictation request without user authorization.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8502</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A buffer overflow was addressed with improved size			

apple -- multiple_products	validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8527</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted font may result in the disclosure of process memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. An application may be able to gain elevated privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8514</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may be able to cause unexpected system termination	2019-12-18	not yet calculated	<a href="#">CVE-2019-8545</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	or read kernel memory.			
apple -- multiple_products	Multiple input validation issues existed in MIG generated code. These issues were addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may be able to read kernel memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7293</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15, tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing a maliciously crafted text file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8745</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A memory corruption issue			

apple -- multiple_products	was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8535</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8544</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8551</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS Mojave	2019-		<a href="#">CVE-2019-8542</a> <a href="#">MISC</a> <a href="#">MISC</a>



apple -- multiple_products	10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious application may be able to elevate privileges.	12-18	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8726</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8536</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud	2019-12-18	not yet calculated	<a href="#">CVE-2019-8523</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.			<a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8782</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8786</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to elevate privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8552</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

apple -- multiple_products	A cross-origin issue existed with the fetch API. This was addressed with improved input validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may disclose sensitive user information.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8515</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-6201</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed by removing the vulnerable code. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to elevate privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8602</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues			

apple -- multiple_products	were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8518</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8783</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious website may be able to execute scripts in the context of another website.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8503</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An out-of-bounds read was			

apple -- multiple_products	addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8607</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8808</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8785</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An authentication issue was			



apple -- multiple_products	addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 19.0.0, tvOS 13.2, watchOS 6.1. A local attacker may be able to login to the account of a previously logged in user without valid credentials..	2019-12-18	not yet calculated	<a href="#">CVE-2019-8803</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8583</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7285</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory			

apple -- multiple_products	corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8707</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8506</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-6237</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A memory			

apple -- multiple_products	corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8798</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may result in the disclosure of process memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7292</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed			

apple -- multiple_products	in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8733</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8587</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to read restricted memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8794</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS	2019-12-18	not yet calculated	<a href="#">CVE-2019-8797</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges.			
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8784</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- shazam_android_app_and_shazam_ios_app	An injection issue was addressed with improved validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam iOS App Version 12.11.0. Processing a maliciously crafted URL may lead to arbitrary javascript code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8792</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- shazam_android_app_and_shazam_ios_app	An issue existed in the parsing of URL schemes. This issue was addressed with improved URL validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam iOS App Version 12.11.0. Processing a	2019-12-18	not yet calculated	<a href="#">CVE-2019-8791</a> <a href="#">MISC</a> <a href="#">MISC</a>



	maliciously crafted URL may lead to an open redirect.			
apple -- shortcuts_for_ios	An access issue was addressed with additional sandbox restrictions. This issue is fixed in Shortcuts 2.1.3 for iOS. A sandboxed process may be able to circumvent sandbox restrictions.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7290</a> <a href="#">MISC</a>
apple -- shortcuts_for_ios	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in Shortcuts 2.1.3 for iOS. A local user may be able to view sensitive user information.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7289</a> <a href="#">MISC</a>
apple -- swift-nio-ssl	The issue was addressed by signaling that an executable stack is not required. This issue is fixed in SwiftNIO SSL 2.4.1. A SwiftNIO application using TLS may be able to execute arbitrary code.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8849</a> <a href="#">MISC</a>
apple -- texture_for_ios_and_texture_for_android	Some analytics data was sent using HTTP rather than HTTPS. This was addressed by no longer sending this analytics data. This issue is fixed in Texture 5.11.10 for iOS, Texture 4.22.0.4 for Android. An attacker in a privileged network	2019-12-18	not yet calculated	<a href="#">CVE-2019-8632</a> <a href="#">MISC</a> <a href="#">MISC</a>

	position may be able to intercept analytics data.			
apple -- watchos	An issue existed where partially entered passcodes may not clear when the device went to sleep. This issue was addressed by clearing the passcode when a locked device sleeps. This issue is fixed in watchOS 5.2. A partially entered passcode may not clear when the device goes to sleep.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8548</a> <a href="#">MISC</a>
apple -- xcode	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8721</a> <a href="#">MISC</a>
apple -- xcode	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8722</a> <a href="#">MISC</a>
	A memory corruption issue			

apple -- xcode	was addressed with improved validation. This issue is fixed in Xcode 11.2. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8806</a> <a href="#">MISC</a>
apple -- xcode	A memory corruption issue was addressed with improved state management. This issue is fixed in Xcode 11.0. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8738</a> <a href="#">MISC</a>
apple -- xcode	A memory corruption issue was addressed with improved state management. This issue is fixed in Xcode 11.0. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8739</a> <a href="#">MISC</a>
apple -- xcode	A memory corruption issue was addressed with improved validation. This issue is fixed in Xcode 11.2. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8800</a> <a href="#">MISC</a>
	In CloudVision Portal all releases in the 2018.1 and 2018.2 Code train allows users with read-only permissions to			

aristia -- cloudvision	bypass permissions for restricted functionality via CVP API calls through the Configlet Builder modules. This vulnerability can potentially enable authenticated users with read-only access to take actions that are otherwise restricted in the GUI.	2019-12-19	not yet calculated	<a href="#">CVE-2019-18181</a> <a href="#">CONFIRM</a>
aristia -- cloudvision	In CloudVision Portal (CVP) for all releases in the 2018.2 Train, under certain conditions, the application logs user passwords in plain text for certain API calls, potentially leading to user password exposure. This only affects CVP environments where: 1. Devices have enable mode passwords which are different from the user's login password, OR 2. There are configlet builders that use the Device class and specify username and password explicitly Application logs are not accessible or visible from the CVP GUI. Application logs can only be read by authorized users with privileged access to the VM hosting	2019-12-19	not yet calculated	<a href="#">CVE-2019-18615</a> <a href="#">CONFIRM</a>

	the CVP application.			
asus -- atk_package_execution_dot_exe	AsLdrSrv.exe in ASUS ATK Package before V1.0.0061 (for Windows 10 notebook PCs) could lead to unsigned code execution and additional execution. The user must put an application at a particular path, with a particular file name.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19235</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
asus -- hg100_and_ws-101_and_ts-101_devices	An issue was discovered on ASUS HG100 1.05.12, WS-101 1.05.12, and TS-101 1.05.12 devices using ZigBee PRO. Attackers can utilize the "discover ZigBee network procedure" to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15910</a> <a href="#">MISC</a>
asus -- hg100_and_ws-101_and_ts-101_devices	An issue was discovered on ASUS HG100 1.05.12, WS-101 1.05.12, and TS-101 1.05.12 devices using ZigBee PRO. Attackers can use the ZigBee trust center rejoin procedure to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered on ASUS HG100 1.05.12, WS-101 1.05.12, and TS-101 1.05.12			



asus -- hg100_and_ws- 101_and_ts- 101_devices	devices using ZigBee PRO. Because of insecure key transport in ZigBee communication, attackers can obtain sensitive information, cause a denial of service attack, take over smart home devices, and tamper with messages.	2019- 12- 20	not yet calculated	<a href="#">CVE-2019-15911</a> <a href="#">MISC</a>
atlassian - - bitbucket_kopano_group_core	HrAddFBBlock in libfreebusy/freebusyutil.cpp in Kopano Groupware Core before 8.7.7 allows out-of-bounds access as demonstrated by mishandling of an array copy during parsing of ICal data.	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-19907</a> <a href="#">MISC</a> <a href="#">MISC</a>
	There was a man- in-the-middle (MITM) vulnerability present in the Confluence Previews plugin in Confluence Server and Confluence Data Center. This plugin was used to facilitate communication with the Atlassian Companion application. The Confluence Previews plugin in Confluence Server and Confluence Data Center communicated with the Companion application via the atlassian-domain- for-localhost-			

atlassian - confluence	connections-only.com domain name, the DNS A record of which points at 127.0.0.1. Additionally, a signed certificate for the domain was publicly distributed with the Companion application. An attacker in the position to control DNS resolution of their victim could carry out a man-in-the-middle (MITM) attack between Confluence Server and Confluence (or Confluence Data Center) and the atlassian-domain-for-localhost-connections-only.com domain intended to be used with the Companion application. This certificate has been revoked, however, usage of the atlassian-domain-for-localhost-connections-only.com domain name was still present in Confluence Server and Confluence Data Center. An attacker could perform the described attack by denying their victim access to certificate revocation information, and carry out a man-in-the-middle (MITM)	2019-12-10	not yet calculated	<a href="#">CVE-2019-15006</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
---------------------------	---	------------	--------------------	---

	attack to observe files being edited using the Companion application and/or modify them, and access some limited user information.			
atlassian - crowd	Various resources in the Crowd Demo application of Atlassian Crowd before version 3.1.1 allow remote attackers to modify add, modify and delete users & groups via a Cross-site request forgery (CSRF) vulnerability. Please be aware that the Demo application is not enabled by default.	2019-12-17	not yet calculated	<a href="#">CVE-2017-18107</a> <a href="#">MISC</a>
atlassian - jira_application_links	The ListEntityLinksServlet resource in Application Links before version 5.0.12, from version 5.1.0 before version 5.2.11, from version 5.3.0 before version 5.3.7, from version 5.4.0 before 5.4.13, and from version 6.0.0 before 6.0.5 disclosed application link information to non-admin users via a missing permissions check.	2019-12-17	not yet calculated	<a href="#">CVE-2019-15011</a> <a href="#">MISC</a>
	An issue was discovered in Backdrop CMS 1.14.x before 1.14.2. It doesn't			

backdrop -- backdrop_cms	sufficiently filter output when displaying file type descriptions created by administrators. An attacker could potentially craft a specialized description, then have an administrator execute scripting when viewing the list of file types, aka XSS. This vulnerability is mitigated by the fact that an attacker must have a role with the "Administer file types" permission.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19903</a> <a href="#">MISC</a>
backdrop -- backdrop_cms	An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying content type names in the content creation interface. An attacker could potentially craft a specialized content type name, then have an editor execute scripting when creating content, aka XSS. This vulnerability is mitigated by the fact that an attacker must have a role with the "Administer content types" permission.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19900</a> <a href="#">MISC</a>
	An issue was discovered in			

backdrop -- backdrop_	<p>Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying certain block descriptions created by administrators. An attacker could potentially craft a specialized description, then have an administrator execute scripting when configuring a layout, aka XSS. This issue is mitigated by the fact that the attacker would be required to have the permission to create custom blocks, which is typically an administrative task.</p>	2019-12-19	not yet calculated	<a href="#">CVE-2019-19901</a> <a href="#">MISC</a>
backdrop -- backdrop_	<p>An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It allows the upload of entire-site configuration archives through the user interface or command line. It does not sufficiently check uploaded archives for invalid data, allowing non-configuration scripts to potentially be uploaded to the server. This issue is mitigated by the fact that the attacker would be</p>	2019-12-19	not yet calculated	<a href="#">CVE-2019-19902</a> <a href="#">MISC</a>



	required to have the "Synchronize, import, and export configuration" permission, a permission that only trusted administrators should be given. Other measures in the product prevent the execution of PHP scripts, so another server-side scripting language must be accessible on the server to execute code.			
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to the host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18830</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Improper Following of a Certificate's Chain of Trust. The			

barco -- clickshare	embedded 'dongle_bridge' button_r9861500d0 program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain.	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-18826</a> <a href="#">MISC</a>
barco -- clickshare	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This button_r9861500d0 means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware.	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-18827</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via debug button_r9861500d0 interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password.	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-18828</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Barco ClickShare Button R9861500D01 devices before 1.9.0 have			

barco -- clickshare	incorrect Credentials Management. The ClickShare Button implements encryption at rest button_r9861500d0 which uses a one- time programmable (OTP) AES encryption key. This key is shared across all ClickShare Buttons of model R9861500D01.	2019- 12- 17	not yet calculated devices	<a href="#">CVE-2019-18832</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The ClickShare Button does not verify the integrity of the mutable content on the UBIFS partition before being used.	2019- 12- 17	not yet calculated devices	<a href="#">CVE-2019-18824</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information exposure (issue 2 of 2).. The encryption key of the media content which is shared between a ClickShare Button and a ClickShare Button_r9861500d0 randomly generated for each new session and communicated over a TLS connection. An attacker who is able to perform a	2019- 12- 17	not yet calculated devices	<a href="#">CVE-2019-18833</a> <a href="#">MISC</a> <a href="#">MISC</a>

	Man-in-the-Middle attack between the TLS connection, is able to obtain the encryption key.			
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The button, R9861500d01 encrypted ClickShare Button firmware contains the private key of a test device-certificate.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18831</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The Barco signed 'Clickshare_For_Windows.exe' binary on the ClickShare Button (R9861500D01) loads a number of DLL files dynamically without verifying their integrity.	2019-12-17	not yet calculated	<a href="#">CVE-2019-18829</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare 100_devices	Barco ClickShare Huddle CS-100 devices before 1.9.0 and CSE-200 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Base Unit implements encryption at rest using encryption keys which are shared across all ClickShare Base Units of models CS-100 & CSE-	2019-12-17	not yet calculated	<a href="#">CVE-2019-18825</a> <a href="#">MISC</a> <a href="#">MISC</a>

	200.			
beckhoff - - embedded	Beckhoff Embedded Windows PLCs through 3.1.4024.0, and Beckhoff Twincat on Windows Engineering stations, allow an attacker to achieve Remote Code Execution (as SYSTEM) via the Beckhoff ADS protocol.	2019-12-10	not yet calculated	<a href="#">CVE-2019-16871</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
broadcom - ca_client_	An insecure file access vulnerability exists in CA Client Automation 14.0, 14.1, 14.2, and 14.3 Agent for Windows that can allow a local attacker to gain escalated privileges.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19231</a> <a href="#">CONFIRM</a>
cloud_foundry - cloud_controller	Cloud Foundry Cloud Controller API (CAPI), version 1.88.0, allows space developers to list all global service brokers including service broker URLs and GUIDs, which should only be accessible to admins.	2019-12-19	not yet calculated	<a href="#">CVE-2019-11294</a> <a href="#">CONFIRM</a>
contao -- contao	Contao 4.0 through 4.8.5 has Insecure Permissions. Back end users can manipulate the details view URL to show pages and articles that have not been enabled for them.	2019-12-17	not yet calculated	<a href="#">CVE-2019-19712</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	cups (Common			



cups -- cups	Unix Printing System) 'Listen localhost:631' option not honored correctly which could provide unauthorized access to the system	2019-12-20	not yet calculated	<a href="#">CVE-2012-6094</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cyrus -- imap	An issue was discovered in Cyrus IMAP before 2.5.15, 3.0.x before 3.0.13, and 3.1.x through 3.1.8. If sieve script uploading is allowed (3.x) or certain non-default sieve options are enabled (2.x), a user with a mail account on the service can use a sieve script containing a fileinto directive to create any mailbox with administrator privileges, because of folder mishandling in autosieve_createfolder() in imap/lmtp_sieve.c.	2019-12-16	not yet calculated	<a href="#">CVE-2019-19783</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
cyrus -- sasl	cyrus-sasl (aka Cyrus SASL) 2.1.27 has an out-of-bounds write leading to unauthenticated remote denial-of-service in OpenLDAP via a malformed LDAP packet. The OpenLDAP crash is ultimately caused by an off-by-one error in _sasl_add_string in common.c in cyrus-sasl.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19906</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>

d-link -- dir- 615_devices	On D-Link DIR-615 devices, the User Account Configuration page is vulnerable to blind XSS via the name field.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19742</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir- 615_devices	On D-Link DIR-615 devices, a normal user is able to create a root(admin) user from the D-Link portal.	2019-12-16	not yet calculated	<a href="#">CVE-2019-19743</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- rsa_identity	The RSA Identity Governance and Lifecycle and RSA Via Lifecycle and Governance products prior to 7.1.1 P03 contain a Session Fixation vulnerability. An authenticated malicious local user could potentially exploit this vulnerability as the session token is exposed as part of the URL. A remote attacker can gain access to victim's session and perform arbitrary actions with privileges of the user within the compromised session.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18573</a> <a href="#">MISC</a> lifecycle_and_rsa_via_lifecycle_and_governance
	The RSA Identity Governance and Lifecycle and RSA Via Lifecycle and Governance products prior to 7.1.1 P03 contain a reflected cross-site scripting vulnerability in the My Access Live module [MAL]. An authenticated			

dell -- rsa_identity	malicious local user could potentially exploit this vulnerability by sending crafted URL with scripts. When victim users access the module through their browsers, the malicious code gets injected and executed by the web browser in the context of the vulnerable web application.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18571</a> <a href="#">MISC</a> <a href="#">lifecycle_and_rsa_via_lifecycle_and_governance</a>
dell -- rsa_identity	The RSA Identity Governance and Lifecycle and RSA Via Lifecycle and Governance products prior to 7.1.1 P03 contain an Improper Authentication vulnerability. A Java JMX agent running on the remote host is configured with plain text password authentication. An unauthenticated remote attacker can connect to the JMX agent and monitor and manage the Java application.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18572</a> <a href="#">MISC</a> <a href="#">lifecycle_and_rsa_via_lifecycle_and_governance</a>
dell -- xps_13_2-in-1_bios	Settings for the Dell XPS 13 2-in-1 (7390) BIOS versions prior to 1.1.3 contain a configuration vulnerability. The BIOS configuration for the "Enable Thunderbolt (and PCIe behind TBT) pre-boot modules" setting is enabled	2019-12-16	not yet calculated	<a href="#">CVE-2019-18579</a> <a href="#">MISC</a>

	by default. A local unauthenticated attacker with physical access to a user's system can obtain read or write access to main memory via a DMA attack during platform boot.		
divisa_it -- proxia_suite	<p>Divisa Proxia Suite 9 &lt; 9.12.16, 9.11.19, 9.10.26, 9.9.8, 9.8.43 and 9.7.10, 10.0 &lt; 10.0.32, and 10.1 &lt; 10.1.5, SparkSpace 1.0 &lt; 1.0.30, 1.1 &lt; 1.1.2, and 1.2 &lt; 1.2.4, and Proxia PHR 1.0 &lt; 1.0.30 and 1.1 &lt; 1.1.2 allows remote code execution via untrusted Java deserialization. The proxia-error cookie is insecurely deserialized in every request (GET or POST). Thus, an unauthenticated attacker can easily craft a serialized payload in order to execute arbitrary code via the prepareError function in the com.divisait.dv2ee.controller.MVCControllerServlet class of the dv2eemvc.jar component. allows remote code execution via untrusted Java deserialization. The proxia-error cookie is insecurely</p>	2019-12-12, not yet calculated	<a href="#">CVE-2019-18956</a> <a href="#">MISC</a>

	<p>deserialized in every request (GET or POST). Thus, an unauthenticated attacker can easily craft a serialized payload in order to execute arbitrary code via the prepareError function in the com.divisait.dv2ee.controller.MVCCControllerServlet class of the dv2eemvc.jar component. Affected products include Proxia Premium Edition 2017 and Sparkspace.</p>			
django -- django	<p>Django before 1.11.27, 2.x before 2.2.9, and 3.x before 3.0.1 allows account takeover. A suitably crafted email address (that is equal to an existing user's email address after case transformation of Unicode characters) would allow an attacker to be sent a password reset token for the matched user account. (One mitigation in the new releases is to send password reset tokens only to the registered user email address.)</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-19844</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a>
	<p>Docker Engine before 1.8.3 and CS Docker Engine before 1.6.2-CS7 do not use a</p>			<a href="#">CVE-2014-8178</a>



docker -- docker_engine_and_cs_docker_engine	globally unique identifier to store image layers, which makes it easier for attackers to poison the image cache via a crafted image in pull or push commands.	2019-12-17	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
drupal -- drupal	The Views Dynamic Fields module through 7.x-1.0-alpha4 for Drupal makes insecure unserialize calls in handlers/views_handler_filter_dynamic_fields.inc, as demonstrated by PHP object injection, involving a field_names object and an Archive_Tar object, for file deletion. Code execution might also be possible.	2019-12-16	not yet calculated	<a href="#">CVE-2019-19826</a> <a href="#">MISC</a>
eclipse -- che	For Eclipse Che versions 6.16 to 7.3.0, with both authentication and TLS disabled, visiting a malicious web site could trigger the start of an arbitrary Che workspace. Che with no authentication and no TLS is not usually deployed on a public network but is often used for local installations (e.g. on personal laptops). In that case, even if the Che API is not exposed externally, some javascript running	2019-12-19	not yet calculated	<a href="#">CVE-2019-17633</a> <a href="#">CONFIRM</a>

	in the local browser is able to send requests to it.			
ecryptfs -- ecryptfs- utils	ecryptfs-utils: suid helper does not restrict mounting filesystems with nosuid,nodev which creates a possible privilege escalation	2019- 12- 20	not yet calculated	<a href="#">CVE-2012-3409</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- kibana	Kibana versions before 6.8.6 and 7.5.1 contain a cross site scripting (XSS) flaw in the coordinate and region map visualizations. An attacker with the ability to create coordinate map visualizations could create a malicious visualization. If another Kibana user views that visualization or a dashboard containing the visualization it could execute JavaScript in the victim's browser.	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-7621</a> <a href="#">MISC</a> <a href="#">MISC</a>
excon_gem -- excon_gem	In RubyGem excon before 0.71.0, there was a race condition around persistent connections, where a connection which is interrupted (such as by a timeout) would leave data on the socket. Subsequent requests would then read this data, returning content from the previous response. The	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-16779</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	race condition window appears to be short, and it would be difficult to purposefully exploit this.			
ffjpeg --ffjpeg	bitstr_tell at bitstr.c in ffjpeg through 2019-08-21 has a NULL pointer dereference related to jfif_encode.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19887</a> <a href="#">MISC</a>
ffjpeg --ffjpeg	jfif_decode in jfif.c in ffjpeg through 2019-08-21 has a divide-by-zero error.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19888</a> <a href="#">MISC</a>
ge --s2020/s2020g	An issue was found in GE S2020/S2020G Fast Switch 61850, S2020/S2020G Fast Switch 61850 Versions 07A03 and prior. An attacker can inject arbitrary Javascript in a specially crafted HTTP request that may be reflected back in the HTTP response. The device is also vulnerable to a stored cross-site scripting vulnerability that may allow session hijacking, disclosure of sensitive data, cross-site request forgery (CSRF) attacks, and remote code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18267</a> <a href="#">MISC</a>
	An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3,			

git_project - git	v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. Recursive clones are currently affected by a vulnerability that is caused by too-lax validation of submodule names, allowing very targeted attacks via remote code execution in recursive clones.	2019-12-18	not yet calculated	<a href="#">CVE-2019-1387</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a>
gitlab -- gitlab	An IDOR vulnerability exists in GitLab <v12.1.2, <v12.0.4, and <v11.11.6 that allowed uploading files from project archive to replace other users files potentially allowing an attacker to replace project binaries or other uploaded assets.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5469</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and_enterprise	A command injection exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to inject commands via the API through the blobs scope.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15575</a> <a href="#">MISC</a>
gitlab -- gitlab_community_and_enterprise	An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to view private system notes from a GraphQL endpoint.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15576</a> <a href="#">MISC</a>
	An information disclosure vulnerability exists			

gitlab -- gitlab_com	in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.10 that allowed project milestones to be disclosed via groups browsing.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15577</a> <a href="#">MISC</a>
gitlab -- gitlab_com	A authentication bypass vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.10 in the Salesforce login integration that could be used by an attacker to create an account that bypassed domain restrictions and email verification requirements.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5486</a> <a href="#">MISC</a>
gitlab -- enterprise	An improper access control vulnerability exists in Gitlab EE <v12.3.3, <v12.2.7, & <v12.1.13 that allowed the group search feature with Elasticsearch to return private code, merge requests and commits.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5487</a> <a href="#">MISC</a>
gitlab -- gitlab	A denial of service exists in gitlab <v12.3.2, <v12.2.6, and <v12.1.10 that would let an attacker bypass input validation in markdown fields take down the affected page.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15584</a> <a href="#">MISC</a>
gitlab --	An improper access control vulnerability exists in GitLab <12.3.3 that allows an attacker to obtain container and	2019-		<a href="#">CVE-2019-15591</a>



gitlab	dependency scanning reports through the merge request widget even though public pipelines were disabled.	12-18	not yet calculated	<a href="#">MISC</a>
gitlab -- gitlab	An information exposure vulnerability exists in gitlab.com <v12.3.2, <v12.2.6, and <v12.1.10 when using the blocking merge request feature, it was possible for an unauthenticated user to see the head pipeline data of a public project even though pipeline visibility was restricted.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15580</a> <a href="#">MISC</a>
gitlab -- gitlab	An improper access control vulnerability exists in Gitlab <v12.3.2, <v12.2.6, <v12.1.12 which would allow a blocked user would be able to use GIT clone and pull if he had obtained a CI/CD token before.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15589</a> <a href="#">MISC</a>
gnome -- gnome-keyring	gnome-keyring does not discard stored secrets when using gnome_keyring_lock_all_sync function	2019-12-20	not yet calculated	<a href="#">CVE-2012-6111</a> <a href="#">MISC</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnutls -- gnutls	GnuTLS incorrectly validates the first byte of padding in CBC modes	2019-12-20	not yet calculated	<a href="#">CVE-2015-8313</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Versions of			

handlebars - handlebars	handlebars prior to 4.3.0 are vulnerable to Prototype Pollution leading to Remote Code Execution. Templates may alter an Object's __proto__ and __defineGetter__ properties, which may allow an attacker to execute arbitrary code through crafted payloads.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19919 MISC</a>
hcl_software - hcl_appscan_source	HCL AppScan Source 9.0.3.13 and earlier is susceptible to cross-site scripting (XSS) attacks by allowing users to embed arbitrary JavaScript code in the Web UI.	2019-12-18	not yet calculated	<a href="#">CVE-2019-4388 CONFIRM</a>
hpe -- universal_i	Security vulnerabilities in HPE UIoT version 1.2.4.2 could allow unauthorized remote access and access to sensitive data. HPE has addressed this issue in HPE UIoT: For customers with release UIoT 1.2.4.2 fixes are made available with 1.2.4.2 RP3 HF1. For things_platform customers with release older than 1.2.4.2, such as 1.2.4.1, 1.2.4.0, the resolution will be to upgrade to 1.2.4.2 RP3 HF1. Customers are requested to upgrade to the updated versions	2019-12-18	not yet calculated	<a href="#">CVE-2019-11995 MISC</a>

	or contact HPE support for further assistance.			
huawei -- multiple_products	There is an information leakage vulnerability on some Huawei products(AR120-S;AR1200;AR1200-S;AR150;AR150-S;AR160;AR200;AR200-S;AR2200;AR2200-S;AR3200;AR3600). An attacker with low permissions can view some high-privilege information by running specific commands. Successful exploit could cause an information disclosure condition.	2019-12-16	not yet calculated	<a href="#">CVE-2019-5259</a> <a href="#">MISC</a>
humax -- wireless_voice_gateway_hgb10R-2_devices	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 devices. Admin credentials are sent over cleartext HTTP.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19890</a> <a href="#">MISC</a>
humax -- wireless_voice_gateway_hgb10R-2_devices	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 devices. The attacker can discover admin credentials in the backup file, aka backupsettings.conf.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19889</a> <a href="#">MISC</a>
	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site request forgery which could allow			

ibm -- cognos_analytics	an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 159356.	2019-12-20	not yet calculated	<a href="#">CVE-2019-4231</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 166204.	2019-12-20	not yet calculated	<a href="#">CVE-2019-4555</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cognos_business_intelligence	IBM Cognos Business Intelligence 10.2.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 153179.	2019-12-20	not yet calculated	<a href="#">CVE-2018-1934</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm --	IBM Financial Transaction Manager 3.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote	2019-12-	not yet calculated	<a href="#">CVE-2019-4742</a> <a href="#">XF</a>

financial_transaction_manager	attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 172877.	20		<a href="#">CONFIRM</a>
ibm -- financial_transaction_manager	IBM Financial Transaction Manager 3.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 172706.	2019-12-20	not yet calculated	<a href="#">CVE-2019-4736</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0.0 through 2.0.8 is vulnerable to a configuration overwrite that allows an unauthenticated user to login as "admin", and then execute code as root or SYSTEM via TM1 scripting. IBM X-Force ID: 172094.	2019-12-18	not yet calculated	<a href="#">CVE-2019-4716</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intel -- active_management_technology	Insufficient input validation in subsystem for Intel(R) AMT before version 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11086</a> <a href="#">MISC</a>
	Logic issue in			



intel -- active_management technology	subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11131</a> <a href="#">MISC</a>
intel -- active_management technology	Insufficient input validation in subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11088</a> <a href="#">MISC</a>
intel -- active_management technology	Insufficient input validation in the subsystem for Intel(R) AMT before version 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11107</a> <a href="#">MISC</a>
intel -- active_management technology	Insufficient input validation in the subsystem for Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable information disclosure via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0166</a> <a href="#">MISC</a>
	Insufficient input validation in the subsystem for Intel(R) AMT before versions			

intel -- active_management_technology	11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable information disclosure via physical access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11100</a> <a href="#">MISC</a>
intel -- active_management_technology	Cross site scripting in subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow a privileged user to potentially enable escalation of privilege via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11132</a> <a href="#">MISC</a>
intel -- active_management_technology	Insufficient input validation in subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0131</a> <a href="#">MISC</a>
intel -- converged_security_and_active_management_engine	Insufficient input validation in subsystem for Intel(R) CSME before versions 12.0.45 and 13.0.10 may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11108</a> <a href="#">MISC</a>
	Logic issue in subsystem for Intel(R) CSME before versions 12.0.45, 13.0.10 and 14.0.10 may	2019-		

intel -- converged	allow a privileged user to potentially enable escalation of privilege and information disclosure via local access.	12-18	not yet calculated	<a href="#">CVE-2019-11105</a> <a href="#">MISC</a>
intel -- converged	Insufficient input validation in firmware update software for Intel(R) CSME before versions 12.0.45, 13.0.10 and 14.0.10 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11103</a> <a href="#">MISC</a>
intel -- converged	Insufficient Input validation in the subsystem for Intel(R) CSME before versions 12.0.45, 13.0.10 and 14.0.10 may allow a privileged user to potentially enable denial of service via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0165</a> <a href="#">MISC</a>
intel -- converged	Authentication bypass in the subsystem for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11110</a> <a href="#">MISC</a>
	Heap overflow in subsystem in			

intel -- converged	Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow an unauthenticated user to potentially enable escalation of privileges, information disclosure or denial of service via adjacent access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0169</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient input validation in Intel(R) DAL software for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable information disclosure via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11102</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient input validation in MEInfo software for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11104</a> <a href="#">MISC</a> execution_engine

intel -- converged	Insufficient input validation in the subsystem for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable information disclosure via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11101</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient session validation in the subsystem for Intel(R) CSME before versions 11.8.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11106</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient input validation in the subsystem for Intel(R) CSME before versions 11.8.70, 12.0.45 and 13.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable information disclosure via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0168</a> <a href="#">MISC</a> execution_engine
	Insufficient input validation in the subsystem for Intel(R) CSME			



intel -- converged	before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.10 and 4.0.20 may allow a privileged user to potentially enable escalation of privilege, information disclosure or denial of service via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11087</a> <a href="#">MISC</a>
intel -- dynamic_p	Improper permissions in the Intel(R) Dynamic Platform and Thermal Framework v8.3.10208.5643 allow an authenticated user to potentially execute code at an elevated level of privilege.	2019-12-16	not yet calculated	<a href="#">CVE-2019-0134</a> <a href="#">MISC</a>
intel -- ethernet_i218	Insufficient memory protection for Intel(R) Ethernet I218 Adapter driver for Windows* 10 before version 24.1 may allow an authenticated user to potentially enable information disclosure via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-11096</a> <a href="#">MISC</a>
intel -- fpga_sdk	Improper conditions check in the Linux kernel driver for the Intel(R) FPGA SDK for OpenCL(TM) Pro Edition before version 19.4 may allow an	2019-12-16	not yet calculated	<a href="#">CVE-2019-11165</a> <a href="#">MISC</a>

	authenticated user to potentially enable denial of service via local access.			
intel -- management_engine_driver_for_windows	Improper directory permissions in the installer for Intel(R) Management Engine Consumer Driver for Windows before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10 Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-11097</a> <a href="#">MISC</a>
intel -- multiple_processors	Improper conditions check in voltage settings for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege and/or information disclosure via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-11157</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
intel -- multiple_processors	Improper conditions check in multiple Intel? Processors may allow an authenticated user to potentially enable partial escalation of privilege, denial of service and/or information disclosure via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14607</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
	Cryptographic timing conditions in			

intel -- multiple_products	the subsystem for Intel(R) PTT before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.0 and 14.0.10; Intel(R) TXE 3.1.70 and 4.0.20; Intel(R) SPS before versions SPS_E5_04.01.04.305.0, SPS_SoC-X_04.00.04.108.0, SPS_SoC-A_04.00.04.191.0, SPS_E3_04.01.04.086.0, SPS_E3_04.08.04.047.0 may allow an unauthenticated user to potentially enable information disclosure via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11090</a> <a href="#">MISC</a>
intel -- multiple_products	Insufficient access control in hardware abstraction driver for MEInfo software for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.0, 14.0.10; TXEInfo software for Intel(R) TXE before versions 3.1.70 and 4.0.20; INTEL-SA-00086 Detection Tool version 1.2.7.0 or before; INTEL-SA-00125 Detection Tool version 1.0.45.0 or before may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11147</a> <a href="#">MISC</a>
	Insufficient memory protection			

intel -- network_adapters	in the Linux Administrative Tools for Intel(R) Network Adapters before version 24.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-0159</a> <a href="#">MISC</a>
intel -- nuc	Out of bounds write in firmware for Intel(R) NUC(R) may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14612</a> <a href="#">MISC</a>
intel -- nuc	Improper input validation in firmware for Intel(R) NUC(R) may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14609</a> <a href="#">MISC</a>
intel -- nuc	Improper access control in firmware for Intel(R) NUC(R) may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14610</a> <a href="#">MISC</a>
intel -- nuc	Integer overflow in firmware for Intel(R) NUC(R) may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14611</a> <a href="#">MISC</a>
	Improper buffer restrictions in firmware for Intel(R) NUC(R)	2019-		

intel -- nuc	may allow an authenticated user to potentially enable escalation of privilege via local access.	12-16	not yet calculated	<a href="#">CVE-2019-14608</a> <a href="#">MISC</a>
intel -- quartus_prime	Null pointer dereference in the FPGA kernel driver for Intel(R) Quartus(R) Prime Pro Edition before version 19.3 may allow an authenticated user to potentially enable denial of service via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14604</a> <a href="#">MISC</a>
intel -- quartus_prime	Improper permissions in the installer for the License Server software for Intel? Quartus? Prime Pro Edition before version 19.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14603</a> <a href="#">MISC</a>
intel -- rapid_storage	Improper permissions in the executable for Intel(R) RST before version 17.7.0.1006 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14568</a> <a href="#">MISC</a>
intel -- scs_platform_discovery	Improper permissions in the installer for the Intel(R) SCS Platform Discovery Utility, all versions, may allow an authenticated user	2019-12-16	not yet calculated	<a href="#">CVE-2019-14605</a> <a href="#">MISC</a>



	to potentially enable escalation of privilege via local attack.			
intel -- server_platform	Logic issue in the subsystem for Intel(R) SPS before versions SPS_E5_04.01.04.275.0, SPS_SoC-X_04.00.04.100.0 and SPS_SoC-A_04.00.04.191.0 may allow a privileged user to potentially enable denial of service via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11109</a> <a href="#">MISC</a>
ivanti -- workspace_control	In Ivanti Workspace Control before 10.3.180.0, a locally authenticated user with low privileges can bypass Managed Application Security by controlling an unspecified attack vector in Workspace Preferences, when it is enabled. As a result, the attacker can start applications that should be blocked.	2019-12-17	not yet calculated	<a href="#">CVE-2019-19675</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Rundeck Plugin 3.6.5 and earlier stores credentials unencrypted in its global configuration file and in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the	2019-12-17	not yet calculated	<a href="#">CVE-2019-16556</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

	master file system.			
jenkins -- jenkins	A missing permission check in Jenkins Build Failure Analyzer Plugin 1.24.1 and earlier allows attackers with Overall/Read permission to have Jenkins evaluate a computationally expensive regular expression.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16554</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Spira Importer Plugin 3.2.3 and earlier disables SSL/TLS certificate validation for the Jenkins master JVM.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16558</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins WebSphere Deployer Plugin 1.6.1 and earlier allows attackers with Overall/Read permission to perform connection tests and determine whether files with an attacker-specified path exist on the Jenkins master file system.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16559</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Gerrit Trigger Plugin 2.30.1 and earlier allows attackers to connect to an attacker-specified HTTP URL or SSH server using attacker-specified credentials.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16551</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Build Failure Analyzer Plugin 1.24.1 and earlier allows attackers to have Jenkins evaluate a computationally expensive regular expression.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16553</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins WebSphere Deployer Plugin 1.6.1 and earlier allows attackers to perform connection tests and determine whether files with an attacker-specified path exist on the Jenkins master file system.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16560</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in a connection test form method in Jenkins Maven Release Plugin 0.16.1 and earlier allows attackers to have Jenkins connect to an attacker specified web server and parse XML documents.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16550</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Gerrit Trigger Plugin 2.30.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified	2019-12-	not yet calculated	<a href="#">CVE-2019-16552</a> <a href="#">MLIST</a>

	HTTP URL or SSH server using attacker-specified credentials, or determine the existence of a file with a given path on the Jenkins master.	17		<a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Maven Release Plugin 0.16.1 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks, allowing man-in-the-middle attackers to have Jenkins parse crafted XML documents.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16549</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A user-supplied regular expression in Jenkins Build Failure Analyzer Plugin 1.24.1 and earlier was processed in a way that wasn't interruptible, allowing attackers to have Jenkins evaluate a regular expression without the ability to interrupt this process.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16555</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Redgate SQL Change Automation Plugin 2.0.3 and earlier stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16557</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

joomla! -- joomla!	dataForDependantField in models/customfields.php in the JS JOBS FREE extension before 1.2.7 for Joomla! allows SQL Injection via the index.php? option=com_jsjobs&task=customfields.getfieldtitlebyfieldandfieldforchild parameter.	2019-12-19	not yet calculated	<a href="#">CVE-2019-17527</a> <a href="#">MISC</a>
lansweeper - lansweeper	The web console in Lansweeper 7.2.105.2 has XSS via the URL path. Product vulnerability has been fixed and disclosed within changelog as of 02 Dec 2019.	2019-12-19	not yet calculated	<a href="#">CVE-2019-18955</a> <a href="#">CONFIRM</a>
libreoffice - libreoffice	LibreOffice and Apache - OpenOffice automatically open and openoffice embedded content	2019-12-20	not yet calculated	<a href="#">CVE-2012-5639</a> <a href="#">MISC</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development_corporat - rumpus_ftp_web_file_manager	A Reflected Cross Site Scripting was discovered in the Login page of Rumpus FTP Web File Manager 8.2.9.1. An attacker can exploit it by sending a crafted link to end users and can execute arbitrary Javascripts	2019-12-16	not yet calculated	<a href="#">CVE-2019-19368</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki -- mediawiki	The MinervaNeue Skin in MediaWiki from 2019-11-05 to 2019-12-13 (1.35 and/or 1.34) mishandles certain HTML attributes, as demonstrated by IMG onmouseover= (impact is XSS) and IMG src=http (impact is	2019-12-19	not yet calculated	<a href="#">CVE-2019-19910</a> <a href="#">MISC</a> <a href="#">MISC</a>



	disclosing the client's IP address). This can occur within a talk page topical header that is viewed within a mobile (MobileFrontend) context.			
midori -- midori_browser	In Midori Browser 0.5.11 (on Windows 10), Content Security Policy (CSP) is not applied correctly to all parts of multipart content sent with the multipart/x-mixed-replace MIME type. This could result in script running where CSP should have blocked it, allowing for cross-site scripting (XSS) and other attacks when the product renders the content as HTML. Remediating this would also need to consider the polyglot case, e.g., a file that is a valid GIF image and also valid JavaScript.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19916</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
myphpchat-plus -- myphpchat-plus	phpMyChat-Plus 1.98 is vulnerable to reflected XSS via JavaScript injection into the password reset URL. In the URL, the pmc_username parameter to pass_reset.php is vulnerable.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19908</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	NLSSRV32.EXE in Nalpeiron			

nalpeiron -- nalpeiron	Licensing Service 7.3.4.0, as used with Nitro PDF and other products. Licensing service allows Elevation of Privilege via the \\.\mailslot\lsX86ccMails ot mailslot.	2019-12-17	not yet calculated	<a href="#">CVE-2019-19315</a> <a href="#">MISC</a>
nathack -- nathack	In NatHack between 3.6.0 and 3.6.3, a buffer overflow issue exists when reading very long lines from a NetHack configuration file (usually named .nethackrc). This vulnerability affects systems that have NetHack installed suid/sgid and shared systems that allow users to upload their own configuration files. All users are urged to upgrade to NetHack 3.6.4 as soon as possible.	2019-12-20	not yet calculated	<a href="#">CVE-2019-16787</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
negotiator -- negotiator	negotiator before 0.6.1 is vulnerable to a regular expression DoS	2019-12-20	not yet calculated	<a href="#">CVE-2016-100022</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nethack -- nethack	NetHack before 3.6.4 is prone to a buffer overflow vulnerability when reading very long lines from configuration files. This affects systems that have NetHack installed suid/sgid, and shared systems that allow users to upload their own configuration files.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19905</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

neuvector - neuvector	NeuVector 3.1 when configured to allow authentication via Active Directory, does not enforce non-empty passwords which allows an attacker with access to the Neuvector portal to authenticate as any valid LDAP user by providing a valid username and an empty password (provided that the active directory server has not been configured to reject empty passwords).	2019-12-20	not yet calculated	<a href="#">CVE-2019-19747</a> <a href="#">MISC</a> <a href="#">MISC</a>
node-df -- node-df	A code injection exists in node-df v0.1.4 that can allow an attacker to remote code execution by unsanitized input.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15597</a> <a href="#">MISC</a>
odoo -- community	Improper access control in the computed fields system of the framework of Odoo Community 13.0 and Odoo Enterprise 13.0 allows remote attackers to access sensitive information via crafted RPC requests, which could lead to privilege escalation.	2019-12-19	not yet calculated	<a href="#">CVE-2019-11780</a> <a href="#">MISC</a>
	In Omron PLC CJ series, all versions, and Omron PLC CS series, all versions, the			

omron -- cj_and_cs	software properly checks for the existence of a lock, but the programmable logic controllers externally controlled or influenced by an actor that is outside of the intended sphere of control.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18269</a> <a href="#">MISC</a>
omron -- cj_and_cs	In Omron PLC CJ series, all versions, and Omron PLC CS series, all versions, an attacker could monitor traffic between the PLC and the controller and replay requests that could result in the opening and closing of industrial valves.	2019-12-16	not yet calculated	<a href="#">CVE-2019-13533</a> <a href="#">MISC</a>
omron -- cj_and_cs	In Omron PLC CJ series, all versions and Omron PLC CS series, all versions, an attacker could spoof arbitrary messages or execute commands.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18259</a> <a href="#">MISC</a>
omron -- cj_and_nj	In Omron PLC CS series, all versions, Omron PLC CJ series, all versions, and Omron PLC NJ series, all versions, the software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more	2019-12-16	not yet calculated	<a href="#">CVE-2019-18261</a> <a href="#">MISC</a>

	susceptible to brute force attacks.			
opera -- opera_for	Opera for Android before 54.0.2669.49432 is vulnerable to a sandboxed cross-origin iframe bypass attack. By using a service working inside a sandboxed iframe it is possible to bypass the normal sandboxing attributes. This allows an attacker to make forced redirections without any user interaction from a third-party context.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19788</a> <a href="#">MISC</a>
palo_alto -- pan-os	Improper restriction of communications to Log Forwarding Card (LFC) on PA-7000 Series devices with second-generation Switch Management Card (SMC) may allow an attacker with network access to the LFC to gain root access to PAN-OS. This issue affects PAN-OS 9.0 versions prior to 9.0.5-h3 on PA-7080 and PA-7050 devices with an LFC installed and configured. This issue does not affect PA-7000 Series deployments using the first-generation SMC and the Log Processing Card (LPC). This issue	2019-12-20	not yet calculated	<a href="#">CVE-2019-17440</a> <a href="#">CONFIRM</a>



	<p>does not affect any other PA series devices. This issue does not affect devices without an LFC. This issue does not affect PAN-OS 8.1 or prior releases. This issue only affects a very limited number of customers and we undertook individual outreach to help them upgrade. At the time of publication, all identified customers have upgraded SW or content and are not impacted.</p>			
<p>pebble_templates - pebble_templates</p>	<p>Pebble Templates 3.1.2 allows attackers to bypass a protection mechanism (intended to block access to instances of java.lang.Class) because getClass is accessible via the public static java.lang.Class java.lang.Class.forName(java.lang.Module,java lang.String) signature.</p>	<p>2019-12-19</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19899 MISC</a></p>
	<p>An issue was found in Philips Veradius Unity, Pulsera, and Endura Dual WAN Router, Veradius Unity (718132) with wireless option (shipped between 2016-August 2018), Veradius Unity (718132) with ViewForum option</p>			

phillips -- multiple_router	(shipped between 2016-August 2018), Pulsera (718095) and Endura (718075) with wireless option (shipped between 26-June-2017 through 07-August 2018), Pulsera (718095) and Endura (718075) with ViewForum option (shipped between 26-June-2017 through 07-August 2018). The router software uses an encryption scheme that is not strong enough for the level of protection required.	2019-12-20	not yet calculated	<a href="#">CVE-2019-18263</a> <a href="#">MISC</a>
plex -- media_server	The Camera Upload functionality in Plex Media Server through 1.18.2.2029 allows remote authenticated users to write files anywhere the user account running the Plex Media Server has permissions. This allows remote code execution via a variety of methods, such as (on a default Ubuntu installation) creating a .ssh folder in the plex user's home directory via directory traversal, uploading an SSH authorized_keys file there, and logging into the host as the Plex	2019-12-19	not yet calculated	<a href="#">CVE-2019-19141</a> <a href="#">MISC</a>

	user via SSH.			
pronestor - pronestor	An issue was discovered in the Outlook add-in in Pronestor Planner before 8.1.77. There is local privilege escalation in the Health Monitor service because PronestorHealthMonitor.exe access control is mishandled, aka PNB-2359.	2019-12-18	not yet calculated	<a href="#">CVE-2019-17390</a> <a href="#">MISC</a> <a href="#">MISC</a>
public_knowledge - pkp-lib	An issue was discovered in Public Knowledge Project (PKP) pkp-lib before 3.1.2-2, as used in Open Journal Systems (OJS) before 3.1.2-2. Code injection can occur in the OJS report generator if an authenticated Journal Manager user visits a crafted URL, because unserialize is used.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19909</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Waitress through version 1.3.1 would parse the Transfer-Encoding header and only look for a single string value, if that value was not chunked it would fall through and use the Content-Length header instead. According to the HTTP standard Transfer-Encoding should be a comma separated list, with the inner-most encoding first,			

pylons_project - waitress	<p>followed by any further transfer codings, ending with chunked. Requests sent with: "Transfer-Encoding: gzip, chunked" would incorrectly get ignored, and the request would use a Content-Length header instead to determine the body size of the HTTP message. This could allow for Waitress to treat a single request as multiple requests in the case of HTTP pipelining. This issue is fixed in Waitress 1.4.0.</p>	2019-12-20	not yet calculated	<a href="#">CVE-2019-16786</a> MISC MISC CONFIRM
pylons_project - waitress	<p>Waitress through version 1.3.1 implemented a "MAY" part of the RFC7230 which states: "Although the line terminator for the start-line and header fields is the sequence CRLF, a recipient MAY recognize a single LF as a line terminator and ignore any preceding CR." Unfortunately if a front-end server does not parse header fields with an LF the same way as it does those with a CRLF it can lead to the front-end and the back-end server parsing the same HTTP message in two different ways. This can lead to a</p>	2019-12-20	not yet calculated	<a href="#">CVE-2019-16785</a> MISC MISC CONFIRM

	potential for HTTP request smuggling/splitting whereby Waitress may see two requests while the front-end server only sees a single HTTP message. This issue is fixed in Waitress 1.4.0.			
qualcomm -- multiple_snapdragon	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, products MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	2019-12-18	not yet calculated	<a href="#">CVE-2019-10516</a> <a href="#">CONFIRM</a>



	MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130			
qualcomm -- multiple_snapdragon_products	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10517</a> <a href="#">CONFIRM</a>

	MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10544</a> <a href="#">CONFIRM</a>

	MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10557</a> <a href="#">CONFIRM</a>

	MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130			
qualcomm -- multiple_snapdragon_products	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10536</a> <a href="#">CONFIRM</a>

	MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064,			



qualcomm -- multiple_snapdragon_products	APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10518</a> <a href="#">CONFIRM</a>
	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,			

<p>qualcomm -- multiple_snapdragon_products</p>	<p>Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p>	<p>2019- 12- 18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10525</a> <a href="#">CONFIRM</a></p>
	<p>Improper validation</p>			

<p>qualcomm -- multiple_snapdragon_products</p>	<p>of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p>	<p>2019-12-18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10537</a> <a href="#">CONFIRM</a></p>
	<p>Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon</p>			

<p>qualcomm -- multiple_snapdragon_products</p>	<p>Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p>	<p>2019- 12- 18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10482</a> <a href="#">CONFIRM</a></p>
	<p>Out of bound access occurs while handling the WMI FW event due</p>			

<p>qualcomm</p> <p>--</p> <p>multiple_snapdragon_products</p>	<p>to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150</p>	<p>2019-12-18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10481</a></p> <p><a href="#">CONFIRM</a></p>
	<p>Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends unintended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wearables in APQ8009,</p>			



<p>qualcomm -- multiple_snapdragon_products</p>	<p>APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p>	<p>2019- 12- 18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10487</a> <a href="#">CONFIRM</a></p>
	<p>Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto,</p>			

	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10513</a> <a href="#">CONFIRM</a>
qualcomm	multiple_snapdragon_products			

	SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130			
qualcomm -- multiple_sn	<p>Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon products</p> <p>Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-10564</a> <a href="#">CONFIRM</a>

	SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10500 CONFIRM</a>

	SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130			
qualcomm -- multiple_snapdragon_products	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10572</a> <a href="#">CONFIRM</a>



	MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130			
rack_gem - rack_gem	<p>There's a possible information leak / session hijack vulnerability in Rack (RubyGem rack). This vulnerability is patched in versions 1.6.12 and 2.0.8. Attackers may be able to find and hijack sessions by using timing attacks targeting the session id. Session ids are usually stored and indexed in a database that uses <del>some kind of</del> <del>some kind of</del> rails - scheme for <del>speeding up</del> <del>speeding up</del> rails lookups of that session id. By carefully measuring the amount of time it</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-16782</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	<p>takes to look up a session, an attacker may be able to find a valid session id and hijack the session. The session id itself may be generated randomly, but the way the session is indexed by the backing store does not use a secure comparison.</p>			
<p>red_hat -- ansible_tower</p>	<p>A flaw was found in Ansible Tower, versions 3.6.x before 3.6.2 and 3.5.x before 3.5.4, when /websocket is requested and the password contains the '#' character. This request would cause a socket error in RabbitMQ when parsing the password and an HTTP error code 500 and partial password disclose will occur in plaintext. An attacker could easily guess some predictable passwords or brute force the password.</p>	<p>2019-12-19</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19342</a> <a href="#">CONFIRM</a></p>
<p>red_hat -- ansible_tower</p>	<p>A flaw was found in Ansible Tower, versions 3.6.x before 3.6.2 and 3.5.x before 3.5.3, where enabling RabbitMQ manager by setting it with '-e rabbitmq_enable_manager=true' exposes the RabbitMQ</p>	<p>2019-12-19</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19340</a> <a href="#">CONFIRM</a></p>

	management interface publicly, as expected. If the default admin user is still active, an attacker could guess the password and gain access to the system.			
red_hat -- ansible_tower	A flaw was found in Ansible Tower, versions 3.6.x before 3.6.2, where files in '/var/backup/tower' are left world-readable. These files include both the SECRET_KEY and the database backup. Any user with access to the Tower server, and knowledge of when a backup is run, could retrieve every credential stored in Tower. Access to data is the highest threat with this vulnerability.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19341</a> <a href="#">CONFIRM</a>
red_hat -- jboss_application_server	An Elevated Privileges issue exists in JBoss AS 7 Community Release due to the improper implementation in the security context propagation. A thread gets reused from the thread pool that still retains the security context from the process last used, which lets a local user obtain elevated privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2012-2312</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Roxy Fileman			

<p>roxy_fileman - roxy_fileman</p>	<p>1.4.5 for .NET is vulnerable to path traversal. A remote attacker can write uploaded files to arbitrary locations via the RENAMEFILE action. This can be leveraged for code execution by uploading a specially crafted Windows shortcut file and writing the file to the Startup folder (because an incomplete blacklist of file extensions allows Windows shortcut files to be uploaded).</p>	<p>2019-12-16</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19731</a> <a href="#">MISC</a> <a href="#">MISC</a></p>
<p>shadowsocks-libev - shadowsocks-libev</p>	<p>An exploitable information disclosure vulnerability exists in the network packet handling functionality of Shadowsocks-libev 3.3.2. When utilizing a Stream Cipher, a specially crafted set of network packets can cause an outbound connection from the server, resulting in information disclosure. An attacker can send arbitrary packets to trigger this vulnerability.</p>	<p>2019-12-18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-5152</a> <a href="#">MISC</a></p>
	<p>shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void</p>			

shadow -- shadow	<p>Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8).</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-19882</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplifile - - recordfusion	<p>In Simplifile RecordFusion through 2019-11-25, the logs and hist parameters allow remote attackers to access local files via a</p>	2019-12-17	not yet calculated	<a href="#">CVE-2019-19264</a> <a href="#">MISC</a>



	logger/logs?/../ or logger/hist?/../ URI.			
solarwinds - serv- u_ftp_server	A cross-site scripting (XSS) vulnerability exists in SolarWinds Serv-U FTP Server 15.1.7 in the email parameter, a different vulnerability than CVE-2018-19934 and CVE-2019-13182.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19829</a> <a href="#">MISC</a>
sonicos -- ssl_vpn_name	Installation of the SonicOS SSLVPN NACagent 3.5 on the Windows operating system, an autorun value is created does not quote the path in quotes, so if a malicious binary by an attacker within the parent path could allow code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7487</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Code injection in SonicWall SMA100 allows an authenticated user to execute arbitrary code in viewcacert.cer. Descript. This vulnerability impacted SMA100 version 9.0.0.4 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7486</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Buffer overflow in SonicWall SMA100 allows an authenticated user to execute arbitrary code in DEARRegister CGI script. This vulnerability impacted SMA100 version 9.0.0.3 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7485</a> <a href="#">CONFIRM</a>
	In SonicWall			

sonicwall - - sma100_devices	SMA100, an unauthenticated Directory Traversal vulnerability in the handleWAFRedirect CGI allows the user to test for the presence of a file on the server.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7483</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Authenticated SQL Injection in SonicWall SMA100 allow user to gain read-only access to unauthorized resources using viewasact CGI script. This vulnerability impacted SMA100 version 9.0.0.3 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7484</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Stack-based buffer overflow in SonicWall SMA100 allows an unauthenticated user to execute arbitrary code in function libSys.so. This vulnerability impacted SMA100 version 9.0.0.3 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7482</a> <a href="#">CONFIRM</a>
statics_server - statics_server	A path traversal in statics-server exists in all version that allows an attacker to perform a path traversal when a symlink is used within the working directory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15596</a> <a href="#">MISC</a>
sudo -- sudo	In Sudo through 1.8.29, an attacker with access to a Runas ALL sudoer account can impersonate a nonexistent user by invoking sudo with a numeric uid that is not	2019-12-19	not yet calculated	<a href="#">CVE-2019-19232</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	associated with any user.			
sudo -- sudo	In Sudo through 1.8.29, the fact that a user has been blocked (e.g., by using the ! character in the shadow file instead of a password hash) is not considered, allowing an attacker (who has access to a Runas ALL sudoer account) to impersonate any blocked user.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19234</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
swagger - - swagger_u	swagger-ui has XSS in key names	2019-12-20	not yet calculated	<a href="#">CVE-2016-1000229</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sylabs -- singularity	Insecure permissions (777) are set on \$HOME/.singularity when it is newly created by Singularity (version from 3.3.0 to 3.5.1), which could lead to an information leak, and malicious redirection of operations performed against Sylabs cloud services.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19724</a> <a href="#">CONFIRM</a>
talend -- restlet_framework	An XML eXternal Entity (XXE) issue exists in Restlet 1.1.10 in an endpoint using SOAP transport, which lets a remote attacker obtain sensitive information.	2019-12-18	not yet calculated	<a href="#">CVE-2012-2656</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In Tautulli 2.1.9,			

tautulli -- tautulli	CSRF in the /shutdown URI allows an attacker to shut down the remote media server. (Also, anonymous access can be achieved in applications that do not have a user login area).	2019-12-18	not yet calculated	<a href="#">CVE-2019-19833</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco -- multiple_tibco_products	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Deployment Kit, TIBCO Spotfire Desktop, and TIBCO Spotfire Desktop Language Packs contains a vulnerability that theoretically allows an attacker with permission to write DXP files to the Spotfire library to remotely execute code of their choice on the user account of other users who access the affected system. This attack is a risk only when the attacker has write access to a network file system shared with the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0,	2019-12-17	not yet calculated	<a href="#">CVE-2019-17334</a> <a href="#">MISC</a> <a href="#">MISC</a>

	<p>10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0, TIBCO Spotfire Deployment Kit: versions 7.11.1 and below, TIBCO Spotfire Desktop: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, and TIBCO Spotfire Desktop Language Packs: versions 7.11.1 and below.</p>			
<p>tibco -- spotfire_analytics_platform_for_aws_marketplace_and_spotfire_server</p>	<p>The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to data cached from a data source, or a portion of a data source, that the attacker should not have access to. The attacker would need privileges to access Spotfire files to the library.</p> <p>Affected releases</p>	<p>2019-12-17</p> <p>not yet calculated</p>	<p>CVE-2019-17335</p> <p>MISC</p> <p>MISC</p>	<p>aws_marketplace_and_spotfire_server</p>



	are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0.			
tibco -- spotfire_analytics_platform_for_aws_marketplace_and_spotfire_server	<p>The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to information that can lead to obtaining credentials used to access Spotfire data sources. The attacker would need privileges to save a Spotfire file to the library, and only applies in a just platform NTLM credentials, or a credentials profile is in use. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace:</p>	2019-12-17	not yet calculated	<a href="#">CVE-2019-17336</a> MISC MISC

	version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0.			
tree-kill --tree-kill	A Code Injection exists in treekill on Windows which allows a remote code execution when an attacker is able to control the input into the command.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15598</a> <a href="#">MISC</a>
tree-kill --tree-kill	A Code Injection exists in tree-kill on Windows which allows a remote code execution when an attacker is able to control the input into the command.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15599</a> <a href="#">MISC</a>
trend_micro-apex_one	Trend Micro Apex One (2019) is affected by a cross-site scripting (XSS) vulnerability on the product console. Note that the Japanese version of the product is NOT affected.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19692</a> <a href="#">MISC</a>
trend_micro-apex_one-dev_office_scan	A vulnerability in Trend Micro Apex One and OfficeScan XG could allow an attacker to expose a masked credential key by manipulating page elements using developer tools.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19691</a> <a href="#">MISC</a>

	Note that the attacker must already have admin/root privileges on the product console to exploit this vulnerability.			
trend_micro-deep_security	A privilege escalation vulnerability in the Trend Micro Deep Security as a Service Quick Setup cloud formation template could allow an authenticated entity with certain unrestricted AWS execution privileges to escalate to full privileges within the target AWS account.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18191</a> <a href="#">N/A</a>
trend_micro-housecall	A privilege escalation vulnerability in Trend Micro HouseCall for Home Networks (versions below 5.3.0.1063) could be exploited for home networks allowing an attacker to place a malicious DLL file into the application directory and elevate privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19688</a> <a href="#">MISC</a>
trend_micro-housecall	Trend Micro HouseCall for Home Networks (versions below 5.3.0.1063) could be exploited via a DLL Hijack related to a vulnerability on the packer that the program uses.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19689</a> <a href="#">MISC</a>
	The Trend Micro Security 2020			

trend_micro- security_2020	consumer family of products contains a vulnerability that could allow a local attacker to disclose sensitive information or to create a denial-of-service condition on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19693</a> <a href="#">MISC</a> <a href="#">MISC</a>
trend_micro- mobile_security_for_android	Trend Micro Mobile Security for Android (Consumer) versions 10.3.1 and below on Android 8.0+ has an issue in which an attacker could bypass the product's App Password Protection feature.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19690</a> <a href="#">MISC</a>
trendnet -- tew-651br_and_tew-652brp_and_tew-652bru_devices	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11399</a> <a href="#">MISC</a> <a href="#">MISC</a>
trendnet -- tew-651br_and_tew-652brp_and_tew-652bru_devices	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A	2019-12-18	not yet calculated	<a href="#">CVE-2019-11400</a> <a href="#">MISC</a> <a href="#">MISC</a>

	buffer overflow occurs through the get_set.ccp ccp_act parameter.			
typo3 -- typo3	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. It has been discovered that the extraction of manually uploaded ZIP archives in Extension Manager is vulnerable to directory traversal. Admin privileges are required in order to exploit this vulnerability. (In v9 LTS and later, System Maintainer privileges are also required.)	2019-12-17	not yet calculated	<a href="#">CVE-2019-19848</a> <a href="#">MISC</a> <a href="#">MISC</a>
typo3 -- typo3	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. It has been discovered that the classes QueryGenerator and QueryView are vulnerable to insecure deserialization. One exploitable scenario requires having the system extension ext:lowlevel (Backend Module: DB Check) installed, with a valid backend user who has administrator privileges. The	2019-12-17	not yet calculated	<a href="#">CVE-2019-19849</a> <a href="#">MISC</a> <a href="#">MISC</a>



	other exploitable scenario requires having the system extension ext:sys_action installed, with a valid backend user who has limited privileges.			
vmware -- vcenter	A security vulnerability in HPE OneView for VMware vCenter 9.5 could be exploited remotely to allow Cross-Site Scripting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11992</a> <a href="#">MISC</a>
wago -- pfc100_and_pfc200_driver	An exploitable denial of service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5078</a> <a href="#">MISC</a>
	An exploitable heap buffer overflow vulnerability exists in the iocheckd service "I/O-Chec" functionality of WAGO PFC 200			

wago -- pfc100_and_pfc200_devices	Firmware version 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5081</a> <a href="#">MISC</a> <a href="#">MISC</a>
wago -- pfc100_and_pfc200_devices	An exploitable information exposure vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause an external tool to fail, resulting in uninitialized stack data to be copied to the response packet buffer. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5073</a> <a href="#">MISC</a>
	An exploitable stack buffer overflow vulnerability exists in the command line utility getcouplerdetails of WAGO PFC200			

wago -- pfc100_and	Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets sent to the iocheckd service "I/O-Check" can cause a stack buffer overflow in the sub-process getcouplerdetails, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5075</a> <a href="#">MISC</a>
wago -- pfc100_and	An exploitable stack buffer overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware version 03.01.07(13), WAGO PFC200 Firmware version 03.00.39(12) and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a stack buffer overflow, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5074</a> <a href="#">CONFIRM</a>
	An exploitable denial-of-service vulnerability exists in the iocheckd service ??I/O-			

wago -- pfc100_and_pfc200_devices	<p>Chec??</p> <p>functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC 100 Firmware version 03.00.39(12). A set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-5077</a> <a href="#">MISC</a>
wago -- pfc100_and_pfc200_devices	<p>An exploitable denial-of-service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A set of packets can cause a denial of service and weaken credentials resulting in the default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-5080</a> <a href="#">MISC</a>
	An exploitable heap buffer			

wago -- pfc100_and	<p>overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware versions 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-5079</a> <a href="#">MISC</a>
wordpress - wordpress	<p>The "301 Redirects - Easy Redirect Manager" plugin before 2.45 for WordPress allows users (with subscriber or greater access) to modify, delete, or inject redirect rules, and exploit XSS, with the /admin-ajax.php?action=eps_redirect_save and /admin-ajax.php?action=eps_redirect_delete actions. This could result in a loss of site availability, malicious redirects, and user infections. This could also be exploited via CSRF.</p>	2019-12-19	not yet calculated	<a href="#">CVE-2019-19915</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Xerox AltaLink C8035 printers allow CSRF. A			



xerox -- altalink_c8035	request to add users is made in the Device User Data page form field to the xerox.set URI. (The frmUserName value must have a unique name.)	2019-12-18	not yet calculated	<a href="#">CVE-2019-19832</a> <a href="#">MISC</a>
xiaomi-- multiple_devices	An issue was discovered on Xiaomi DGNWG03LM, ZNCZ03LM, MCCGQ01LM, WSDCGQ01LM, RTCGQ01LM 5.5.48 devices. Because of insecure key support in ZigBee communication, attackers can obtain sensitive information, cause a denial of service attack, take over smart home devices, and tamper with messages.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15913</a> <a href="#">MISC</a>
xiaomi -- multiple_devices	An issue was discovered on Xiaomi DGNWG03LM, ZNCZ03LM, MCCGQ01LM, WSDCGQ01LM, RTCGQ01LM 5.5.48 devices. Attackers can utilize the "discover ZigBee network procedure" to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15915</a> <a href="#">MISC</a>
	An issue was discovered on Xiaomi DGNWG03LM, ZNCZ03LM, MCCGQ01LM,			

xiaomi -- multiple_devices	WSDCGQ01LM, RTCGQ01LM 5.5.48 devices. Attackers can use the ZigBee trust center rejoin procedure to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15914</a> <a href="#">MISC</a> <a href="#">MISC</a>
yarn -- yarn	In Yarn before 1.21.1, the package install functionality can be abused to generate arbitrary symlinks on the host filesystem by using specially crafted "bin" keys. Existing files could be overwritten depending on the current user permission set.	2019-12-16	not yet calculated	<a href="#">CVE-2019-10773</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zoho_manageengine-adselfservice_plus	An open redirect vulnerability was discovered in Zoho ManageEngine ADSelfService Plus 5.x before 5809 that allows attackers to force users who click on a crafted link to be sent to a specified external site.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18781</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us) using GovDelivery Communications Cloud on behalf of: United States  
Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of December 16, 2019  
**Date:** Monday, December 23, 2019 1:34:33 PM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of December 16, 2019](#)

12/23/2019 06:26 AM EST

Original release date: December 23, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
advantech -- diaganywhere_server	In Advantech DiagAnywhere Server, Versions 3.07.11 and prior, multiple stack-based buffer overflow vulnerabilities exist in the file transfer service listening on the TCP port. Successful exploitation could allow an unauthenticated attacker to execute arbitrary code with the privileges of the user running DiagAnywhere Server.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-18257</a> <a href="#">MISC</a>
apple -- icloud_for_windows	A race condition existed during the installation of iTunes for Windows. This was addressed with improved state handling. This issue is fixed in iCloud for Windows 7.11. Running the iTunes installer in an untrusted directory may result in arbitrary code execution.	2019-12-18	<a href="#">7.6</a>	<a href="#">CVE-2019-6232</a> <a href="#">MISC</a>
apple --	A race condition existed during the installation of iCloud for Windows. This was addressed with improved state			<a href="#">CVE-2019-</a>

icloud_for_windows	handling. This issue is fixed in iCloud for Windows 7.11. Running the iCloud installer in an untrusted directory may result in arbitrary code execution.	2019-12-18	<a href="#">7.6</a>	<a href="#">6236 MISC</a>
apple -- macos_catalina	A validation issue was addressed with improved logic. This issue is fixed in macOS Catalina 10.15.1. A malicious application may be able to gain root privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8802 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8748 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8781 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8758 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8807 MISC</a>
apple -- macos_catalina_and_tvos	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15, tvOS 13. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8717 MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8694 MISC</a>
apple -- macos_mojave	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8590 MISC</a>
	A memory corruption issue was			



apple -- macos_mojave	addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8695</a> <a href="#">MISC</a>
apple -- macos_mojave	This issue was addressed with improved checks. This issue is fixed in macOS Mojave 10.14.4. A local user may be able to execute arbitrary shell commands.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8513</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8629</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8635</a> <a href="#">MISC</a>
apple -- macos_mojave	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.6. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8661</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8697</a> <a href="#">MISC</a>
apple -- macos_mojave	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8555</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8616</a> <a href="#">MISC</a>
apple -- macos_mojave	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.5. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8604</a> <a href="#">MISC</a>
	A buffer overflow was addressed with			

apple -- macos_mojave	improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. Mounting a maliciously crafted NFS network share may lead to arbitrary code execution with system privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8508</a> <a href="#">MISC</a>
apple -- macos_mojave	A race condition was addressed with additional validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. A malicious application may be able to gain root privileges.	2019-12-18	<a href="#">7.6</a>	<a href="#">CVE-2019-8565</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_mojave	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.4. An application may be able to gain elevated privileges.	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-8526</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A maliciously crafted SQL query may lead to arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8600</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to cause unexpected system termination or write kernel memory.	2019-12-18	<a href="#">8.8</a>	<a href="#">CVE-2019-8591</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8814</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8676</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	execution.			MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	9.3	<a href="#">CVE-2019-8816</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	7.5	<a href="#">CVE-2019-8613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	9.3	<a href="#">CVE-2019-8685</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	9.3	<a href="#">CVE-2019-8574</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	7.5	<a href="#">CVE-2019-8648</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to execute arbitrary code with system privileges.	2019-12-18	9.3	<a href="#">CVE-2019-8605</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.4, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause arbitrary code execution.	2019-12-18	7.5	<a href="#">CVE-2019-8647</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An out-of-bounds read was addressed			<a href="#">CVE-2019-</a>

apple -- multiple_products	with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">8641</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. An attacker may be able to trigger a use-after-free in an application deserializing an untrusted NSDictionary.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8662</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to gain root privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8637</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8660</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8672</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- watchos	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8747</a> <a href="#">MISC</a>
apple -- watchos_and_icloud_for_windows	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Multiple issues in libxslt.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-8750</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- xcode	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8723</a> <a href="#">MISC</a>



apple -- xcode	Multiple issues in Id64 in the Xcode toolchains were addressed by updating to version Id64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege.	2019-12-18	<a href="#">9.3</a>	<a href="#">CVE-2019-8724</a> <a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below can be used as an HTTP GET request proxy when unauthenticated remote attackers send crafted HTTP POST requests.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-3996</a> <a href="#">MISC</a>
envoy_proxy -- envoy	An issue was discovered in Envoy 1.12.0. An untrusted remote client may send an HTTP header (such as Host) with whitespace after the header content. Envoy will treat "header-value " as a different string from "header-value" so for example with the Host header "example.com " one could bypass "example.com" matchers.	2019-12-13	<a href="#">7.5</a>	<a href="#">CVE-2019-18802</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
envoy_proxy -- envoy	An issue was discovered in Envoy 1.12.0. An untrusted remote client may send HTTP/2 requests that write to the heap outside of the request buffers when the upstream is HTTP/1. This may be used to corrupt nearby heap contents (leading to a query-of-death scenario) or may be used to bypass Envoy's access control mechanisms such as path based routing. An attacker can also modify requests from other users that happen to be proximal temporally and spatially.	2019-12-13	<a href="#">7.5</a>	<a href="#">CVE-2019-18801</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
fontforge -- libspiro	Libspiro through 20190731 has a stack-based buffer overflow in the spiro_to_bpath0() function in spiro.c.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-19847</a> <a href="#">MISC</a>
google -- tensorflow	In TensorFlow before 1.15, a heap buffer overflow in UnsortedSegmentSum can be produced when the Index template argument is int32. In this case data_size and num_segments fields are truncated from int64 to int32 and can produce negative numbers, resulting in accessing out of bounds heap memory. This is unlikely to be exploitable and was detected and fixed internally in TensorFlow 1.15 and 2.0.	2019-12-16	<a href="#">7.5</a>	<a href="#">CVE-2019-16778</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
joomla -- joomla!	class.upload.php in verot.net class.upload through 1.0.3 and 2.x through 2.0.4, as used in the K2 extension for Joomla! and other products, omits .pht from the set of dangerous file extensions, a similar issue to CVE-2019-19576.	2019-12-17	<a href="#">7.5</a>	<a href="#">CVE-2019-19634</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

joomla -- joomla!	In Joomla! before 3.9.14, the lack of validation of configuration parameters used in SQL queries caused various SQL injection vectors.	2019-12-18	<a href="#">7.5</a>	<a href="#">CVE-2019-19846</a> <a href="#">MISC</a>
labf -- aceaxe_plus	The FTP client in AceaXe Plus 1.0 allows a buffer overflow via a long EHLO response from an FTP server.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-19782</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause a NULL pointer dereference in f2fs_recover_fsync_data in fs/f2fs/recovery.c. This is related to F2FS_P_SB in fs/f2fs/f2fs.h.	2019-12-17	<a href="#">7.1</a>	<a href="#">CVE-2019-19815</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty_segment slab-out-of-bounds write access because an array is bounded by the number of dirty types (8) but the array index can exceed this.	2019-12-17	<a href="#">9.3</a>	<a href="#">CVE-2019-19814</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.	2019-12-17	<a href="#">9.3</a>	<a href="#">CVE-2019-19816</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in __mutex_lock in kernel/locking/mutex.c. This is related to mutex_can_spin_on_owner in kernel/locking/mutex.c, __btrfs_qgroup_free_meta in fs/btrfs/qgroup.c, and btrfs_insert_delayed_items in fs/btrfs/delayed-inode.c.	2019-12-17	<a href="#">9.3</a>	<a href="#">CVE-2019-19813</a> <a href="#">MISC</a>
petwant_and_skymee -- pf-103_and_petalk_ai	The processCommandSetMac() function of libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16737</a> <a href="#">MISC</a>
petwant_and_skymee -- pf-103_and_petalk_ai	processCommandSetUid() in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16733</a> <a href="#">MISC</a>

petwant_and_skymee -- pf- 103_and_petalk_ai	Unencrypted HTTP communications for firmware upgrades in Petalk AI and PF-103 allow man-in-the-middle attackers to run arbitrary code as the root user.	2019-12-13	<a href="#">9.3</a>	<a href="#">CVE-2019-16732</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	A stack-based buffer overflow in processCommandUploadLog in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to cause denial of service or run arbitrary code as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16735</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	processCommandUpgrade() in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16730</a> <a href="#">MISC</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	The processCommandUploadLog() function of libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-17364</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	A stack-based buffer overflow in processCommandUploadSnapshot in libcommon.so in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to cause denial of service or run arbitrary code as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16736</a> <a href="#">MISC</a>
petwant_and_skymee -- pf- 103_and_petalk_ai	Use of default credentials for the TELNET server in Petwant PF-103 firmware 4.3.2.50 and Petalk AI 3.2.2.30 allows remote attackers to execute arbitrary system commands as the root user.	2019-12-13	<a href="#">10</a>	<a href="#">CVE-2019-16734</a> <a href="#">MISC</a>
puppet -- mcollective	mcollective has a default password set at install	2019-12-13	<a href="#">7.5</a>	<a href="#">CVE-2014-0175</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
python-requests-kerberos -- python-requests-kerberos	python-requests-Kerberos through 0.5 does not handle mutual authentication	2019-12-15	<a href="#">7.5</a>	<a href="#">CVE-2014-8650</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Out of boundary access is possible as there is no validation of data accessed against the received size of the packet in case of malicious firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon			

qualcomm -- multiple_snapdragon_products	Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2019-12-18	7.5	<a href="#">CVE-2019-10614</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Buffer overwrite can occur in IEEE80211 header filling function due to lack of range check of array index received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, IPQ8074, MDM9607, MDM9650, MSM8909, MSM8939, QCN7605, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24	2019-12-18	7.2	<a href="#">CVE-2019-10605</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Integer overflow to buffer overflow due to lack of validation of event arguments received from firmware. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8917, MSM8920, MSM8937, MSM8940, QCN7605, QCS405, QCS605, SDA845, SDM660, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2019-2304</a> <a href="#">CONFIRM</a>
qualcomm --	Out of bound access can occur while processing firmware event due to lack of validation of WMI message received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	2019-12-	7.2	<a href="#">CVE-2019-10601</a>

multiple_snapdragon_products	Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MSM8996AU, Nicobar, QCA6574AU, QCN7605, QCS405, SDM630, SDM636, SDM660, SDM845, SM6150, SM7150, SM8150	18		<a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	When a fake broadcast/multicast 11w rmf without mmie received, since no proper length check in wma_process_bip, buffer overflow will happen in both cds_is_mmie_valid and qdf_nbuf_trim_tail in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8937, MSM8996AU, MSM8998, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDM630, SDM636, SDM660, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2018-11980</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bound write can happen in WMI firmware event handler due to lack of validation of data received from WLAN firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9980, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-10480</a> <a href="#">CONFIRM</a>
	Device memory may get corrupted because of buffer overflow/underflow. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics			



qualcomm -- multiple_snapdragon_products	Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8016, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SM6150, SM7150, SXR1130	2019-12-18	10	<a href="#">CVE-2019-2242</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Improper Access Control for RPU write access from secure processor in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8017, APQ8053, APQ8098, IPQ8074, MDM9150, MDM9650, MDM9655, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCA8081, QCN7605, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2019-2274</a> <a href="#">CONFIRM</a>
qualcomm -- multiple_snapdragon_products	Out of bounds memcpy can occur by providing the embedded NULL character string and length greater than the actual string length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206,	2019-12-18	7.2	<a href="#">CVE-2019-10607</a> <a href="#">CONFIRM</a>

	MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996, MSM8996AU, QCA4531, QCA8081, QCA9531, QCA9558, QCA9886, QCA9980, QCN7605, QCS605, SDA660, SDX20, SDX24, SDX55, SM8150, SXR1130			
qualcomm -- multiple_snapdragon_products	Out of bound access can occur while processing peer info in IBSS connection mode due to lack of upper bounds check to ensure that for loop further will not cause an overflow in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8053, APQ8096AU, MDM9607, MSM8996AU, QCA6574AU, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130	2019-12-18	7.2	<a href="#">CVE-2019-10598</a> CONFIRM
qualcomm -- multiple_snapdragon_products	Possible buffer overwrite in message handler due to lack of validation of tid value calculated from packets received from firmware in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8053, APQ8064, APQ8096AU, IPQ4019, IPQ8064, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909, MSM8909W, MSM8939, MSM8996AU, QCA4531, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCA9558, QCA9880, QCA9886, QCA9980, SDA660, SDM630, SDM636, SDM660, SDX20, SDX24	2019-12-18	7.2	<a href="#">CVE-2019-10595</a> CONFIRM
	Use of local variable as argument to netlink CB callback goes out of it scope when callback triggered lead to invalid stack memory in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and			

qualcomm -- multiple_snapdragon_products	Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCA8081, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2019-12-18	<a href="#">7.2</a>	<a href="#">CVE-2019-10600</a> <a href="#">CONFIRM</a>
red_hat -- edeploy	eDeploy has tmp file race condition flaws	2019-12-15	<a href="#">9.3</a>	<a href="#">CVE-2014-3701</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- edeploy	eDeploy has RCE via cPickle deserialization of untrusted data	2019-12-15	<a href="#">7.5</a>	<a href="#">CVE-2014-3699</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
xfig -- fig2dev	read_colordef in read.c in Xfig fig2dev 3.2.7b has an out-of-bounds write.	2019-12-15	<a href="#">7.5</a>	<a href="#">CVE-2019-19797</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- incubator_superset	In Apache Incubator Superset before 0.31 user could query database metadata information from a database he has no access to, by using a specially crafted complex query.	2019-12-16	<a href="#">5</a>	<a href="#">CVE-2019-12413</a> <a href="#">MISC</a>
apache -- incubator_superset	In Apache Incubator Superset before 0.32, a user can view database names that he has no access to on a dropdown list in SQLLab	2019-12-16	<a href="#">5</a>	<a href="#">CVE-2019-12414</a> <a href="#">MISC</a>
apple -- ios	A logic issue was addressed with improved state management. This issue is fixed in iOS 13. Visiting a malicious website may lead to address bar spoofing.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8727</a> <a href="#">MISC</a>
	A user privacy issue was addressed by			

apple -- ios	removing the broadcast MAC address. This issue is fixed in iOS 12.2. A device may be passively tracked by its WiFi MAC address.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8567</a> <a href="#">MISC</a>
apple -- ios	A permissions issue existed in which execute permission was incorrectly granted. This issue was addressed with improved permission validation. This issue is fixed in iOS 13. Processing a maliciously crafted file may disclose user information.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8731</a> <a href="#">MISC</a>
apple -- ios	A logic issue existed with the display of notification previews. This issue was addressed with improved validation. This issue is fixed in iOS 13. Notification previews may show on Bluetooth accessories even when previews are disabled.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8711</a> <a href="#">MISC</a>
apple -- ios	An access issue was addressed with additional sandbox restrictions. This issue is fixed in iOS 12.3. A sandboxed process may be able to circumvent sandbox restrictions.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8617</a> <a href="#">MISC</a>
apple -- ios	A permissions issue existed in the handling of motion and orientation data. This issue was addressed with improved restrictions. This issue is fixed in iOS 12.2. A website may be able to access sensor information without user consent.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8554</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave	This issue was addressed with improved checks. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6. A remote attacker may be able to leak memory.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8663</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_safari	A logic issue was addressed with improved state management. This issue is fixed in iOS 13, Safari 13. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8674</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_tvos	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in iOS 12.4, tvOS 12.4. A malicious application may be able to restrict access to websites.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8698</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_watchos	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.4, watchOS 5.3. A remote attacker may cause an unexpected application termination.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8665</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An input validation issue was addressed			<a href="#">CVE-2019-</a>

apple -- ios_and_watchos	with improved input validation. This issue is fixed in iOS 12.3, watchOS 5.2.1. Processing a maliciously crafted message may lead to a denial of service.	2019-12-18	<a href="#">4.3</a>	<a href="#">8626</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_catalina	"Clear History and Website Data" did not clear the history. The issue was addressed with improved data deletion. This issue is fixed in macOS Catalina 10.15. A user may be unable to delete browsing history items.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8768</a> <a href="#">MISC</a>
apple -- macos_catalina	The issue was addressed with improved permissions logic. This issue is fixed in macOS Catalina 10.15. A malicious application may be able to access recent documents.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8770</a> <a href="#">MISC</a>
apple -- macos_catalina	An issue existed in the handling of links in encrypted PDFs. This issue was addressed by adding a confirmation prompt. This issue is fixed in macOS Catalina 10.15. An attacker may be able to exfiltrate the contents of an encrypted PDF.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8772</a> <a href="#">MISC</a>
apple -- macos_catalina_and_tvos	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15, tvOS 13. Processing a maliciously crafted movie may result in the disclosure of process memory.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8705</a> <a href="#">MISC</a>
apple -- macos_mojave	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.6. The encryption status of a Time Machine backup may be incorrect.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8667</a> <a href="#">MISC</a>
apple -- macos_mojave	This issue was addressed with improved handling of file metadata. This issue is fixed in macOS Mojave 10.14.4. A malicious application may bypass Gatekeeper checks.	2019-12-18	<a href="#">4.6</a>	<a href="#">CVE-2019-6239</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.5. An application may be able to read restricted memory.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8603</a> <a href="#">MISC</a>
apple -- macos_mojave	An authentication issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.5. A user may be unexpectedly logged in to another user's account.	2019-12-18	<a href="#">6.5</a>	<a href="#">CVE-2019-8634</a> <a href="#">MISC</a>
apple --	A logic issue was addressed with improved validation. This issue is fixed in	2019-12-		<a href="#">CVE-2019-</a>



macos_mojave	macOS Mojave 10.14.4. A malicious application may be able to elevate privileges.	18	<a href="#">6.8</a>	<a href="#">8561 MISC</a>
apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8693 MISC</a>
apple -- macos_mojave	This issue was addressed with improved checks. This issue is fixed in macOS Mojave 10.14.5. A malicious application may bypass Gatekeeper checks.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8589 MISC</a>
apple -- macos_mojave_and_safari	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.6, Safari 12.1.2. Visiting a malicious website may lead to address bar spoofing.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8670 MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	<a href="#">4.3</a>	<a href="#">CVE-2019-8690 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A remote attacker may be able to leak memory.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-8787 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8822 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	<a href="#">6.8</a>	<a href="#">CVE-2019-8821 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8820</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8819</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8812</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8678</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to cause unexpected system termination or read kernel memory.	2019-12-18	6.6	<a href="#">CVE-2019-8576</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8763</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A logic issue was addressed with			

apple -- multiple_products	improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	4.3	<a href="#">CVE-2019-8625</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. A malicious application may be able to read restricted memory.	2019-12-18	4.3	<a href="#">CVE-2019-8598</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	4.3	<a href="#">CVE-2019-8597</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	4.3	<a href="#">CVE-2019-8658</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8735</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8595</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were			<a href="#">CVE-2019-</a>

apple -- multiple_products	addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">8596</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8563</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8686</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	4.3	<a href="#">CVE-2019-8649</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8811</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. A remote attacker may be able to leak memory.	2019-12-18	5	<a href="#">CVE-2019-8646</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple --	A user privacy issue was addressed by removing the broadcast MAC address.			<a href="#">CVE-2019-8620</a>

multiple_products	This issue is fixed in iOS 12.3, tvOS 12.3, watchOS 5.2.1. A device may be passively tracked by its WiFi MAC address.	2019-12-18	5	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8609</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8594</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8687</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A malicious application may be able to read restricted memory.	2019-12-18	4.3	<a href="#">CVE-2019-8560</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8823</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3. Parsing a maliciously crafted office document may lead to an unexpected application	2019-12-18	6.8	<a href="#">CVE-2019-8657</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>





apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8559</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8558</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8556</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2. Clicking a malicious SMS link may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8553</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8571</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	4.3	<a href="#">CVE-2019-8813</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	4.3	<a href="#">CVE-2019-8719</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8601</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8622</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8681</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8623</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8677</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple --	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari	2019-12-		<a href="#">CVE-2019-8611</a> <a href="#">MISC</a> <a href="#">MISC</a>

multiple_products	12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	18	6.8	MISC MISC MISC MISC MISC
apple -- multiple_products	An input validation issue was addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. An application may be able to gain elevated privileges.	2019-12-18	6.8	<a href="#">CVE-2019-8577</a> MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8683</a> MISC MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8610</a> MISC MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8680</a> MISC MISC MISC MISC MISC MISC MISC
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8628</a> MISC MISC MISC MISC MISC MISC MISC
	Multiple memory corruption issues were			<a href="#">CVE-2019-</a>

apple -- multiple_products	addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">8644</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. Processing a maliciously crafted movie file may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8585</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8671</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8679</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8666</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- safari	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in Safari 13.0.1. Visiting a malicious website may lead to user interface spoofing.	2019-12-18	4.3	<a href="#">CVE-2019-8654</a> <a href="#">MISC</a>
apple -- safari	The issue was addressed with improved handling of service worker lifetime. This issue is fixed in Safari 13.0.1. Service workers may leak private browsing history.	2019-12-18	5	<a href="#">CVE-2019-8725</a> <a href="#">MISC</a>
	This issue was addressed with improved			



apple -- watchos	checks. This issue is fixed in watchOS 5.3. Users removed from an iMessage conversation may still be able to alter state.	2019-12-18	5	<a href="#">CVE-2019-8659</a> <a href="#">MISC</a>
apple -- watchos	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 5.3. A remote attacker may be able to leak memory.	2019-12-18	5	<a href="#">CVE-2019-8624</a> <a href="#">MISC</a>
apple -- watchos	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8765</a> <a href="#">MISC</a>
apple -- watchos	A logic issue was addressed with improved state management. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	4.3	<a href="#">CVE-2019-8764</a> <a href="#">MISC</a>
apple -- watchos	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8743</a> <a href="#">MISC</a>
apple -- watchos_and_icloud_for_windows	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	6.8	<a href="#">CVE-2019-8766</a> <a href="#">MISC</a> <a href="#">MISC</a>
atlassian -- jira	The WorkflowResource class removeStatus method in Jira before version 7.13.12, from version 8.0.0 before version 8.4.3, and from version 8.5.0 before version 8.5.2 allows authenticated remote attackers who do not have project administration access to remove a configured issue status from a project via a missing authorisation check.	2019-12-18	4	<a href="#">CVE-2019-15013</a> <a href="#">MISC</a>
atlassian -- multiple_products	An issue was discovered in the SAML Single Sign On (SSO) plugin for several Atlassian products affecting versions 3.1.0 through 3.2.2 for Jira and Confluence, versions 2.4.0 through 3.0.3 for Bitbucket, and versions 2.4.0 through 2.5.2 for Bamboo. It allows locally disabled users to reactivate their accounts just by browsing the affected Jira/Confluence/Bitbucket/Bamboo instance, even when the applicable configuration option of the plugin has	2019-12-13	6	<a href="#">CVE-2019-13347</a> <a href="#">MISC</a> <a href="#">MISC</a>

	been disabled ("Reactivate inactive users"). Exploiting this vulnerability requires an attacker to be authorized by the identity provider and requires that the plugin's configuration option "User Update Method" have the "Update from SAML Attributes" value.			
centos-webpanel -- centos_web_panel	CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.864 allows an attacker to get a victim's session file name from /home/[USERNAME]/tmp/session/sess_XXXXXXXXXX and the victim's token value from /usr/local/cwpsrv/logs/access_log, then use them to gain access to the victim's password (for the OS and phpMyAdmin) via an attacker account. This is different from CVE-2019-14782.	2019-12-17	4	<a href="#">CVE-2019-15235</a> <a href="#">MISC</a> <a href="#">MISC</a>
centos-webpanel -- centos_web_panel	CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.856 through 0.9.8.864 allows an attacker to get a victim's session file name from the /tmp directory, and the victim's token value from /usr/local/cwpsrv/logs/access_log, then use them to make a request to extract the victim's password (for the OS and phpMyAdmin) via an attacker account.	2019-12-17	4	<a href="#">CVE-2019-14782</a> <a href="#">MISC</a> <a href="#">MISC</a>
contao -- contao	Contao 4.8.4 and 4.8.5 has Improper Encoding or Escaping of Output. It is possible to inject insert tags into the login module which will be replaced when the page is rendered.	2019-12-17	5	<a href="#">CVE-2019-19714</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
contao -- contao	Contao 4.0 through 4.8.5 allows PHP local file inclusion. A back end user with access to the form generator can upload arbitrary files and execute them on the server.	2019-12-17	6.5	<a href="#">CVE-2019-19745</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
coredns -- coredns	The miekg Go DNS package before 1.1.25, as used in CoreDNS before 1.6.6 and other products, improperly generates random numbers because math/rand is used. The TXID becomes predictable, leading to response forgeries.	2019-12-13	4.3	<a href="#">CVE-2019-19794</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
docker -- docker_engine_and_cs	Docker Engine before 1.8.3 and CS Docker Engine before 1.6.2-CS7 does not properly validate and extract the manifest object from the JSON representation during a pull, which allows attackers to inject new attributes in a JSON object and bypass pull-by-digest validation.	2019-12-17	5	<a href="#">CVE-2014-8179</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

				<a href="#">CONFIRM</a>
dovecot -- dovecot	In Dovecot before 2.3.9.2, an attacker can crash a push-notification driver with a crafted email when push notifications are used, because of a NULL Pointer Dereference. The email must use a group address as either the sender or the recipient.	2019-12-13	5	<a href="#">CVE-2019-19722</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
duplicity -- duplicity	duplicity 0.6.24 has improper verification of SSL certificates	2019-12-13	5	<a href="#">CVE-2014-3495</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below is affected by an information disclosure vulnerability. A remote unauthenticated attacker can recover a user's password hash by sending a crafted HTTP POST request.	2019-12-17	5	<a href="#">CVE-2019-3993</a> <a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below is affected by a denial of service vulnerability due to a use after free. A remote unauthenticated attacker can crash the ELOG server by sending multiple HTTP POST requests which causes the ELOG function retrieve_url() to use a freed variable.	2019-12-17	5	<a href="#">CVE-2019-3994</a> <a href="#">MISC</a>
elog -- elog	ELOG 3.1.4-57bea22 and below is affected by a denial of service vulnerability due to a NULL pointer dereference. A remote unauthenticated attacker can crash the ELOG server by sending a crafted HTTP GET request.	2019-12-17	5	<a href="#">CVE-2019-3995</a> <a href="#">MISC</a>
elog-- elog	ELOG 3.1.4-57bea22 and below is affected by an information disclosure vulnerability. A remote unauthenticated attacker can access the server's configuration file by sending an HTTP GET request. Amongst the configuration data, the attacker may gain access to valid admin usernames and, in older versions of ELOG, passwords.	2019-12-17	5	<a href="#">CVE-2019-3992</a> <a href="#">MISC</a>
envoy_proxy -- envoy	An issue was discovered in Envoy 1.12.0. Upon receipt of a malformed HTTP request without a Host header, it sends an internally generated "Invalid request" response. This internally generated response is dispatched through the configured encoder filter chain before being sent to the client. An encoder filter that invokes route manager APIs that	2019-12-13	5	<a href="#">CVE-2019-18838</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	access a request's Host header causes a NULL pointer dereference, resulting in abnormal termination of the Envoy process.			<a href="#">MISC</a>
huawei -- campusinsight	There is an out-of-bounds read vulnerability in the Advanced Packages feature of the Gauss100 OLTP database in CampusInsight before V100R019C00SPC200. Attackers who gain the specific permission can use this vulnerability by sending elaborate SQL statements to the database. Successful exploit of this vulnerability may cause the database to crash.	2019-12-13	<a href="#">4</a>	<a href="#">CVE-2019-5278</a> <a href="#">MISC</a>
huawei -- cloudengine	CloudEngine 12800 has a DoS vulnerability. An attacker of a neighboring device sends a large number of specific packets. As a result, a memory leak occurs after the device uses the specific packet. As a result, the attacker can exploit this vulnerability to cause DoS attacks on the target device.	2019-12-13	<a href="#">6.1</a>	<a href="#">CVE-2019-5248</a> <a href="#">MISC</a>
huawei -- cloudusm-eua_product	Huawei CloudUSM-EUA V600R006C10;V600R019C00 have an information leak vulnerability. Due to improper configuration, the attacker may cause information leak by successful exploitation.	2019-12-13	<a href="#">5</a>	<a href="#">CVE-2019-5277</a> <a href="#">MISC</a>
huawei -- mate_20_pro_smartphones	Mate 20 Pro smartphones with versions earlier than 9.1.0.135(C00E133R3P1) have an improper authorization vulnerability. The software does not properly restrict certain operation of certain privilege, the attacker could trick the user into installing a malicious application before the user turns on student mode function. Successful exploit could allow the attacker to bypass the limit of student mode function.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-5250</a> <a href="#">MISC</a>
huawei -- multiple_products	There is a weak algorithm vulnerability in some Huawei products. The affected products use weak algorithms by default. Attackers may exploit the vulnerability to cause information leaks.	2019-12-13	<a href="#">5</a>	<a href="#">CVE-2019-19397</a> <a href="#">MISC</a>
huawei -- multiple_products	Some Huawei products have an insufficient verification of data authenticity vulnerability. A remote, unauthenticated attacker has to intercept specific packets between two devices, modify the packets, and send the modified packets to the peer device. Due to insufficient verification of some fields in the packets, an attacker	2019-12-13	<a href="#">4.3</a>	<a href="#">CVE-2019-5291</a> <a href="#">MISC</a>

	may exploit the vulnerability to cause the target device to be abnormal.			
huawei -- multiple_products	Certain Huawei products (AP2000;IPS Module;NGFW Module;NIP6300;NIP6600;NIP6800;S5700;SVN5600;SVN5800;SVN5800-C;SeMG9811;Secospace AntiDDoS8000;Secospace USG6300;Secospace USG6500;Secospace USG6600;USG6000V;eSpace U1981) have an out-of-bounds read vulnerability. An attacker who logs in to the board may send crafted messages from the internal network port or tamper with inter-process message packets to exploit this vulnerability. Due to insufficient validation of the message, successful exploit may cause the affected board to be abnormal.	2019-12-13	5	<a href="#">CVE-2019-5254</a> <a href="#">MISC</a>
huawei -- multiple_smartphones	There is a path traversal vulnerability in several Huawei smartphones. The system does not sufficiently validate certain pathnames from the application. An attacker could trick the user into installing, backing up and restoring a malicious application. Successful exploit could cause information disclosure.	2019-12-13	4.3	<a href="#">CVE-2019-5251</a> <a href="#">MISC</a>
huawei -- s5700_and_s6700_devices	Huawei S5700 and S6700 have a DoS security vulnerability. Attackers with certain permissions perform specific operations on affected devices. Because the pointer in the program is not processed properly, the vulnerability can be exploited to cause the device to be abnormal.	2019-12-13	4	<a href="#">CVE-2019-5290</a> <a href="#">MISC</a>
huawei -- y9_2019_and_honor_v	Huawei smartphones HUAWEI Y9 2019 and Honor View 20 have a denial of service vulnerability. Due to insufficient input validation of specific value when parsing the messages, an attacker may send specially crafted TD-SCDMA messages from a rogue base station to the affected devices to exploit this vulnerability. Successful exploit may cause an infinite loop and the device to reboot.	2019-12-13	6.1	<a href="#">CVE-2019-5260</a> <a href="#">MISC</a>
ibm -- api_connect	IBM API Connect 2018.4.1.7 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 168510.	2019-12-18	5	<a href="#">CVE-2019-4609</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
	IBM Financial Transaction Manager 3.0 is vulnerable to cross-site scripting. This			



ibm -- financial_transaction_manager	vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 172882.	2019-12-20	4.3	<a href="#">CVE-2019-4744</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- financial_transaction_manager	IBM Financial Transaction Manager 3.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 172880.	2019-12-20	4.3	<a href="#">CVE-2019-4743</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- mq_and_mq_appliance	IBM MQ and IBM MQ Appliance 9.1 CD, 9.1 LTS, 9.0 LTS, and 8.0 is vulnerable to a denial of service attack caused by channels processing poorly formatted messages. IBM X-Force ID: 166357.	2019-12-16	4	<a href="#">CVE-2019-4560</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	imagemagick 6.8.9.6 has remote DOS via infinite loop	2019-12-15	4.3	<a href="#">CVE-2014-8561</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
intel -- control_center-i	Unquoted service path in Control Center-I version 2.1.0.0 and earlier may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	4.6	<a href="#">CVE-2019-14599</a> <a href="#">MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Alauda DevOps Pipeline Plugin 2.3.2 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-12-17	4	<a href="#">CVE-2019-16574</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Team Concert Plugin 1.3.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-12-17	6.8	<a href="#">CVE-2019-16565</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Team Concert Plugin 1.3.0 and earlier in form-related methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in	2019-12-17	4	<a href="#">CVE-2019-16567</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

	Jenkins.			
jenkins -- jenkins	A missing permission check in Jenkins RapidDeploy Plugin 4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified web server.	2019-12-17	4	<a href="#">CVE-2019-16571</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins WebSphere Deployer Plugin 1.6.1 and earlier allows users with Overall/Read access to disable SSL/TLS certificate and hostname validation for the entire Jenkins master JVM.	2019-12-17	5.5	<a href="#">CVE-2019-16561</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Alauda DevOps Pipeline Plugin 2.3.2 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-12-17	6.8	<a href="#">CVE-2019-16573</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins SCTMExecutor Plugin 2.2 and earlier transmits previously configured service credentials in plain text as part of the global configuration, as well as individual jobs' configurations.	2019-12-17	5	<a href="#">CVE-2019-16568</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Mantis Plugin 0.26 and earlier allows attackers to connect to an attacker-specified web server using attacker-specified credentials.	2019-12-17	4.3	<a href="#">CVE-2019-16569</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Alauda Kubernetes Suport Plugin 2.3.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing the Kubernetes service account token or credentials stored in Jenkins.	2019-12-17	4	<a href="#">CVE-2019-16576</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Alauda Kubernetes Suport Plugin 2.3.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing the Kubernetes service account token or credentials stored in Jenkins.	2019-12-17	6.8	<a href="#">CVE-2019-16575</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Team Concert Plugin 1.3.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another	2019-12-17	4	<a href="#">CVE-2019-16566</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

	method, capturing credentials stored in Jenkins.			
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins RapidDeploy Plugin 4.1 and earlier allows attackers to connect to an attacker-specified web server.	2019-12-17	<a href="#">6.8</a>	<a href="#">CVE-2019-16570</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jersey -- jersey	jersey: XXE via parameter entities not disabled by the jersey SAX parser	2019-12-15	<a href="#">5</a>	<a href="#">CVE-2014-3643</a> <a href="#">REDHAT</a> <a href="#">MISC</a>
joomla -- joomla!	In Joomla! before 3.9.14, a missing access check in framework files could lead to a path disclosure.	2019-12-18	<a href="#">5</a>	<a href="#">CVE-2019-19845</a> <a href="#">MISC</a>
knot-resolver -- knot-resolver	knot-resolver before version 4.3.0 is vulnerable to denial of service through high CPU utilization. DNS replies with very many resource records might be processed very inefficiently, in extreme cases taking even several CPU seconds for each such uncached message. For example, a few thousand A records can be squashed into one DNS message (limit is 64kB).	2019-12-16	<a href="#">5</a>	<a href="#">CVE-2019-19331</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libsixel_project -- libsixel	stb_image.h (aka the stb image loader) 2.23, as used in libsixel and other products, has a heap-based buffer over-read in stbi_load_main.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-19777</a> <a href="#">MISC</a>
libsixel_project -- libsixel	An issue was discovered in libsixel 1.8.2. There is a heap-based buffer over-read in the function load_sixel at loader.c.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-19778</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.3.11, sound/core/timer.c has a use-after-free caused by erroneous code refactoring, aka CID-e7af6307a8a5. This is related to snd_timer_open and snd_timer_close_locked. The timeri variable was originally intended to be for a newly created timer instance, but was used for a different purpose after refactoring.	2019-12-15	<a href="#">4.9</a>	<a href="#">CVE-2019-19807</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.4.2, the io_uring feature leads to requests that inadvertently have UID 0 and full capabilities, aka CID-181e448d8709. This is related to fs/io-wq.c, fs/io_uring.c, and net/socket.c. For example, an attacker can bypass intended restrictions on adding an IPv4 address to the loopback interface. This occurs because IORING_OP_SENDMSG operations, although requested in the context of an	2019-12-17	<a href="#">4.6</a>	<a href="#">CVE-2019-19241</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	unprivileged user, are sometimes performed by a kernel worker thread without considering that context.			
lout -- lout	Lout 3.40 has a heap-based buffer overflow in the srcnext() function in z02.c.	2019-12-20	<a href="#">6.8</a>	<a href="#">CVE-2019-19918</a> <a href="#">MISC</a>
lout -- lout	Lout 3.40 has a buffer overflow in the StringQuotedWord() function in z39.c.	2019-12-20	<a href="#">6.8</a>	<a href="#">CVE-2019-19917</a> <a href="#">MISC</a>
mahara -- mahara	Multiple cross-site scripting (XSS) vulnerabilities in Mahara 1.4.x before 1.4.3 and 1.5.x before 1.5.2 allow remote attackers to inject arbitrary web script or HTML via vectors related to (1) javascript innerHTML as used when generating login forms, (2) links or (3) resources URLs, and (4) the Display name in a user profile.	2019-12-17	<a href="#">4.3</a>	<a href="#">CVE-2012-2237</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
micro_focus -- arcsight_logger	Cross-Site Request Forgery vulnerability in all Micro Focus ArcSight Logger affecting all product versions below version 7.0. The vulnerability could be exploited to perform CSRF attack.	2019-12-17	<a href="#">6.8</a>	<a href="#">CVE-2019-11657</a> <a href="#">MISC</a>
nitro -- nitro_free_pdf_reader	The JBIG2Decode library in npdf.dll in Nitro Free PDF Reader 12.0.0.112 has a CAPPDAnnotHandlerUtils::PDAnnotHandlerDestroyData+0x208a Out-of-Bounds Read via crafted Unicode content.	2019-12-16	<a href="#">4.2</a>	<a href="#">CVE-2019-19818</a> <a href="#">MISC</a> <a href="#">MISC</a>
npm -- cli	Versions of the npm CLI prior to 6.13.3 are vulnerable to an Arbitrary File Write. It fails to prevent access to folders outside of the intended node_modules folder through the bin field. A properly constructed entry in the package.json bin field would allow a package publisher to modify and/or gain access to arbitrary files on a user's system when the package is installed. This behavior is still possible through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option.	2019-12-13	<a href="#">5.5</a>	<a href="#">CVE-2019-16776</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
npm -- cli	Versions of the npm CLI prior to 6.13.3 are vulnerable to an Arbitrary File Write. It is possible for packages to create symlinks to files outside of the node_modules folder through the bin field upon installation. A properly constructed entry in the package.json bin field would allow a package publisher to create a symlink pointing to arbitrary files on a user's system when the package is installed. This behavior is still possible	2019-12-13	<a href="#">4</a>	<a href="#">CVE-2019-16775</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option.			
npm -- cli	Versions of the npm CLI prior to 6.13.4 are vulnerable to an Arbitrary File Overwrite. It fails to prevent existing globally-installed binaries to be overwritten by other package installations. For example, if a package was installed globally and created a serve binary, any subsequent installs of packages that also create a serve binary would overwrite the previous serve binary. This behavior is still allowed in local installations and also through install scripts. This vulnerability bypasses a user using the --ignore-scripts install option.	2019-12-13	5.5	<a href="#">CVE-2019-16777</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
owncloud -- owncloud	Cross-site scripting (XSS) vulnerability in ownCloud 4.5.5, 4.0.10, and earlier allows remote attackers to inject arbitrary web script or HTML via the action parameter to core/ajax/sharing.php.	2019-12-17	4.3	<a href="#">CVE-2013-0202</a> <a href="#">MISC</a> <a href="#">MISC</a>
pen -- pen	Pen 0.18.0 has Insecure Temporary File Creation vulnerabilities	2019-12-13	4.6	<a href="#">CVE-2014-2387</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
petwant_and_skymee -- pf-103_and_petalk_ai	The udpServerSys service in Petwant PF-103 firmware 4.22.2.42 and Petalk AI 3.2.2.30 allows remote attackers to initiate firmware upgrades and alter device settings.	2019-12-13	5	<a href="#">CVE-2019-16731</a> <a href="#">MISC</a>
puppet -- puppet_agent	Previous versions of Puppet Agent didn't verify the peer in the SSL connection prior to downloading the CRL. This issue is resolved in Puppet Agent 6.4.0.	2019-12-16	5	<a href="#">CVE-2018-11751</a> <a href="#">MISC</a>
qpid-cpp -- qpid-cpp	qpid-cpp: ACL policies only loaded if the acl-file option specified enabling DoS by consuming all available file descriptors	2019-12-13	5	<a href="#">CVE-2014-0212</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Possibility of out of bound access in debug queue, if packet size field is corrupted in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial			



qualcomm -- multiple_snapdragon_products	IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCN7605, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2019-12-18	<a href="#">4.6</a>	<a href="#">CVE-2019-10584</a> <a href="#">CONFIRM</a>
red_hat -- cloudforms_management_engine	CFME: CSRF protection vulnerability via permissive check of the referrer header	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2014-0197</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- jboss_keycloak	JBoss KeyCloak: Open redirect vulnerability via failure to validate the redirect URL.	2019-12-15	<a href="#">5.8</a>	<a href="#">CVE-2014-3652</a> <a href="#">MISC</a> <a href="#">MISC</a>
samurai -- samurai	samurai 0.7 has a heap-based buffer overflow in canonpath in util.c via a crafted build file.	2019-12-13	<a href="#">6.8</a>	<a href="#">CVE-2019-19795</a> <a href="#">MISC</a>
sap -- treasury_and_risk_management	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-12-17	<a href="#">6.5</a>	<a href="#">CVE-2019-0383</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- treasury_and_risk_management	Transaction Management in SAP Treasury and Risk Management (corrected in S4CORE versions 1.01, 1.02, 1.03, 1.04 and EA-FINSERV versions 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0) does not perform necessary authorization checks for functionalities that require user identity.	2019-12-17	<a href="#">6.5</a>	<a href="#">CVE-2019-0384</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
solarwinds -- serv-u_ftp_server	A CSV injection vulnerability exists in the web UI of SolarWinds Serv-U FTP Server v15.1.7.	2019-12-16	<a href="#">4</a>	<a href="#">CVE-2019-13181</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
sonicwall -- sma100_devices	Vulnerability in SonicWall SMA100 allow unauthenticated user to gain read-only access to unauthorized resources. This vulnerability impacted SMA100 version	2019-12-17	<a href="#">5</a>	<a href="#">CVE-2019-7481</a> <a href="#">CONFIRM</a>

	9.0.0.3 and earlier.			
spip -- spip	_core_/plugins/medias in SPIP 3.2.x before 3.2.7 allows remote authenticated authors to inject content into the database.	2019-12-17	4	<a href="#">CVE-2019-19830</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
sqlite -- sqlite	exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because constant integer values in ORDER BY clauses of window definitions are mishandled.	2019-12-18	5	<a href="#">CVE-2019-19880</a> <a href="#">MISC</a>
suphp -- suphp	suPHP before 0.7.2 source-highlighting feature allows security bypass which could lead to arbitrary code execution	2019-12-13	4.4	<a href="#">CVE-2014-1867</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tematres -- tematres	TemaTres 3.0 has reflected XSS via the replace_string or search_string parameter to the vocab/admin.php?doAdmin=bulkReplace URI.	2019-12-13	4.3	<a href="#">CVE-2019-14344</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco -- spotfire_analytics_platform	The Spotfire library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains a vulnerability that theoretically allows an attacker to perform a reflected cross-site scripting (XSS) attack. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0.	2019-12-17	4.3	<a href="#">CVE-2019-17337</a> <a href="#">MISC</a> <a href="#">MISC</a>
typo3 -- typo3	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. Because escaping of user-submitted content is mishandled, the class QueryGenerator is vulnerable to SQL injection. Exploitation requires having the system extension ext:lowlevel installed, and a valid backend user who has administrator privileges.	2019-12-17	6.5	<a href="#">CVE-2019-19850</a> <a href="#">MISC</a> <a href="#">MISC</a>
veracrypt -- veracrypt	VeraCrypt 1.24 allows Local Privilege Escalation during execution of VeraCryptExpander.exe.	2019-12-13	4.6	<a href="#">CVE-2019-19501</a> <a href="#">MISC</a> <a href="#">MISC</a>

wordpress -- wordpress	The quiz-master-next (aka Quiz And Survey Master) plugin before 6.3.5 for WordPress is affected by: Cross Site Scripting (XSS). The impact is: Allows an attacker to execute arbitrary HTML and JavaScript code via the from or till parameter (and/or the quiz_id parameter). The component is: admin/quiz-options-page.php. The attack vector is: When the Administrator is logged in, a reflected XSS may execute upon a click on a malicious URL.	2019-12-13	4.3	<a href="#">CVE-2019-17599</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
yabasic -- yabasic	Yabasic 2.86.2 has a heap-based buffer overflow in myformat in function.c via a crafted BASIC source file.	2019-12-13	6.8	<a href="#">CVE-2019-19796</a> <a href="#">MISC</a>
zend_framework -- zend_framework	ZF2014-03 has a potential cross site scripting vector in multiple view helpers	2019-12-15	4.3	<a href="#">CVE-2014-4913</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zulip -- zulip_server	The image thumbnailing handler in Zulip Server versions 1.9.0 to before 2.0.8 allowed an open redirect that was visible to logged-in users.	2019-12-18	5.8	<a href="#">CVE-2019-19775</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
altn -- mdaemon_email_server	MDaemon Email Server 17.5.1 allows XSS via the filename of an attachment to an email message.	2019-12-17	3.5	<a href="#">CVE-2019-19497</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 12.3. A person with physical access to an iOS device may be able to see the email address used for iTunes.	2019-12-18	2.1	<a href="#">CVE-2019-8599</a> <a href="#">MISC</a>
apple -- ios	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 13. A person with physical access to an iOS device may be able to access contacts from the lock screen.	2019-12-18	2.1	<a href="#">CVE-2019-8742</a> <a href="#">MISC</a>
apple --	The issue was addressed with improved UI handling. This issue is fixed in iOS			<a href="#">CVE-2019-</a>

ios_and_watchos	12.4, watchOS 5.3. A user may inadvertently complete an in-app purchase while on the lock screen.	2019-12-18	<a href="#">2.1</a>	<a href="#">8682</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_mojave	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.4. Processing malicious data may lead to unexpected application termination.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8507</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8691</a> <a href="#">MISC</a>
apple -- macos_mojave	An access issue was addressed with improved memory management. This issue is fixed in macOS Mojave 10.14.4. A local user may be able to view a user's locked notes.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8537</a> <a href="#">MISC</a>
apple -- macos_mojave	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. A malicious application may be able to read restricted memory.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8520</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Mojave 10.14.6. An application may be able to read restricted memory.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8692</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1. A local user may be able to modify protected parts of the file system.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8568</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory layout.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8510</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to determine kernel memory	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-6207</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	layout.			
apple -- tvos	An authentication issue was addressed with improved state management. This issue is fixed in tvOS 13. A local user may be able to leak sensitive user information.	2019-12-18	<a href="#">2.1</a>	<a href="#">CVE-2019-8704</a> <a href="#">MISC</a> <a href="#">MISC</a>
hammer_cli_foreman_github_cli_omni rails foreman -- hammer_cli_foreman_github_cli_omni rails foreman	File /etc/hammer/cli.modules.d/foreman.yml	2019-12-13	<a href="#">2.1</a>	<a href="#">CVE-2014-0241</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- api_connect	IBM API Connect 2018.1 through 2018.4.1.7 Developer Portal's user registration page does not disable password autocomplete. An attacker with access to the browser instance and local system credentials can steal the credentials used for registration. IBM X-Force ID: 163453.	2019-12-16	<a href="#">2.1</a>	<a href="#">CVE-2019-4444</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- case_builder_and_case_manager	The Case Builder component shipped with 18.0.0.1 through 19.0.0.2 and IBM Case Manager 5.1.1 through 5.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 162772.	2019-12-13	<a href="#">3.5</a>	<a href="#">CVE-2019-4426</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins buildgraph-view Plugin 1.8 and earlier does not escape the description of builds shown in its view, resulting in a stored XSS vulnerability exploitable by users able to change build descriptions.	2019-12-17	<a href="#">3.5</a>	<a href="#">CVE-2019-16562</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Weibo Plugin 1.0.1 and earlier stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2019-12-17	<a href="#">2.1</a>	<a href="#">CVE-2019-16572</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Pipeline Aggregator View Plugin 1.8 and earlier does not escape information shown on its view, resulting in a stored XSS vulnerability exploitable by attackers able to affects view content such as job display name or pipeline stage names.	2019-12-17	<a href="#">3.5</a>	<a href="#">CVE-2019-16564</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Mission Control Plugin 0.9.16 and earlier does not escape job display names and build names shown on its view, resulting in a stored XSS vulnerability exploitable by attackers able to change these properties.	2019-12-17	<a href="#">3.5</a>	<a href="#">CVE-2019-16563</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>



red_hat -- cloudforms_management_console	CFME (CloudForms Management Engine) 5: RHN account information is logged to /etc/ssh/ssh_host_rsa_key.pub during registration	2019-12-15	<a href="#">2.1</a>	<a href="#">CVE-2014-3536</a> <a href="#">MISC</a> <a href="#">MISC</a>
solarwinds -- serv-u_ftp_server	A stored cross-site scripting (XSS) vulnerability exists in the web UI of SolarWinds Serv-U FTP Server 15.1.7.	2019-12-16	<a href="#">3.5</a>	<a href="#">CVE-2019-13182</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3s-smart - multiple_codesys_products	3S-Smart CODESYS SP Realtime NT before V2.3.7.28, CODESYS Runtime Toolkit 32 bit full before V2.4.7.54 and CODESYS PLCWinNT before V2.4.7.54 allow a NULL pointer dereference.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19789</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
abb -- pb610_panel_builder_600	The HMISimulator component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier fails to validate the content-length field for HTTP requests, exposing HMISimulator to denial of service via crafted HTTP requests manipulating the content-length setting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18995</a> <a href="#">MISC</a>
	The HMISimulator component of ABB PB610 Panel Builder 600 uses			

abb -- pb610_panel_builder_600	the readFile/writeFile interface to manipulate the work file. Path configuration in PB610 HMISidePanel versions 2.8.0.424 and earlier potentially allows access to files outside of the working directory, thus potentially supporting unauthorized file access.	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-18997</a> <a href="#">MISC</a>
abb -- pb610_panel_builder_600	Due to a lack of file length check, the HMISidePanel component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier crashes when trying to load an empty *.JPR application file. An attacker with access to the file system might be able to cause application malfunction such as denial of service.	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-18994</a> <a href="#">MISC</a>
abb -- pb610_panel_builder_600	Path settings in HMISidePanel component of ABB PB610 Panel Builder 600 versions 2.8.0.424 and earlier accept DLLs outside of the program directory, - potentially allowing an attacker with access to the local file system the execution of code in the application?	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-18996</a> <a href="#">MISC</a>

	context.			
acer -- quick_access	<p>In the Quick Access Service (QAAAdminAgent.exe) in Acer Quick Access V2.01.3000 through 2.01.3027 and V3.00.3000 through V3.00.3008, a REGULAR user can load an arbitrary unsigned DLL into the signed service's process, which is running as NT AUTHORITY\SYSTEM. This is a DLL Hijacking vulnerability (including search order hijacking, which searches for the missing DLL in the PATH environment variable), which is caused by an uncontrolled search path element for nvapi.dll, atiadlxx.dll, or atiadlxy.dll.</p>	2019-12-17	not yet calculated	<a href="#">CVE-2019-18670</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
adobe -- coldfusion	<p>ColdFusion versions Update 6 and earlier have an insecure inherited permissions of default installation directory vulnerability. Successful exploitation could lead to privilege escalation.</p>	2019-12-19	not yet calculated	<a href="#">CVE-2019-8256</a> <a href="#">CONFIRM</a>
	<p>Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152</p>			

adobe -- acrobat_reader	and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16448</a> <a href="#">CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16457</a> <a href="#">CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16464</a> <a href="#">CONFIRM</a>
	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier,			

adobe -- acrobat_reader	2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a security bypass vulnerability. Successful exploitation could lead to arbitrary code execution.	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16453 CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16452 CONFIRM</a>
adobe -- acrobat_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16449 CONFIRM</a>
	Adobe Acrobat and Reader versions , 2019.021.20056			



adobe -- acrobat_and_reader	and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16465</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a binary planting (default folder privilege escalation) vulnerability. Successful exploitation could lead to privilege escalation.	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16444</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-16445</a> <a href="#">CONFIRM</a>



	lead to arbitrary code execution .			
adobe -- acrobat_ and reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16463</a> <a href="#">CONFIRM</a>
adobe -- acrobat_ and reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16459</a> <a href="#">CONFIRM</a>
adobe -- acrobat_ and reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds read vulnerability.	2019-12-19	not yet calculated	<a href="#">CVE-2019-16461</a> <a href="#">CONFIRM</a>

	Successful exploitation could lead to information disclosure .			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16455</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16454</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an	2019-12-19	not yet calculated	<a href="#">CVE-2019-16458</a> <a href="#">CONFIRM</a>

	out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .			
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16462</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16446</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions , 2019.021.20056 and earlier, 2017.011.30152 and earlier, 2017.011.30155 and earlier version, 2017.011.30152 and earlier, and 2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	2019-12-19	not yet calculated	<a href="#">CVE-2019-16460</a> <a href="#">CONFIRM</a>



	2015.006.30505 and earlier have an untrusted pointer dereference vulnerability. Successful exploitation could lead to arbitrary code execution .	19		
adobe -- brackets	Brackets versions 1.14 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-8255</a> <a href="#">CONFIRM</a>
adobe -- photoshop CC	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-8253</a> <a href="#">CONFIRM</a>
adobe -- photoshop CC	Adobe Photoshop CC versions before 20.0.8 and 21.0.x before 21.0.2 have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-8254</a> <a href="#">CONFIRM</a>
apache -- http_server	A Path traversal exists in http_server which allows an attacker to read arbitrary system files.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15600</a> <a href="#">MISC</a>
	Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data			

apache --log4j	which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.	2019-12-20	not yet calculated	<a href="#">CVE-2019-17571</a> <a href="#">CONFIRM</a>
apache --xerces-c	The Apache Xerces-C 3.0.0 to 3.2.2 XML parser contains a use-after-free error triggered during the scanning of external DTDs. This flaw has not been addressed in the maintained version of the library and has no current mitigation other than to disable DTD processing. This can be accomplished via the DOM using a standard parser feature, or via SAX using the XERCES_DISABLE_DTD environment variable.	2019-12-18	not yet calculated	<a href="#">CVE-2018-1311</a> <a href="#">CONFIRM</a>
apple --macos_catalina	A validation issue existed in the entitlement verification. This issue was addressed with improved validation of the process entitlement. This issue is fixed in macOS Catalina 10.15.1. An	2019-12-18	not yet calculated	<a href="#">CVE-2019-8805</a> <a href="#">MISC</a>

	application may be able to execute arbitrary code with system privileges.			
apple -- macos_catalina	A validation issue was addressed with improved input sanitization. This issue is fixed in macOS Catalina 10.15.1. An application may be able to read restricted memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8817 MISC</a>
apple -- macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Catalina 10.15. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8701 MISC</a>
apple -- icloud_for_windows	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8710 MISC</a>
apple -- ios	A logic issue existed in the handling of answering phone calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.4. The initiator of a phone call may be able to cause the recipient to answer a	2019-12-18	not yet calculated	<a href="#">CVE-2019-8699 MISC</a>

	simultaneous Walkie-Talkie connection.			
apple -- ios	The issue was addressed with improved UI handling. This issue is fixed in iOS 12.3. The lock screen may show a locked icon after unlocking.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8630 MISC</a>
apple -- ios	This issue was addressed with improved checks. This issue is fixed in iOS 12.2. Processing a maliciously crafted mail message may lead to S/MIME signature spoofing.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7284 MISC</a>
apple -- ios	A consistency issue was addressed with improved state handling. This issue is fixed in iOS 12.2. A website may be able to access the microphone without the microphone use indicator being shown.	2019-12-18	not yet calculated	<a href="#">CVE-2019-6222 MISC</a>
apple -- ios	An API issue existed in the handling of microphone data. This issue was addressed with improved validation. This issue is fixed in iOS 12.2. A malicious application may be able to access the microphone without indication to the user.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8566 MISC</a>

apple -- ios	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.4. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7287</a> <a href="#">MISC</a>
apple -- ios	This issue was addressed with improved transparency. This issue is fixed in iOS 12.2. A user may authorize an enterprise administrator to remotely wipe their device without appropriate disclosure.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8512</a> <a href="#">MISC</a>
apple -- ios	This issue was addressed by improving Face ID machine learning models. This issue is fixed in iOS 13. A 3D model constructed to look like the enrolled user may authenticate via Face ID.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8760</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A logic issue applied the incorrect restrictions. This issue was addressed by updating the logic to apply the correct restrictions. This issue is fixed in iOS 13.1.1 and iPadOS 13.1.1. Third party app extensions may not receive the correct sandbox restrictions.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8779</a> <a href="#">MISC</a>



apple -- ios_and_ipados	The issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 13.1 and iPadOS 13.1. A person with physical access to an iOS device may be able to access contacts from the lock screen.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8775</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_ipados	A consistency issue existed in deciding when to show the screen recording indicator. The issue was resolved with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2. A local user may be able to record the screen without a visible screen recording indicator.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8793</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An inconsistency in Wi-Fi network configuration settings was addressed. This issue is fixed in iOS 13.2 and iPadOS 13.2. An attacker in physical proximity may be able to force a user onto a malicious Wi-Fi network during device setup.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8804</a> <a href="#">MISC</a>
apple -- ios_and_ipados	An issue existed in the drawing of web page elements. The issue was addressed with improved logic. This issue is fixed in iOS 13.1 and iPadOS 13.1.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8769</a> <a href="#">MISC</a>

	iPadOS 13.1, macOS Catalina 10.15. Visiting a maliciously crafted website may reveal browsing history.			
apple -- ios_and_ipad_and_macos_catalina	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Improper URL processing may lead to data exfiltration.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8788</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_ipad_and_macos_catalina	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1. Parsing a maliciously crafted iBooks file may lead to disclosure of user information.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8789</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_ipad_and_macos_catalina	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8795</a> <a href="#">MISC</a> <a href="#">MISC</a>
	This issue was addressed with			

apple -- ios_and_macos_mojave	improved checks. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. A malicious application may be able to overwrite arbitrary files.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8521</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. A local user may be able to read kernel memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8504</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8529</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.4, macOS Mojave 10.14.3 Supplemental Update. An application may be able to gain elevated privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7286</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An access issue was addressed with additional sandbox restrictions. This			

apple -- ios_and_macos_mojave_and_tvos	issue is fixed in iOS 12.2, macOS Mojave 10.14.4, and tvOS 12.2. A local user may be able to view sensitive user information.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8546</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave_and_tvos	This issue was addressed with improved checks. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2. A malicious application may be able to overwrite arbitrary files.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8530</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave_and_watchos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, and watchOS 5.2. A malicious application may be able to elevate privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8511</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_macos_mojave_and_watchos	An issue existed in the pausing of FaceTime video. The issue was resolved with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, and watchOS 5.2. A user's video may not be paused in a FaceTime call if they exit the FaceTime app while the call is ringing.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8550</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A logic issue was addressed with improved			

apple -- ios_and_safari	validation. This issue is fixed in iOS 12.2, Safari 12.1. Enabling the Safari Reader feature on a maliciously crafted webpage may lead to universal cross site scripting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8505</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_safari	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, Safari 12.1. Enabling the Safari Reader feature on a maliciously crafted webpage may lead to universal cross site scripting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-6204</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- ios_and_watchos	A privacy issue existed in motion sensor calibration. This issue was addressed with improved motion sensor processing. This issue is fixed in iOS 12.2, watchOS 5.2. A malicious app may be able to track users between installs.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8541</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_catalina	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Catalina 10.15. A malicious application may be able to determine kernel memory layout.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8755</a> <a href="#">MISC</a>
	A race condition existed when reading and writing user preferences. This was			



apple -- macos_catalina	addressed with improved state handling. This issue is fixed in macOS Catalina 10.15. The "Share Mac Analytics" setting may not be disabled when a user deselects the switch to share analytics.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8757</a> <a href="#">MISC</a>
apple -- macos_catalina	The contents of locked notes sometimes appeared in search results. This issue was addressed with improved data cleanup. This issue is fixed in macOS Catalina 10.15. A local user may be able to view a user's locked notes.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8730</a> <a href="#">MISC</a>
apple -- macos_catalina_and_itunes_for_windows	A dynamic library loading issue existed in iTunes setup. This was addressed with improved path searching. This issue is fixed in macOS Catalina 10.15.1, iTunes for Windows 12.10.2. Running the iTunes installer in an untrusted directory may result in arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8801</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- macos_mojave	A lock handling issue was addressed with improved lock handling. This issue is fixed in macOS Mojave 10.14.4. A Mac may not lock when disconnecting from	2019-12-18	not yet calculated	<a href="#">CVE-2019-8533</a> <a href="#">MISC</a>

	an external monitor.			
apple -- macos_mojave	A logic issue was addressed with improved state management. This issue is fixed in macOS Mojave 10.14.4. An encrypted volume may be unmounted and remounted by a different user without prompting for the password.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8522</a> <a href="#">MISC</a>
apple -- macos_mojave	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Mojave 10.14.4. An application may be able to read restricted memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8519</a> <a href="#">MISC</a>
apple -- macos_mojave	A validation issue existed in the handling of symlinks. This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Mojave 10.14.5. A local user may be able to load unsigned kernel extensions.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8606</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be	2019-12-18	not yet calculated	<a href="#">CVE-2019-8540</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	able to determine kernel memory layout.			
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8619</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted string may lead to a denial of service.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8516</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An API issue existed in the handling of dictation requests. This issue was addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to initiate a Dictation request without user authorization.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8502</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

apple -- multiple_products	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8527</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. Processing a maliciously crafted font may result in the disclosure of process memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8517</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. An application may be able to gain elevated privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8514</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may	2019-12-18	not yet calculated	<a href="#">CVE-2019-8545</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	be able to cause unexpected system termination or read kernel memory.			
apple -- multiple_products	Multiple input validation issues existed in MIG generated code. These issues were addressed with improved validation. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A local user may be able to read kernel memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7293</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Catalina 10.15, tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing a maliciously crafted text file may lead to arbitrary code	2019-12-18	not yet calculated	<a href="#">CVE-2019-8745</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	execution.			
apple -- multiple_products	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8535</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8544</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8551</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A buffer overflow was addressed with improved bounds checking.			

apple -- multiple_products	This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious application may be able to elevate privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8542</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8726</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8536</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS	2019-		<a href="#">CVE-2019-8523</a> <a href="#">MISC</a>

apple -- multiple_products	iTunes 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8782</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with kernel privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8786</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, macOS Mojave 10.14.4, tvOS 12.2, watchOS 5.2. A malicious	2019-12-18	not yet calculated	<a href="#">CVE-2019-8552</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	privileges.			
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8518</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8783</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. A malicious website may be able to execute scripts in the context of another	2019-12-18	not yet calculated	<a href="#">CVE-2019-8503</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	website.			
apple -- multiple_products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8607</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8808</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with	2019-12-18	not yet calculated	<a href="#">CVE-2019-8785</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	system privileges.			
apple -- multiple_products	An authentication issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. A local attacker may be able to login to the account of a previously logged in user without valid credentials..	2019-12-18	not yet calculated	<a href="#">CVE-2019-8803</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8583</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may	2019-12-18	not yet calculated	<a href="#">CVE-2019-7285</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>



	lead to arbitrary code execution.			
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8798</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue was addressed with improved logic. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may result in the disclosure of process memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7292</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8524</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Multiple memory corruption issues were addressed			

apple -- multiple_products	with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8733</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8587</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to read restricted memory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8794</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple --	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and	2019-		<a href="#">CVE-2019-8797</a> <a href="#">MISC</a>



multiple_products	iPadOS 13.2, macOS Catalina 10.15.1, tvOS 13.2, watchOS 6.1. An application may be able to execute arbitrary code with system privileges.	12-18	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, macOS Catalina 10.15.1, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. An application may be able to execute arbitrary code with system privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8784</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- shazam_android_app_and_shazam_ios_app	An injection issue was addressed with improved validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam iOS App Version 12.11.0. Processing a maliciously crafted URL may lead to arbitrary javascript code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8792</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- shazam_android_app_and_shazam_ios_app	An issue existed in the parsing of URL schemes. This issue was addressed with improved URL validation. This issue is fixed in Shazam Android App Version 9.25.0, Shazam	2019-12-18	not yet calculated	<a href="#">CVE-2019-8791</a> <a href="#">MISC</a> <a href="#">MISC</a>

	iOS App Version 12.11.0. Processing a maliciously crafted URL may lead to an open redirect.			
apple -- shortcuts_ios	An access issue was addressed with additional sandbox restrictions. This issue is fixed in Shortcuts 2.1.3 for iOS. A sandboxed process may be able to circumvent sandbox restrictions.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7290</a> <a href="#">MISC</a>
apple -- shortcuts_ios	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in Shortcuts 2.1.3 for iOS. A local user may be able to view sensitive user information.	2019-12-18	not yet calculated	<a href="#">CVE-2019-7289</a> <a href="#">MISC</a>
apple -- swift-nio-ssl	The issue was addressed by signaling that an executable stack is not required. This issue is fixed in SwiftNIO SSL 2.4.1. A SwiftNIO application using TLS may be able to execute arbitrary code.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8849</a> <a href="#">MISC</a>
apple -- texture_for_ios_and_texture_for_android	Some analytics data was sent using HTTP rather than HTTPS. This was addressed by no longer sending this analytics data. This issue is fixed in Texture 5.11.10 for iOS, Texture 4.22.0.4 for	2019-12-18	not yet calculated	<a href="#">CVE-2019-8632</a> <a href="#">MISC</a> <a href="#">MISC</a>

	Android. An attacker in a privileged network position may be able to intercept analytics data.			
apple -- watchos	An issue existed where partially entered passcodes may not clear when the device went to sleep. This issue was addressed by clearing the passcode when a locked device sleeps. This issue is fixed in watchOS 5.2. A partially entered passcode may not clear when the device goes to sleep.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8548</a> <a href="#">MISC</a>
apple -- xcode	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user privilege.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8721</a> <a href="#">MISC</a>
apple -- xcode	Multiple issues in ld64 in the Xcode toolchains were addressed by updating to version ld64-507.4. This issue is fixed in Xcode 11.0. Compiling code without proper input validation could lead to arbitrary code execution with user	2019-12-18	not yet calculated	<a href="#">CVE-2019-8722</a> <a href="#">MISC</a>

	privilege.			
apple -- xcode	A memory corruption issue was addressed with improved validation. This issue is fixed in Xcode 11.2. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8806</a> <a href="#">MISC</a>
apple -- xcode	A memory corruption issue was addressed with improved state management. This issue is fixed in Xcode 11.0. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8738</a> <a href="#">MISC</a>
apple -- xcode	A memory corruption issue was addressed with improved state management. This issue is fixed in Xcode 11.0. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8739</a> <a href="#">MISC</a>
apple -- xcode	A memory corruption issue was addressed with improved validation. This issue is fixed in Xcode 11.2. Processing a maliciously crafted file may lead to arbitrary code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-8800</a> <a href="#">MISC</a>
	In CloudVision Portal all releases in the 2018.1 and			

aristia -- cloudvision	2018.2 Code train allows users with read-only permissions to bypass permissions for restricted functionality via CVP API calls through the Configlet Builder modules. This vulnerability can potentially enable authenticated users with read-only access to take actions that are otherwise restricted in the GUI.	2019-12-19	not yet calculated	<a href="#">CVE-2019-18181</a> <a href="#">CONFIRM</a>
aristia -- cloudvision_portal	In CloudVision Portal (CVP) for all releases in the 2018.2 Train, under certain conditions, the application logs user passwords in plain text for certain API calls, potentially leading to user password exposure. This only affects CVP environments where: 1. Devices have enable mode passwords which are different from the user's login password, OR 2. There are configlet builders that use the Device class and specify username and password explicitly Application logs are not accessible or visible from the CVP GUI. Application logs can only be read	2019-12-19	not yet calculated	<a href="#">CVE-2019-18615</a> <a href="#">CONFIRM</a>



	by authorized users with privileged access to the VM hosting the CVP application.			
asus -- atk_package_execution_ind0	AsLdrSrv.exe in ASUS ATK Package before V1.0.0061 (for Windows 10 notebook PCs) could lead to unsigned code execution with additional execution. The user must put an application at a particular path, with a particular file name.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19235</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
asus -- hg100_and_ws-101_and_ts-101_devices	An issue was discovered on ASUS HG100 1.05.12, WS-101 1.05.12, and TS-101 1.05.12 devices using ZigBee PRO. Attackers can utilize the "discover ZigBee network procedure" to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15910</a> <a href="#">MISC</a>
asus -- hg100_and_ws-101_and_ts-101_devices	An issue was discovered on ASUS HG100 1.05.12, WS-101 1.05.12, and TS-101 1.05.12 devices using ZigBee PRO. Attackers can use the ZigBee trust center rejoin procedure to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15912</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered on			

asus -- hg100_ and ws- 101_ and ts- 101_devices	ASUS HG100 1.05.12, WS-101 1.05.12, and TS- 101 1.05.12 devices using ZigBee PRO. Because of insecure key transport in ZigBee communication, attackers can obtain sensitive information, cause a denial of service attack, take over smart home devices, and tamper with messages.	2019- 12- 20	not yet calculated	<a href="#">CVE-2019-15911</a> <a href="#">MISC</a>
atlassian - - bitbucket_kopano_group_core	HrAddFBBlock in libfreebusy/freebusyutil.cpp in Kopano Groupware Core before 8.7.7 allows out-of-bounds access, as demonstrated by mishandling of an array copy during parsing of ICal data.	2019- 12- 19	not yet calculated	<a href="#">CVE-2019-19907</a> <a href="#">MISC</a> <a href="#">MISC</a>
	There was a man- in-the-middle (MITM) vulnerability present in the Confluence Previews plugin in Confluence Server and Confluence Data Center. This plugin was used to facilitate communication with the Atlassian Companion application. The Confluence Previews plugin in Confluence Server and Confluence Data Center communicated with			

atlassian - - confluence	<p>the Companion application via the atlassian-domain-for-localhost-connections-only.com domain name, the DNS A record of which points at 127.0.0.1. Additionally, a signed certificate for the domain was publicly distributed with the Companion application. An attacker in the position to control DNS resolution of their victim could carry out a man-in-the-middle (MITM) attack between Confluence Server and Confluence Data Center (or Confluence Data Center) and the atlassian-domain-for-localhost-connections-only.com domain intended to be used with the Companion application. This certificate has been revoked, however, usage of the atlassian-domain-for-localhost-connections-only.com domain name was still present in Confluence Server and Confluence Data Center. An attacker could perform the described attack by denying their victim access to certificate</p>	2019-12-19	not yet calculated	<a href="#">CVE-2019-15006</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
--------------------------------	--	------------	--------------------	---

	revocation information, and carry out a man-in-the-middle (MITM) attack to observe files being edited using the Companion application and/or modify them, and access some limited user information.			
atlassian - crowd	Various resources in the Crowd Demo application of Atlassian Crowd before version 3.1.1 allow remote attackers to modify add, modify and delete users & groups via a Cross-site request forgery (CSRF) vulnerability. Please be aware that the Demo application is not enabled by default.	2019-12-17	not yet calculated	<a href="#">CVE-2017-18107 MISC</a>
atlassian - jira_application_links	The ListEntityLinksServlet resource in Application Links before version 5.0.12, from version 5.1.0 before version 5.2.11, from version 5.3.0 before version 5.3.7, from version 5.4.0 before 5.4.13, and from version 6.0.0 before 6.0.5 disclosed application link information to non-admin users via a missing permissions check.	2019-12-17	not yet calculated	<a href="#">CVE-2019-15011 MISC</a>
	An issue was			

backdrop -- backdrop_cms	discovered in Backdrop CMS 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying file type descriptions created by administrators. An attacker could potentially craft a specialized description, then have an administrator execute scripting when viewing the list of file types, aka XSS. This vulnerability is mitigated by the fact that an attacker must have a role with the "Administer file types" permission.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19903</a> <a href="#">MISC</a>
backdrop -- backdrop_cms	An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying content type names in the content creation interface. An attacker could potentially craft a specialized content type name, then have an editor execute scripting when creating content, aka XSS. This vulnerability is mitigated by the fact that an attacker must have a role with the "Administer content types"	2019-12-19	not yet calculated	<a href="#">CVE-2019-19900</a> <a href="#">MISC</a>



	permission.			
backdrop -- backdrop_	<p>An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It doesn't sufficiently filter output when displaying certain block descriptions created by administrators. An attacker could potentially craft a specialized description, then have an administrator execute scripting when configuring a layout, aka XSS. This issue is mitigated by the fact that the attacker would be required to have the permission to create custom blocks, which is typically an administrative task.</p>	2019-12-19	not yet calculated	<a href="#">CVE-2019-19901 MISC</a>
backdrop	<p>An issue was discovered in Backdrop CMS 1.13.x before 1.13.5 and 1.14.x before 1.14.2. It allows the upload of entire-site configuration archives through the user interface or command line. It does not sufficiently check uploaded archives for invalid data, allowing non-configuration scripts to potentially be uploaded to the</p>	2019-		

-- backdrop_cms	server. This issue is mitigated by the fact that the attacker would be required to have the "Synchronize, import, and export configuration" permission, a permission that only trusted administrators should be given. Other measures in the product prevent the execution of PHP scripts, so another server-side scripting language must be accessible on the server to execute code.	12-19	not yet calculated	<a href="#">CVE-2019-19902</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow OS Command Injection. The embedded 'dongle_bridge' program used to expose the functionalities of the ClickShare Button to the host, is vulnerable to OS command injection vulnerabilities. These vulnerabilities could lead to code execution on the ClickShare Button with the privileges of the user 'nobody'.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18830</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Barco ClickShare Button R9861500D01 devices before			

barco -- clickshare	1.9.0 have Improper Following of a Certificate's Chain of Trust. The embedded 'dongle_bridge' button_r9861500d0 program used to expose the functionalities of the ClickShare Button to a USB host, does not properly validate the whole certificate chain.	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-18826</a> <a href="#">MISC</a>
barco -- clickshare	On Barco ClickShare Button R9861500D01 devices (before firmware version 1.9.0) JTAG access is disabled after ROM code execution. This button_r9861500d0 means that JTAG access is possible when the system is running code from ROM before handing control over to embedded firmware.	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-18827</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Insufficiently Protected Credentials. The root account (present for access via the button_r9861500d0 interfaces, which are by default not enabled on production devices) of the embedded Linux on the ClickShare Button is using a weak password.	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-18828</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Barco ClickShare			

barco -- clickshare	Button R9861500D01 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Button implements encryption at rest which uses a one-time programmable (OTP) AES encryption key. This key is shared across all ClickShare Buttons of model R9861500D01.	2019-12-17	not yet calculated	<a href="#">CVE-2019-18832</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The ClickShare Button does not verify the integrity of the mutable content on the UBIFS partition before being used.	2019-12-17	not yet calculated	<a href="#">CVE-2019-18824</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information exposure (issue 2 of 2).. The encryption key of the media content which is shared between a ClickShare Button and a ClickShare Button is randomly generated for each new session and communicated	2019-12-17	not yet calculated	<a href="#">CVE-2019-18833</a> <a href="#">MISC</a> <a href="#">MISC</a>

	over a TLS connection. An attacker who is able to perform a Man-in-the-Middle attack between the TLS connection, is able to obtain the encryption key.			
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 allow Information Exposure. The button, r9861500d01 encrypted ClickShare Button firmware contains the private key of a test device-certificate.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18831</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare	Barco ClickShare Button R9861500D01 devices before 1.9.0 have Missing Support for Integrity Check. The Barco signed 'Clickshare For Windows.exe' binary on the ClickShare Button (R9861500D01) loads a number of DLL files dynamically without verifying their integrity.	2019-12-17	not yet calculated	<a href="#">CVE-2019-18829</a> <a href="#">MISC</a> <a href="#">MISC</a>
barco -- clickshare 100_devices	Barco ClickShare Huddle CS-100 devices before 1.9.0 and CSE-200 devices before 1.9.0 have incorrect Credentials Management. The ClickShare Base Unit implements encryption at rest using encryption keys which are	2019-12-17	not yet calculated	<a href="#">CVE-2019-18825</a> <a href="#">MISC</a> <a href="#">MISC</a>



	shared across all ClickShare Base Units of models CS-100 & CSE-200.			
beckhoff - - embedded	Beckhoff Embedded Windows PLCs through 3.1.4024.0, and Beckhoff Twincat on Windows Engineering stations, allow an attacker to achieve Remote Code Execution (as SYSTEM) via the Beckhoff ADS protocol.	2019-12-10	not yet calculated	<a href="#">CVE-2019-16871</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
broadcom - ca_client_automation_agent	An insecure file access vulnerability exists in CA Client Automation 14.0, 14.1, 14.2, and 14.3 Agent for Windows that can allow a local attacker to gain escalated privileges.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19231</a> <a href="#">CONFIRM</a>
cloud_foundry - cloud_controller	Cloud Foundry Cloud Controller API (CAPI), version 1.88.0, allows space developers to list all global service brokers, including service broker URLs and GUIDs, which should only be accessible to admins.	2019-12-19	not yet calculated	<a href="#">CVE-2019-11294</a> <a href="#">CONFIRM</a>
contao -- contao	Contao 4.0 through 4.8.5 has Insecure Permissions. Back end users can manipulate the details view URL to show pages and articles that have	2019-12-17	not yet calculated	<a href="#">CVE-2019-19712</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	not been enabled for them.			
cups -- cups	cups (Common Unix Printing System) 'Listen localhost:631' option not honored correctly which could provide unauthorized access to the system	2019-12-20	not yet calculated	<a href="#">CVE-2012-6094</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cyrus -- imap	An issue was discovered in Cyrus IMAP before 2.5.15, 3.0.x before 3.0.13, and 3.1.x through 3.1.8. If sieve script uploading is allowed (3.x) or certain non-default sieve options are enabled (2.x), a user with a mail account on the service can use a sieve script containing a fileinto directive to create any mailbox with administrator privileges, because of folder mishandling in autosieve_createfolder() in imap/lmtp_sieve.c.	2019-12-16	not yet calculated	<a href="#">CVE-2019-19783</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
cyrus -- sasl	cyrus-sasl (aka Cyrus SASL) 2.1.27 has an out-of-bounds write leading to unauthenticated remote denial-of-service in OpenLDAP via a malformed LDAP packet. The OpenLDAP crash is ultimately caused by an off-by-one error in	2019-12-19	not yet calculated	<a href="#">CVE-2019-19906</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>



dell -- rsa_identity	My Access Live module [MAL]. An authenticated malicious local user could potentially exploit this vulnerability by sending crafted URL with scripts. When victim users access the module through their browsers, the malicious code gets injected and executed by the web browser in the context of the vulnerable web application.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18571</a> <a href="#">MSC</a> and_governance
dell -- rsa_identity	The RSA Identity Governance and Lifecycle and RSA Via Lifecycle and Governance products prior to 7.1.1 P03 contain an Improper Authentication vulnerability. A Java JMX agent running on the remote host is configured with plain text password authentication. An unauthenticated remote attacker can connect to the JMX agent and monitor and manage the Java application.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18572</a> <a href="#">MSC</a> and_governance
	Settings for the Dell XPS 13 2-in-1 (7390) BIOS versions prior to 1.1.3 contain a configuration vulnerability. The BIOS configuration for the "Enable Thunderbolt (and			

dell -- xps_13_2- in-1_bios	PCIe behind TBT) pre-boot modules" setting is enabled by default. A local unauthenticated attacker with physical access to a user's system can obtain read or write access to main memory via a DMA attack during platform boot.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18579</a> <a href="#">MISC</a>
divisa_it -- proxia_suite	Divisa Proxia Suite 9 < 9.12.16, 9.11.19, 9.10.26, 9.9.8, 9.8.43 and 9.7.10, 10.0 < 10.0.32, and 10.1 < 10.1.5, SparkSpace 1.0 < 1.0.30, 1.1 < 1.1.2, and 1.2 < 1.2.4, and Proxia PHR 1.0 < 1.0.30 and 1.1 < 1.1.2 allows remote code execution via untrusted Java deserialization. The proxia-error cookie is insecurely deserialized in every request (GET or POST). Thus, an unauthenticated attacker can easily craft a seria1.0lized payload in order to execute arbitrary code via the prepareError function in the com.divisat.dv2ee.controller.MvCControllerServlet class of the dv2eemvc.jar component. allows remote code execution via untrusted Java deserialization.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18956</a> <a href="#">MISC</a>



	<p>The proxia-error cookie is insecurely deserialized in every request (GET or POST). Thus, an unauthenticated attacker can easily craft a serialized payload in order to execute arbitrary code via the prepareError function in the com.divisait.dv2ee.controller.MVCCControllerServlet class of the dv2eemvc.jar component. Affected products include Proxia Premium Edition 2017 and Sparkspace.</p>			
django -- django	<p>Django before 1.11.27, 2.x before 2.2.9, and 3.x before 3.0.1 allows account takeover. A suitably crafted email address (that is equal to an existing user's email address after case transformation of Unicode characters) would allow an attacker to be sent a password reset token for the matched user account. (One mitigation in the new releases is to send password reset tokens only to the registered user email address.)</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-19844</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a>
	Docker Engine before 1.8.3 and			

docker -- docker_engine and cs_docker_engine	CS Docker Engine before 1.6.2-CS7 do not use a globally unique identifier to store image layers, which makes it easier for attackers to poison the image cache via a crafted image in pull or push commands.	2019-12-17	not yet calculated	<a href="#">CVE-2014-8178</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
drupal -- drupal	The Views Dynamic Fields module through 7.x-1.0-alpha4 for Drupal makes insecure unserialize calls in handlers/views_handler_filter_dynamic_fields.inc, as demonstrated by PHP object injection, involving a field_names object and an Archive_Tar object, for file deletion. Code execution might also be possible.	2019-12-16	not yet calculated	<a href="#">CVE-2019-19826</a> <a href="#">MISC</a>
eclipse -- che	For Eclipse Che versions 6.16 to 7.3.0, with both authentication and TLS disabled, visiting a malicious web site could trigger the start of an arbitrary Che workspace. Che with no authentication and no TLS is not usually deployed on a public network but is often used for local installations (e.g. on personal laptops). In that case, even if the Che API is not	2019-12-19	not yet calculated	<a href="#">CVE-2019-17633</a> <a href="#">CONFIRM</a>

	exposed externally, some javascript running in the local browser is able to send requests to it.			
ecryptfs -- ecrpytfs- utils	ecryptfs-utils: suid helper does not restrict mounting filesystems with nosuid,nodev which creates a possible privilege escalation	2019- 12- 20	not yet calculated	<a href="#">CVE-2012-3409</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- kibana	Kibana versions before 6.8.6 and 7.5.1 contain a cross site scripting (XSS) flaw in the coordinate and region map visualizations. An attacker with the ability to create coordinate map visualizations could create a malicious visualization. If another Kibana user views that visualization or a dashboard containing the visualization it could execute JavaScript in the victim's browser.	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-7621</a> <a href="#">MISC</a> <a href="#">MISC</a>
excon_gem_for_ruby_on_rails -- excon_gem_for_ruby_on_rails	In RubyGem excon before 0.71.0, there was a race condition around persistent connections, where a connection which is interrupted (such as by a timeout) would leave data on the socket. Subsequent requests would then read this data,	2019- 12- 16	not yet calculated	<a href="#">CVE-2019-16779</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

	returning content from the previous response. The race condition window appears to be short, and it would be difficult to purposefully exploit this.			
ffjpeg --ffjpeg	bitstr_tell at bitstr.c in ffjpeg through 2019-08-21 has a NULL pointer dereference related to jfif_encode.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19887</a> <a href="#">MISC</a>
ffjpeg --ffjpeg	jfif_decode in jfif.c in ffjpeg through 2019-08-21 has a divide-by-zero error.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19888</a> <a href="#">MISC</a>
ge --s2020/s2020g	An issue was found in GE S2020/S2020G Fast Switch 61850, S2020/S2020G Fast Switch 61850 Versions 07A03 and prior. An attacker can inject arbitrary Javascript in a specially crafted HTTP request that may be reflected back in the HTTP response. The device is also vulnerable to a stored cross-site scripting vulnerability that may allow session hijacking, disclosure of sensitive data, cross-site request forgery (CSRF) attacks, and remote code execution.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18267</a> <a href="#">MISC</a>
	An issue was found in Git before			

git_project - git	v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. Recursive clones are currently affected by a vulnerability that is caused by too-lax validation of submodule names, allowing very targeted attacks via remote code execution in recursive clones.	2019-12-18	not yet calculated	<a href="#">CVE-2019-1387</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a>
gitlab --gitlab	An IDOR vulnerability exists in GitLab <v12.1.2, <v12.0.4, and <v11.11.6 that allowed uploading files from project archive to replace other users files potentially allowing an attacker to replace project binaries or other uploaded assets.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5469</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitlab --gitlab_community_and_enterprise	A command injection exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to inject commands via the API through the blobs scope.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15575</a> <a href="#">MISC</a>
gitlab --gitlab_community_and_enterprise	An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to view private system notes from a GraphQL endpoint.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15576</a> <a href="#">MISC</a>



gitlab -- gitlab_community_12.18_enterprise	An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.10 that allowed project milestones to be disclosed via groups browsing.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15577</a> <a href="#">MISC</a>
gitlab -- gitlab_community_12.18_enterprise	A authentication bypass vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.10 in the Salesforce login integration that could be used by an attacker to create an account that bypassed domain restrictions and email verification requirements.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5486</a> <a href="#">MISC</a>
gitlab -- enterprise	An improper access control vulnerability exists in Gitlab EE <v12.3.3, <v12.2.7, & <v12.1.13 that allowed the group search feature with Elasticsearch to return private code, merge requests and commits.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5487</a> <a href="#">MISC</a>
gitlab -- gitlab	A denial of service exists in gitlab <v12.3.2, <v12.2.6, and <v12.1.10 that would let an attacker bypass input validation in markdown fields take down the affected page.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15584</a> <a href="#">MISC</a>
	An improper access control vulnerability exists in GitLab <12.3.3			



				<a href="#">MISC</a>
handlebars - handlebars	<p>Versions of handlebars prior to 4.3.0 are vulnerable to Prototype Pollution leading to Remote Code Execution. Templates may alter an Object's __proto__ and __defineGetter__ properties, which may allow an attacker to execute arbitrary code through crafted payloads.</p>	2019-12-20	not yet calculated	<a href="#">CVE-2019-19919</a> <a href="#">MISC</a>
hcl_software - hcl_appscan_source	<p>HCL AppScan Source 9.0.3.13 and earlier is susceptible to cross-site scripting (XSS) attacks by allowing users to embed arbitrary JavaScript code in the Web UI.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-4388</a> <a href="#">CONFIRM</a>
hpe -- universal_infinity	<p>Security vulnerabilities in HPE UIoT version 1.2.4.2 could allow unauthorized remote access and access to sensitive data. HPE has addressed this issue in HPE UIoT: For customers with release UIoT 1.2.4.2 fixes are made available with 1.2.4.2 RP3 HF1. For customers with release older than 1.2.4.2, such as 1.2.4.1, 1.2.4.0, the resolution will be to upgrade to 1.2.4.2 RP3 HF1. Customers are requested to</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-11995</a> <a href="#">MISC</a>

	upgrade to the updated versions or contact HPE support for further assistance.			
huawei -- multiple_products	There is an information leakage vulnerability on some Huawei products (AR120-S; AR1200; AR1200-S; AR150; AR150-S; AR160; AR200; AR200-S; AR2200; AR2200-S; AR3200; AR3600). An attacker with low permissions can view some high-privilege information by running specific commands. Successful exploit could cause an information disclosure condition.	2019-12-16	not yet calculated	<a href="#">CVE-2019-5259</a> <a href="#">MISC</a>
humax -- wireless_voice_gateway_hgb10r-2_devices	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 devices. Admin credentials are sent over cleartext HTTP.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19890</a> <a href="#">MISC</a>
humax -- wireless_voice_gateway_hgb10r-2_devices	An issue was discovered on Humax Wireless Voice Gateway HGB10R-2 devices. The attacker can discover admin credentials in the backup file, aka backupsettings.conf.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19889</a> <a href="#">MISC</a>
	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site			

ibm -- cognos_analytics	request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 159356.	2019-12-20	not yet calculated	<a href="#">CVE-2019-4231</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- cognos_analytics	IBM Cognos Analytics 11.0 and 11.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 166204.	2019-12-20	not yet calculated	<a href="#">CVE-2019-4555</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- cognos_business_intelligence	IBM Cognos Business Intelligence 10.2.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 153179.	2019-12-20	not yet calculated	<a href="#">CVE-2018-1934</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
	IBM Financial Transaction Manager 3.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a			



ibm -- financial_transaction_manager	malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 172877.	2019-12-20	not yet calculated	<a href="#">CVE-2019-4742</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- financial_transaction_manager	IBM Financial Transaction Manager 3.0 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 172706.	2019-12-20	not yet calculated	<a href="#">CVE-2019-4736</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0.0 through 2.0.8 is vulnerable to a configuration overwrite that allows an unauthenticated user to login as "admin", and then execute code as root or SYSTEM via TM1 scripting. IBM X-Force ID: 172094.	2019-12-18	not yet calculated	<a href="#">CVE-2019-4716</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
intel -- active_management_technology	Insufficient input validation in subsystem for Intel(R) AMT before version 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via physical access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11086</a> <a href="#">MISC</a>

intel -- active_management technology	Logic issue in subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11131</a> <a href="#">MISC</a>
intel -- active_management technology	Insufficient input validation in subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11088</a> <a href="#">MISC</a>
intel -- active_management technology	Insufficient input validation in the subsystem for Intel(R) AMT before version 12.0.45 may allow an unauthenticated user to potentially enable escalation of privilege via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11107</a> <a href="#">MISC</a>
intel -- active_management technology	Insufficient input validation in the subsystem for Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable information disclosure via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0166</a> <a href="#">MISC</a>
	Insufficient input validation in the subsystem for Intel(R) AMT			

intel -- active_management_technology	before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable information disclosure via physical access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11100</a> <a href="#">MISC</a>
intel -- active_management_technology	Cross site scripting in subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow a privileged user to potentially enable escalation of privilege via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11132</a> <a href="#">MISC</a>
intel -- active_management_technology	Insufficient input validation in subsystem in Intel(R) AMT before versions 11.8.70, 11.11.70, 11.22.70 and 12.0.45 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0131</a> <a href="#">MISC</a>
intel -- converged_security_and_active_management_engine	Insufficient input validation in subsystem for Intel(R) CSME before versions 12.0.45 and 13.0.10 may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11108</a> <a href="#">MISC</a>
	Logic issue in subsystem for Intel(R) CSME before versions 12.0.45, 13.0.10			

intel -- converged	and 14.0.10 may allow a privileged user to potentially enable escalation of privilege and information disclosure via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11105</a> <a href="#">MISC</a>
intel -- converged	Insufficient input validation in firmware update software for Intel(R) CSME before versions 12.0.45, 13.0.10 and 14.0.10 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11103</a> <a href="#">MISC</a>
intel -- converged	Insufficient Input validation in the subsystem for Intel(R) CSME before versions 12.0.45, 13.0.10 and 14.0.10 may allow a privileged user to potentially enable denial of service via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0165</a> <a href="#">MISC</a>
intel -- converged	Authentication bypass in the subsystem for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11110</a> <a href="#">MISC</a>
	Heap overflow in subsystem in			

intel -- converged	Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow an unauthenticated user to potentially enable escalation of privileges, information disclosure or denial of service via adjacent access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0169</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient input validation in Intel(R) DAL software for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable information disclosure via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11102</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient input validation in MEInfo software for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11104</a> <a href="#">MISC</a> execution_engine



intel -- converged	Insufficient input validation in the subsystem for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable information disclosure via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11101</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient session validation in the subsystem for Intel(R) CSME before versions 11.8.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11106</a> <a href="#">MISC</a> execution_engine
intel -- converged	Insufficient input validation in the subsystem for Intel(R) CSME before versions 11.8.70, 12.0.45 and 13.0.10; Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow a privileged user to potentially enable information disclosure via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-0168</a> <a href="#">MISC</a> execution_engine
	Insufficient input validation in the subsystem for Intel(R) CSME			

intel -- converged	before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10; Intel(R) TXE before versions 3.10 and 4.0.20 may allow a privileged user to potentially enable escalation of privilege, information disclosure or denial of service via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11087</a> <a href="#">MISC</a>
intel -- dynamic_p	Improper permissions in the Intel(R) Dynamic Platform and Thermal Framework v8.3.10208.5643 allow an authenticated user to potentially execute code at an elevated level of privilege.	2019-12-16	not yet calculated	<a href="#">CVE-2019-0134</a> <a href="#">MISC</a>
intel -- ethernet_i218	Insufficient memory protection for Intel(R) Ethernet I218 Adapter driver for Windows* 10 before version 24.1 may allow an authenticated user to potentially enable information disclosure via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-11096</a> <a href="#">MISC</a>
intel -- fpga_sdk	Improper conditions check in the Linux kernel driver for the Intel(R) FPGA SDK for OpenCL(TM) Pro Edition before version 19.4 may allow an	2019-12-16	not yet calculated	<a href="#">CVE-2019-11165</a> <a href="#">MISC</a>

	authenticated user to potentially enable denial of service via local access.			
intel -- management_engine_driver_for_windows	Improper directory permissions in the installer for Intel(R) Management Engine Consumer Driver for Windows before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.10 and 14.0.10. Intel(R) TXE before versions 3.1.70 and 4.0.20 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-11097</a> <a href="#">MISC</a>
intel -- multiple_processors	Improper conditions check in voltage settings for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege and/or information disclosure via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-11157</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
intel -- multiple_processors	Improper conditions check in multiple Intel? Processors may allow an authenticated user to potentially enable partial escalation of privilege, denial of service and/or information disclosure via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14607</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
	Cryptographic timing conditions in			

intel -- multiple_products	the subsystem for Intel(R) PTT before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.0 and 14.0.10; Intel(R) TXE 3.1.70 and 4.0.20; Intel(R) SPS before versions SPS_E5_04.01.04.305.0, SPS_SoC-X_04.00.04.108.0, SPS_SoC-A_04.00.04.191.0, SPS_E3_04.01.04.086.0, SPS_E3_04.08.04.047.0 may allow an unauthenticated user to potentially enable information disclosure via network access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11090</a> <a href="#">MISC</a>
intel -- multiple_products	Insufficient access control in hardware abstraction driver for MEInfo software for Intel(R) CSME before versions 11.8.70, 11.11.70, 11.22.70, 12.0.45, 13.0.0, 14.0.10; TXEInfo software for Intel(R) TXE before versions 3.1.70 and 4.0.20; INTEL-SA-00086 Detection Tool version 1.2.7.0 or before; INTEL-SA-00125 Detection Tool version 1.0.45.0 or before may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11147</a> <a href="#">MISC</a>
	Insufficient memory protection			

intel -- network_adapters	in the Linux Administrative Tools for Intel(R) Network Adapters before version 24.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-0159</a> <a href="#">MISC</a>
intel -- nuc	Out of bounds write in firmware for Intel(R) NUC(R) may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14612</a> <a href="#">MISC</a>
intel -- nuc	Improper input validation in firmware for Intel(R) NUC(R) may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14609</a> <a href="#">MISC</a>
intel -- nuc	Improper access control in firmware for Intel(R) NUC(R) may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14610</a> <a href="#">MISC</a>
intel -- nuc	Integer overflow in firmware for Intel(R) NUC(R) may allow a privileged user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14611</a> <a href="#">MISC</a>
	Improper buffer restrictions in firmware for Intel(R) NUC(R)	2019-		



intel -- nuc	may allow an authenticated user to potentially enable escalation of privilege via local access.	12-16	not yet calculated	<a href="#">CVE-2019-14608</a> <a href="#">MISC</a>
intel -- quartus_prime_pro_edition	Null pointer dereference in the FPGA kernel driver for Intel(R) Quartus(R) Prime Pro Edition before version 19.3 may allow an authenticated user to potentially enable denial of service via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14604</a> <a href="#">MISC</a>
intel -- quartus_prime_edition	Improper permissions in the installer for the License Server software for Intel? Quartus? Prime Pro Edition before version 19.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14603</a> <a href="#">MISC</a>
intel -- rapid_storage_technology	Improper permissions in the executable for Intel(R) RST before version 17.7.0.1006 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-12-16	not yet calculated	<a href="#">CVE-2019-14568</a> <a href="#">MISC</a>
intel -- scs_platform_discovery_utility	Improper permissions in the installer for the Intel(R) SCS Platform Discovery Utility, all versions, may allow an authenticated user	2019-12-16	not yet calculated	<a href="#">CVE-2019-14605</a> <a href="#">MISC</a>

	to potentially enable escalation of privilege via local attack.			
intel -- server_platform	Logic issue in the subsystem for Intel(R) SPS before versions SPS_E5_04.01.04.275.0, SPS_SoC-X_04.00.04.100.0 and SPS_SoC-A_04.00.04.191.0 may allow a privileged user to potentially enable denial of service via local access.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11109</a> <a href="#">MISC</a>
ivanti -- workspace_control	In Ivanti Workspace Control before 10.3.180.0, a locally authenticated user with low privileges can bypass Managed Application Security by controlling an unspecified attack vector in Workspace Preferences, when it is enabled. As a result, the attacker can start applications that should be blocked.	2019-12-17	not yet calculated	<a href="#">CVE-2019-19675</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Rundeck Plugin 3.6.5 and earlier stores credentials unencrypted in its global configuration file and in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the	2019-12-17	not yet calculated	<a href="#">CVE-2019-16556</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

	master file system.			
jenkins -- jenkins	A missing permission check in Jenkins Build Failure Analyzer Plugin 1.24.1 and earlier allows attackers with Overall/Read permission to have Jenkins evaluate a computationally expensive regular expression.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16554</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Spira Importer Plugin 3.2.3 and earlier disables SSL/TLS certificate validation for the Jenkins master JVM.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16558</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins WebSphere Deployer Plugin 1.6.1 and earlier allows attackers with Overall/Read permission to perform connection tests and determine whether files with an attacker-specified path exist on the Jenkins master file system.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16559</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Gerrit Trigger Plugin 2.30.1 and earlier allows attackers to connect to an attacker-specified HTTP URL or SSH server using attacker-specified credentials.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16551</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Build Failure Analyzer Plugin 1.24.1 and earlier allows attackers to have Jenkins evaluate a computationally expensive regular expression.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16553</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins WebSphere Deployer Plugin 1.6.1 and earlier allows attackers to perform connection tests and determine whether files with an attacker-specified path exist on the Jenkins master file system.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16560</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in a connection test form method in Jenkins Maven Release Plugin 0.16.1 and earlier allows attackers to have Jenkins connect to an attacker specified web server and parse XML documents.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16550</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A missing permission check in Jenkins Gerrit Trigger Plugin 2.30.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified	2019-12-	not yet calculated	<a href="#">CVE-2019-16552</a> <a href="#">MLIST</a>

	HTTP URL or SSH server using attacker-specified credentials, or determine the existence of a file with a given path on the Jenkins master.	17		<a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Maven Release Plugin 0.16.1 and earlier does not configure the XML parser to prevent XML external entity (XXE) attacks, allowing man-in-the-middle attackers to have Jenkins parse crafted XML documents.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16549</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A user-supplied regular expression in Jenkins Build Failure Analyzer Plugin 1.24.1 and earlier was processed in a way that wasn't interruptible, allowing attackers to have Jenkins evaluate a regular expression without the ability to interrupt this process.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16555</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Redgate SQL Change Automation Plugin 2.0.3 and earlier stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-12-17	not yet calculated	<a href="#">CVE-2019-16557</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>



joomla! -- joomla!	dataForDependantField in models/customfields.php in the JS JOBS FREE extension before 1.2.7 for Joomla! allows SQL Injection via the index.php? option=com_jsjobs&task=customfields.getfieldtitlebyfieldandfieldfo child parameter.	2019-12-19	not yet calculated	<a href="#">CVE-2019-17527</a> <a href="#">MISC</a>
lansweeper - lansweeper	The web console in Lansweeper 7.2.105.2 has XSS via the URL path. Product vulnerability has been fixed and disclosed within changelog as of 02 Dec 2019.	2019-12-19	not yet calculated	<a href="#">CVE-2019-18955</a> <a href="#">CONFIRM</a>
libreoffice - libreoffice	LibreOffice and OpenOffice automatically open embedded content	2019-12-20	not yet calculated	<a href="#">CVE-2012-5639</a> <a href="#">MISC</a> <a href="#">REDHAT</a> <a href="#">MISC</a> <a href="#">MISC</a>
maxum_development_corporat - rumpus_ftp_web_file_manager	A Reflected Cross Site Scripting was discovered in the Login page of Rumpus FTP Web File Manager 8.2.9.1. An attacker can exploit it by sending a crafted link to end users and can execute arbitrary Javascripts	2019-12-16	not yet calculated	<a href="#">CVE-2019-19368</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mediawiki -- mediawiki	The MinervaNeue Skin in MediaWiki from 2019-11-05 to 2019-12-13 (1.35 and/or 1.34) mishandles certain HTML attributes, as demonstrated by IMG onmouseover= (impact is XSS) and IMG src=http (impact is	2019-12-19	not yet calculated	<a href="#">CVE-2019-19910</a> <a href="#">MISC</a> <a href="#">MISC</a>

	disclosing the client's IP address). This can occur within a talk page topical header that is viewed within a mobile (MobileFrontend) context.			
midori -- midori_browser	In Midori Browser 0.5.11 (on Windows 10), Content Security Policy (CSP) is not applied correctly to all parts of multipart content sent with the multipart/x-mixed-replace MIME type. This could result in script running where CSP should have blocked it, allowing for cross-site scripting (XSS) and other attacks when the product renders the content as HTML. Remediating this would also need to consider the polyglot case, e.g., a file that is a valid GIF image and also valid JavaScript.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19916</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
myphpchat-plus -- myphpchat-plus	phpMyChat-Plus 1.98 is vulnerable to reflected XSS via JavaScript injection into the password reset URL. In the URL, the pmc_username parameter to pass_reset.php is vulnerable.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19908</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	NLSSRV32.EXE in Nalpeiron			

nalpeiron -- nalpeiron	Licensing Service 7.3.4.0, as used with Nitro PDF and other products, allows Elevation of Privilege via the \\mailslot\lsX86ccMails ot mailslot.	2019-12-17	not yet calculated	<a href="#">CVE-2019-19315</a> <a href="#">MISC</a>
nathack -- nathack	In NatHack between 3.6.0 and 3.6.3, a buffer overflow issue exists when reading very long lines from a NetHack configuration file (usually named .nethackrc). This vulnerability affects systems that have NetHack installed suid/sgid and shared systems that allow users to upload their own configuration files. All users are urged to upgrade to NetHack 3.6.4 as soon as possible.	2019-12-20	not yet calculated	<a href="#">CVE-2019-16787</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
negotiator -- negotiator	negotiator before 0.6.1 is vulnerable to a regular expression DoS	2019-12-20	not yet calculated	<a href="#">CVE-2016-100022</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nethack -- nethack	NetHack before 3.6.4 is prone to a buffer overflow vulnerability when reading very long lines from configuration files. This affects systems that have NetHack installed suid/sgid, and shared systems that allow users to upload their own configuration files.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19905</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

neuvector - neuvector	NeuVector 3.1 when configured to allow authentication via Active Directory, does not enforce non-empty passwords which allows an attacker with access to the Neuvector portal to authenticate as any valid LDAP user by providing a valid username and an empty password (provided that the active directory server has not been configured to reject empty passwords).	2019-12-20	not yet calculated	<a href="#">CVE-2019-19747</a> <a href="#">MISC</a> <a href="#">MISC</a>
node-df -- node-df	A code injection exists in node-df v0.1.4 that can allow an attacker to remote code execution by unsanitized input.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15597</a> <a href="#">MISC</a>
odoo -- community	Improper access control in the computed fields system of the framework of Odoo Community 13.0 and Odoo Enterprise 13.0 allows remote attackers to access sensitive information via crafted RPC requests, which could lead to privilege escalation.	2019-12-19	not yet calculated	<a href="#">CVE-2019-11780</a> <a href="#">MISC</a>
	In Omron PLC CJ series, all versions, and Omron PLC CS series, all versions, the			

omron -- cj_and_cs	software properly checks for the existence of a lock, but the programmable logic controllers externally controlled or influenced by an actor that is outside of the intended sphere of control.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18269</a> <a href="#">MISC</a>
omron -- cj_and_cs	In Omron PLC CJ series, all versions, and Omron PLC CS series, all versions, an attacker could monitor traffic between the PLC and the controller and replay requests that could result in the opening and closing of industrial valves.	2019-12-16	not yet calculated	<a href="#">CVE-2019-13533</a> <a href="#">MISC</a>
omron -- cj_and_cs	In Omron PLC CJ series, all versions and Omron PLC CS series, all versions, an attacker could spoof arbitrary messages or execute commands.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18259</a> <a href="#">MISC</a>
omron -- cj_and_nj	In Omron PLC CS series, all versions, Omron PLC CJ series, all versions, and Omron PLC NJ series, all versions, the software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more	2019-12-16	not yet calculated	<a href="#">CVE-2019-18261</a> <a href="#">MISC</a>



	susceptible to brute force attacks.			
opera -- opera_for	Opera for Android before 54.0.2669.49432 is vulnerable to a sandboxed cross-origin iframe bypass attack. By using a service working inside a sandboxed iframe it is possible to bypass the normal sandboxing attributes. This allows an attacker to make forced redirections without any user interaction from a third-party context.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19788</a> <a href="#">MISC</a>
palo_alto -- pan-os	Improper restriction of communications to Log Forwarding Card (LFC) on PA-7000 Series devices with second-generation Switch Management Card (SMC) may allow an attacker with network access to the LFC to gain root access to PAN-OS. This issue affects PAN-OS 9.0 versions prior to 9.0.5-h3 on PA-7080 and PA-7050 devices with an LFC installed and configured. This issue does not affect PA-7000 Series deployments using the first-generation SMC and the Log Processing Card (LPC). This issue	2019-12-20	not yet calculated	<a href="#">CVE-2019-17440</a> <a href="#">CONFIRM</a>

	<p>does not affect any other PA series devices. This issue does not affect devices without an LFC. This issue does not affect PAN-OS 8.1 or prior releases. This issue only affects a very limited number of customers and we undertook individual outreach to help them upgrade. At the time of publication, all identified customers have upgraded SW or content and are not impacted.</p>			
<p>pebble_templates - pebble_templates</p>	<p>Pebble Templates 3.1.2 allows attackers to bypass a protection mechanism (intended to block access to instances of java.lang.Class) because getClass is accessible via the public static java.lang.Class java.lang.Class.forName(java.lang.Module,java lang.String) signature.</p>	<p>2019-12-19</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19899 MISC</a></p>
	<p>An issue was found in Philips Veradius Unity, Pulsera, and Endura Dual WAN Router, Veradius Unity (718132) with wireless option (shipped between 2016-August 2018), Veradius Unity (718132) with ViewForum option</p>			

phillips -- multiple_router	(shipped between 2016-August 2018), Pulsera (718095) and Endura (718075) with wireless option (shipped between 26-June-2017 through 07-August 2018), Pulsera (718095) and Endura (718075) with ViewForum option (shipped between 26-June-2017 through 07-August 2018). The router software uses an encryption scheme that is not strong enough for the level of protection required.	2019-12-20	not yet calculated	<a href="#">CVE-2019-18263</a> <a href="#">MISC</a>
plex -- media_server	The Camera Upload functionality in Plex Media Server through 1.18.2.2029 allows remote authenticated users to write files anywhere the user account running the Plex Media Server has permissions. This allows remote code execution via a variety of methods, such as (on a default Ubuntu installation) creating a .ssh folder in the plex user's home directory via directory traversal, uploading an SSH authorized_keys file there, and logging into the host as the Plex	2019-12-19	not yet calculated	<a href="#">CVE-2019-19141</a> <a href="#">MISC</a>

	user via SSH.			
pronestor - pronestor	An issue was discovered in the Outlook add-in in Pronestor Planner before 8.1.77. There is local privilege escalation in the Health Monitor service because PronestorHealthMonitor.exe access control is mishandled, aka PNB-2359.	2019-12-18	not yet calculated	<a href="#">CVE-2019-17390</a> <a href="#">MISC</a> <a href="#">MISC</a>
public_knowledge - pkp-lib	An issue was discovered in Public Knowledge Project (PKP) pkp-lib before 3.1.2-2, as used in Open Journal Systems (OJS) before 3.1.2-2. Code injection can occur in the OJS report generator if an authenticated Journal Manager user visits a crafted URL, because unserialize is used.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19909</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Waitress through version 1.3.1 would parse the Transfer-Encoding header and only look for a single string value, if that value was not chunked it would fall through and use the Content-Length header instead. According to the HTTP standard Transfer-Encoding should be a comma separated list, with the inner-most encoding first,			

pylons_project - waitress	<p>followed by any further transfer codings, ending with chunked. Requests sent with: "Transfer-Encoding: gzip, chunked" would incorrectly get ignored, and the request would use a Content-Length header instead to determine the body size of the HTTP message. This could allow for Waitress to treat a single request as multiple requests in the case of HTTP pipelining. This issue is fixed in Waitress 1.4.0.</p>	2019-12-20	not yet calculated	<a href="#">CVE-2019-16786</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
pylons_project - waitress	<p>Waitress through version 1.3.1 implemented a "MAY" part of the RFC7230 which states: "Although the line terminator for the start-line and header fields is the sequence CRLF, a recipient MAY recognize a single LF as a line terminator and ignore any preceding CR." Unfortunately if a front-end server does not parse header fields with an LF the same way as it does those with a CRLF it can lead to the front-end and the back-end server parsing the same HTTP message in two different ways. This can lead to a</p>	2019-12-20	not yet calculated	<a href="#">CVE-2019-16785</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



	potential for HTTP request smuggling/splitting whereby Waitress may see two requests while the front-end server only sees a single HTTP message. This issue is fixed in Waitress 1.4.0.			
qualcomm -- multiple_snapdragon	Multiple read overflows in MM while decoding service accept,service reject,attach reject and MT detach in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, products MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937,	2019-12-18	not yet calculated	<a href="#">CVE-2019-10516</a> <a href="#">CONFIRM</a>

	MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130			
qualcomm -- multiple_snapdragon_products	Memory is being freed up twice when two concurrent threads are executing in parallel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9650,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10517</a> <a href="#">CONFIRM</a>

	MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8996AU, QCS405, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	Improper length check on source buffer to handle userspace data received can lead to out-of-bound access in diag handlers in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10544</a> <a href="#">CONFIRM</a>

	MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCN7605, QCS405, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	Out-of-bound read in the wireless driver in the Linux kernel due to lack of check of buffer length. in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10557</a> <a href="#">CONFIRM</a>

	MDM9607, MDM9650, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCN7605, QCS605, SDA660, SDA845, SDM630, SDM636, SDM660, SDX20, SDX55, SXR1130			
qualcomm -- multiple_snapdragon_products	Potential double free scenario if driver receives another DIAG_EVENT_LOG_SUPPORTED event from firmware as the pointer is not set to NULL on first call in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8917,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10536</a> <a href="#">CONFIRM</a>



	MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA8081, QCA9377, QCA9379, QCN7605, QCS405, QCS605, SDA660, SDA845, SDM450, SDM630, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130			
	Use after free of a pointer in iWLAN scenario during netmgr state transition to CONNECT in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8064,			

qualcomm -- multiple_snapdragon_products	APQ8096AU, APQ8098, IPQ4019, IPQ8064, IPQ8074, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, SDA660, SDA845, SDM429, SDM439, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10518</a> <a href="#">CONFIRM</a>
	Buffer overflow during SIB read when network configures complete sib list along with first and last segment of other SIB in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,			

<p>qualcomm -- multiple_snapdragon_products</p>	<p>Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p>	<p>2019- 12- 18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10525</a> <a href="#">CONFIRM</a></p>
	<p>Improper validation</p>			

<p>of event buffer extracted from FW response can lead to integer overflow, which will allow to pass the length check and eventually will lead to buffer overwrite when event data is copied to context buffer in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music in MDM9607, Nicobar, QCA6574AU, QCN7605, QCS405, QCS605, SDM660, SDM845, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p>	<p>2019-12-18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10537</a> <a href="#">CONFIRM</a></p>
<p>Due to the use of non-time-constant comparison functions there is issue in timing side channels which can be used as a potential side channel for SUI corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon</p>			

<p>qualcomm -- multiple_snapdragon_products</p>	<p>Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9650, MSM8905, MSM8909, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCS404, QCS405, QCS605, QM215, SA6155P, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130</p>	<p>2019- 12- 18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10482</a> <a href="#">CONFIRM</a></p>
	<p>Out of bound access occurs while handling the WMI FW event due</p>			



<p>qualcomm</p> <p>--</p> <p>multiple_snapdragon_products</p>	<p>to lack of check of buffer argument which comes directly from the WLAN FW in Snapdragon Auto, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wired Infrastructure and Networking in APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8996AU, QCA6574AU, QCA8081, QCN7605, SDX55, SM6150, SM7150, SM8150</p>	<p>2019-12-18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10481</a></p> <p><a href="#">CONFIRM</a></p>
	<p>Buffer over read can happen while parsing SMS OTA messages at transport layer if network sends unintended values in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon Wearables in APQ8009,</p>			

<p>qualcomm -- multiple_snapdragon_products</p>	<p>APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130</p>	<p>2019- 12- 18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-10487</a> <a href="#">CONFIRM</a></p>
	<p>Possibility of Null pointer access if the SPDM commands are executed in the non-standard way in Trustzone in Snapdragon Auto,</p>			

	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, IPQ8074, MDM9205, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA8081, QCS404, QCS605, QM215, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10513</a> <a href="#">CONFIRM</a>
--	---	--------------------	--------------------	---

	SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130, SXR2130			
qualcomm -- multiple_sn	<p>Possible OOB issue in EEPROM due to lack of check while accessing memory map array at the time of reading operation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &amp; Music, Snapdragon products</p> <p>Wearables in APQ8009, APQ8053, MSM8909W, MSM8917, MSM8953, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA845, SDM429, SDM439, SDM450, SDM632, SDM670, SDM710, SDM845, SDX24, SDX55, SM6150, SM7150, SM8150, SM8250,</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-10564</a> <a href="#">CONFIRM</a>

	SXR1130, SXR2130			
qualcomm -- multiple_snapdragon_products	While processing MT Secondary PDP request, Buffer overflow will happen due to incorrect calculation of buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096, APQ8096AU, APQ8098, MDM9150, MDM9205, MDM9206, MDM9607, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8939, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10500 CONFIRM</a>



	SC8180X, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDM850, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130			
qualcomm -- multiple_snapdragon_products	Improper check in video driver while processing data from video firmware can lead to integer overflow and then buffer overflow in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	2019- 12- 18	not yet calculated	<a href="#">CVE-2019-10572</a> <a href="#">CONFIRM</a>

	MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCS405, QCS605, QM215, SA6155P, SDA660, SDA845, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SDX55, SM6150, SM7150, SM8150, SXR1130			
rack_gem - rack_gem	<p>There's a possible information leak / session hijack vulnerability in Rack (RubyGem rack). This vulnerability is patched in versions 1.6.12 and 2.0.8. Attackers may be able to find and hijack sessions by using timing attacks targeting the session id. Session ids are usually stored and indexed in a database that uses <del>some kind of</del> <del>some kind of</del> rails - scheme for <del>speeding up</del> <del>speeding up</del> rails lookups of that session id. By carefully measuring the amount of time it</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-16782</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	<p>takes to look up a session, an attacker may be able to find a valid session id and hijack the session. The session id itself may be generated randomly, but the way the session is indexed by the backing store does not use a secure comparison.</p>			
<p>red_hat -- ansible_tower</p>	<p>A flaw was found in Ansible Tower, versions 3.6.x before 3.6.2 and 3.5.x before 3.5.4, when /websocket is requested and the password contains the '#' character. This request would cause a socket error in RabbitMQ when parsing the password and an HTTP error code 500 and partial password disclose will occur in plaintext. An attacker could easily guess some predictable passwords or brute force the password.</p>	<p>2019-12-19</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19342</a> <a href="#">CONFIRM</a></p>
<p>red_hat -- ansible_tower</p>	<p>A flaw was found in Ansible Tower, versions 3.6.x before 3.6.2 and 3.5.x before 3.5.3, where enabling RabbitMQ manager by setting it with '-e rabbitmq_enable_manager=true' exposes the RabbitMQ</p>	<p>2019-12-19</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19340</a> <a href="#">CONFIRM</a></p>

	management interface publicly, as expected. If the default admin user is still active, an attacker could guess the password and gain access to the system.			
red_hat -- ansible_tower	A flaw was found in Ansible Tower, versions 3.6.x before 3.6.2, where files in '/var/backup/tower' are left world-readable. These files include both the SECRET_KEY and the database backup. Any user with access to the Tower server, and knowledge of when a backup is run, could retrieve every credential stored in Tower. Access to data is the highest threat with this vulnerability.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19341</a> <a href="#">CONFIRM</a>
red_hat -- jboss_application_server	An Elevated Privileges issue exists in JBoss AS 7 Community Release due to the improper implementation in the security context propagation. A thread gets reused from the thread pool that still retains the security context from the process last used, which lets a local user obtain elevated privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2012-2312</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Roxy Fileman			

<p>roxy_fileman - roxy_fileman</p>	<p>1.4.5 for .NET is vulnerable to path traversal. A remote attacker can write uploaded files to arbitrary locations via the RENAMEFILE action. This can be leveraged for code execution by uploading a specially crafted Windows shortcut file and writing the file to the Startup folder (because an incomplete blacklist of file extensions allows Windows shortcut files to be uploaded).</p>	<p>2019-12-16</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-19731</a> <a href="#">MISC</a> <a href="#">MISC</a></p>
<p>shadowsocks-libev - shadowsocks-libev</p>	<p>An exploitable information disclosure vulnerability exists in the network packet handling functionality of Shadowsocks-libev 3.3.2. When utilizing a Stream Cipher, a specially crafted set of network packets can cause an outbound connection from the server, resulting in information disclosure. An attacker can send arbitrary packets to trigger this vulnerability.</p>	<p>2019-12-18</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-5152</a> <a href="#">MISC</a></p>
	<p>shadow 4.8, in certain circumstances affecting at least Gentoo, Arch Linux, and Void</p>			



shadow -- shadow	Linux, allows local users to obtain root access because setuid programs are misconfigured. Specifically, this affects shadow 4.8 when compiled using --with-libpam but without explicitly passing --disable-account-tools-setuid, and without a PAM configuration suitable for use with setuid account management tools. This combination leads to account management tools (groupadd, groupdel, groupmod, useradd, userdel, usermod) that can easily be used by unprivileged local users to escalate privileges to root in multiple ways. This issue became much more relevant in approximately December 2019 when an unrelated bug was fixed (i.e., the chmod calls to suidusbins were fixed in the upstream Makefile which is now included in the release version 4.8).	2019-12-18	not yet calculated	<a href="#">CVE-2019-19882</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
simplifile - - recordfusion	In Simplifile RecordFusion through 2019-11-25, the logs and hist parameters allow remote attackers to access local files via a	2019-12-17	not yet calculated	<a href="#">CVE-2019-19264</a> <a href="#">MISC</a>

	logger/logs?/../ or logger/hist?/../ URI.			
solarwinds - serv- u_ftp_server	A cross-site scripting (XSS) vulnerability exists in SolarWinds Serv-U FTP Server 15.1.7 in the email parameter, a different vulnerability than CVE-2018-19934 and CVE-2019-13182.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19829</a> <a href="#">MISC</a>
sonicos -- ssl_vpn_name	Installation of the SonicOS SSLVPN NACagent 3.5 on the Windows operating system, an autorun value is created does not quote the path in quotes, so if a malicious binary by an attacker within the parent path could allow code execution.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7487</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Code injection in SonicWall SMA100 allows an authenticated user to execute arbitrary code in viewcacert.cacert. This vulnerability impacted SMA100 version 9.0.0.4 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7486</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Buffer overflow in SonicWall SMA100 allows an authenticated user to execute arbitrary code in DEARRegister CGI script. This vulnerability impacted SMA100 version 9.0.0.3 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7485</a> <a href="#">CONFIRM</a>
	In SonicWall			

sonicwall - - sma100_devices	SMA100, an unauthenticated Directory Traversal vulnerability in the handleWAFRedirect CGI allows the user to test for the presence of a file on the server.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7483</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Authenticated SQL Injection in SonicWall SMA100 allow user to gain read-only access to unauthorized resources using viewasacert CGI script. This vulnerability impacted SMA100 version 9.0.0.3 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7484</a> <a href="#">CONFIRM</a>
sonicwall - - sma100_devices	Stack-based buffer overflow in SonicWall SMA100 allows an unauthenticated user to execute arbitrary code in function libSys.so. This vulnerability impacted SMA100 version 9.0.0.3 and earlier.	2019-12-19	not yet calculated	<a href="#">CVE-2019-7482</a> <a href="#">CONFIRM</a>
statics_server - statics_server	A path traversal in statics-server exists in all version that allows an attacker to perform a path traversal when a symlink is used within the working directory.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15596</a> <a href="#">MISC</a>
sudo -- sudo	In Sudo through 1.8.29, an attacker with access to a Runas ALL sudoer account can impersonate a nonexistent user by invoking sudo with a numeric uid that is not	2019-12-19	not yet calculated	<a href="#">CVE-2019-19232</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	associated with any user.			
sudo -- sudo	In Sudo through 1.8.29, the fact that a user has been blocked (e.g., by using the ! character in the shadow file instead of a password hash) is not considered, allowing an attacker (who has access to a Runas ALL sudoer account) to impersonate any blocked user.	2019-12-19	not yet calculated	<a href="#">CVE-2019-19234</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
swagger - - swagger_u	swagger-ui has XSS in key names	2019-12-20	not yet calculated	<a href="#">CVE-2016-1000229</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sylabs -- singularity	Insecure permissions (777) are set on \$HOME/.singularity when it is newly created by Singularity (version from 3.3.0 to 3.5.1), which could lead to an information leak, and malicious redirection of operations performed against Sylabs cloud services.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19724</a> <a href="#">CONFIRM</a>
talend -- restlet_framework	An XML eXternal Entity (XXE) issue exists in Restlet 1.1.10 in an endpoint using SOAP transport, which lets a remote attacker obtain sensitive information.	2019-12-18	not yet calculated	<a href="#">CVE-2012-2656</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	In Tautulli 2.1.9,			

tautulli -- tautulli	CSRF in the /shutdown URI allows an attacker to shut down the remote media server. (Also, anonymous access can be achieved in applications that do not have a user login area).	2019-12-18	not yet calculated	<a href="#">CVE-2019-19833</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco -- multiple_tibco_products	The Visualizations component of TIBCO Software Inc.'s TIBCO Spotfire Analyst, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Deployment Kit, TIBCO Spotfire Desktop, and TIBCO Spotfire Desktop Language Packs contains a vulnerability that theoretically allows an attacker with permission to write DXP files to the Spotfire library to remotely execute code of their choice on the user account of other users who access the affected system. This attack is a risk only when the attacker has write access to a network file system shared with the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analyst: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0,	2019-12-17	not yet calculated	<a href="#">CVE-2019-17334</a> <a href="#">MISC</a> <a href="#">MISC</a>



	<p>10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0, TIBCO Spotfire Deployment Kit: versions 7.11.1 and below, TIBCO Spotfire Desktop: versions 7.11.1 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.1.0, 10.2.0, 10.3.0, 10.3.1, and 10.3.2, versions 10.4.0, 10.5.0, and 10.6.0, and TIBCO Spotfire Desktop Language Packs: versions 7.11.1 and below.</p>			
<p>tibco -- spotfire_analytics_platform_for_aws_marketplace_and_spotfire_server</p>	<p>The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to data cached from a data source, or a portion of a data source, that the attacker should not have access to. The attacker would need privileges to access Spotfire to the library.</p> <p>Affected releases</p>	<p>2019-12-17</p>	<p>not yet calculated</p>	<p><a href="#">CVE-2019-17335</a> MISC MISC</p>

	are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace: version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0.			
tibco -- spotfire_analytics_platform_for_aws_marketplace_and_spotfire_server	<p>The Data access layer component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace and TIBCO Spotfire Server contains multiple vulnerabilities that theoretically allow an attacker access to information that can lead to obtaining credentials used to access Spotfire data sources. The attacker would need privileges to save a Spotfire file to the library, and only applies in a situation where NTLM credentials, or a credentials profile is in use. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace:</p>	2019-12-17	not yet calculated	<a href="#">CVE-2019-17336</a> MISC MISC

	version 10.6.0 and TIBCO Spotfire Server: versions 7.11.7 and below, versions 7.12.0, 7.13.0, 7.14.0, 10.0.0, 10.0.1, 10.1.0, 10.2.0, 10.2.1, 10.3.0, 10.3.1, 10.3.2, 10.3.3, and 10.3.4, versions 10.4.0, 10.5.0, and 10.6.0.			
tree-kill --tree-kill	A Code Injection exists in treekill on Windows which allows a remote code execution when an attacker is able to control the input into the command.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15598</a> <a href="#">MISC</a>
tree-kill --tree-kill	A Code Injection exists in tree-kill on Windows which allows a remote code execution when an attacker is able to control the input into the command.	2019-12-18	not yet calculated	<a href="#">CVE-2019-15599</a> <a href="#">MISC</a>
trend_micro - apex_one	Trend Micro Apex One (2019) is affected by a cross-site scripting (XSS) vulnerability on the product console. Note that the Japanese version of the product is NOT affected.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19692</a> <a href="#">MISC</a>
trend_micro - apex_one	A vulnerability in Trend Micro Apex One and OfficeScan XG could allow an attacker to expose a masked credential key by manipulating page elements using developer tools.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19691</a> <a href="#">MISC</a>

	Note that the attacker must already have admin/root privileges on the product console to exploit this vulnerability.			
trend_micro-deep_security	A privilege escalation vulnerability in the Trend Micro Deep Security as a Service Quick Setup cloud formation template could allow an authenticated entity with certain unrestricted AWS execution privileges to escalate to full privileges within the target AWS account.	2019-12-16	not yet calculated	<a href="#">CVE-2019-18191</a> <a href="#">N/A</a>
trend_micro-housecall	A privilege escalation vulnerability in Trend Micro HouseCall for Home Networks (versions below 5.3.0.1063) could be exploited for home networks allowing an attacker to place a malicious DLL file into the application directory and elevate privileges.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19688</a> <a href="#">MISC</a>
trend_micro-housecall	Trend Micro HouseCall for Home Networks (versions below 5.3.0.1063) could be exploited via a DLL Hijack related to a vulnerability on the packer that the program uses.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19689</a> <a href="#">MISC</a>
	The Trend Micro Security 2020			

trend_micro- security_2020	consumer family of products contains a vulnerability that could allow a local attacker to disclose sensitive information or to create a denial-of-service condition on affected installations. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	2019-12-20	not yet calculated	<a href="#">CVE-2019-19693</a> <a href="#">MISC</a> <a href="#">MISC</a>
trend_micro- mobile_security_for_android	Trend Micro Mobile Security for Android (Consumer) versions 10.3.1 and below on Android 8.0+ has an issue in which an attacker could bypass the product's App Password Protection feature.	2019-12-18	not yet calculated	<a href="#">CVE-2019-19690</a> <a href="#">MISC</a>
trendnet -- tew-651br_and_tew-652brp_and_tew-652bru_devices	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. OS command injection occurs through the get_set.ccp lanHostCfg_HostName_1.1.1.0.0 parameter.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11399</a> <a href="#">MISC</a> <a href="#">MISC</a>
trendnet -- tew-651br_and_tew-652brp_and_tew-652bru_devices	An issue was discovered on TRENDnet TEW-651BR 2.04B1, TEW-652BRP 3.04b01, and TEW-652BRU 1.00b12 devices. A	2019-12-18	not yet calculated	<a href="#">CVE-2019-11400</a> <a href="#">MISC</a> <a href="#">MISC</a>



	buffer overflow occurs through the get_set.ccp ccp_act parameter.			
typo3 -- typo3	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. It has been discovered that the extraction of manually uploaded ZIP archives in Extension Manager is vulnerable to directory traversal. Admin privileges are required in order to exploit this vulnerability. (In v9 LTS and later, System Maintainer privileges are also required.)	2019-12-17	not yet calculated	<a href="#">CVE-2019-19848</a> <a href="#">MISC</a> <a href="#">MISC</a>
typo3 -- typo3	An issue was discovered in TYPO3 before 8.7.30, 9.x before 9.5.12, and 10.x before 10.2.2. It has been discovered that the classes QueryGenerator and QueryView are vulnerable to insecure deserialization. One exploitable scenario requires having the system extension ext:lowlevel (Backend Module: DB Check) installed, with a valid backend user who has administrator privileges. The	2019-12-17	not yet calculated	<a href="#">CVE-2019-19849</a> <a href="#">MISC</a> <a href="#">MISC</a>

	other exploitable scenario requires having the system extension ext:sys_action installed, with a valid backend user who has limited privileges.			
vmware -- vcenter	A security vulnerability in HPE OneView for VMware vCenter 9.5 could be exploited remotely to allow Cross-Site Scripting.	2019-12-18	not yet calculated	<a href="#">CVE-2019-11992</a> <a href="#">MISC</a>
wago -- pfc100_and_pfc200_interfaces	An exploitable denial of service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5078</a> <a href="#">MISC</a>
	An exploitable heap buffer overflow vulnerability exists in the iocheckd service "I/O-Chec" functionality of WAGO PFC 200			

wago -- pfc100_and_pfc200_devices	Firmware version 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5081</a> <a href="#">MISC</a> <a href="#">MISC</a>
wago -- pfc100_and_pfc200_devices	An exploitable information exposure vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause an external tool to fail, resulting in uninitialized stack data to be copied to the response packet buffer. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5073</a> <a href="#">MISC</a>
	An exploitable stack buffer overflow vulnerability exists in the command line utility getcouplerdetails of WAGO PFC200			

wago -- pfc100_and	Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets sent to the iocheckd service "I/O-Check" can cause a stack buffer overflow in the sub-process getcouplerdetails, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5075</a> <a href="#">MISC</a>
wago -- pfc100_and	An exploitable stack buffer overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware version 03.01.07(13), WAGO PFC200 Firmware version 03.00.39(12) and WAGO PFC100 Firmware version 03.00.39(12). A specially crafted set of packets can cause a stack buffer overflow, resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.	2019-12-18	not yet calculated	<a href="#">CVE-2019-5074</a> <a href="#">CONFIRM</a>
	An exploitable denial-of-service vulnerability exists in the iocheckd service ??I/O-			

wago -- pfc100_and_pfc200_devices	<p>Chec??</p> <p>functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC 100 Firmware version 03.00.39(12). A set of packets can cause a denial of service, resulting in the device entering an error state where it ceases all network communications. An attacker can send unauthenticated packets to trigger this vulnerability.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-5077</a> <a href="#">MISC</a>
wago -- pfc100_and_pfc200_devices	<p>An exploitable denial-of-service vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC 200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware version 03.00.39(12). A set of packets can cause a denial of service and weaken credentials resulting in the default documented credentials being applied to the device. An attacker can send an unauthenticated packet to trigger this vulnerability.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-5080</a> <a href="#">MISC</a>
	An exploitable heap buffer			



wago -- pfc100_and	<p>overflow vulnerability exists in the iocheckd service "I/O-Check" functionality of WAGO PFC200 Firmware versions 03.01.07(13) and 03.00.39(12), and WAGO PFC100 Firmware versions 03.00.39(12). A specially crafted set of packets can cause a heap buffer overflow, potentially resulting in code execution. An attacker can send unauthenticated packets to trigger this vulnerability.</p>	2019-12-18	not yet calculated	<a href="#">CVE-2019-5079</a> <a href="#">MISC</a>
wordpress - wordpress	<p>The "301 Redirects - Easy Redirect Manager" plugin before 2.45 for WordPress allows users (with subscriber or greater access) to modify, delete, or inject redirect rules, and exploit XSS, with the /admin-ajax.php?action=eps_redirect_save and /admin-ajax.php?action=eps_redirect_delete actions. This could result in a loss of site availability, malicious redirects, and user infections. This could also be exploited via CSRF.</p>	2019-12-19	not yet calculated	<a href="#">CVE-2019-19915</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Xerox AltaLink C8035 printers allow CSRF. A			

xerox -- altalink_c8035	request to add users is made in the Device User Data page form field to the xerox.set URI. (The frmUserName value must have a unique name.)	2019-12-18	not yet calculated	<a href="#">CVE-2019-19832</a> <a href="#">MISC</a>
xiaomi-- multiple_devices	An issue was discovered on Xiaomi DGNWG03LM, ZNCZ03LM, MCCGQ01LM, WSDCGQ01LM, RTCGQ01LM 5.5.48 devices. Because of insecure key support in ZigBee communication, attackers can obtain sensitive information, cause a denial of service attack, take over smart home devices, and tamper with messages.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15913</a> <a href="#">MISC</a>
xiaomi -- multiple_devices	An issue was discovered on Xiaomi DGNWG03LM, ZNCZ03LM, MCCGQ01LM, WSDCGQ01LM, RTCGQ01LM 5.5.48 devices. Attackers can utilize the "discover ZigBee network procedure" to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15915</a> <a href="#">MISC</a>
	An issue was discovered on Xiaomi DGNWG03LM, ZNCZ03LM, MCCGQ01LM,			

xiaomi -- multiple_devices	WSDCGQ01LM, RTCGQ01LM 5.5.48 devices. Attackers can use the ZigBee trust center rejoin procedure to perform a denial of service attack.	2019-12-20	not yet calculated	<a href="#">CVE-2019-15914</a> <a href="#">MISC</a> <a href="#">MISC</a>
yarn -- yarn	In Yarn before 1.21.1, the package install functionality can be abused to generate arbitrary symlinks on the host filesystem by using specially crafted "bin" keys. Existing files could be overwritten depending on the current user permission set.	2019-12-16	not yet calculated	<a href="#">CVE-2019-10773</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
zoho_manageengine-adselfservice_plus	An open redirect vulnerability was discovered in Zoho ManageEngine ADSelfService Plus 5.x before 5809 that allows attackers to force users who click on a crafted link to be sent to a specified external site.	2019-12-18	not yet calculated	<a href="#">CVE-2019-18781</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

---

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: United States  
Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fggurina@sunnyvale.ca.gov](mailto:fggurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for December 16, 2019  
**Date:** Monday, December 16, 2019 4:03:22 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)





### **LAPD must warn that making false complaints against officers is illegal, judge rules**

A judge has tentatively ruled that the Los Angeles Police Department must warn people that deliberately filing false complaints against officers is a misdemeanor under the law, a practice the city maintained was unconstitutional. Los Angeles Superior Court Judge Robert Broadbelt ruled in favor of the Los Angeles Police Protective League, the LAPD officers' labor union, which sued former Chief Charlie Beck and the city in September 2017.

[City News Service](#)

### **Secretly recorded conversations admissible in criminal cases**

Secretly recording someone else's conversation is illegal in California, but prosecutors can use the illicit recording as evidence in a criminal case, the state Supreme Court ruled Thursday. In their unanimous ruling, the justices cited a 1982 ballot measure passed by voters that allows all "relevant evidence" to be introduced in any criminal trial or pretrial hearing, the San Francisco Chronicle reported.

[AP](#)

### **Federal judge halts enforcement of L.A.'s NRA disclosure law**

A federal judge has blocked Los Angeles from enforcing a law requiring companies that seek contracts with the city to disclose whether they have ties to the National Rifle Assn. The preliminary injunction issued Wednesday marks an initial victory for the gun rights group, which sued the city earlier this year over the law.

[Los Angeles Times](#)

### **Supreme Court may hear Martin vs. Boise criminalizing homelessness case**

An Idaho lawsuit concerning how cities across the West enforce laws about sleeping in public - potentially changing how they treat their homeless populations - may be making its way to the Supreme Court. The high court is currently weighing an appeal to the case of Martin v. City of Boise, which emerged in 2009 when Robert Martin and five other homeless individuals challenged the Idaho city's ability to fine them for violating an anti-camping ordinance.

[Curbed](#)

### **Senate confirms Trump nominee as highest-ranking out gay judge**

In a counter-intuitive development, the U.S. Senate approved on Tuesday an openly gay federal prosecutor named by President Trump for a seat on the U.S. Ninth Circuit Court of Appeals, making him the highest-ranking openly gay federal judge in the country. The Republican-majority chamber approved Patrick Bumatay, who previously worked as a U.S. attorney in Southern California, to a lifetime seat on the federal appeals court. The vote was 53-40.

[Washington Blade](#)

### **Federal court says animal rights protesters OK to use bullhorns outside Six Flags**

Animal-rights protesters at Six Flags Discovery Kingdom in Vallejo must be allowed to use bullhorns to amplify their voices over the noise of the crowd without seeking police permission, a federal appeals court ruled Tuesday. "In a crowded park or bustling intersection, where a single voice is easily drowned out, volume enables speech," said the Ninth U.S. Circuit Court of Appeals in San Francisco.

[San Francisco Chronicle](#)

### **Panel poised to toss \$44M award to man shot by drunken cop**

The Seventh Circuit appeared convinced at oral arguments Tuesday that Chicago cannot be held liable for a police officer's off-duty misconduct, placing in jeopardy a historic \$44.7 million verdict against the city for a drunken cop's shooting of his friend. "Upholding this verdict really places responsibility on every police department in this circuit for anything a police officer does off-duty," U.S. Circuit Judge Diane Sykes said during Tuesday's hearing, in just one of many instances where she expressed skepticism about the jury verdict's legal grounds.

[Courthouse News Service](#)

### **Supreme Court vacates 9th Circuit Court's ruling on Alaska's \$500 limit for campaign contributions**

The U.S. Supreme Court vacated a Ninth Circuit Court decision that upheld Alaska's limitation on the amount an individual can contribute to a candidate for political office, or to an election-oriented group other than a political party. The case, Thompson v. Hebron, was a First Amendment challenge to Alaska's campaign finance law, including its contribution limits for state legislative candidates and its limit on contributions from out-of-state donors.

[Sit News](#)

### **U.S. Supreme Court rejects Trump bid to resume federal executions**

The U.S. Supreme Court on Friday rejected a request by President Donald Trump's administration to proceed with plans to carry out the first executions of federal death row inmates since 2003. The justices left in place a hold imposed by a federal judge on four executions that had been scheduled by U.S. Attorney General William Barr for this month and next month as Trump's administration embraces the death penalty at a time when increasing numbers of states have given up the practice.

[Reuters](#)

### **Calif. appeals court shoots down class cert bid in Twitter sex bias case**

A California state appeals court has ruled that Twitter Inc's lack of a

company-wide policy on job promotions precludes certification of a class of female software engineers who claim the social media giant routinely promoted men over women. A three-judge panel of the California Court of Appeal, First Appellate District in San Francisco on Wednesday found that the broad discretion that Twitter, represented by Lynne Hermle of Orrick Herrington & Sutcliffe, gave managers in deciding which engineers were promoted rendered the proposed class of about 135 female engineers inappropriate.

[Reuters](#)

### **Is encouraging or inducing the illegal entry of aliens 'constitutionally protected speech'?**

I've written before about the case of Evelyn Sineneng-Smith, who was convicted in U.S. District Court for the Northern District of California for the crime of illegally encouraging or inducing the entry of aliens not entitled to do so under the immigration laws. The crime for which she was convicted was 8 U.S.C. Section 1324(a)(1)(A)(iv), "Bringing in and harboring certain aliens".

[Center for Immigration Studies](#)

### **Judge urges Legislature to bar police from using 'deceptive schemes' to skirt Miranda rights**

A judge on California's top court implored the Legislature on Wednesday to bar a "pervasive" police practice of using deception to obtain confessions from suspects who have invoked their right to remain silent. "The use of deceptive schemes to continue questioning a suspect who has invoked Miranda rights appears to be a common police practice throughout California," Justice Goodwin Liu wrote in a dissent.

[Los Angeles Times](#)

### **Legal experts debate judicial independence in California**

Retaining judicial independence is an increasingly thorny proposition as judges grapple with politically charged elections, recall efforts and social media attacks. Legal experts explored this topic in a panel discussion Tuesday evening at the Commonwealth Club of San Francisco, concluding that eliminating elections altogether might be the logical solution.

[Courthouse News Service](#)

### **L.A. wins legal battle over laws meant to ease the way for homeless housing**

Los Angeles city officials won a key battle Thursday over a pair of local laws meant to ease the way for more housing for homeless people, defeating a challenge from a Venice group that sought to overturn the ordinances. Fight Back, Venice! sued the city over the two ordinances, arguing the city flouted state law when it approved the local laws.

[Los Angeles Times](#)

### **Rights groups urge secrecy for Nunes parody accounts**

A cadre of civil liberties groups filed an amicus brief in Devin Nunes' defamation lawsuit against Twitter, claiming the Republican congressman's attempt to unmask users behind parody accounts could lead to a First Amendment violation. In the 39-page brief filed late Monday in the Circuit Court of Henrico County, Virginia, attorneys with Public Citizen Litigation Group and the American Civil Liberties Union argued that forcing Twitter to reveal the people behind an account called Devin Nunes' Cow and a since-deleted account claiming to be the lawmaker's mother would run afoul of the right to free speech.

[Courthouse News Service](#)

### **Bribery conviction of ex-congressional aide is affirmed**

The Ninth U.S. Circuit Court of Appeals has affirmed the bribery conviction of a man who was at the time of his offense a field representative for then-U.S. Rep. Janice Hahn, now a member of the Los Angeles County Board of Supervisors, rejecting his contention that no "official act" was involved because he was powerless to provide the benefit he promised in exchange for a \$5,000 pay-off.

[Metropolitan News-Enterprise](#)

## **Prosecutors/ Prosecutions**

### **Pair of LA County sheriff's deputies charged with perjury, filing false reports**

Two Los Angeles County sheriff's deputies pleaded not guilty today to felony charges that they filed false reports and committed perjury relating to traffic stops made in 2016, the Los Angeles County District Attorney's Office announced. Michael Berk was charged in case BA482714 with four counts each of filing a false report and perjury. Justin Fisk was charged in case BA482715 with two counts each of filing a false report and perjury.

[Los Angeles County District Attorney's Office](#)

### **LAPD officer arrested after bodycam footage allegedly shows him fondling deceased woman's breasts**

A Los Angeles police officer was arrested Thursday after footage captured by a body-worn camera allegedly showed him fondling a deceased woman's breasts. On Thursday morning, investigators from the Los Angeles Police Department's Internal Affairs Division arrested 27-year-old David Rojas, a 4-year veteran of the department. Rojas was charged with one felony count of having sexual contact with human remains without authority, the Los Angeles County District Attorney's Office announced.

CBS [LA](#)

### **To bring a boy's murderers to justice, a prosecutor wrestled with his own childhood abuse**

Jon Hatami's voice shook and he stared down at the courthouse floor as reporters packed around him. Minutes before, the prosecutor had won a

conviction in the killing of Gabriel Fernandez, one of the most infamous and chilling child abuse cases in California history. When paramedics arrived at Gabriel's Palmdale home in the spring of 2013, the 8-year-old had shattered ribs, a cracked skull and cigarette burns dotting his unconscious body, signs of the torture inflicted by his mother and her boyfriend.

[Los Angeles Times](#)

### **L.A. City Attorney warns of pet scams: 'These are not gentle people'**

Surrounded by city officials holding wide-eyed puppies, Los Angeles City Attorney Mike Feuer told reporters on Thursday that although the small dogs can steal people's hearts, criminals are online looking to steal money from unsuspecting hopeful pet owners. "Most victims who are swindled never get a puppy at all, others get different dogs with health or genetic problems, and the majority of victims are too embarrassed to come forward," Feuer said.

[City News Service](#)

### **Bellflower man charged with murder in Inglewood shooting**

Prosecutors filed a murder case Friday against a Bellflower man accused of shooting another man to death in Inglewood in September, authorities said. Lancelot Joshua Wilbur, 38, of Bellflower, is accused in the Sept. 27 killing of 23-year-old Adrian Dewayne Johnson of Inglewood in the 100 block of North Ash Street, according to Inglewood Police Department officials and Los Angeles County booking records.

[KTLA](#)

### **Tampering with food charge only filed twice in Kern in past four years: Once for allegedly spitting in a burger, once for suspected poisoned pudding**

The charge of attempting to mingle harmful substances with food or drink is one the Kern County District Attorney's office is rarely asked to file. In fact, it's only been filed twice in the past four years. "We don't often get referrals for this charge," said DA's office spokesman Joseph Kinzel.

[KGET](#)

### **LA County District Attorney candidates promise reforms, chide incumbent**

Candidates vying to be Los Angeles County's top prosecutor promised Friday to cease death penalty convictions, bolster police accountability and rollback policies embraced by incumbent District Attorney Jackie Lacey, who skipped the campaign debate. The March 2020 primary election for the leadership role at the largest prosecutorial agency in the country has been framed by social movements as a referendum on Lacey's record in office.

[Courthouse News Service](#)



## **LA City Attorney talks scooter DUIs, porch pirates and whether homeless people have right to sleep on sidewalks (Video)**

Los Angeles City Attorney Mike Feuer spoke with Eyewitness News about the penalties for DUI on a scooter, how to protect yourself from porch pirates, and whether homeless people should have the right to sleep on sidewalks.

[ABC7](#)

## **States prepare to purge tens of thousands of pot convictions**

With the tap of a computer key, prosecutors in Los Angeles and Chicago plan over the coming weeks to erase tens of thousands of marijuana convictions from people's criminal records, a key part of a progressive crime-fighting strategy that is seeking to rectify the wrongs of a decades-long drug war.

[Los Angeles Times](#)

## **Policy Legal Issues**

### **LAX chief's side-job on a corporate board could violate city ethics rules**

In what could amount to a violation of city ethics rules, an appointee of Mayor Eric Garcetti accepted a paid board position at an outside company in October without getting formal approval, records show. Deborah Flint, who earns more than \$390,000 overseeing Los Angeles International Airport and Van Nuys Airport, is on the board of Honeywell International, which has sought contracts with the city.

[Los Angeles Times](#)

### **San Diego launching police home-buying incentive to help with officer shortage**

San Diego's chronic police officer shortage has prompted the city to start a home-buying incentive that will give officers as much as \$50,000 toward a down payment if they buy a house in the city. The \$750,000 program will help the Police Department recruit and retain more officers, while also boosting community policing by encouraging more officers to live in the city instead of other parts of the region, city officials said.

[Los Angeles Times](#)

### **After robberies, California city considers new police tech**

Davis, Calif., may install surveillance cameras throughout the city, after a series of armed robberies in the last two months have prompted officials to find more ways to deter crime. In a presentation to the Davis City Council this week, Davis Police Chief Darren Pytel asked city officials to consider buying more cameras or automated license plate reader technology to deter certain criminal activity and assist in investigations.

[Sacramento Bee](#)

### **OC sheriff's officials selective in punishing deputies who mishandled evidence over two-year period**

Orange County sheriff's officials selectively punished deputies who mishandled evidence over a two-year period, protecting some employees deemed to be in the "cool kids club," according to recent testimony during a confidential personnel hearing. Retired Sgt. William West testified in September that he was told by Detective Kristin Hayman, who worked on an audit of evidence problems, that deputies favored or assigned to special details were spared punishment.

[Orange County Register](#)

### **LAPD is considering using a lasso, kind of like Wonder Woman**

The Los Angeles Police Department will begin testing a device designed to ensnare a person from a distance, giving officers an alternative to firing a Taser or a gun, as police departments nationwide are being criticized for their uses of force. The Los Angeles Times reports Tuesday that officers will start testing the non-lethal tool for free for 90 days beginning in January.

[NBC4](#)

### **Houston police chief vents frustrations over gun legislation (Video)**

Houston Police Chief Art Acevedo criticized politicians for failing to act on the Violence Against Women Act over fear of the NRA.

[NBC News](#)

### **Changing the culture of community supervision**

The U.S. probation and parole system, generally referred to as community supervision, is at a crossroads. An analysis of research gathered by Pew Charitable Trusts and Arnold Ventures, shows that since 1980 the population under community supervision has grown 239 percent. Today, 4.5 million Americans are under probation or parole - larger than the combined population of the country's jails and prisons.

[The Crime Report](#)

### **Los Angeles Rams continue to inspire at Camarillo youth facility, now with a foodie twist**

A relationship between a pro football team and a youth correctional institution outside Camarillo has, for the past year and a half, bloomed in unexpected ways. The Los Angeles Rams first visited the Ventura Youth Correctional Facility in May 2018, when a high-profile "Cleats for Character" session brought current and former players from the NFL team to the campus for a motivational event that included play time on the outdoor field.

[Ventura County Star](#)

## **Prop 47 & 57 & AB 109**

### **California's gray zone between good intentions and reality**

California is stuck in the gray zone. "Gray zone" is a military term for the space between peace and war, a time and place that provides

opportunities for the well-armed while posing dangers for citizens caught in the middle. In California today, I think the phrase explains the perilous condition of our communities as the state pursues major changes in how we regulate drugs, respond to homelessness and sentence criminals.

[The Mercury News](#)

### **Why the law?**

In the 1997 movie *The Devil's Advocate*, Al Pacino portrays Satan, and Keanu Reeves portrays his son, who is unaware that Pacino is his father. Reeves is a hotshot lawyer from Florida who is lured away to New York City to work for Pacino's law firm. Near the end of the movie, Reeves confronts Pacino about his identity. Pacino proceeds to give a speech about who he is and what his plans are. There is a revealing part of the speech where Reeves asks Pacino why he, Satan, is using the law as part of his plan.

[American Thinker](#)

## **Los Angeles County**

### **Lawsuit over fired LA Sheriff's deputy costing county taxpayers millions in attorney fees**

It should be no surprise that Los Angeles County is involved in a lot of lawsuits, but when was the last time you heard of the county suing itself? The skyrocketing costs of one particular lawsuit is costing millions of your tax dollars... with much of it pouring into the pockets of attorneys.

[ABC7](#)

### **Fired LA County sheriff's department deputy Caren Carl Mandoyan sues again**

Fired Los Angeles County sheriff's deputy Caren Carl Mandoyan is again asking a judge to reinstate him, this time based on a new report conducted by the sheriff's department that finds Mandoyan was denied due process. Mandoyan was fired as a deputy in 2016 after a yearlong investigation into his actions. The department determined Mandoyan assaulted a female deputy he was having an affair with, tried to break into her apartment and stalked her.

[ABC7](#)

### **County OKs mental health treatment fix**

The Los Angeles County Board of Supervisors on Tuesday unanimously approved a motion by Supervisor Kathryn Barger to improve access to mental health treatment in Los Angeles County by adopting a two-year pilot program to procure up to 500 beds for those in need of care. "Mental health hospital beds have dwindled, leaving a significant number of patients and their families without access to critically needed care," Supervisor Barger said.

[Antelope Valley Press](#)

### **L.A. County Sheriff's employee & Commerce mayor sponsor pot bus to Las Vegas**

John Soria is the Mayor of Commerce, a tiny town in Los Angeles county that has the biggest card room in the world, the Commerce Casino, along with one of the biggest high-end outlet malls in the country, the Citadel. As Mayor of a city that has huge investment opportunities around the Citadel and the Casino, one would think Soria would work hard to enhance the City's image to attract much needed investment, which would increase tax revenue and give the City money to augment public services and increase public safety.

[Cerritos Community News](#)

### **Undercover on Skid Row; FOX 11 embeds with county mental health team to expose 'broken system'**

In an exclusive investigation, FOX 11 is going undercover to Skid Row, embedding with a Los Angeles County mental health team tasked with helping the most vulnerable on the streets in a system the team and a County Supervisor say is 'broken.' There are an estimated 58,000 homeless people living on the streets in Los Angeles County, and more than sixty percent of them are believed to be suffering from mental illness.

[Fox11](#)

### **Registrar-Recorder's Office bounces 'retired army general' label**

The Office of Los Angeles County Registrar-Recorder has vetoed a Glendale attorney's chosen ballot designation of "Retired Army General." It decided after-hours on Tuesday that lawyer Marc MacCarley's desired billing on the March 3 ballot is legally impermissible. MacCarley retired from his military post in 2015 and has been in law practice.

[Metropolitan News-Enterprise](#)

## **Consumer**

### **Amazon faces U.S. govt notorious markets blacklist**

Amazon has engaged in a pattern of conduct so reprehensible that it may be placed on the U.S. Trade Representative's "Notorious Markets List." The government list is reserved for the worst online markets that enable and facilitate the world's largest criminal enterprise; copyright piracy, trademark infringement, and counterfeit product sales. The Trump administration is considering the move, a public shaming of the e-commerce juggernaut.

[The Counterfeit Report](#)

### **'CBD has the potential to harm you,' FDA warns consumers**

The U.S. Food and Drug Administration updated its stance on CBD late Monday, saying that the cannabis derivative may have the potential to harm users. Cannabidiol, or CBD, is a compound derived from the

cannabis plant that is believed to be nonintoxicating. It has proliferated in drinks, cosmetics, foods and many other consumer products, even in states where marijuana is not recreationally or medically legal, including being sold in major retail chains such as CVS Health Corp., Walgreens Boots Alliance Inc., and Rite Aid Corp.

[MarketWatch](#)

### **Consumer Alert: Hackers using toys to spy on your children?**

The interactive toy your kid wants could be the worst gift this holiday season. Call For Action is warning consumers of potential hackers targeting toys. The Federal Bureau of Investigation has issued warnings on smart televisions and how hackers can monitor you at home through the device, and now toys are tools for scammers.

[WKRC](#)

## **Crime**

### **FBI releases 2018 NIBRS Crime Data as transition to NIBRS 2021 continues**

The FBI released detailed data on nearly 6.6 million criminal offenses reported via the National Incident-Based Reporting System (NIBRS) in 2018. The Uniform Crime Reporting (UCR) Program's latest report, NIBRS, 2018, presents data about victims, known offenders, and relationships for offenses reported in 52 categories. In addition, the report provides information on arrests for those crimes as well as 10 additional categories for which only arrest data is collected.

[FBI](#)

### **Ex-con fondles sleeping woman days after he's released from jail?**

A man with a lengthy criminal history was charged Wednesday with breaking into a Santa Ana apartment and groping a woman as she slept just a few days after the ex-con was released from jail this past weekend. David Rivas Ceja, 38, was charged with burglary and assault with the intent to commit a sex offense, both felonies, as well as a misdemeanor count of disorderly conduct by loitering on private property.

[My News LA](#)

### **Father takes action when he sees car thief behind wheel of daughter's graduation gift**

A father who had bought his daughter a car for a graduation gift took matters into his own hands when he saw someone else behind the wheel. The father spotted the car, a Toyota Matrix, in the Azusa area on Monday and notified police. The chase began at about 10 a.m. and eventually entered the westbound 210 Freeway. The driver exited in the Duarte area, and the pursuit was called off due to safety concerns.

[NBC4](#)



### **Swastikas, threatening graffiti discovered near school in Topanga**

Threatening graffiti near Topanga Elementary Charter School in Topanga found on two separate occasions over the last three weeks were both deemed "non-credible" and not a "direct threat to the school," it was reported Tuesday morning. The first message, which included a swastika and the words "mass shoot everyone," was scrawled on a vinyl banner for a play posted near Topanga School Road and Highway 27.

[My News LA](#)

### **Just-released sex offender accused of making sexual comments to girl in Claremont**

A man arrested for committing lewd act at a Claremont library just over two weeks ago, then released from jail after serving five days in custody, was again arrested this week on suspicion of making sexual comment to a girl, authorities said. Javier Sanchez, 26, described as a transient known to frequent the Claremont Village area, was arrested Thursday on suspicion of child annoyance, according to the Claremont Police Department.

[KTLA](#)

### **Federal authorities bust drug trafficking ring in Fresno**

A recent multi-agency operation spearheaded in Fresno by federal authorities netted several arrests connected to alleged participation in a network that trafficked drugs from Mexico for distribution in California and Washington state. Recently unsealed court records show a wiretap investigation was mainly carried out by the U.S. Drug Enforcement Administration at the request of the Fresno Police Department, which had initiated its own probe in the summer 2018.

[Fresno Bee](#)

### **CA food tampering suspect dumped bleach at AZ stores**

A man facing charges for dumping bleach on food and drinks at retail stores across California is in even more legal trouble - in another state. David Lohr, who was arrested on federal food tampering charges this year in the San Francisco Bay Area, has been indicted on similar charges by a grand jury in Arizona, the state's attorney general announced in a news release on Thursday.

[Sacramento Bee](#)

### **Feds: CA man harasses, threatens government in 10,000 calls**

A man was arrested at his Southern California home on Friday after federal prosecutors said he made more than 10,000 harassing phone calls to government offices - including death threats that targeted congressional staffers. Robert Stahlnecker, a 48-year-old from Twentynine Palms in San Bernardino County, made all of those harassing phone calls between January and November of this year, the U.S. Attorney for the Central District of California said in a

news release.  
[Sacramento Bee](#)

## Public Safety

### **Olympic & Bundy: A shining star in the LAPD - Hollenbeck PAL**

In an era of community policing, LAPD's Hollenbeck division is ahead of the curve with its Hollenbeck PAL program. HPAL was founded in 1992 in the heart of Boyle Heights. HPAL, long known for its positive interactions for kids and law enforcement, is now expanding with mental health services. As the LAPD marks 150 years, we highlight Hollenbeck PAL and the police officers attached to it.

[Fox11](#)

### **In the wake of domestic violence, apologies often follow, according to LAPD data**

We analyzed LAPD data to find crime reports tagged with MO Code 381, "Suspect Apologizes," in order to see how apologetic suspects were in the City of Los Angeles. From 2010 to 2018, the number of apologies has remained fairly consistent. There have been 979 reported apologies in total since 2010, including the first nine months of 2019. Eighty-seven of those took place from January to September of this year, putting this year on track to reach a little over a hundred reported apologies.

[Witness LA](#)

### **Chicago police chief's firing puts spotlight on cops who let fellow officers go**

When Chicago police officers discovered their chief asleep behind the wheel of his running SUV, they did not conduct any sobriety tests and let their boss drive home - a decision that has thrown a spotlight on what happens when one officer confronts another on patrol. Many details of that mid-October encounter are still unclear.

[AP](#)

### **Why are cops around the world using this outlandish mind-reading tool?**

The police gave Ricky Joyner a pen and a nine-page questionnaire. Write what you did, beginning to end, on the day Sandra Hernandez disappeared, one question asked. "Went ot work ...," Joyner wrote, transposing the letters in "to." "Went home toke shower got dress pick Sandra up ... went out to eat ... went the movies ... toke Sandra home ... stop at [bar] for little while, then spent the night with a grilfriend."

[ProPublica](#)

### **LAPD releases bodycam video of Boyle Heights shooting (Video)**

Police say the suspect Rudolfo Coleman immediately began shooting at officers as they pulled up. Suzanne Marques reports.

[CBS LA](#)

## **Orange County Sheriff's Dept. mishandled evidence; kept it quiet for nearly 2 years**

A law enforcement scandal that could impact thousands of criminal cases in Orange County, Calif., is pitting the region's top attorneys and sheriffs against one another. The county's public defender's office on Wednesday suggested that top prosecutors covered for law enforcement, helping to keep widespread lapses in evidence booking out of public view. Now, Assistant Public Defender Scott Sanders is demanding to know who knew what and when.

[NPR](#)

## **California/National**

### **Thousands of lawful California gun owners are being denied ammunition purchases. Here's why**

Zachary Berg usually buys guns and ammunition with relative ease. After all, he's a Sutter County sheriff's deputy and needs them for his job. California's stringent gun laws usually don't apply to him. But Berg couldn't buy shotgun shells at his local hardware store in Yuba City prior to a duck hunting trip last month. He was rejected under California's stringent ammunition background check program that took effect July 1, because his personal information didn't match what state officials had in their database.

[Sacramento Bee](#)

### **Moment two gunmen shoot a Jersey City cop after they killed a detective, stole a U-Haul and killed three civilians before SWAT shot them dead in a kosher store at the end of a two-hour standoff**

One police officer, three innocent civilians, and two suspects are dead after a multi-hour SWAT standoff at a kosher market in Jersey City. Detective Joseph Seals, 39, was gunned down and killed on Tuesday by the two unnamed suspects, who then went on to hijack a U-Haul truck, kill three civilians in a market, and engage in an hours-long shootout with police before police killed the suspects.

[Daily Mail](#)

### **San Francisco's 'poor street conditions' a factor in city's loss of \$64M Oracle tech conference**

Oracle, a major Silicon Valley tech company, will move its annual OpenWorld conference to Las Vegas next year due to San Francisco's expensive hotel rates and the city's "poor street conditions," according to reports. The loss of OpenWorld, which has been held in San Francisco for about 20 years, is raising new concerns about whether the city's struggles with homelessness, open drug use and street violence may be scaring off tourism and other business, the San Francisco Chronicle reported.

[Fox News](#)

### **California needs more housing, and 97% of its cities and counties fail to issue enough RHNA permits**

Neighborhood leaders gathered in Long Beach in the spring of 2017 to discuss a City Hall plan to address the city's housing shortage. What they learned sparked a revolt. To increase the housing supply and stem skyrocketing residential costs, planners proposed multi-story apartment buildings line major streets and boulevards throughout the city, including its affluent, mainly suburban east side.

[Orange County Register](#)

### **A new blow to the FBI: Watchdog report details dysfunction, missteps in wiretap of Trump aide**

Since his confirmation more than two years ago, FBI Director Christopher Wray has adopted a simple axiom for the embattled bureau. "Keep calm; tackle hard," he has repeatedly urged the agent-and-analyst ranks during some of the worst of political storms to batter the century-old institution. From the foundation-shaking removal of Director James Comey in the midst of the Russia investigation to near-unceasing assaults on the bureau's credibility by President Donald Trump himself, the journey has been fraught at best.

[USA Today](#)

### **New bill would empower U.S. Customs to enforce design patents at U.S. border to combat imported counterfeit goods**

Yesterday, the Counterfeit Goods Seizure Act of 2019 was introduced in the U.S. Senate to empower U.S. Customs and Border Protection to enforce U.S. design patents at the U.S. border. The bill is co-sponsored by Senators Thom Tillis (R-NC), Chris Coons (D-DE), Bill Cassidy (R-LA), and Mazie Hirono (D-HI). Currently, Section 1595a(c)(2)(C) of Title 19 of the U.S. Code empowers Customs to enforce copyrights and trademarks that have been previously recorded with Customs.

[IP Watchdog](#)

### **California voters face another ballot showdown on crime**

No California ballot would be complete without at least one measure about crime and punishment and 2020 will be no exception. A referendum seeking to overturn California's landmark ban on cash bail in criminal cases will once again test voters' sentiments about the treatment of accused lawbreakers. During previous decades, particularly in the 1980s and 1990s, voters endorsed a tough, lock-'em-up attitude, culminating in passage of the state's famous - or infamous - three-strikes-and-you're-out law aimed at repeat offenders.

[CalMatters](#)

### **How many Californians own guns? Does gun control stop them?**

California may have some of the nation's most restrictive gun control laws, from bans on assault rifle sales to mandatory background checks for ammunition sales, but that isn't stopping Golden State residents

from buying firearms. A quarter of Californians live in a house with a gun, according to a new survey. The survey, published by the peer-reviewed medical journal BMJ in the magazine "Injury Prevention," also says that one in seven Californians, an estimated 4.2 million people, owns a firearm.

[Sacramento Bee](#)

### **More than 500 cities and counties reject opioid class action, will pursue lawsuits on their own**

More than 500 cities and counties opted out of the unprecedented "negotiation class" proposed by plaintiff lawyers to settle sprawling opioid litigation, leaving 98% of the 34,458 U.S. cities and counties technically still in the class. The opt-outs could make it difficult for defendant companies to use the mechanism to negotiate a global settlement, however.

[Legal Newsline](#)

### **Business groups fight California ban on mandatory arbitration agreements for workers**

Fighting a pro-worker law that bars mandatory arbitration agreements, the U.S. Chamber of Commerce and a host of business groups have sued to stop a California law set to take effect Jan. 1. The influential coalition says the law, Assembly Bill 51, wrongly seeks to remove a common tool that businesses use to swiftly end and keep employment disputes out of the courts. According to the chamber and National Retail Federation, AB 51 is anti-business and pre-empted by federal law.

[Courthouse News Service](#)

## **Sentences/Convictions**

### **Mom sentenced for infant's death in horrific porsche crash**

A 25-year-old Rancho Mirage woman was sentenced to a life term of probation plus community service Friday for her part in the death of her infant daughter during a car crash in Palm Desert. Kristen Lauer, who sat weeping in a wheelchair as the decision was handed down, was left permanently disabled after the Porsche sportscar in which her boyfriend was driving struck a metal guardrail and tumbled down an embankment about 200 feet off state Route 74 on May 1, 2016.

[City News Service](#)

### **Decades after horrific crimes, victim confronts her abuser**

A man was sentenced to state prison nearly 30 years after he first molested his young neighbor. Prosecutors charged Charles LeRoy Rutledge on Thursday with 20 counts of sexual abuse of a child, lewd acts on a child, unlawful sexual intercourse with a minor, and other sex crimes. Rutledge, 77, pleaded guilty in the face of strong evidence that included a tape-recorded phone conversation in March with his victim.

[NBC7 San Diego](#)



### **Man sentenced to 7 years in prison for E-scooter attack on 75-year-old man in DTLA**

A man who hurled an electric scooter at a 75-year-old man in downtown Los Angeles, causing head and arm injuries, was sentenced Wednesday to seven years in state prison. Janai Washington, 41, pleaded no contest Nov. 20 to an elder abuse charge and admitted an allegation that he had personally inflicted great bodily injury. Washington approached the victim on June 13 as he sat in a chair at Sixth and Spring streets. A bystander intervened and the defendant fled, according to authorities.

[City News Service](#)

### **Man sentenced to death for killing transgender cellmate**

A California inmate was sentenced to death Thursday for the 2013 killing of his transgender cellmate in a shocking case that shined a light on the dangers of sexual assault and violence trans people face when they are not housed according to their gender identity. Miguel Crespo, 48, was housed with Carmen Guerrero, a trans woman, at Kern Valley State Prison for just eight hours in October 2013. During that time, Crespo bound, gagged, tortured and murdered Guerrero in their shared cell.

[NBC News](#)

### **Tarzana man gets 9 years in prison for scam involving high-end cars**

A Tarzana man involved in a scheme centered in the San Fernando Valley that targeted buyers of luxury cars including Bentleys and Maseratis was sentenced Friday to nine years in state prison. Arman Mave Hazarian, also known as Dean Hazarian, pleaded no contest in October to three felony counts of grand theft auto and one felony count of grand theft.

[City News Service](#)

### **Man who 'freaked out' on plane, forced landing pleads guilty**

A Washington man who ingested methamphetamine before getting on a plane in Seattle and had what a prosecutor called a "freak out" on board pleaded guilty Thursday to interfering with crew members after the California-bound flight was forced to land in Portland. The Oregonian/OregonLive reports Douglas Smyser, of Bonney Lake, is expected to face four months on home detention when sentenced in December.

[AP](#)

### **Hit-and-run driver convicted of manslaughter for death of motorcyclist in Pasadena**

A man faces nearly two decades in prison after pleading no contest Friday to charges for fatally striking a motorcyclist while driving a Tesla through Pasadena three years ago, then fleeing the scene, authorities said. Donte Antoine Fox, 23, of Pasadena, pleaded no contest to vehicular manslaughter with gross negligence and hit-and-run, the Los Angeles County District Attorney's Office said in a written statement.

[KTLA](#)

### **Andy Dick spends 1 night in jail for sexual battery case**

Andy Dick was sentenced to 14 days in jail for his sexual battery case but spent just one night behind bars, RadarOnline.com confirmed. Rob Wilcox, the spokesman with the Los Angeles City Attorney's Office, confirmed the troubled actor was in the L.A. County jail from December 6 to 7. Dick, 53, was charged with two misdemeanors for the 2018 incident where the victim claimed he "squeezed her butt twice," as he walked past her on a sidewalk. She also said he made "lewd comments."

[Radar Online](#)

## **Corrections/Parole**

### **Calls grow in California to protect inmates at women's lockups from sexual abuse (Audio and Script)**

To California now and efforts to protect female inmates from sexual abuse. A new state transparency law means that disciplinary records of officers fired for sexual misconduct are now being released. That is happening as former inmates work with state legislators to increase oversight of corrections officers. Julie Small with member station KQED of San Francisco reports. And a warning to our listeners - this story contains graphic descriptions of sexual assault.

[KQED](#)

### **Tulare woman denied parole in 1987 murder of husband**

On Tuesday at the California Institution for Women in Corona, a California parole board issued a three-year denial for June Gravlee, 65, for the 1987 murder of her husband. In 1990, Gravlee was convicted of first-degree murder with the special circumstance of murder for financial gain. In the penalty phase of the trial, the Tulare County jury recommended a death sentence. However, the trial judge at the time modified the verdict to a penalty of life imprisonment without the possibility of parole.

[The Porterville Recorder](#)

### **California prison reform, regressing rehabilitation - Part 1**

Preparing to walk across the stage and receive his graduation certificate, Jose Becerra cannot help but feel bittersweet. While incredibly proud of his ability to overcome his delinquency and successfully rehabilitate himself, he also laments. What if his brother had volunteered for the microchip implant program when he was released from prison; maybe he wouldn't have reverted to his old ways, leading to his death in 2019.

[Corrections.com](#)

### **Two officers at North Kern State Prison injured in inmate attack**

Two correctional officers at North Kern State Prison were attacked by an inmate on Tuesday and are recovering from their injuries, according to the California Department of Corrections and Rehabilitation. The

department said the incident happened at around 8:45 p.m., when 23-year-old inmate Traymar Robinson approached an officer who was monitoring inmate movement in the Reception Center on Facility D and hit him in the face with his fist.

[KGET](#)

## Articles of Interest

### **CNN insider blows whistle on network president Jeff Zucker's personal vendetta against POTUS**

A brave CNN insider came to Project Veritas to expose anti-Trump bias at the cable giant. Cary Poarch, who works at CNN's Washington D.C. Bureau, tells Project Veritas "I decided to wear a hidden camera...to expose the bias running rampant" at the network. Poarch documented CNN's bias for months; recording undercover footage of numerous long-term employees, some of which talk about Jeff Zucker's anti-Trump agenda.

[Project Veritas](#)

### **Nike backs legislation to battle counterfeit goods**

According to a new report, Nike is now among a larger group of companies pressuring Congress to tighten border inspections and block imports of counterfeit goods. The sportswear giant is backing a piece of proposed legislation that will give US Customs and Border Protection the power to seize goods that are believed to infringe on existing patented designs and block them from being imported into the country. Currently, only copyrighted and trademarked goods enjoy this kind of protection.

[HypeBeast](#)

### **Fighting for what matters: Patrisse Cullors' approach to social justice is artful and powerful**

There are a handful of historical women of color whose names we all know due to their bravery and significance as activists. Harriet Tubman. Rosa Parks. Ida B. Wells. Angela Davis. These figures were not alone in their fervor and fights for equality, but their resistance to oppression was so bold they could not be ignored, even if it meant putting themselves in danger to right wrongs against their people and create change.

[LA Weekly](#)

### **Can Spectrum News 1 capture diverse L.A.?**

I drove into the Spectrum News 1 headquarters parking lot Monday, a day after the cable news channel had won four Los Angeles Press Club awards for its coverage of local news. It was a notable accomplishment for a journalistic operation that been in the crowded L.A. media scene for just over a year. I thought of the significance of my destination. Spectrum News 1 is located in El Segundo, which is also the new home of the Los Angeles Times. The South Bay city of just fewer than 17,000, once best known for oil refineries and aerospace, is becoming a

Southland media capital.

[LA Observed](#)

***For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).***



Los Angeles Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [The Washington Post](#)  
**To:** [aaquino@sunnyvale.ca.gov](mailto:aaquino@sunnyvale.ca.gov)  
**Subject:** The Daily 202: FBI director shows independence from Trump and Barr in responding to IG report on Russia probe  
**Date:** Tuesday, December 10, 2019 7:44:53 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.


If you're having trouble reading this, [click here](#).

---

# The Daily 202



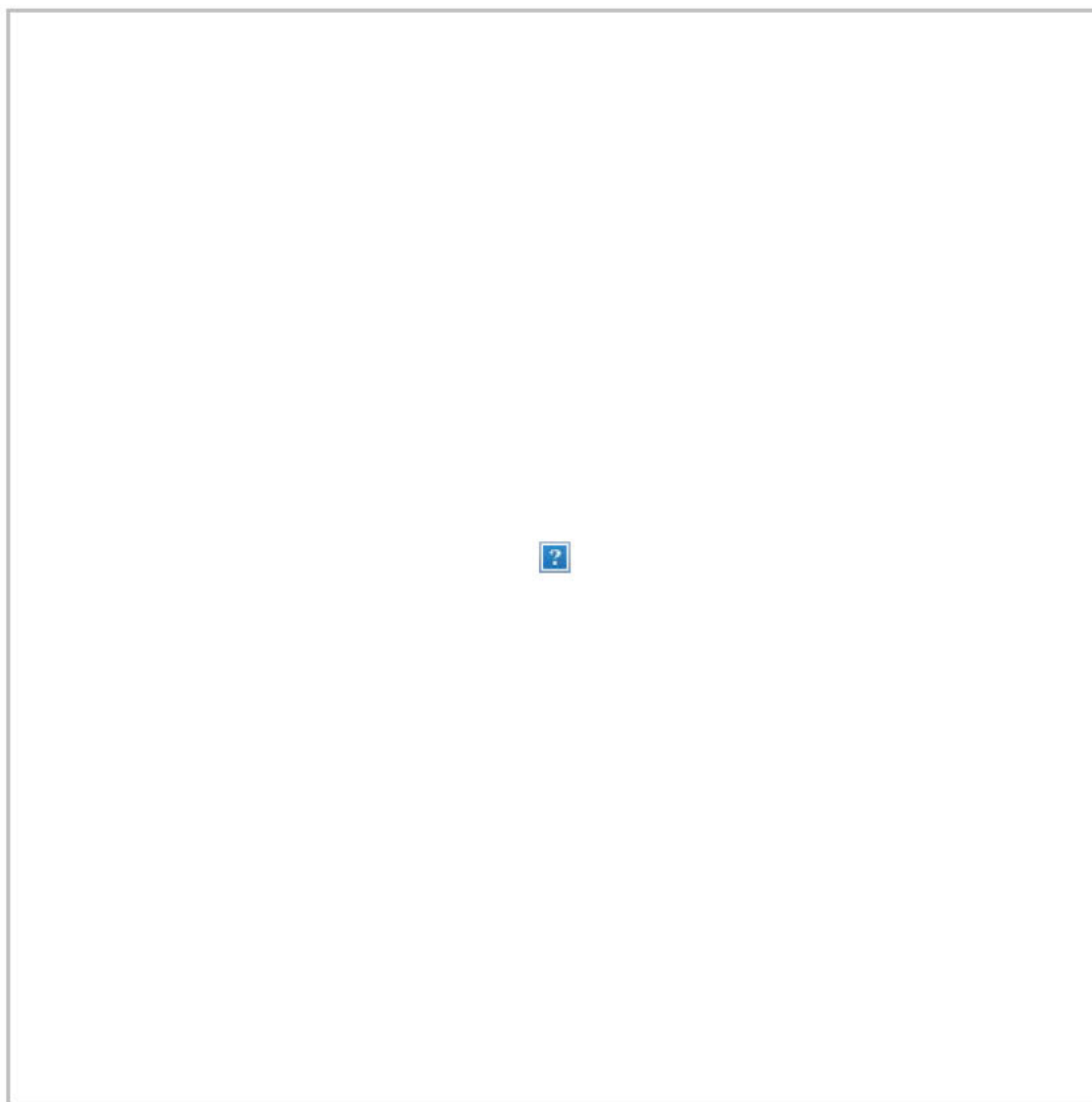


Share:  

 Listen to The Big Idea



## FBI director shows independence from Trump and Barr in responding to IG report on Russia probe



FBI Director Christopher Wray poses for a photo on Monday. (Jacquelyn Martin/AP)

**BY JAMES HOHMANN**



*with Mariana Alfaro*

## **THE BIG IDEA: FBI Director Chris Wray's response to the Justice Department's independent watchdog was nuanced.**

"The inspector general did not find political bias or improper motivations impacting the opening of the investigation or the decision to use certain investigative tools," Wray told [ABC News](#) on Monday afternoon, "but the inspector general did find a number of instances where employees either failed to follow our policies, neglected to exercise appropriate diligence or in some other way fell short of the standard of conduct and performance that we ... expect of all our employees."

This is an accurate [summary](#) of what Justice Department Inspector General Michael Horowitz [concluded](#) in [his 434-page report](#) examining the FBI's investigation of President Trump's 2016 campaign. Wray also announced that he's ordered "more than 40 corrective steps" to address what the report identified as "serious performance failures."

**But Trump has little tolerance for shades of gray.** You're either with him or against him. The president [lashed out](#) Tuesday morning at Wray, whom he appointed in 2017 after firing Jim Comey.

"I don't know what report [Wray] was reading, but it sure wasn't the one given to me," Trump [tweeted](#). "With that kind of attitude, he will never be able to fix the FBI, which is badly broken despite having some of the greatest men & women working there!"

**-- Asked whether he thought the FBI unfairly targeted the Trump**

**campaign in 2016, Wray told ABC: “I do not.”** While careful not to criticize the president directly, Wray said that calling FBI agents part of “the deep state,” something Trump has done, is “an affront to them.”

“I think it's important that the inspector general found that, in this particular instance, the investigation was opened with appropriate predication and authorization,” he said.

Asked about the latest conspiracy theory being pushed by Trump and his congressional loyalists, Wray answered: “We have no information that indicates that Ukraine interfered with the 2016 presidential election. As far as the [2020] election itself goes, we think Russia represents the most significant threat.”



When William Barr has echoed Trump's rhetoric

**-- Trump's broadside against Wray puts in stark relief just how deeply in the tank Attorney General Bill Barr is for Trump. Breaking with Horowitz, as well as Wray, Barr disputed the IG's conclusion that there was enough probable cause to launch an investigation.**

"The Inspector General's report now makes clear that the FBI launched an intrusive investigation of a U.S. presidential campaign on the thinnest of suspicions that, in my view, were insufficient to justify



the steps taken,” the attorney general wrote in [a blistering statement](#). “It is also clear that, from its inception, the evidence produced by the investigation was consistently exculpatory. Nevertheless, the investigation and surveillance was pushed forward for the duration of the campaign and deep into President Trump’s administration. In the rush to obtain and maintain FISA surveillance of Trump campaign associates, FBI officials misled the FISA court, omitted critical exculpatory facts from their filings, and suppressed or ignored information negating the reliability of their principal source.”

FISA is short for the Foreign Intelligence Surveillance Act. **Barr testified earlier this year that he believes ["spying did occur"](#) on the Trump campaign. Wray had previously said ["spying" is "not a term I would use."](#)** He reiterated that on Monday. “Again, different people have different colloquial terms, but we use terms like ‘investigation’ and ‘surveillance,’” the FBI director told ABC.

**-- Connecticut U.S. Attorney John Durham put out [his own statement critical of the IG report](#).** He’s been handpicked by Barr to conduct a probe, separate from Horowitz’s, into how the U.S. government investigated Trump’s 2016 campaign. “Our investigation has included developing information from other persons and entities, both in the U.S. and outside of the U.S.,” Durham said. “Based on the evidence collected to date, and while our investigation is ongoing, last month we advised the Inspector General that we do not agree with some of the report’s conclusions as to predication and how the FBI case was opened.”

It is highly irregular for a U.S. attorney to release a statement like this in the middle of an ongoing criminal investigation.



**After Horowitz implicitly debunked several arguments Trump espoused for years, the president has already turned his attention to Durham's investigation of his investigators.** "I look forward to the Durham report, which is coming out in the not-too-distant future," he told reporters at the White House on Monday. "It's got its own information, which is this information plus plus plus."



Trump says inspector general report is 'far worse' than expected

**-- Wray appears focused on protecting the FBI's reputation while Barr seems primarily focused on protecting, and placating, the president. Barr is managing up. Wray is managing down.** This fits with [a pattern](#). While Barr is the nation's chief law enforcement officer, critics say he's consistently acted more like the president's personal lawyer than the nation's lawyer. The attorney general wrote a misleadingly pro-Trump summary of Robert Mueller's report on Russian election interference. He cleared Trump of obstruction of justice, even though the special counsel had not done so. He even embraced Trump's "no collusion" talking points.

**Barr's Justice Department also intervened to help the White House's initial efforts to conceal a CIA analyst's whistleblower complaint that Congress was legally entitled to receive.** And Barr's underlings at DOJ also declined to investigate suggestions of criminal wrongdoing in the complaint. The attorney general declined to recuse himself from these deliberations, even though the whistleblower complaint – and the rough transcript of the July 25 call – showed that Trump brought up Barr during his conversation with Ukrainian President Volodymyr Zelensky.

**-- Barr planned to hold a 200-person holiday party at the Trump hotel in Washington on Sunday night, but he rescheduled the event. A Justice Department spokeswoman declined to say when the event would take place, but she said it would still be at the Trump International.** "Barr signed a contract with the Trump hotel over the summer that required a minimum of \$31,500 in spending. He put up a \$10,000 deposit," [Jonathan O'Connell reports](#). "The total cost of the party could be much higher depending on the menu Barr

chooses to go with a four-hour open bar. Barr planned to pay for the party himself, avoiding concerns about the Constitution's emoluments clause ...

**“Not publicly disclosing the event’s new date could help Barr and his guests avoid protests.** On Sunday night, half a dozen protesters — thinking Barr’s guests would be arriving — held a sign on the sidewalk out front calling for Barr to be disbarred and told guests arriving at the hotel: ‘You’re on the wrong side of history.’”

**Meanwhile, Justice Department attorneys are defending Trump in court this week against two lawsuits claiming that he’s unconstitutionally benefiting from his personal business, including the D.C. hotel, while in the White House.**



Graham says inspector general report shows a 'system off the rails'

**-- This is not the first time Trump has criticized Wray.** This spring, the director testified that any campaign should alert the FBI if foreign agents reach out offering dirt on their political opponents. "My view is that, if any public official or member of any campaign is contacted by any nation-state or anybody acting on behalf of a nation-state about influencing or interfering with our election, then that is something that the FBI would want to know about," Wray testified. Asked about this statement in June, Trump replied, "[The FBI director is wrong.](#)" The



president insisted that “there isn’t anything wrong” with accepting “oppo research” from foreign powers.

**-- Wray has also previously dismissed Trump’s attacks on the FBI as “noise.”** At a Senate Intelligence Committee hearing in February, Wray was asked about the president's criticisms of the FBI. “There's no shortage of opinions about our agency, just like every other agency up here — and just like the Congress,” Wray responded. “I'd encourage our folks not to get too hung up on what I consider to be the noise on TV and in social media.”

Last year, soon after taking the job, Wray [privately warned](#) the White House against releasing that memo by Rep. Devin Nunes (R-Calif.), who was then the chairman of the House Intelligence Committee. When Trump overruled him, Wray signed off on a statement from the FBI that said: “We have grave concerns about material omissions of fact that fundamentally impact the memo's accuracy.”

**-- FBI directors are appointed to 10-year terms. That’s intended to keep them insulated from politics, but they are accountable to the attorney general and can be fired by the president – as Trump fired Comey.** Of course, this isn’t the first time that Trump publicly chastised his appointees in the law enforcement firmament. He routinely disparaged Jeff Sessions before firing him as attorney general and replacing him with the more pliable Barr. He also attacked former deputy attorney general Rod Rosenstein, falsely accusing his own appointee of being a Democrat.





Schumer says inspector general report 'puts conspiracy theories to rest'



-- **The correctives:** Responding to the IG report, Wray **announced** that the **FBI** will modify the processes for applying and renewing warrants under the **Foreign Intelligence Surveillance Act**. For a sensitive investigation to be run out of headquarters, Wray said, prior approval from the FBI deputy director will be required and field offices will be consulted. He announced “significant changes” to how the FBI

manages its Confidential Human Source program, related to how the FBI collects, documents and circulates information from its informants.

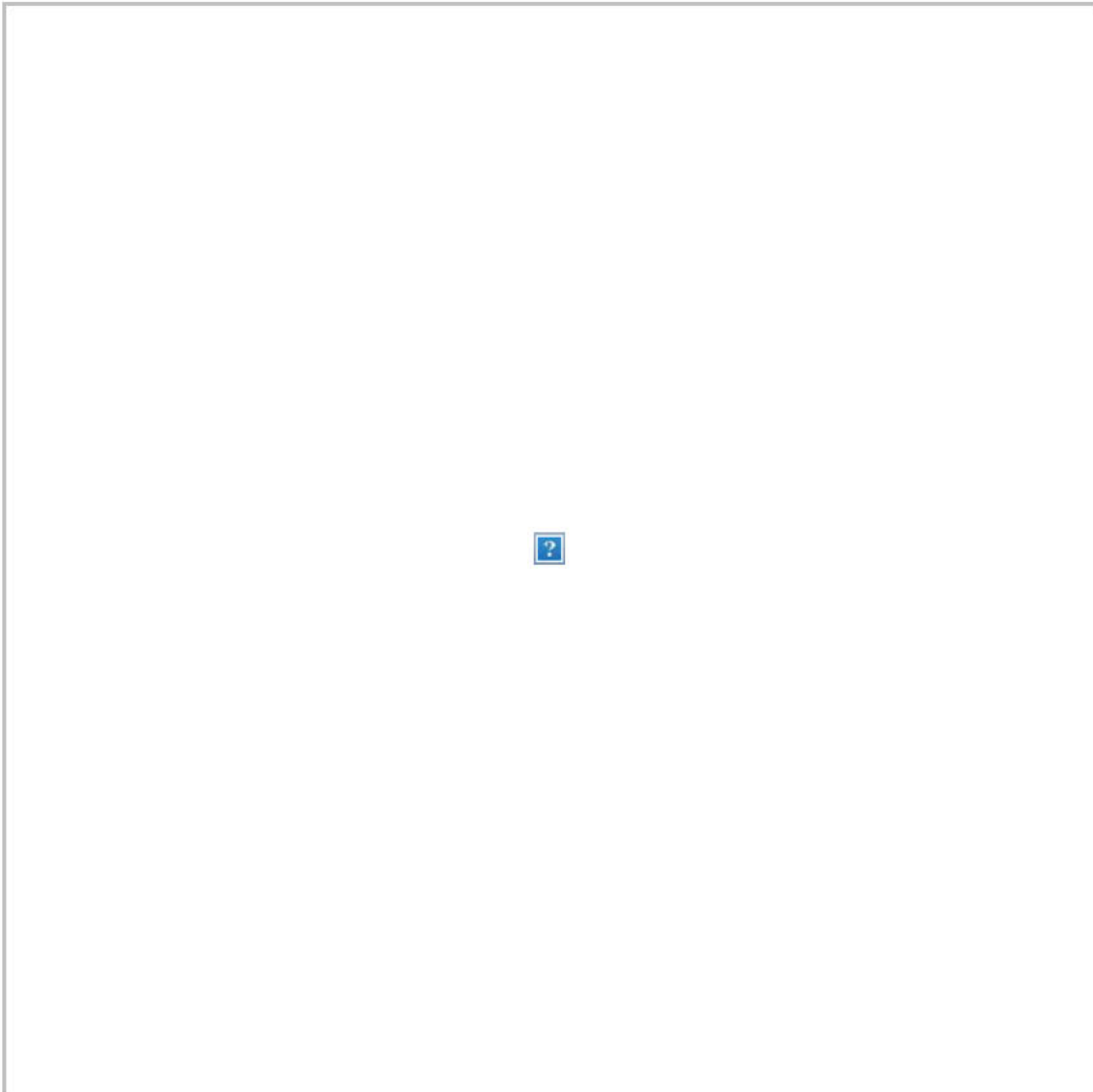
**Wray also established new protocols for the FBI's participation in the strategic intelligence briefings provided to presidential nominees.** Wray said the FBI's role in these briefings should be for national security purposes and not for investigative purposes to ensure that candidates and their advisers trust the people who are talking to them about threats. In 2016, an FBI agent went to the briefing for Trump to keep an eye on how Michael Flynn reacted to certain information.

**Wray said he's mandating specialized, semiannual training for all FBI personnel who handle FISA warrants or confidential human sources.** He noted that he reinstated an annual ethics training program for all FBI employees that had been discontinued in prior years. Finally, Wray said that the FBI will take appropriate disciplinary action where warranted against any wrongdoing identified in the report.

**"I am very committed to the FBI being agile in its tackling of foreign threats. But I believe you can be agile and still scrupulously follow our rules, policies and processes," Wray said in an [interview with the Associated Press](#).** "As a general matter, there are a number of things in the report that in my view are unacceptable and unrepresentative of who we are as an institution. ... This is a serious report, and we take it serious."

**-- Barr said in his statement on Monday that he still has "full**

**confidence” in Wray and praised these “proposed reforms.”** “No one is more dismayed about the handling of these FISA applications than Director Wray,” Barr said at the end of the statement criticizing Horowitz’s core conclusion.



Former FBI Director James Comey speaks to reporters at the Capitol last December. (J. Scott Applewhite/AP)

**-- In an op-ed for [The Post](#) in response to the IG report, Comey demands an apology from the attorney general:** “Barr owes the institution he leads, and the American people, an acknowledgment of

the truth. Unfortunately, it appears that Barr will continue his practice of deriding the Justice Department when the facts don't agree with Trump's fiction. Pointing to his personally commissioned 'review' of the FBI's case-opening, Barr has declared it is too soon to conclude that the FBI was right to start an investigation. If his goal is simply to support the president's conspiracy theories, it will always be too soon to acknowledge the facts. As the leader of an institution that is supposed to be devoted to truth, Barr needs to stop acting like a Trump spokesperson."

**Comey, like his successor Wray, welcomed the IG's recommendations.** "Inspector-general reports are valuable because they offer the chance to learn," he writes. But he argued that it would have been "a dereliction of duty" not to investigate a tip that Trump foreign policy adviser George Papadopoulos had discussed with a foreign ambassador that Russia had "dirt" on Hillary Clinton in the form of emails.

**Comey also criticized "Fox News personalities" for smearing him.** "There was no illegal wiretapping, there were no informants inserted into the campaign, there was no 'spying' on the Trump campaign," he writes. "The painful part is that millions of good people believed what they heard. My 89-year-old mother-in-law, watching Fox News in her Iowa assisted-living facility, became convinced that I was going to jail. I repeatedly assured her that there was zero percent chance of that."

**-- Chris Christie recommended Wray to Trump in 2017 when he needed someone to replace Comey.** Wray had defended the then-New Jersey governor as his personal lawyer throughout the

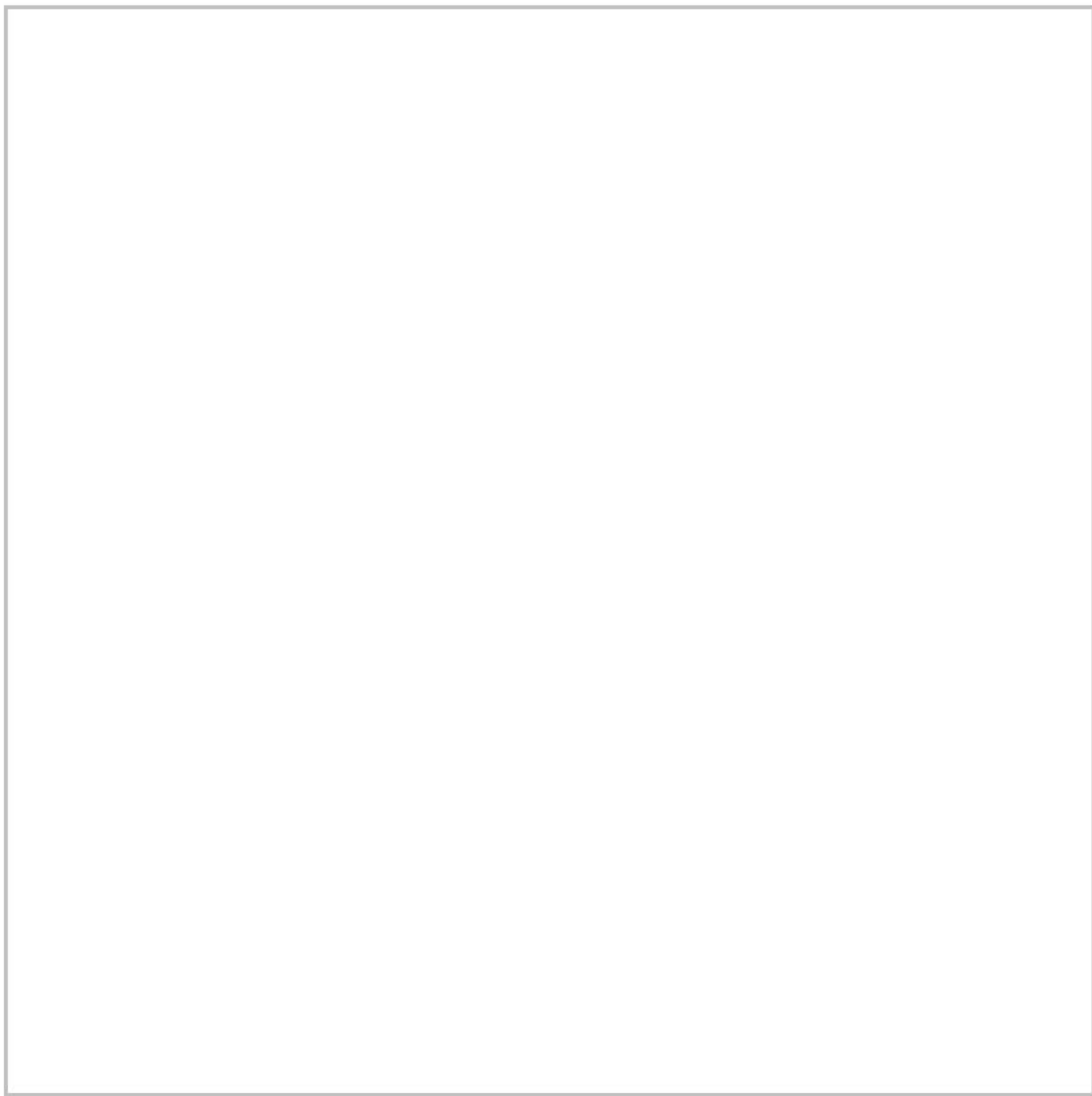


Bridgegate investigations. A registered Republican, Wray had previously served as the assistant attorney general in charge of the criminal division under George W. Bush.

**Here's a fun fact:** Back in 2004, when Comey was prepared to resign as the deputy attorney general over concerns about the legality of Bush's domestic surveillance program, Wray approached him in a corridor at the Justice Department. "Look, I don't know what's going on, but before you guys all pull the rip cords, please give me a heads-up so I can jump with you," Wray told Comey, according to a 2013 story in [Washingtonian magazine](#).

**-- A final thought: Don't listen to spin from pundits and politicians. Read the IG report for yourself.** The executive summary at the top is only 19 pages. It's a measured synthesis, with a summary of what each chapter concludes and Horowitz's recommendations. Horowitz will discuss his findings on Wednesday during a public hearing before a Senate committee.





Democrats and Republicans present final cases in House impeachment inquiry hearing

### **THE LATEST ON THE INVESTIGATIONS:**

**-- House Democrats unveiled two articles of impeachment against Trump this morning, saying he had abused the power of his office and obstructed Congress in its investigation of his conduct regarding Ukraine. The House Judiciary Committee plans to vote on the articles this Thursday, and the full House is expected to vote next week. This announcement means there won't**

be any article of impeachment stemming from the Mueller report, which liberals had pushed to include but moderates balked at. ([Read more on our liveblog.](#))

- “We must be clear: No one, not even the president, is above the law,” House Judiciary Committee Chairman Jerry Nadler (D-N.Y.) said at a news conference.
- “The evidence of the president’s misconduct is overwhelming and uncontested,” said House Intelligence Committee Chairman Adam Schiff (D-Calif.). “The argument, ‘why don’t you just wait?’ comes down to this: Why don’t you just let him cheat in just one more election?”

-- **"Democrats laid the groundwork for the charges Monday, lambasting Trump as a danger to the country during a contentious [nine-hour] hearing that foreshadowed a likely party-line vote on the articles,"** [Rachael Bade](#), [Mike DeBonis](#), [Elise Viebeck](#) and [Toluse Olorunnipa](#) report. "Republicans on the committee sought to vigorously defend Trump, using parliamentary maneuvers, process complaints and occasional theatrics to disrupt the hearing and accuse Democrats of abusing the impeachment process in pursuit of a political vendetta. ... The hearing did not reveal much new information about the underlying conduct at the heart of the impeachment inquiry, instead allowing committee lawyers to summarize the extensive existing evidence and present opposing sides of the case. With dueling staff counsel arguing for and against impeachment — and at one point questioning one another — the

hearing showcased how partisan the proceedings had become ahead of the release of articles for ousting Trump from office. Trump said Saturday that [Rudy] Giuliani would be making a report to [Barr] and to Congress about his findings. On Monday, Giuliani said he wanted to present the information to congressional Republicans ahead of any impeachment vote."

**-- The Senate is looking for a holiday truce on the impeachment trial.** Senators from both parties aren't likely to let an impeachment trial ruin their holiday plans. ([Politico](#))

**-- A surprising revelation from the IG report: Ivanka Trump, the president's daughter, was friends with former British spy Christopher Steele, who wrote the dossier.** [Tom Hamburger and Rosalind S. Helderman report](#): "The [report] said Steele had 'been friendly' with a Trump family member, a relationship he described as 'personal.' Steele told investigators he had visited the Trump family member at Trump Tower in New York and had once gifted the person a family tartan from Scotland. A person familiar with Steele's business Orbis confirmed that the family member was Ivanka Trump. After first meeting in 2007, they emailed over the years ... Between 2010 and 2012, Steele discussed with Ivanka Trump the possibility that the Trump Organization might hire his business to assist with projects in Russia and China. They remained friends through 2015..."

**-- Appeals court judges expressed skepticism that members of Congress as individuals have a legal right to sue Trump to stop his private businesses from accepting payments from foreign governments without lawmakers' consent.** [Ann E. Mariow and Jonathan O'Connell report](#): "Even as the judges seemed troubled that



Congress may have no other viable way to enforce the Constitution's anti-corruption emoluments provision, they did not seem prepared to allow the lawsuit from more than 200 Democratic lawmakers to move forward — and suggested the Supreme Court would have the final word. Judges Thomas B. Griffith and David S. Tatel of the U.S. Court of Appeals for the D.C. Circuit expressed doubt that past Supreme Court decisions permit individual lawmakers to bring lawsuits on behalf of the entire body, and they noted that Congress acts through majority votes in the House and Senate.”

**-- Lawyers for former Trump deputy campaign chairman Rick Gates, who pleaded guilty to fraud and lying to prosecutors, asked a judge to spare him from prison because he cooperated with prosecutors investigating Russia's efforts to sway the 2016 election. [From the Times](#):** “In their sentencing memo, Mr. Gates's lawyers portrayed their client as the consummate cooperating witness. ... It said that **Mr. Gates had spent more than 500 hours in interviews with state and federal prosecutors** and had provided additional information to Congress in response to subpoenas and requests for interviews. ... Experts have said that under sentencing guidelines, Mr. Gates could receive a prison term of four years and nine months to six years for his crimes. But the judge overseeing his case is not required to follow those recommendations.”

**-- The New York attorney general issued a new subpoena to the National Rifle Association, deepening her investigation into whether the pro-Trump organization has illegally diverted money from its charitable foundation. [From the Times](#):** “Because the N.R.A. is chartered in New York and the office of the attorney general,

Letitia James, has a range of enforcement options, the investigation has alarmed N.R.A. officials already grappling with infighting and litigation. ... Among the documents sought by the subpoena are records related to transfers among N.R.A.-controlled entities, including the N.R.A. Foundation, an affiliated charity. Recent tax filings show that the N.R.A. diverted \$36 million last year from the foundation in various ways, far more than ever before, raising concerns among tax experts.”

**-- Attorney Michael Avenatti -- best known for representing adult-film star Stormy Daniels in her lawsuit against Trump -- wants his expensive lifestyle and money troubles off limits at his New York trial on federal charges of attempted extortion and wire fraud. [Shayna Jacobs reports](#):** “Avenatti’s expensive habits do not belong at his trial because motive is not necessary to the government’s case and ‘his general financial condition and spending habits have no bearing on his motivations under the circumstances of this case,’ his lawyers Scott Srebnick and Jose Quinon argued in the filing. ... Prosecutors say his troubles were a driving factor when he allegedly contacted Nike, a publicly traded sports apparel company, threatening to expose employee wrongdoing he claimed to have knowledge of, if Nike did not meet his demands for a \$1.5 million payout to his client Gary Franklin, a youth basketball coach, and \$15 million to \$20 million for a retainer agreement for him to purportedly investigate the wrongdoing.”





Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



Warren earned nearly \$2 million from legal work, records show

## **2020 WATCH:**

-- **“Memo from 1990s pollution case shows Elizabeth Warren in action as corporate consultant,”** [by Annie Linskey and Matt Viser](#):  
“[The memo from then-Professor Elizabeth Warren](#) was written on Harvard Law School letterhead ... Warren was not arguing on behalf of vulnerable families, nor was she offering the sort of stinging rebuke of corporate greed that would later define her political career. Rather, Warren was representing a large development company that was

trying to avoid having to clean up a toxic waste site. The [eight-page] memo, which Warren wrote in 1996, used legalistic and often dense language to argue that businesses faced the ‘risk of the unknown’ from a growing threat of lawsuits, and that defended the company’s right to ‘maximize its returns to its unpaid creditors and to survive as an employer.’

“Warren’s compensation in the 1996 case was included in a summary released by her campaign late Sunday night showing that **she had been paid about \$2 million as a legal consultant during her time as a professor, most of it between 1995 and 2009.** But Warren, who has released 11 years of tax returns, has not disclosed her tax records from most of that time period. And her campaign has provided few details about her private legal business beyond short descriptions ... **Among the corporations that hired Warren was Dow Chemical, which spent years trying to ward off liability after a subsidiary company’s silicone breast implants began to rupture.** She also worked for LTV Steel, a firm that battled with the labor movement as it tried to avoid paying millions of dollars for retired coal miners’ health care.

“The 1996 case, in which she represented a real estate development company called CMC Heartland fighting in court to avoid having to pay to clean up a polluted old rail yard along the Puget Sound in Washington state, stands out ... Warren was paid about \$21,000 for the work, according to the data released Sunday by her campaign. ... **The Supreme Court declined to take the case,** letting stand lower court rulings against Heartland and requiring it to finance the cleanup. Warren’s argument put her in line with other major corporations ...

**CMC Heartland Partners' counsel of record for the case was Kenneth W. Starr**, who at the time also served as the independent counsel examining allegations against President Bill Clinton.”

**-- Pete Buttigieg, bowing to days of attacks from Warren, announced that he will open his fundraisers to journalists and disclose the names of people raising money for his campaign. His campaign also announced that McKinsey, the consulting firm where Buttigieg used to work, will allow him to disclose the identity of his clients there.** [Amy B Wang reports](#): “Reporters will be allowed into Buttigieg’s large-dollar fundraising events starting Tuesday, and the South Bend, Ind., mayor will release a list of his ‘bundlers’ — those who funnel large sums of money to campaigns — within a week, according to Buttigieg campaign manager Mike Schmuhl. ... McKinsey said in a statement that confidentiality is important to the firm ... Any confidential, proprietary or classified information still must be kept secret, it added. The Buttigieg campaign promised a list of the client names ‘soon.’”

**-- Ronny Jackson, the former White House doctor whose nomination to lead the Department of Veteran Affairs was torpedoed last year over [allegations of professional misconduct](#), is running for Congress in Texas.** [Michael Brice-Saddler reports](#): “Jackson, a rear admiral who served in Iraq, was President Trump’s personal physician in April 2018 when he was nominated to lead the Department of Veterans Affairs. But he withdrew from consideration after Sen. Jon Tester (Mont.), the top Democrat on the Senate Committee on Veterans’ Affairs, released a two-page summary accusing Jackson of improperly dispensing medication to staff



members, drinking on the job and contributing to a hostile work environment during his tenure as White House physician. The report alleged that Jackson was known by the moniker 'Candyman' because he freely distributed medications to White House staff without paperwork, including the sleep aid Ambien. Jackson denied the allegations, and Trump later called the claims 'false accusations against a great man.' In February, Trump tapped Jackson to receive a promotion and to be his top medical adviser.

**"CNN reported this month that Jackson had retired from the Navy despite an ongoing investigation into the allegations against him led by the Defense Department's Inspector General.** Jackson, who also served as White House physician under presidents Barack Obama and George W. Bush, is one of 13 candidates vying for a seat in Texas's heavily Republican 13th District, according to the Tribune. The seat opened when Rep. Mac Thornberry, the top Republican on the House Armed Services Committee, announced in September that he plans to retire."

**-- Former representative Scott Taylor (R-Va.) will drop his challenge to Sen. Mark Warner (D) and run for his old seat in Congress.** The Post [revealed on Sunday](#) that Giuliani was trying to get Trump to nominate him for ambassador to Qatar last year. ([The Hill](#))

**-- A GOP House candidate whose failed bids against Rep. Maxine Waters (D-Calif.) have made him a cause celebre on the right was arrested on three felony charges.** [From the Daily Beast:](#)

"Businessman Omar Navarro ... faces significant legal troubles related to alleged stalking of his ex-girlfriend. San Francisco police



arrested Navarro on Saturday night, after he was allegedly seen near ex-girlfriend DeAnna Lorraine Tesoriero's apartment. Tesoriero, a self-styled MAGA relationship expert who is running a quixotic congressional run of her own against Speaker Nancy Pelosi (D-CA), told The Daily Beast that she saw Navarro skulking outside her home late at night. Tesoriero said she then received a text from an unknown number with the message, '[B----], I came to see you.' 'Clearly, he has a lot of screws loose,' Tesoriero told The Daily Beast. 'I think a lot of this power has gotten into his head. He has a lot of money now from campaign donations.'"



The Supreme Court is seen under stormy skies in Washington. (J. Scott Applewhite/AP)

## **DOMESTIC DEVELOPMENTS THAT SHOULD NOT BE OVERLOOKED:**

**-- The Supreme Court said it will not review a Kentucky law requiring doctors who perform abortions to give a detailed description of the fetus's development while the woman is shown an ultrasound image, even if she objects.** [Robert Barnes reports](#): "Without comment or noted dissent from any of its liberal members, the court said it was not taking up a challenge to the law filed by doctors at Kentucky's only abortion clinic. The doctors contended the state's requirements compelled their speech and violated their First Amendment rights. The Supreme Court already has one high-profile abortion case on its docket this term. Next month, it will consider a Louisiana law that requires physicians to have admitting privileges at a nearby hospital. It is almost identical to a Texas law the court struck down in 2016 as medically unnecessary and meant to limit a woman's access to the procedure. ... The law forcing the physician's words was a 'compelled-speech mandate wholly unrelated to traditional informed consent and therefore presumptively unconstitutional,' the clinic and its doctors argued. ... Without the requirement, there is no reason to believe that abortion providers 'do anything to dispel the mistaken beliefs of women who ... are under the impression that their fetuses are simply masses of inanimate tissue rather than living beings that are assuming the human form,' Kentucky wrote in its brief."

**-- The White House may appoint a former chemical industry**

## **executive as the next head of the Consumer Product Safety**

**Commission.** [Todd C. Frankel and Juliet Eilperin report](#): “Nancy Beck would take over as chairwoman of the Consumer Product Safety Commission, a small but powerful agency that is responsible for the safety of 15,000 everyday products, from cribs and bicycles to refrigerators and trampolines. Beck is in the late stages of being vetted by the White House for the CPSC position, according to the government officials, who spoke on the condition of anonymity to discuss private deliberations. Trump still needs to formally nominate her for the commission’s top job, which requires Senate confirmation. Beck’s selection was expected to be announced in coming weeks, the officials said. Beck joined the Trump administration in May 2017, when she was tapped to be a top deputy in the EPA’s toxic chemical unit. She previously had been an executive with the chemical industry’s main trade organization, the American Chemistry Council. At the EPA, Beck has helped scaled back several policies aimed at curbing federal limits on toxic chemicals.”

## **-- Key congressional lawmakers announced their support for a defense bill establishing both the Space Force and paid parental leave for more than 2 million federal workers, as signs of Republican opposition to the measure appeared to fade.** [Jeff Stein reports](#):

“House and Senate negotiators in both parties said they would back the bill granting \$658 billion to the Department of Defense and other defense programs, a measure that includes dozens of national security provisions prioritized by the armed services. However, the measure faced at least some new opposition from liberals in Congress who quickly announced that they would vote against it because of its provisions related to U.S. support for Saudi-



led efforts in Yemen ... In a major deal struck late last week, the White House and congressional Democrats agreed to create the Space Force as the sixth branch of the U.S. military in exchange for new parental-leave benefits for the federal workforce as part of the must-pass defense package.

**“If approved, it would be the biggest victory for federal employees in nearly 30 years.** ... The biggest remaining hurdle to the compromise appears to be Senate Republicans, who earlier this year rejected a measure to establish similar benefits for federal workers. But as of Monday afternoon, at least before the bill text was released, most in the Senate GOP caucus appeared prepared to approve the plan. Sen. Ron Johnson (R-Wis.), chairman of the committee that oversees government affairs, said he opposed the expansion of the federal benefit but does not expect to be able to stop it. ... Several other Republican senators said they were prepared to support the deal, including Sens. John Barrasso (Wyo.), Mitt Romney (Utah) and Roy Blunt (Mo.).”

**-- Good news for Washington: The Nationals and Stephen Strasburg, the reigning World Series MVP and pitcher who kick-started the team's slow rise to relevance a decade ago, agreed to a seven-year, \$245 million deal.** The record-breaking contract is the largest ever for a pitcher in both total and average annual value.  
([Jesse Dougherty](#))

**-- The North Dakota county poised to become the first in America to bar refugees under a new Trump executive order rejected the motion.** [Antonia Noori Farzan reports](#): “For four hours, sixth-generation North Dakotans and recent arrivals from Cameroon and

Congo took turns delivering impassioned testimony in what was often a contentious debate. Ultimately, the commission voted 3-2 to keep welcoming refugees. The decision largely carried symbolic resonance. The Trump administration has slashed the number of refugee arrivals nationwide, and Burleigh County, which has roughly 95,000 residents, took in just 24 refugees during fiscal year 2019, according to the North Dakota governor's office. The community — home to Bismarck, the state's capital — is slated to receive a similar number of refugees in fiscal year 2020, and the measure that passed on Monday caps the number of new arrivals at 25."

**-- Border arrests fell in November for the sixth consecutive month, new data from U.S. Customs and Border Protection shows.** [Nick Miroff reports](#): "The number of people U.S. authorities took into custody fell nearly 6 percent from October to November, to 42,649, the latest figures show. Arrests have dropped 70 percent since May, when U.S. authorities detained 144,116 amid a record influx of Central American families. Mark Morgan, the acting CBP commissioner, called the change 'staggering, in a very positive way.'"

**-- CBP denied access to a group of doctors trying to vaccinate migrant children against the flu.** [From the San Diego Union-Tribune](#): "About 40 people, including medical doctors licensed to practice medicine in California, marched Monday from Vista Terrace Neighborhood Park to the detention facility on Beyer Boulevard, calling for CBP to let them in or let the children out to participate in a free mobile clinic they set up outside. They were joined by at least another dozen medical students and supporters. ... Holding signs saying 'No more flu deaths' and 'Children don't belong in cages,' the



doctors chanted and sang. Some of them spoke about their own personal journey to the United States as undocumented migrant children. ... Though the agency did not respond directly to the doctors' demonstration, a CBP spokeswoman replied to a media inquiry ... 'It has never been a CBP practice to administer vaccines and this not a new policy,' the official statement read in part. .... 'As a law enforcement agency, and due to the short-term nature of CBP holding and other logistical challenges, operating a vaccine program is not feasible.'"

**-- A Florida official told her deputy to act like a "white supremacist" when stopping a black murder suspect.** [Hannah Knowles reports](#): "'We want it to look like you're the grumpy old man,' a woman, whom the Monroe County Sheriff's Office confirmed to be Capt. Penny Phelps, says in a recording now made public. 'You have nothing better to do than, you're the white supremacist, you're messing with the black guy who's riding his bike.' The sheriff's office, located in the Florida Keys, quickly took Phelps off the murder case last month and opened an internal investigation after receiving multiple allegations of misconduct, spokesman Adam Linhardt said. Last week, it also removed Phelps as commander of the major crimes and narcotics units, according to documents shared by the agency.'"



Ukrainian President Volodymyr Zelensky, left, German Chancellor Angela Merkel, French President Emmanuel Macron and Russian President Vladimir Putin hold a news conference after a summit on Ukraine at the Elysee Palace in Paris. (Ludovic Marin/Pool/AFP/Getty Images)

## **THE NEW WORLD ORDER:**

**-- Russia's Vladimir Putin and Ukraine's Volodymyr Zelensky agreed to a renewed cease-fire and to exchange all known prisoners when they met for the first time in Paris. [James McAuley](#), [Robyn Dixon](#) and [Michael Birnbaum](#) report:** "The talks yielded enough progress to get the peace process moving, but as

expected, there was no major breakthrough. 'We haven't found the magic wand, but we have relaunched talks,' said French President Emmanuel Macron, who convened the gathering. He said the talks had made 'practical, tangible progress.' **The parties agreed to meet again in four months to discuss one of the stumbling blocks: conditions for elections in eastern Ukraine**, which would then lead to special status for the regions. The Ukrainian president has declared that there can be no elections in those regions until all military formations have withdrawn. ... **This is a lonely moment for Zelensky. Once-ironclad U.S. support for Ukraine is shrinking under Trump.** German Chancellor Angela Merkel helped mediate Monday's meetings, but she is distracted by her own roiling domestic politics."

**-- Trump will meet with Russian Foreign Minister Sergey Lavrov today in the Oval Office for a conversation that could include the extension of the last major nuclear treaty between the U.S. and Russia. Lavrov will also meet with Secretary of State Mike Pompeo.** [From the Times](#): "Considerable evidence suggests any conversation with Mr. Lavrov would include the last major nuclear arms control treaty still in force between the United States and Russia: the Obama-era New START treaty, which in recent days [Putin] has said he wants to extend for another five years. In any other presidency that would seem uncontroversial. Democrats and Republicans on Capitol Hill have largely agreed that extending the accord would be good, avoiding a nuclear arms race at a time of heightened tension with Mr. Putin's government ... The result is that Mr. Trump, until recently, has dismissed the agreement as a 'one-sided deal,' and a failure by President Barack Obama. ... At the same time, Mr. Trump



has said he wants to avoid a nuclear arms race ... If Mr. Trump can pull off an extension, it would be the first diplomatic breakthrough of his presidency with Russia.”

**-- Russia called the Olympic committee’s ban “anti-Russia hysteria” that is politically motivated. [Isabelle Khurshudyan reports](#):**

“Russia’s reaction to being banned Monday from the next two Olympics in the wake of one of the biggest international sports doping scandals has been to claim it’s the world’s punching bag. ... Just as Moscow has repeatedly denied interfering in the 2016 U.S. presidential election, claiming allegations were part of an anti-Russian narrative, the official reaction since the sports scandal first surfaced in 2015 has been to complain that this too was political. ‘It’s obvious in this case that there are still significant doping problems on the Russian side — I mean our sports community. This can’t be denied,’ Russian Prime Minister Dmitry Medvedev said at a conference Monday with deputy prime ministers in Moscow.”

**-- The behavior of the trainee who killed three classmates at a Florida Navy base changed after a trip to his native Saudi Arabia, friends said. [Souad Mekhennet, T.S. Strickland and Joby Warrick report](#):**

“Ahmed Mohammed al-Shamrani was described as ‘strange’ and ‘angry’ in the weeks leading up to Friday’s shooting rampage, but schoolmates and other acquaintances said he showed no outward sign that he was preparing to open fire inside a classroom building where he had been training to become a military aviator. The shooting, which also left eight people injured, is being treated by the FBI as a possible terrorist attack.”

**-- The White House blocked a U.N. meeting on North Korean**

**atrocities in an attempt to salvage the faltering diplomatic effort to convince Kim Jong Un to abandon his nuclear weapons program.** [From Foreign Policy](#): “Once again, the U.S. has prevented the U.N. Security Council from scrutinizing North Korea’s abysmal human rights record, apparently because of President Trump’s special relationship with Kim Jong Un,” said Louis Charbonneau, the U.N. director for Human Rights Watch. ‘By blocking this meeting, which was set to go ahead on Human Rights Day..., the Trump administration is sending a message to Kim that the U.S. no longer considers arbitrary detention, starvation, torture, summary executions, sexual violence and other crimes against the North Korean people a priority,’ Charbonneau added. ‘North Korea and many other abusive governments can now rest assured that they have little to fear from the Trump administration when it comes to human rights.’ In response to a request for comment, a State Department spokesman said that the U.S. still plans to press for a council meeting on North Korea this week, but did not say human rights would be discussed.”

**-- Trump and Pelosi are ready to pass a new NAFTA.** [From Politico](#): “The deal remains unofficial until Tuesday, when the top trade officials from the U.S., Mexico and Canada are expected to meet in Mexico City for an afternoon ceremony. Pelosi is also holding off on making a public announcement until she has briefed her caucus on the policy details of the pact, which replaces the 25-year-old North American Free Trade Agreement. ... AFL-CIO President Richard Trumka, whose support is crucial to getting Democrats’ approval, briefed his executive council Monday afternoon on changes to the pact and is now willing to let the agreement move forward ... The new trade deal keeps tariff-free trade among the three countries.”



**-- Poll numbers in the U.K. show Tories maintaining the lead over the Labour Party as the campaign enters its final days.** ([The Guardian](#))

**-- Jonathan Ashworth, the U.K.'s shadow health secretary, dismissed as “banter” a leaked tape showing him saying Labour, his party, will lose the election.** In the recording, Ashworth also says Jeremy Corbyn is a serious problem for the party. ([The Guardian](#))

**-- After two elections in less than a year, Israeli leaders have less than 48 hours to stop a third.** [Ruth Eglash reports](#): “There had been a flurry of attempts to find a solution or form a new government over the past week, but as the clock ticked toward the final deadline, the only thing the sides appeared to agree upon was a date for the next election: March 2, 2020. After two rounds of voting, in April and September, and two 28-day stretches where Prime Minister Benjamin Netanyahu and his political rival, former military chief Benny Gantz, attempted and failed to cobble together a coalition, Israel’s parliament, the Knesset, was given a final 21 days to find someone who might be able to solve the stalemate. If none among the Knesset’s 120 lawmakers comes forward with backing from 61 fellow parliamentarians by midnight on Wednesday, the next election cycle will automatically be underway.”

**-- Ethiopia’s Abiy Ahmed won’t answer any questions when he receives his Nobel Prize, highlighting the Nobel Committee’s awareness that his victory would generate controversy.** [Max Bearak reports](#): “Abiy is refusing to engage with the international media when he receives the prize Tuesday in Oslo — refusing even to

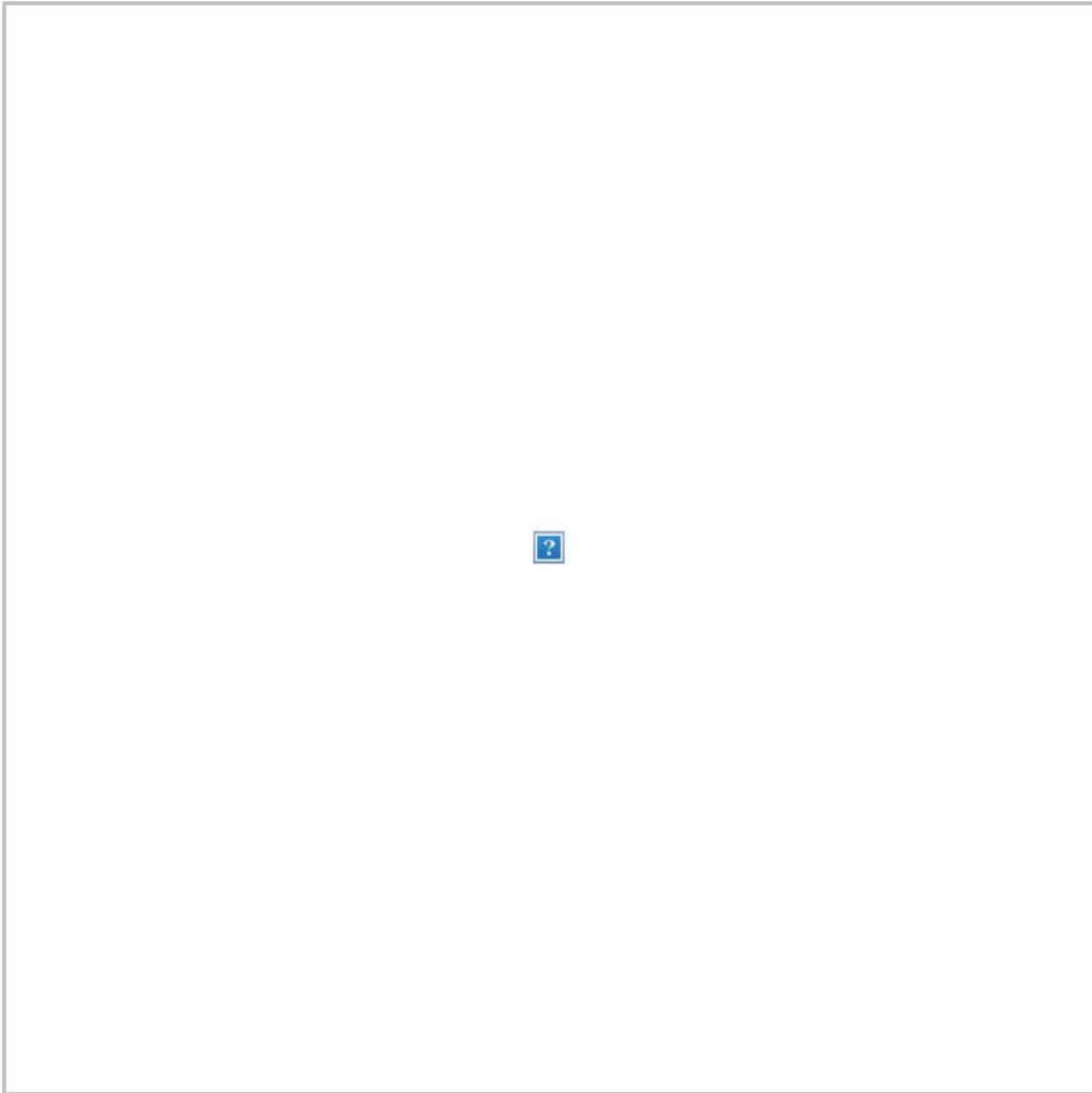
field questions from the young students who traditionally are offered that opportunity at an event hosted by Save the Children — and the Nobel Committee is scrambling to get him to change his mind and spare it a major embarrassment. ... Although Abiy has soaked up public adoration during morale-raising events such as rallies and tree-planting drives, he has often stayed silent for weeks after incidences of ethnic tension, which have been frequent and often bloody over the past two years.”

**-- A Chilean Air Force plane carrying 38 went missing on its way to Antarctica. Authorities believe it crashed.** [From CNN](#): “Its last known position was about 390 nautical miles from Punta Arenas and 280 nautical miles from the Antarctic base ... There were 17 crew members and 21 other passengers on board, who were on their way to perform ‘logistical support tasks’ such as repairing the floating oil pipeline that provides fuel for the base, said the Air Force. In addition to crew members, the plane was also carrying personnel from the armed forces, an engineering firm, and the University of Magallanes.”

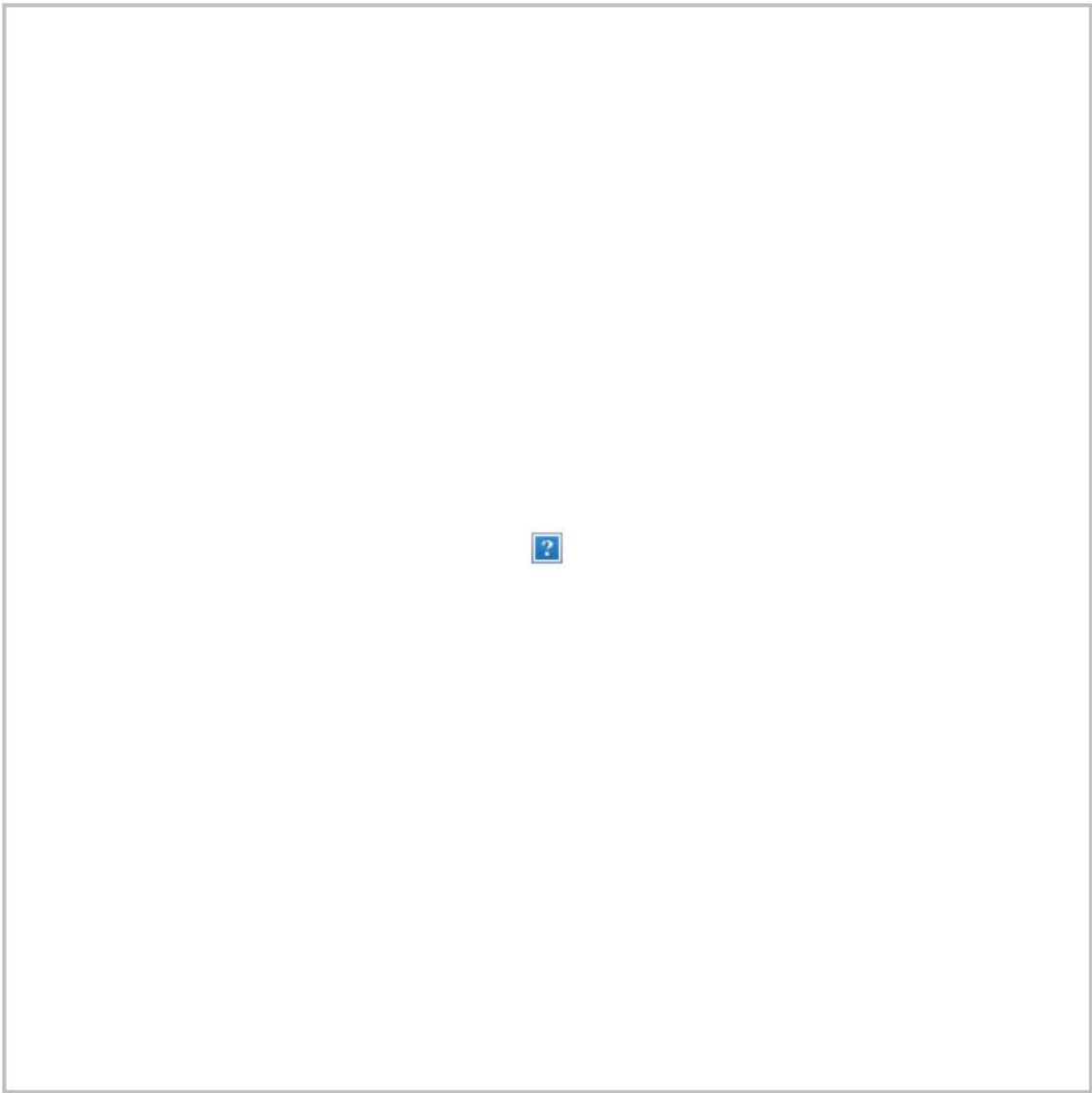
**-- At least six people were shot dead in a Czech Republic hospital last night before the gunman escaped and then shot himself.** [Loveday Morris reports](#): “Police hunted for the 42-year-old suspect for several hours before they tracked him to his vehicle, where he shot himself in the head as the police helicopter hovered overhead, according to regional police head Tomas Kuzel. He added that the gunman was using an illegal 9mm handgun.”

**SOCIAL MEDIA SPEED READ:**

These were this year's most popular politicians on Twitter:



A CNN host noted that, for many, yesterday's big news didn't come from the Inspector General's report or from the impeachment hearing:

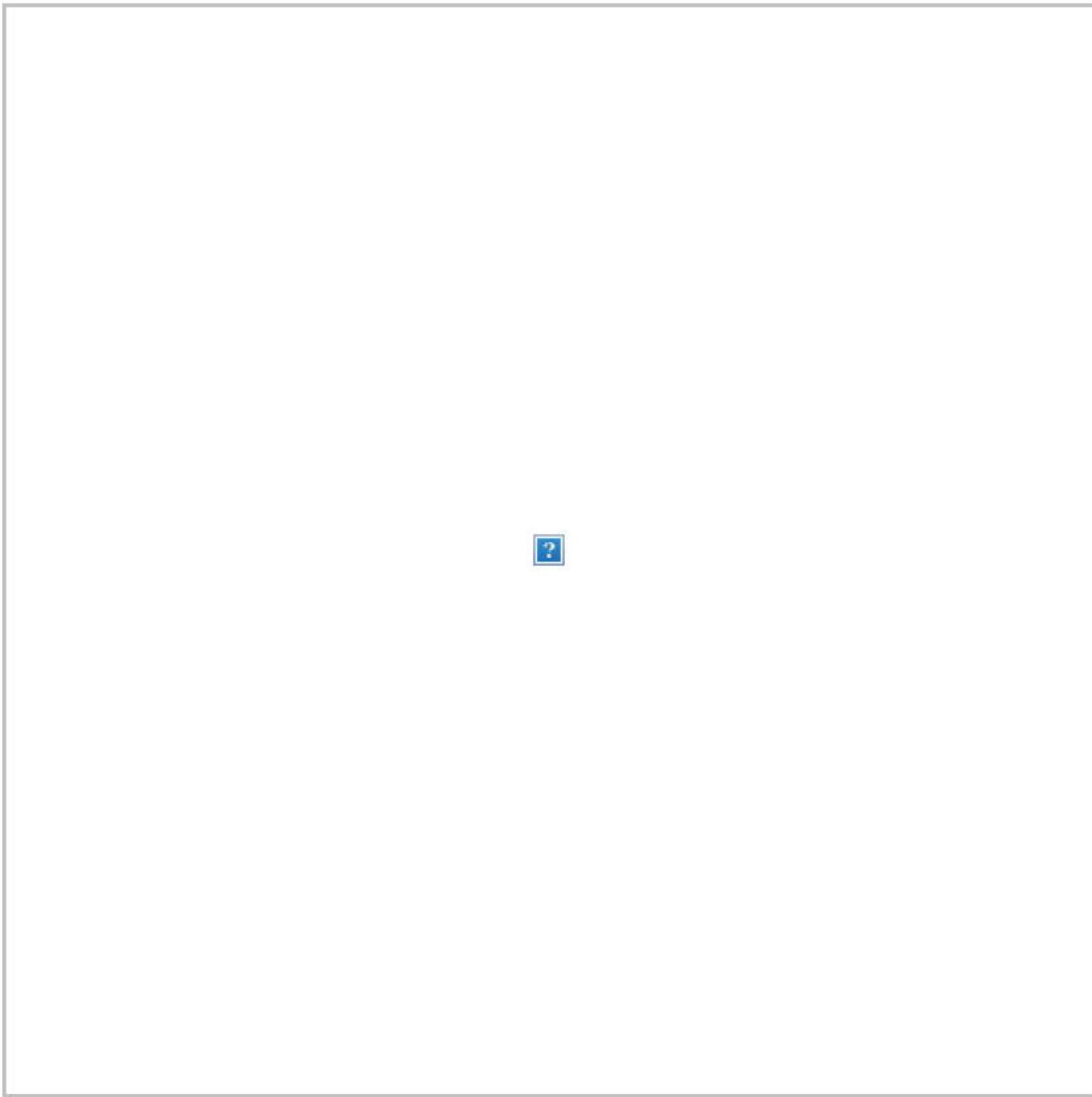


Jim Comey said he agreed to go on Fox News this morning, but the network canceled. Fox responded that his appearance was never confirmed:

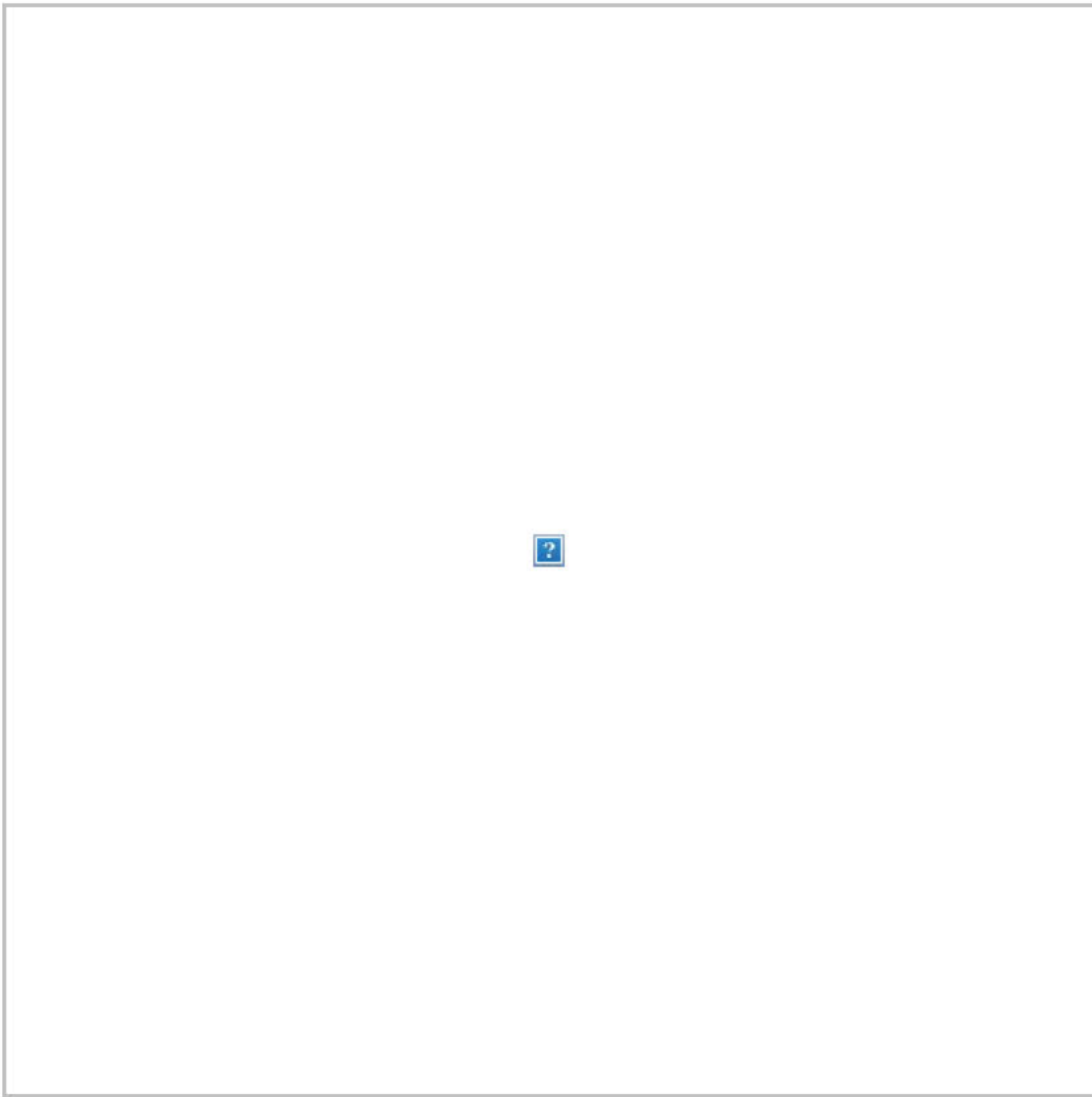


Comey's agent, Keith Urbahn of Javelin, replied to a conservative commentator who took Fox's denial at face value:

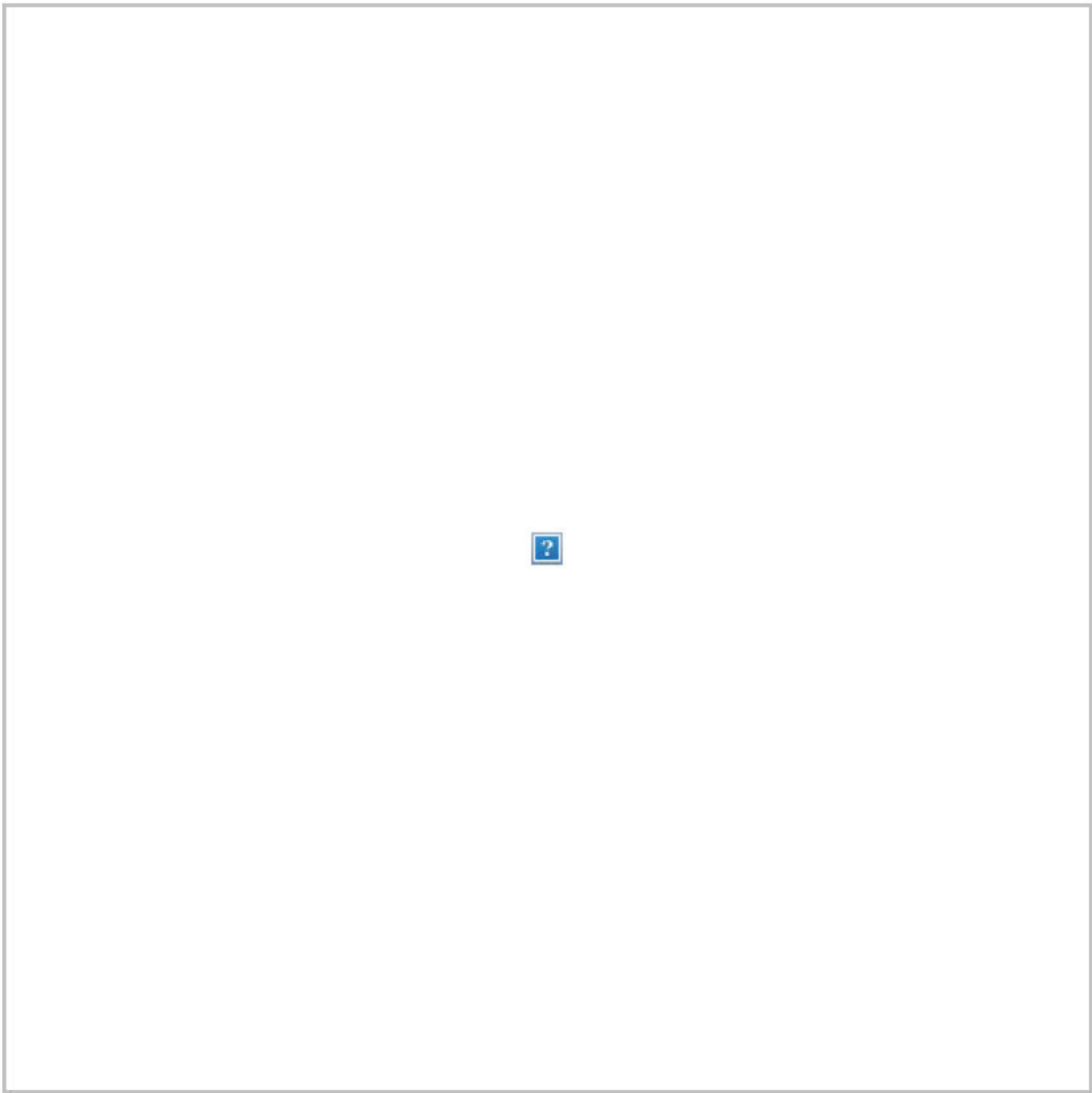




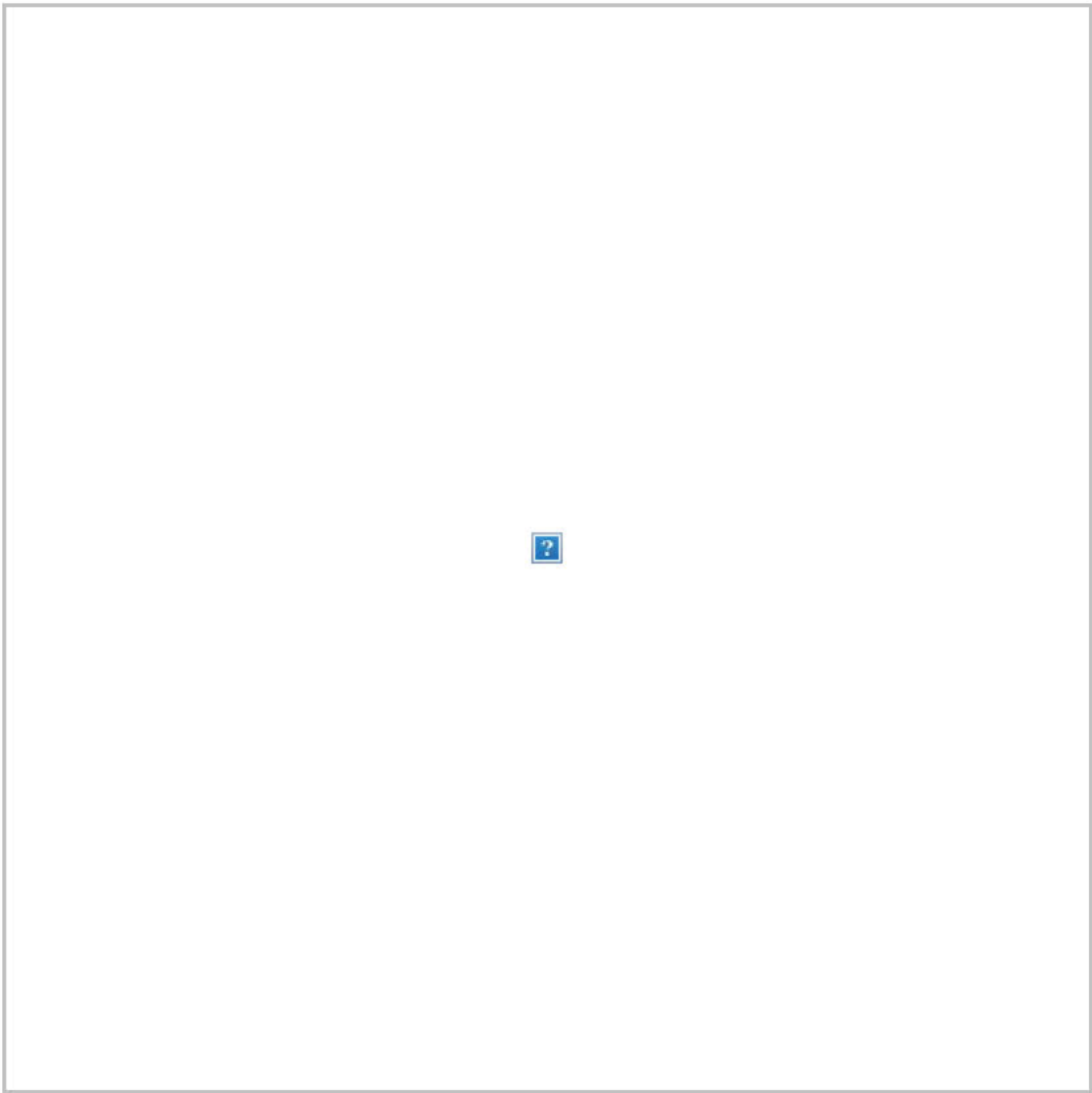
A former director of the Office of Government Ethics highlighted the IG's disclosure that FBI agents were also exchanging pro-Trump messages:



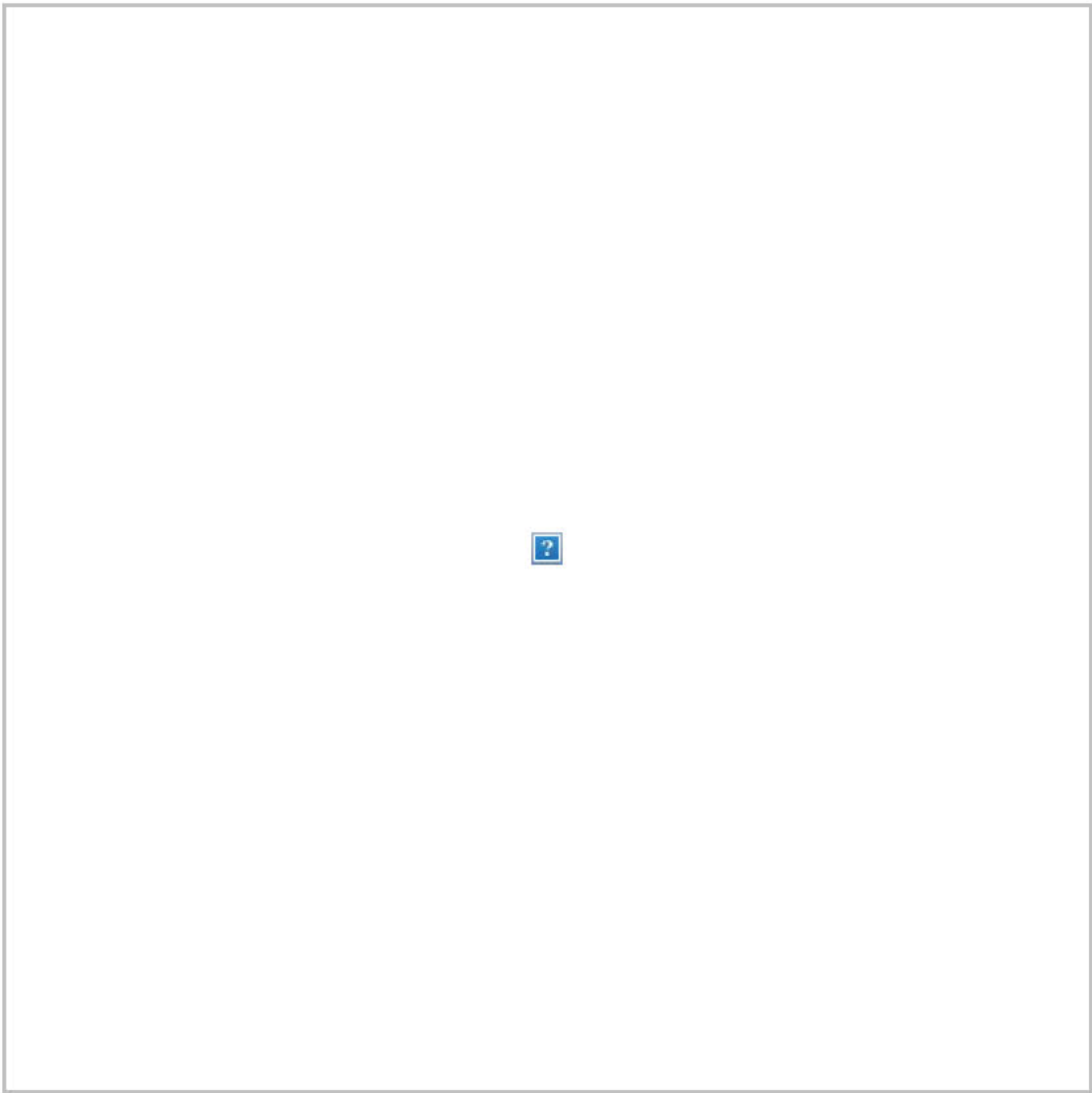
The former FBI lawyer, whose texts were publicized by Trump appointees at the DOJ and who has been a frequent target of the president, claimed vindication from the IG report:



Imagine what's going on in this young man's head:



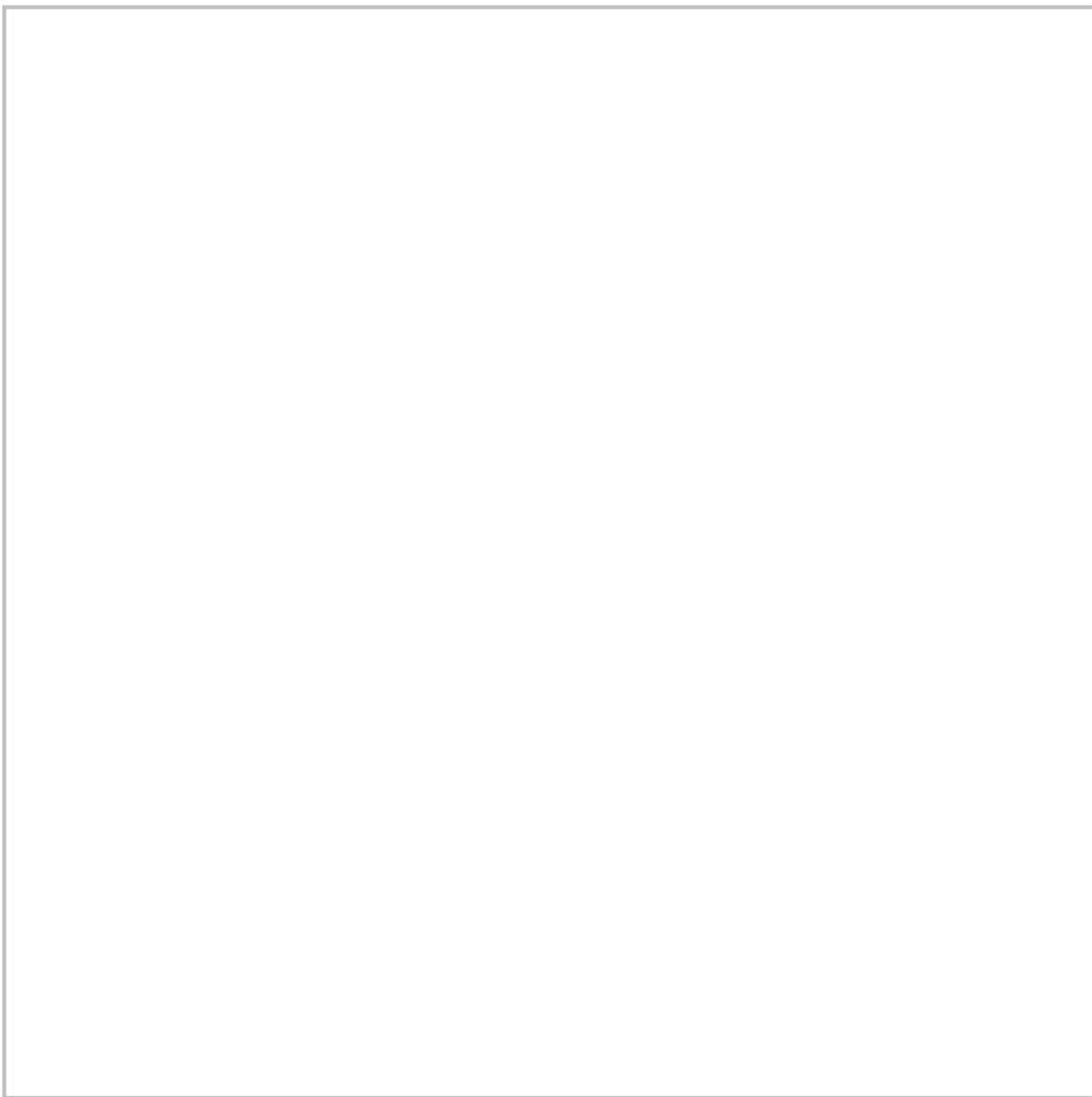
A University of Texas law professor asked Americans to read the IG report after a top Republican shared a misleading tweet about it:



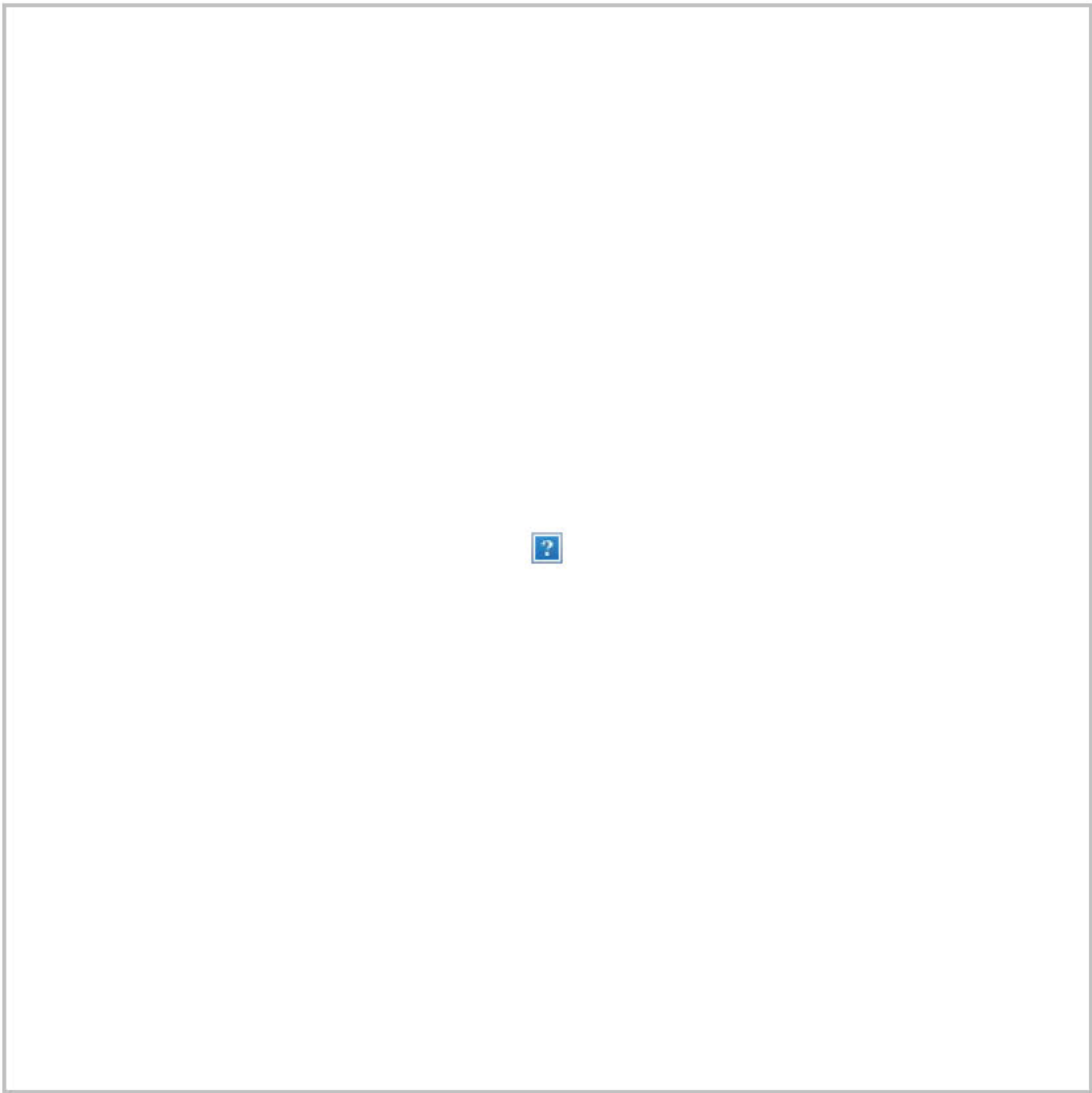
Can't say the latest impeachment hearing was boring, not with these posters:







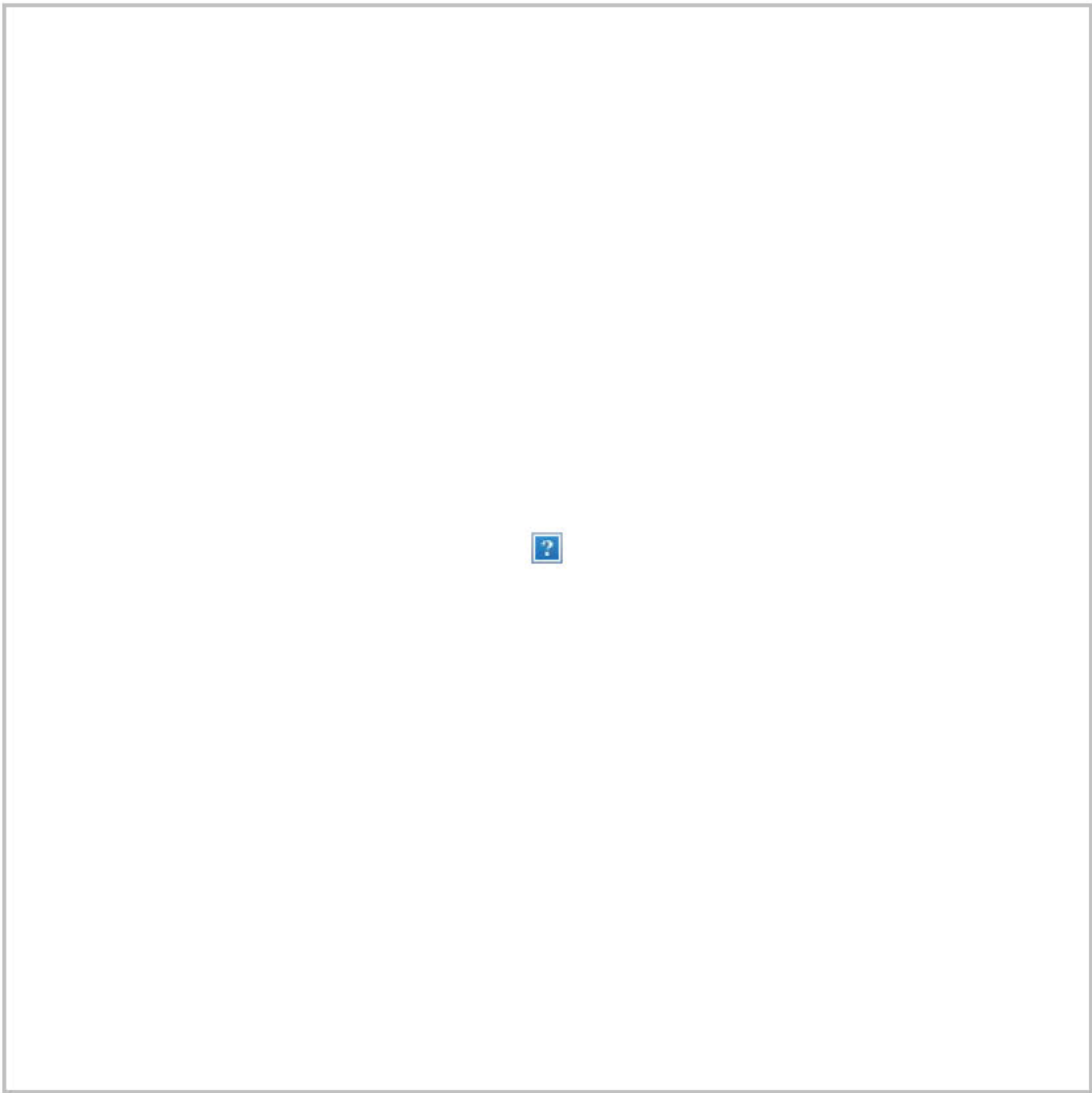
Rep. Tulsi Gabbard (D-Hawaii) announced she won't participate in a debate that she has not qualified for:



Elizabeth Warren's new campaign spokesman might have to update his Twitter bio:



Pete Buttigieg's term as mayor is ending:



And Monica Lewinsky had some life advice to share:

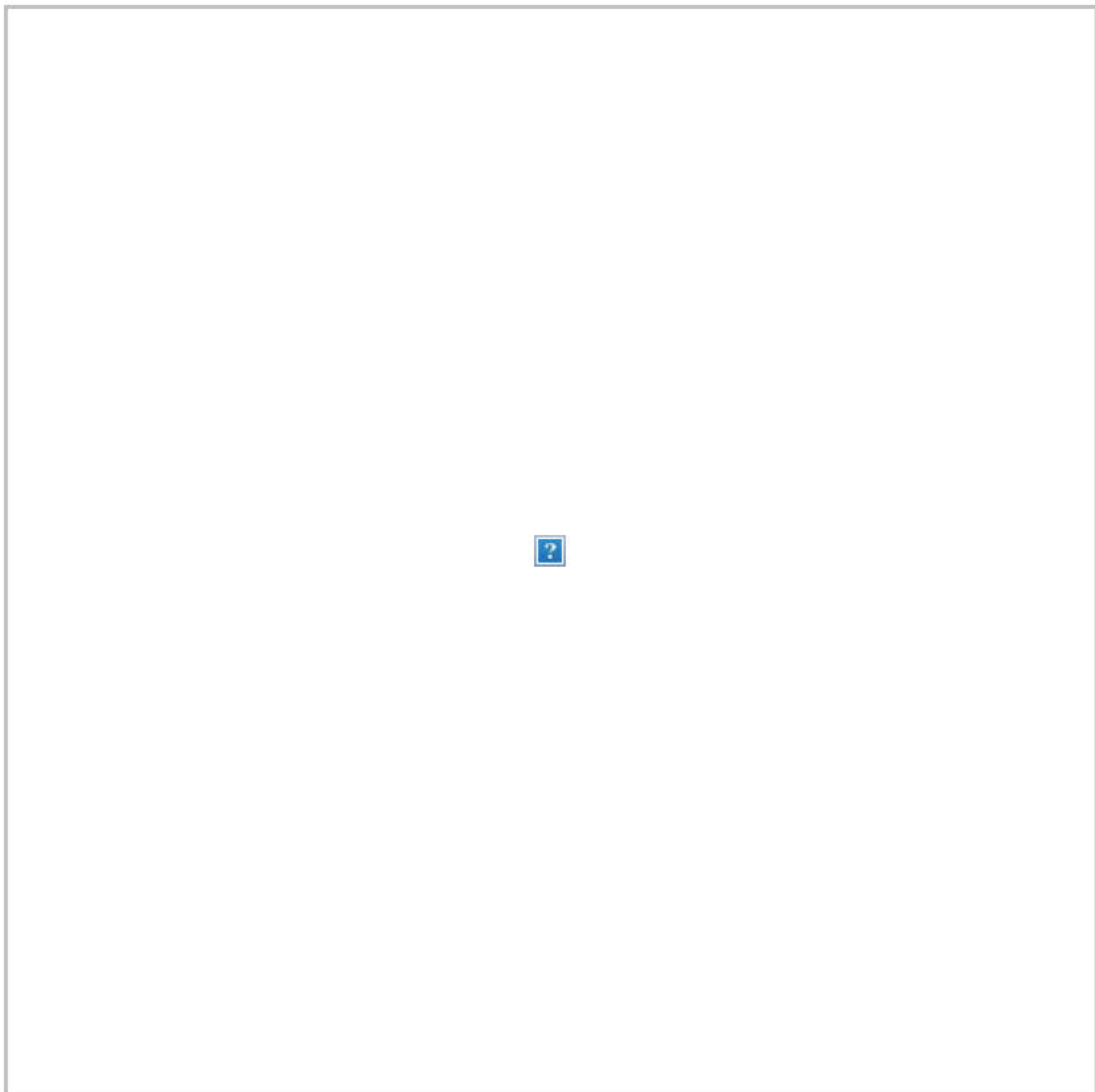




**QUOTE OF THE DAY:** "The most traumatic experiences of our lives didn't have to happen, our friends didn't have to die on the other side of the planet," said Marine Corps veteran Dustin Kelly, who said The Post's report on the U.S. government's distortion over the prosecution of the Afghanistan War reignites the agony of not knowing precisely what comrades gave their lives for. (Alex Horton)

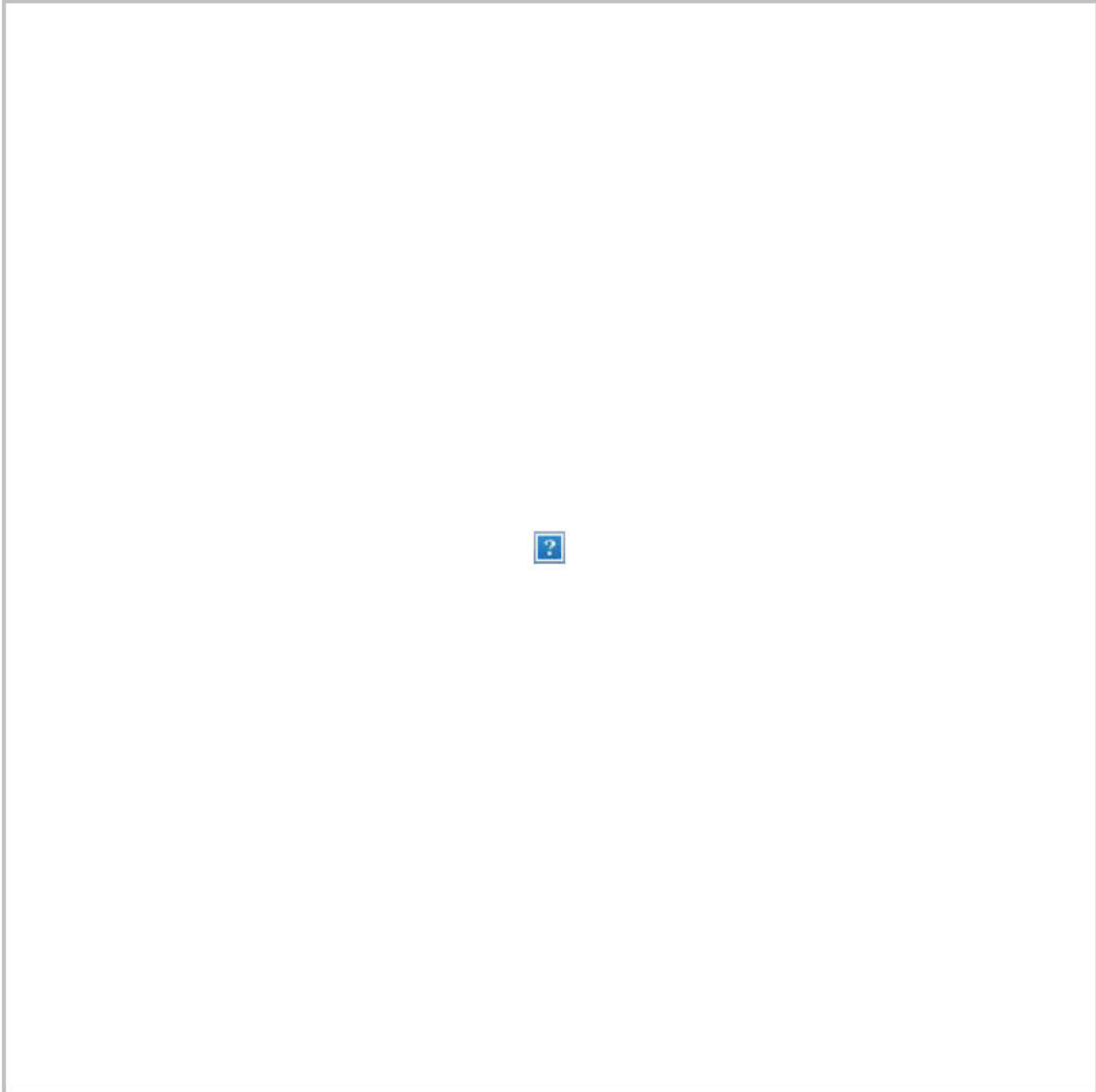
## VIDEOS OF THE DAY:

Houston Police Chief Art Acevedo lashed out at three top Republican lawmakers, including two from his state, for not reauthorizing the Violence Against Women Act. One of his officers, Sgt. Chris Brewster, was fatally shot this weekend after responding to reports of a domestic disturbance:

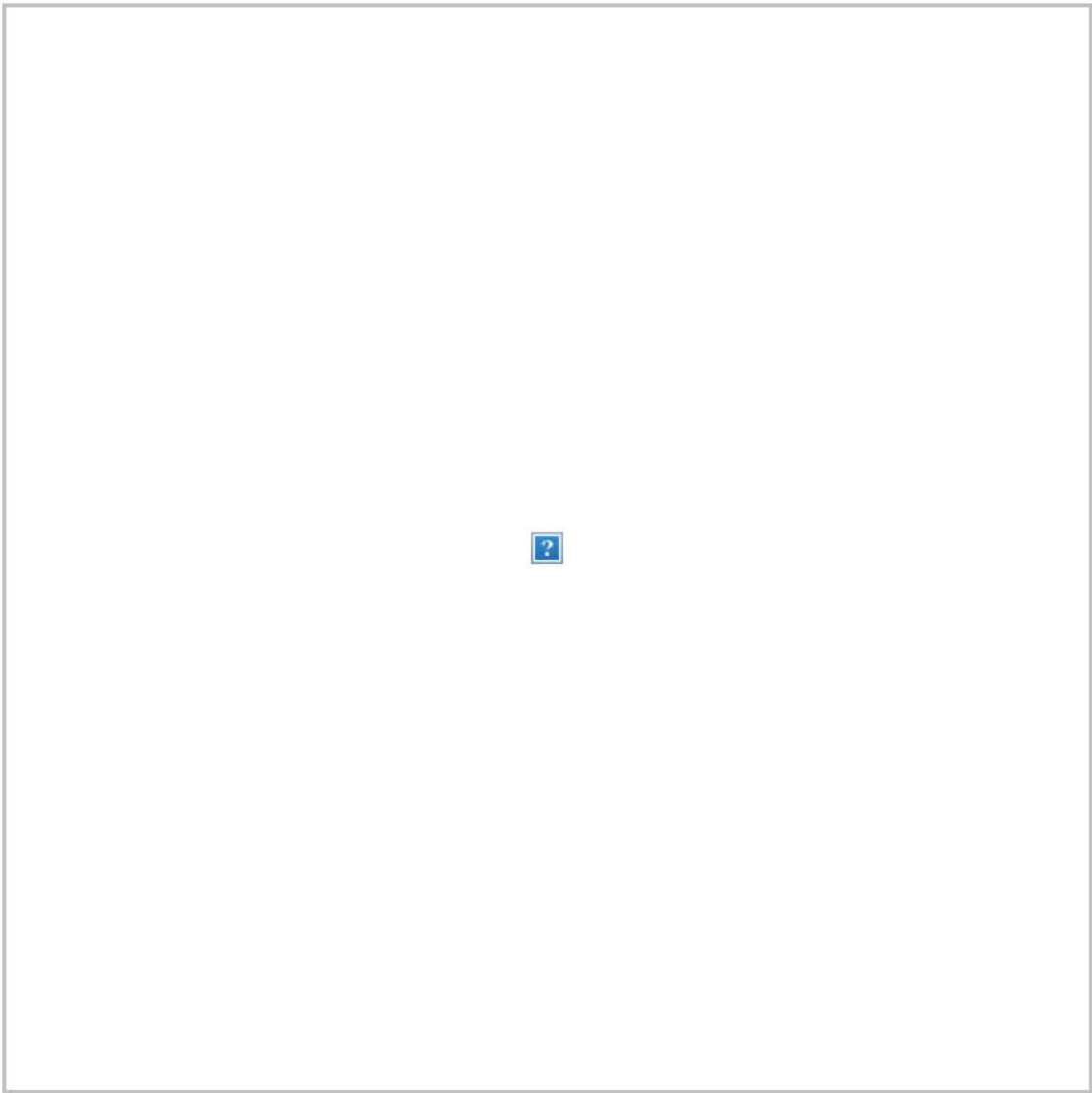


'Whose side are you on?': Houston police chief blasts NRA, senators over inaction on gun legislation

British Prime Minister Boris Johnson remade a famous scene from “Love Actually” to create a viral ad for his reelection:



John Weigel, the veteran who told Bernie Sanders at a rally earlier this year that he was considering suicide because he could not afford his medical bills, told the candidate on Monday that he's received help and tried to offer Sanders his flight jacket:



GOP counsel Steve Castor walked into Monday's House Judiciary Committee hearing not with a briefcase but a reusable grocery bag:

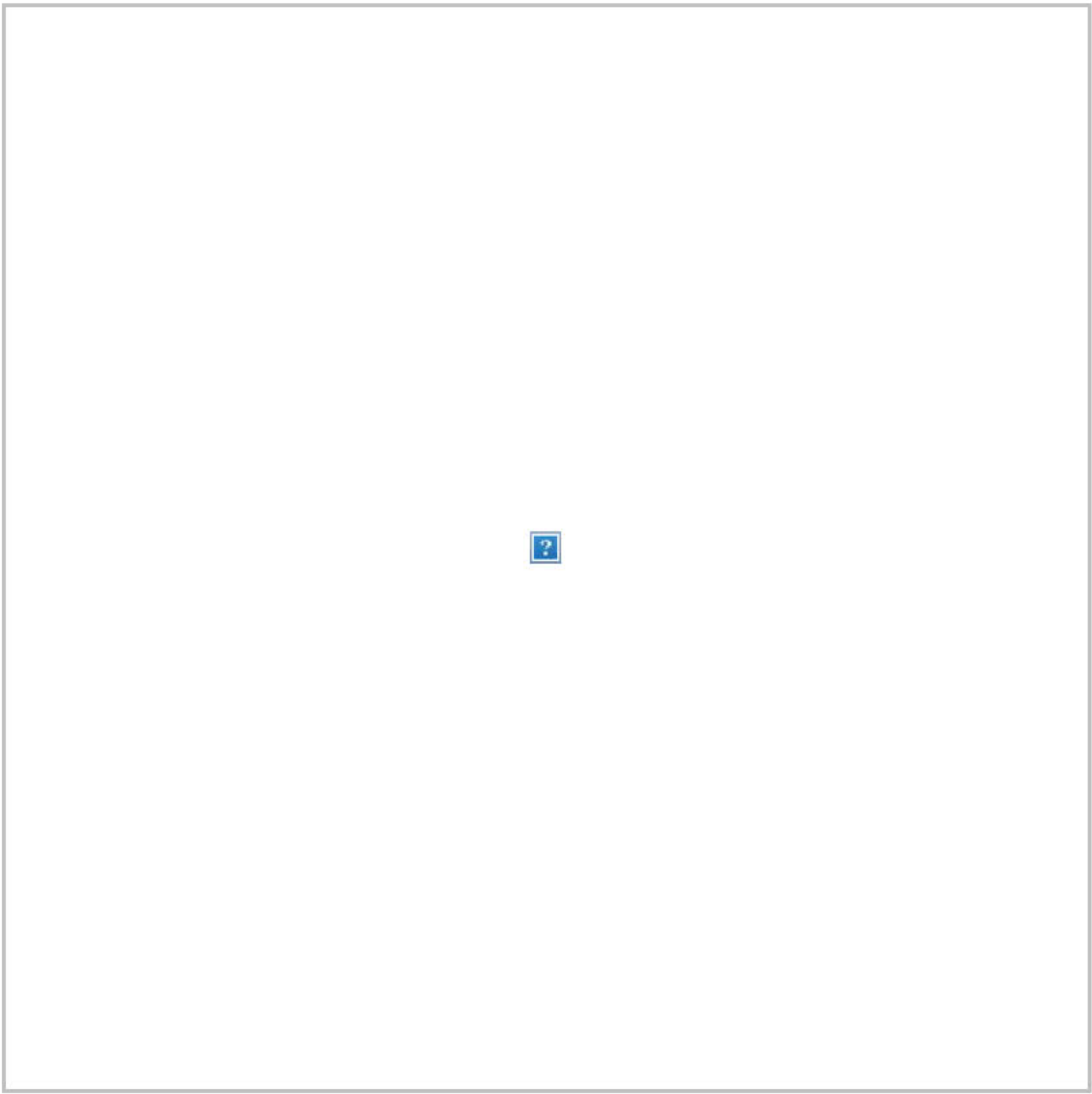


Seth Meyers really, really wants Rudy Giuliani to testify before Congress:





Stephen Colbert thinks Trump's understanding of the Inspector General report is further proof he lives in an alternate reality:



You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)

---

©2019 The Washington Post | 1301 K St NW, Washington DC 20071



**From:** [The Washington Post](#)  
**To:** [achu@sunnyvale.ca.gov](mailto:achu@sunnyvale.ca.gov)  
**Subject:** The Daily 202: FBI director shows independence from Trump and Barr in responding to IG report on Russia probe  
**Date:** Tuesday, December 10, 2019 7:44:13 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you're having trouble reading this, [click here](#).

---

# The Daily 202

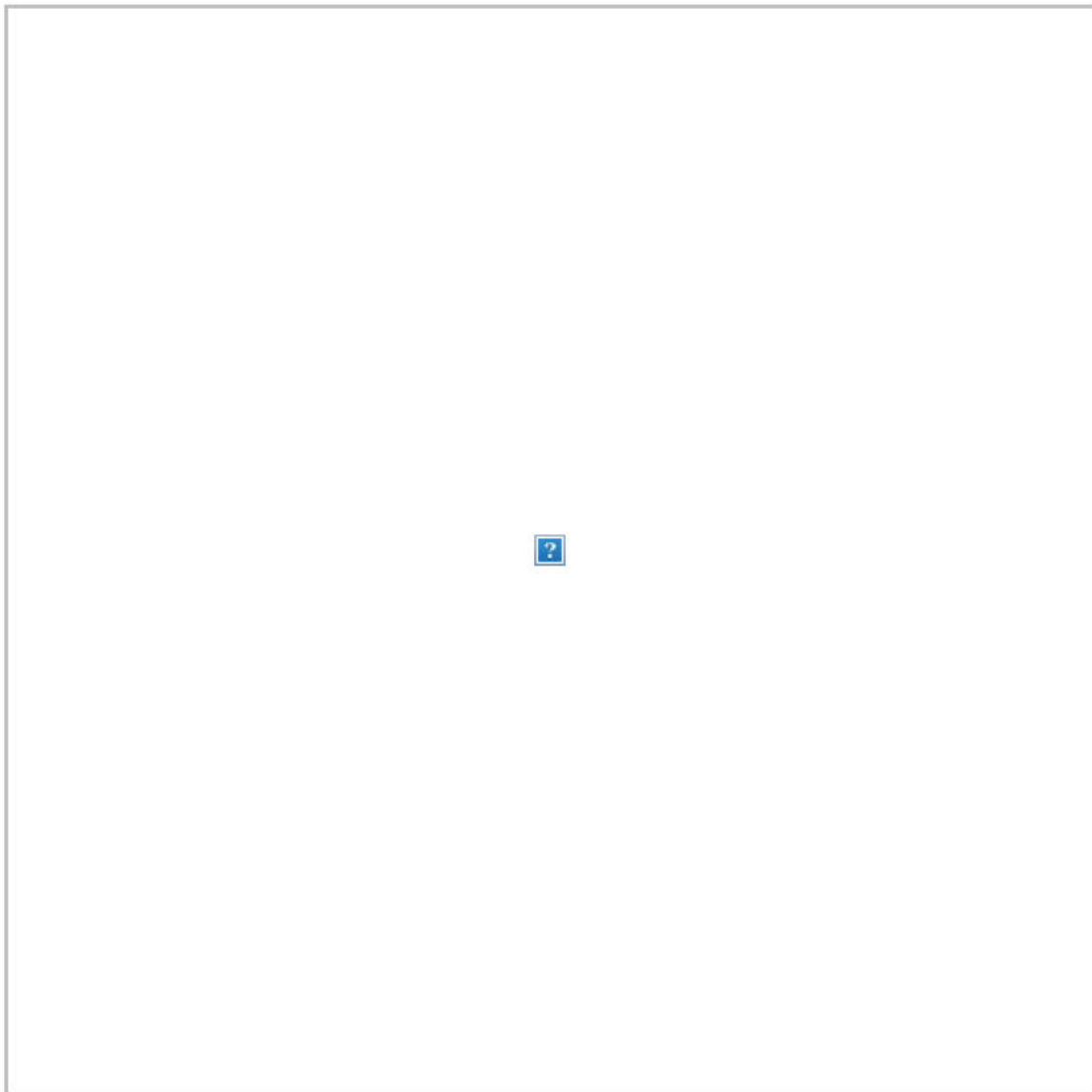


Share:  

 Listen to The Big Idea



## FBI director shows independence from Trump and Barr in responding to IG report on Russia probe



FBI Director Christopher Wray poses for a photo on Monday. (Jacquelyn Martin/AP)

**BY JAMES HOHMANN**



*with Mariana Alfaro*

## **THE BIG IDEA: FBI Director Chris Wray's response to the Justice Department's independent watchdog was nuanced.**

"The inspector general did not find political bias or improper motivations impacting the opening of the investigation or the decision to use certain investigative tools," Wray told [ABC News](#) on Monday afternoon, "but the inspector general did find a number of instances where employees either failed to follow our policies, neglected to exercise appropriate diligence or in some other way fell short of the standard of conduct and performance that we ... expect of all our employees."

This is an accurate [summary](#) of what Justice Department Inspector General Michael Horowitz [concluded](#) in [his 434-page report](#) examining the FBI's investigation of President Trump's 2016 campaign. Wray also announced that he's ordered "more than 40 corrective steps" to address what the report identified as "serious performance failures."

**But Trump has little tolerance for shades of gray.** You're either with him or against him. The president [lashed out](#) Tuesday morning at Wray, whom he appointed in 2017 after firing Jim Comey.

"I don't know what report [Wray] was reading, but it sure wasn't the one given to me," Trump [tweeted](#). "With that kind of attitude, he will never be able to fix the FBI, which is badly broken despite having some of the greatest men & women working there!"

**-- Asked whether he thought the FBI unfairly targeted the Trump**



**campaign in 2016, Wray told ABC: “I do not.”** While careful not to criticize the president directly, Wray said that calling FBI agents part of “the deep state,” something Trump has done, is “an affront to them.”

“I think it's important that the inspector general found that, in this particular instance, the investigation was opened with appropriate predication and authorization,” he said.

Asked about the latest conspiracy theory being pushed by Trump and his congressional loyalists, Wray answered: “We have no information that indicates that Ukraine interfered with the 2016 presidential election. As far as the [2020] election itself goes, we think Russia represents the most significant threat.”



When William Barr has echoed Trump's rhetoric

**-- Trump's broadside against Wray puts in stark relief just how deeply in the tank Attorney General Bill Barr is for Trump. Breaking with Horowitz, as well as Wray, Barr disputed the IG's conclusion that there was enough probable cause to launch an investigation.**

"The Inspector General's report now makes clear that the FBI launched an intrusive investigation of a U.S. presidential campaign on the thinnest of suspicions that, in my view, were insufficient to justify

the steps taken,” the attorney general wrote in [a blistering statement](#). “It is also clear that, from its inception, the evidence produced by the investigation was consistently exculpatory. Nevertheless, the investigation and surveillance was pushed forward for the duration of the campaign and deep into President Trump’s administration. In the rush to obtain and maintain FISA surveillance of Trump campaign associates, FBI officials misled the FISA court, omitted critical exculpatory facts from their filings, and suppressed or ignored information negating the reliability of their principal source.”

FISA is short for the Foreign Intelligence Surveillance Act. **Barr testified earlier this year that he believes “[spying did occur](#)” on the Trump campaign. Wray had previously said “spying” is “[not a term I would use](#).”** He reiterated that on Monday. “Again, different people have different colloquial terms, but we use terms like ‘investigation’ and ‘surveillance,’” the FBI director told ABC.

**-- Connecticut U.S. Attorney John Durham put out [his own statement critical of the IG report](#).** He’s been handpicked by Barr to conduct a probe, separate from Horowitz’s, into how the U.S. government investigated Trump’s 2016 campaign. “Our investigation has included developing information from other persons and entities, both in the U.S. and outside of the U.S.,” Durham said. “Based on the evidence collected to date, and while our investigation is ongoing, last month we advised the Inspector General that we do not agree with some of the report’s conclusions as to predication and how the FBI case was opened.”

It is highly irregular for a U.S. attorney to release a statement like this in the middle of an ongoing criminal investigation.

**After Horowitz implicitly debunked several arguments Trump espoused for years, the president has already turned his attention to Durham's investigation of his investigators.** "I look forward to the Durham report, which is coming out in the not-too-distant future," he told reporters at the White House on Monday. "It's got its own information, which is this information plus plus plus."



Trump says inspector general report is 'far worse' than expected



**-- Wray appears focused on protecting the FBI's reputation while Barr seems primarily focused on protecting, and placating, the president. Barr is managing up. Wray is managing down.** This fits with [a pattern](#). While Barr is the nation's chief law enforcement officer, critics say he's consistently acted more like the president's personal lawyer than the nation's lawyer. The attorney general wrote a misleadingly pro-Trump summary of Robert Mueller's report on Russian election interference. He cleared Trump of obstruction of justice, even though the special counsel had not done so. He even embraced Trump's "no collusion" talking points.

**Barr's Justice Department also intervened to help the White House's initial efforts to conceal a CIA analyst's whistleblower complaint that Congress was legally entitled to receive.** And Barr's underlings at DOJ also declined to investigate suggestions of criminal wrongdoing in the complaint. The attorney general declined to recuse himself from these deliberations, even though the whistleblower complaint – and the rough transcript of the July 25 call – showed that Trump brought up Barr during his conversation with Ukrainian President Volodymyr Zelensky.

**-- Barr planned to hold a 200-person holiday party at the Trump hotel in Washington on Sunday night, but he rescheduled the event. A Justice Department spokeswoman declined to say when the event would take place, but she said it would still be at the Trump International.** "Barr signed a contract with the Trump hotel over the summer that required a minimum of \$31,500 in spending. He put up a \$10,000 deposit," [Jonathan O'Connell reports](#). "The total cost of the party could be much higher depending on the menu Barr



chooses to go with a four-hour open bar. Barr planned to pay for the party himself, avoiding concerns about the Constitution's emoluments clause ...

**“Not publicly disclosing the event’s new date could help Barr and his guests avoid protests.** On Sunday night, half a dozen protesters — thinking Barr’s guests would be arriving — held a sign on the sidewalk out front calling for Barr to be disbarred and told guests arriving at the hotel: ‘You’re on the wrong side of history.’”

**Meanwhile, Justice Department attorneys are defending Trump in court this week against two lawsuits claiming that he’s unconstitutionally benefiting from his personal business, including the D.C. hotel, while in the White House.**



Graham says inspector general report shows a 'system off the rails'

**-- This is not the first time Trump has criticized Wray.** This spring, the director testified that any campaign should alert the FBI if foreign agents reach out offering dirt on their political opponents. "My view is that, if any public official or member of any campaign is contacted by any nation-state or anybody acting on behalf of a nation-state about influencing or interfering with our election, then that is something that the FBI would want to know about," Wray testified. Asked about this statement in June, Trump replied, "[The FBI director is wrong.](#)" The

president insisted that “there isn’t anything wrong” with accepting “oppo research” from foreign powers.

**-- Wray has also previously dismissed Trump’s attacks on the FBI as “noise.”** At a Senate Intelligence Committee hearing in February, Wray was asked about the president's criticisms of the FBI. “There's no shortage of opinions about our agency, just like every other agency up here — and just like the Congress,” Wray responded. “I'd encourage our folks not to get too hung up on what I consider to be the noise on TV and in social media.”

Last year, soon after taking the job, Wray [privately warned](#) the White House against releasing that memo by Rep. Devin Nunes (R-Calif.), who was then the chairman of the House Intelligence Committee. When Trump overruled him, Wray signed off on a statement from the FBI that said: “We have grave concerns about material omissions of fact that fundamentally impact the memo's accuracy.”

**-- FBI directors are appointed to 10-year terms. That’s intended to keep them insulated from politics, but they are accountable to the attorney general and can be fired by the president – as Trump fired Comey.** Of course, this isn’t the first time that Trump publicly chastised his appointees in the law enforcement firmament. He routinely disparaged Jeff Sessions before firing him as attorney general and replacing him with the more pliable Barr. He also attacked former deputy attorney general Rod Rosenstein, falsely accusing his own appointee of being a Democrat.



Schumer says inspector general report 'puts conspiracy theories to rest'



-- **The correctives:** Responding to the IG report, Wray **announced** that the **FBI** will modify the processes for applying and renewing warrants under the **Foreign Intelligence Surveillance Act**. For a sensitive investigation to be run out of headquarters, Wray said, prior approval from the FBI deputy director will be required and field offices will be consulted. He announced “significant changes” to how the FBI



manages its Confidential Human Source program, related to how the FBI collects, documents and circulates information from its informants.

**Wray also established new protocols for the FBI's participation in the strategic intelligence briefings provided to presidential nominees.** Wray said the FBI's role in these briefings should be for national security purposes and not for investigative purposes to ensure that candidates and their advisers trust the people who are talking to them about threats. In 2016, an FBI agent went to the briefing for Trump to keep an eye on how Michael Flynn reacted to certain information.

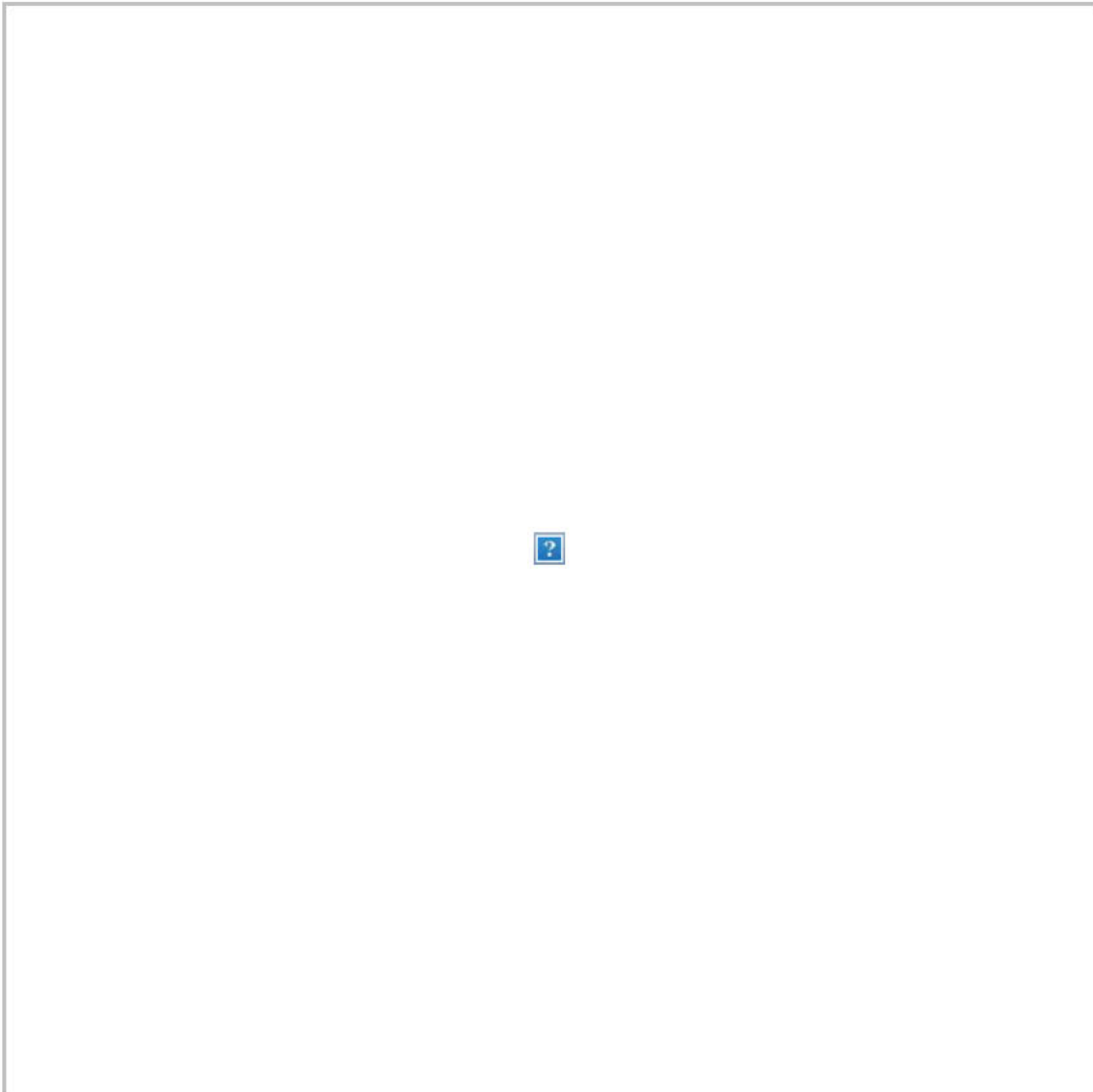
**Wray said he's mandating specialized, semiannual training for all FBI personnel who handle FISA warrants or confidential human sources.** He noted that he reinstated an annual ethics training program for all FBI employees that had been discontinued in prior years. Finally, Wray said that the FBI will take appropriate disciplinary action where warranted against any wrongdoing identified in the report.

**"I am very committed to the FBI being agile in its tackling of foreign threats. But I believe you can be agile and still scrupulously follow our rules, policies and processes," Wray said in an interview with the Associated Press.** "As a general matter, there are a number of things in the report that in my view are unacceptable and unrepresentative of who we are as an institution. ... This is a serious report, and we take it serious."

**-- Barr said in his statement on Monday that he still has "full**



**confidence” in Wray and praised these “proposed reforms.”** “No one is more dismayed about the handling of these FISA applications than Director Wray,” Barr said at the end of the statement criticizing Horowitz’s core conclusion.



Former FBI Director James Comey speaks to reporters at the Capitol last December. (J. Scott Applewhite/AP)

**-- In an op-ed for [The Post](#) in response to the IG report, Comey demands an apology from the attorney general:** “Barr owes the institution he leads, and the American people, an acknowledgment of

the truth. Unfortunately, it appears that Barr will continue his practice of deriding the Justice Department when the facts don't agree with Trump's fiction. Pointing to his personally commissioned 'review' of the FBI's case-opening, Barr has declared it is too soon to conclude that the FBI was right to start an investigation. If his goal is simply to support the president's conspiracy theories, it will always be too soon to acknowledge the facts. As the leader of an institution that is supposed to be devoted to truth, Barr needs to stop acting like a Trump spokesperson."

**Comey, like his successor Wray, welcomed the IG's recommendations.** "Inspector-general reports are valuable because they offer the chance to learn," he writes. But he argued that it would have been "a dereliction of duty" not to investigate a tip that Trump foreign policy adviser George Papadopoulos had discussed with a foreign ambassador that Russia had "dirt" on Hillary Clinton in the form of emails.

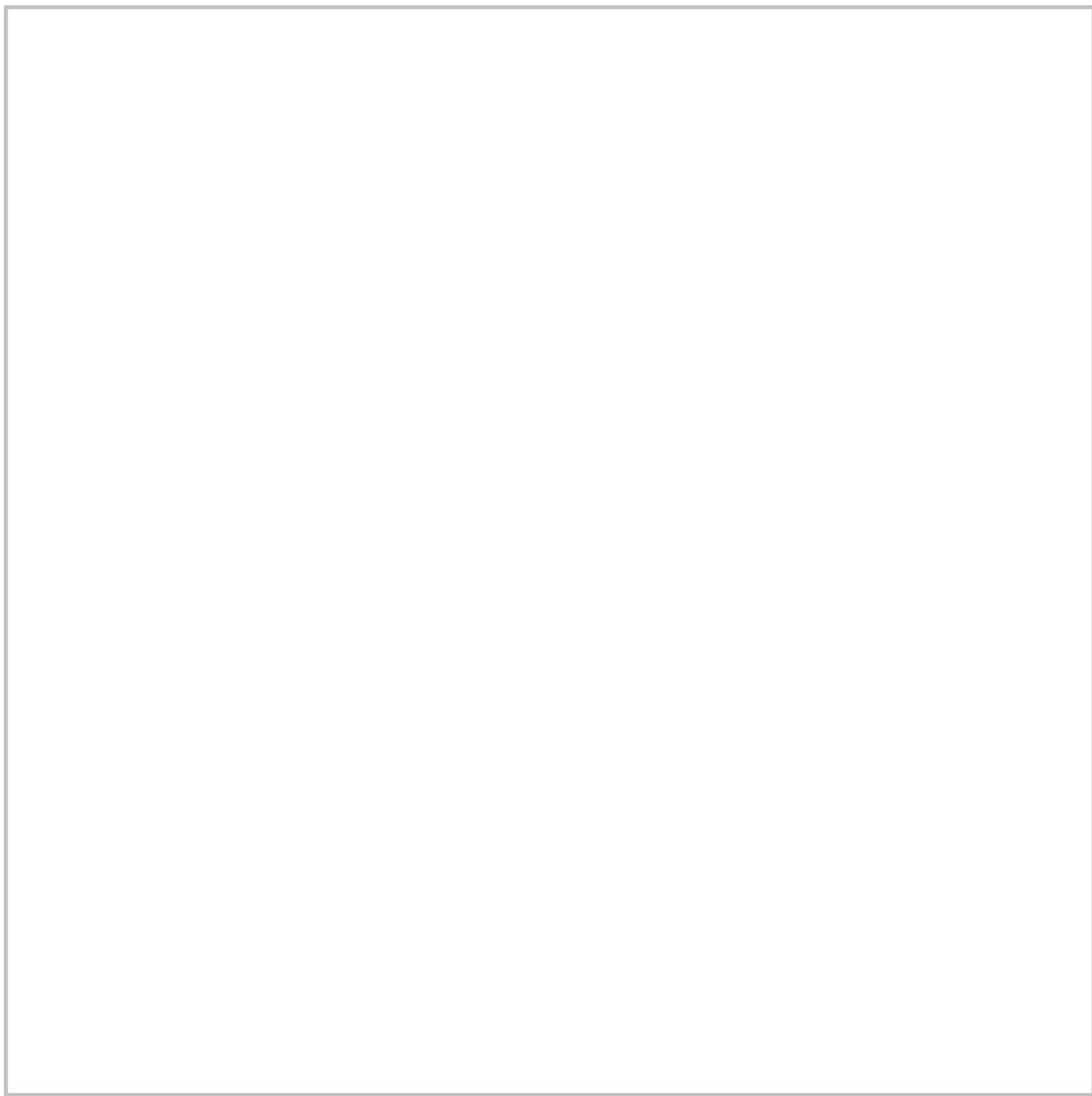
**Comey also criticized "Fox News personalities" for smearing him.** "There was no illegal wiretapping, there were no informants inserted into the campaign, there was no 'spying' on the Trump campaign," he writes. "The painful part is that millions of good people believed what they heard. My 89-year-old mother-in-law, watching Fox News in her Iowa assisted-living facility, became convinced that I was going to jail. I repeatedly assured her that there was zero percent chance of that."

**-- Chris Christie recommended Wray to Trump in 2017 when he needed someone to replace Comey.** Wray had defended the then-New Jersey governor as his personal lawyer throughout the

Bridgegate investigations. A registered Republican, Wray had previously served as the assistant attorney general in charge of the criminal division under George W. Bush.

**Here's a fun fact:** Back in 2004, when Comey was prepared to resign as the deputy attorney general over concerns about the legality of Bush's domestic surveillance program, Wray approached him in a corridor at the Justice Department. "Look, I don't know what's going on, but before you guys all pull the rip cords, please give me a heads-up so I can jump with you," Wray told Comey, according to a 2013 story in [Washingtonian magazine](#).

**-- A final thought: Don't listen to spin from pundits and politicians. Read the IG report for yourself.** The executive summary at the top is only 19 pages. It's a measured synthesis, with a summary of what each chapter concludes and Horowitz's recommendations. Horowitz will discuss his findings on Wednesday during a public hearing before a Senate committee.



Democrats and Republicans present final cases in House impeachment inquiry hearing

### **THE LATEST ON THE INVESTIGATIONS:**

**-- House Democrats unveiled two articles of impeachment against Trump this morning, saying he had abused the power of his office and obstructed Congress in its investigation of his conduct regarding Ukraine. The House Judiciary Committee plans to vote on the articles this Thursday, and the full House is expected to vote next week. This announcement means there won't**



be any article of impeachment stemming from the Mueller report, which liberals had pushed to include but moderates balked at. ([Read more on our liveblog.](#))

- “We must be clear: No one, not even the president, is above the law,” House Judiciary Committee Chairman Jerry Nadler (D-N.Y.) said at a news conference.
- “The evidence of the president’s misconduct is overwhelming and uncontested,” said House Intelligence Committee Chairman Adam Schiff (D-Calif.). “The argument, ‘why don’t you just wait?’ comes down to this: Why don’t you just let him cheat in just one more election?”

-- **"Democrats laid the groundwork for the charges Monday, lambasting Trump as a danger to the country during a contentious [nine-hour] hearing that foreshadowed a likely party-line vote on the articles,"** [Rachael Bade](#), [Mike DeBonis](#), [Elise Viebeck](#) and [Toluse Olorunnipa](#) report. "Republicans on the committee sought to vigorously defend Trump, using parliamentary maneuvers, process complaints and occasional theatrics to disrupt the hearing and accuse Democrats of abusing the impeachment process in pursuit of a political vendetta. ... The hearing did not reveal much new information about the underlying conduct at the heart of the impeachment inquiry, instead allowing committee lawyers to summarize the extensive existing evidence and present opposing sides of the case. With dueling staff counsel arguing for and against impeachment — and at one point questioning one another — the



hearing showcased how partisan the proceedings had become ahead of the release of articles for ousting Trump from office. Trump said Saturday that [Rudy] Giuliani would be making a report to [Barr] and to Congress about his findings. On Monday, Giuliani said he wanted to present the information to congressional Republicans ahead of any impeachment vote."

**-- The Senate is looking for a holiday truce on the impeachment trial.** Senators from both parties aren't likely to let an impeachment trial ruin their holiday plans. ([Politico](#))

**-- A surprising revelation from the IG report: Ivanka Trump, the president's daughter, was friends with former British spy Christopher Steele, who wrote the dossier.** [Tom Hamburger and Rosalind S. Helderman report](#): "The [report] said Steele had 'been friendly' with a Trump family member, a relationship he described as 'personal.' Steele told investigators he had visited the Trump family member at Trump Tower in New York and had once gifted the person a family tartan from Scotland. A person familiar with Steele's business Orbis confirmed that the family member was Ivanka Trump. After first meeting in 2007, they emailed over the years ... Between 2010 and 2012, Steele discussed with Ivanka Trump the possibility that the Trump Organization might hire his business to assist with projects in Russia and China. They remained friends through 2015..."

**-- Appeals court judges expressed skepticism that members of Congress as individuals have a legal right to sue Trump to stop his private businesses from accepting payments from foreign governments without lawmakers' consent.** [Ann E. Mariow and Jonathan O'Connell report](#): "Even as the judges seemed troubled that

Congress may have no other viable way to enforce the Constitution's anti-corruption emoluments provision, they did not seem prepared to allow the lawsuit from more than 200 Democratic lawmakers to move forward — and suggested the Supreme Court would have the final word. Judges Thomas B. Griffith and David S. Tatel of the U.S. Court of Appeals for the D.C. Circuit expressed doubt that past Supreme Court decisions permit individual lawmakers to bring lawsuits on behalf of the entire body, and they noted that Congress acts through majority votes in the House and Senate.”

**-- Lawyers for former Trump deputy campaign chairman Rick Gates, who pleaded guilty to fraud and lying to prosecutors, asked a judge to spare him from prison because he cooperated with prosecutors investigating Russia's efforts to sway the 2016 election. [From the Times](#):** “In their sentencing memo, Mr. Gates's lawyers portrayed their client as the consummate cooperating witness. ... It said that **Mr. Gates had spent more than 500 hours in interviews with state and federal prosecutors** and had provided additional information to Congress in response to subpoenas and requests for interviews. ... Experts have said that under sentencing guidelines, Mr. Gates could receive a prison term of four years and nine months to six years for his crimes. But the judge overseeing his case is not required to follow those recommendations.”

**-- The New York attorney general issued a new subpoena to the National Rifle Association, deepening her investigation into whether the pro-Trump organization has illegally diverted money from its charitable foundation. [From the Times](#):** “Because the N.R.A. is chartered in New York and the office of the attorney general,



Letitia James, has a range of enforcement options, the investigation has alarmed N.R.A. officials already grappling with infighting and litigation. ... Among the documents sought by the subpoena are records related to transfers among N.R.A.-controlled entities, including the N.R.A. Foundation, an affiliated charity. Recent tax filings show that the N.R.A. diverted \$36 million last year from the foundation in various ways, far more than ever before, raising concerns among tax experts.”

**-- Attorney Michael Avenatti -- best known for representing adult-film star Stormy Daniels in her lawsuit against Trump -- wants his expensive lifestyle and money troubles off limits at his New York trial on federal charges of attempted extortion and wire fraud. [Shayna Jacobs reports](#):** “Avenatti’s expensive habits do not belong at his trial because motive is not necessary to the government’s case and ‘his general financial condition and spending habits have no bearing on his motivations under the circumstances of this case,’ his lawyers Scott Srebnick and Jose Quinon argued in the filing. ... Prosecutors say his troubles were a driving factor when he allegedly contacted Nike, a publicly traded sports apparel company, threatening to expose employee wrongdoing he claimed to have knowledge of, if Nike did not meet his demands for a \$1.5 million payout to his client Gary Franklin, a youth basketball coach, and \$15 million to \$20 million for a retainer agreement for him to purportedly investigate the wrongdoing.”



Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



Warren earned nearly \$2 million from legal work, records show

## **2020 WATCH:**

-- **“Memo from 1990s pollution case shows Elizabeth Warren in action as corporate consultant,”** [by Annie Linskey and Matt Viser](#):  
“[The memo from then-Professor Elizabeth Warren](#) was written on Harvard Law School letterhead ... Warren was not arguing on behalf of vulnerable families, nor was she offering the sort of stinging rebuke of corporate greed that would later define her political career. Rather, Warren was representing a large development company that was



trying to avoid having to clean up a toxic waste site. The [eight-page] memo, which Warren wrote in 1996, used legalistic and often dense language to argue that businesses faced the ‘risk of the unknown’ from a growing threat of lawsuits, and that defended the company’s right to ‘maximize its returns to its unpaid creditors and to survive as an employer.’

“Warren’s compensation in the 1996 case was included in a summary released by her campaign late Sunday night showing that **she had been paid about \$2 million as a legal consultant during her time as a professor, most of it between 1995 and 2009.** But Warren, who has released 11 years of tax returns, has not disclosed her tax records from most of that time period. And her campaign has provided few details about her private legal business beyond short descriptions ... **Among the corporations that hired Warren was Dow Chemical, which spent years trying to ward off liability after a subsidiary company’s silicone breast implants began to rupture.** She also worked for LTV Steel, a firm that battled with the labor movement as it tried to avoid paying millions of dollars for retired coal miners’ health care.

“The 1996 case, in which she represented a real estate development company called CMC Heartland fighting in court to avoid having to pay to clean up a polluted old rail yard along the Puget Sound in Washington state, stands out ... Warren was paid about \$21,000 for the work, according to the data released Sunday by her campaign. ... **The Supreme Court declined to take the case,** letting stand lower court rulings against Heartland and requiring it to finance the cleanup. Warren’s argument put her in line with other major corporations ...

**CMC Heartland Partners' counsel of record for the case was Kenneth W. Starr**, who at the time also served as the independent counsel examining allegations against President Bill Clinton.”

**-- Pete Buttigieg, bowing to days of attacks from Warren, announced that he will open his fundraisers to journalists and disclose the names of people raising money for his campaign. His campaign also announced that McKinsey, the consulting firm where Buttigieg used to work, will allow him to disclose the identity of his clients there.** [Amy B Wang reports](#): “Reporters will be allowed into Buttigieg’s large-dollar fundraising events starting Tuesday, and the South Bend, Ind., mayor will release a list of his ‘bundlers’ — those who funnel large sums of money to campaigns — within a week, according to Buttigieg campaign manager Mike Schmuhl. ... McKinsey said in a statement that confidentiality is important to the firm ... Any confidential, proprietary or classified information still must be kept secret, it added. The Buttigieg campaign promised a list of the client names ‘soon.’”

**-- Ronny Jackson, the former White House doctor whose nomination to lead the Department of Veteran Affairs was torpedoed last year over [allegations of professional misconduct](#), is running for Congress in Texas.** [Michael Brice-Saddler reports](#): “Jackson, a rear admiral who served in Iraq, was President Trump’s personal physician in April 2018 when he was nominated to lead the Department of Veterans Affairs. But he withdrew from consideration after Sen. Jon Tester (Mont.), the top Democrat on the Senate Committee on Veterans’ Affairs, released a two-page summary accusing Jackson of improperly dispensing medication to staff



members, drinking on the job and contributing to a hostile work environment during his tenure as White House physician. The report alleged that Jackson was known by the moniker 'Candyman' because he freely distributed medications to White House staff without paperwork, including the sleep aid Ambien. Jackson denied the allegations, and Trump later called the claims 'false accusations against a great man.' In February, Trump tapped Jackson to receive a promotion and to be his top medical adviser.

**"CNN reported this month that Jackson had retired from the Navy despite an ongoing investigation into the allegations against him led by the Defense Department's Inspector General.** Jackson, who also served as White House physician under presidents Barack Obama and George W. Bush, is one of 13 candidates vying for a seat in Texas's heavily Republican 13th District, according to the Tribune. The seat opened when Rep. Mac Thornberry, the top Republican on the House Armed Services Committee, announced in September that he plans to retire."

**-- Former representative Scott Taylor (R-Va.) will drop his challenge to Sen. Mark Warner (D) and run for his old seat in Congress.** The Post [revealed on Sunday](#) that Giuliani was trying to get Trump to nominate him for ambassador to Qatar last year. ([The Hill](#))

**-- A GOP House candidate whose failed bids against Rep. Maxine Waters (D-Calif.) have made him a cause celebre on the right was arrested on three felony charges.** [From the Daily Beast:](#)

"Businessman Omar Navarro ... faces significant legal troubles related to alleged stalking of his ex-girlfriend. San Francisco police

arrested Navarro on Saturday night, after he was allegedly seen near ex-girlfriend DeAnna Lorraine Tesoriero's apartment. Tesoriero, a self-styled MAGA relationship expert who is running a quixotic congressional run of her own against Speaker Nancy Pelosi (D-CA), told The Daily Beast that she saw Navarro skulking outside her home late at night. Tesoriero said she then received a text from an unknown number with the message, '[B----], I came to see you.' 'Clearly, he has a lot of screws loose,' Tesoriero told The Daily Beast. 'I think a lot of this power has gotten into his head. He has a lot of money now from campaign donations.'"



The Supreme Court is seen under stormy skies in Washington. (J. Scott Applewhite/AP)

## **DOMESTIC DEVELOPMENTS THAT SHOULD NOT BE OVERLOOKED:**

**-- The Supreme Court said it will not review a Kentucky law requiring doctors who perform abortions to give a detailed description of the fetus's development while the woman is shown an ultrasound image, even if she objects.** [Robert Barnes reports](#): "Without comment or noted dissent from any of its liberal members, the court said it was not taking up a challenge to the law filed by doctors at Kentucky's only abortion clinic. The doctors contended the state's requirements compelled their speech and violated their First Amendment rights. The Supreme Court already has one high-profile abortion case on its docket this term. Next month, it will consider a Louisiana law that requires physicians to have admitting privileges at a nearby hospital. It is almost identical to a Texas law the court struck down in 2016 as medically unnecessary and meant to limit a woman's access to the procedure. ... The law forcing the physician's words was a 'compelled-speech mandate wholly unrelated to traditional informed consent and therefore presumptively unconstitutional,' the clinic and its doctors argued. ... Without the requirement, there is no reason to believe that abortion providers 'do anything to dispel the mistaken beliefs of women who ... are under the impression that their fetuses are simply masses of inanimate tissue rather than living beings that are assuming the human form,' Kentucky wrote in its brief."

**-- The White House may appoint a former chemical industry**



## **executive as the next head of the Consumer Product Safety**

**Commission.** [Todd C. Frankel and Juliet Eilperin report](#): “Nancy Beck would take over as chairwoman of the Consumer Product Safety Commission, a small but powerful agency that is responsible for the safety of 15,000 everyday products, from cribs and bicycles to refrigerators and trampolines. Beck is in the late stages of being vetted by the White House for the CPSC position, according to the government officials, who spoke on the condition of anonymity to discuss private deliberations. Trump still needs to formally nominate her for the commission’s top job, which requires Senate confirmation. Beck’s selection was expected to be announced in coming weeks, the officials said. Beck joined the Trump administration in May 2017, when she was tapped to be a top deputy in the EPA’s toxic chemical unit. She previously had been an executive with the chemical industry’s main trade organization, the American Chemistry Council. At the EPA, Beck has helped scaled back several policies aimed at curbing federal limits on toxic chemicals.”

## **-- Key congressional lawmakers announced their support for a defense bill establishing both the Space Force and paid parental leave for more than 2 million federal workers, as signs of Republican opposition to the measure appeared to fade.** [Jeff Stein reports](#):

“House and Senate negotiators in both parties said they would back the bill granting \$658 billion to the Department of Defense and other defense programs, a measure that includes dozens of national security provisions prioritized by the armed services. However, the measure faced at least some new opposition from liberals in Congress who quickly announced that they would vote against it because of its provisions related to U.S. support for Saudi-

led efforts in Yemen ... In a major deal struck late last week, the White House and congressional Democrats agreed to create the Space Force as the sixth branch of the U.S. military in exchange for new parental-leave benefits for the federal workforce as part of the must-pass defense package.

**“If approved, it would be the biggest victory for federal employees in nearly 30 years.** ... The biggest remaining hurdle to the compromise appears to be Senate Republicans, who earlier this year rejected a measure to establish similar benefits for federal workers. But as of Monday afternoon, at least before the bill text was released, most in the Senate GOP caucus appeared prepared to approve the plan. Sen. Ron Johnson (R-Wis.), chairman of the committee that oversees government affairs, said he opposed the expansion of the federal benefit but does not expect to be able to stop it. ... Several other Republican senators said they were prepared to support the deal, including Sens. John Barrasso (Wyo.), Mitt Romney (Utah) and Roy Blunt (Mo.).”

**-- Good news for Washington: The Nationals and Stephen Strasburg, the reigning World Series MVP and pitcher who kick-started the team's slow rise to relevance a decade ago, agreed to a seven-year, \$245 million deal.** The record-breaking contract is the largest ever for a pitcher in both total and average annual value.  
([Jesse Dougherty](#))

**-- The North Dakota county poised to become the first in America to bar refugees under a new Trump executive order rejected the motion.** [Antonia Noori Farzan reports](#): “For four hours, sixth-generation North Dakotans and recent arrivals from Cameroon and



Congo took turns delivering impassioned testimony in what was often a contentious debate. Ultimately, the commission voted 3-2 to keep welcoming refugees. The decision largely carried symbolic resonance. The Trump administration has slashed the number of refugee arrivals nationwide, and Burleigh County, which has roughly 95,000 residents, took in just 24 refugees during fiscal year 2019, according to the North Dakota governor's office. The community — home to Bismarck, the state's capital — is slated to receive a similar number of refugees in fiscal year 2020, and the measure that passed on Monday caps the number of new arrivals at 25."

**-- Border arrests fell in November for the sixth consecutive month, new data from U.S. Customs and Border Protection shows.** [Nick Miroff reports](#): "The number of people U.S. authorities took into custody fell nearly 6 percent from October to November, to 42,649, the latest figures show. Arrests have dropped 70 percent since May, when U.S. authorities detained 144,116 amid a record influx of Central American families. Mark Morgan, the acting CBP commissioner, called the change 'staggering, in a very positive way.'"

**-- CBP denied access to a group of doctors trying to vaccinate migrant children against the flu.** [From the San Diego Union-Tribune](#): "About 40 people, including medical doctors licensed to practice medicine in California, marched Monday from Vista Terrace Neighborhood Park to the detention facility on Beyer Boulevard, calling for CBP to let them in or let the children out to participate in a free mobile clinic they set up outside. They were joined by at least another dozen medical students and supporters. ... Holding signs saying 'No more flu deaths' and 'Children don't belong in cages,' the

doctors chanted and sang. Some of them spoke about their own personal journey to the United States as undocumented migrant children. ... Though the agency did not respond directly to the doctors' demonstration, a CBP spokeswoman replied to a media inquiry ... 'It has never been a CBP practice to administer vaccines and this not a new policy,' the official statement read in part. .... 'As a law enforcement agency, and due to the short-term nature of CBP holding and other logistical challenges, operating a vaccine program is not feasible.'"

**-- A Florida official told her deputy to act like a "white supremacist" when stopping a black murder suspect. [Hannah Knowles reports](#):** "'We want it to look like you're the grumpy old man,' a woman, whom the Monroe County Sheriff's Office confirmed to be Capt. Penny Phelps, says in a recording now made public. 'You have nothing better to do than, you're the white supremacist, you're messing with the black guy who's riding his bike.' The sheriff's office, located in the Florida Keys, quickly took Phelps off the murder case last month and opened an internal investigation after receiving multiple allegations of misconduct, spokesman Adam Linhardt said. Last week, it also removed Phelps as commander of the major crimes and narcotics units, according to documents shared by the agency.'"



Ukrainian President Volodymyr Zelensky, left, German Chancellor Angela Merkel, French President Emmanuel Macron and Russian President Vladimir Putin hold a news conference after a summit on Ukraine at the Elysee Palace in Paris. (Ludovic Marin/Pool/AFP/Getty Images)

## **THE NEW WORLD ORDER:**

**-- Russia's Vladimir Putin and Ukraine's Volodymyr Zelensky agreed to a renewed cease-fire and to exchange all known prisoners when they met for the first time in Paris. [James McAuley](#), [Robyn Dixon](#) and [Michael Birnbaum](#) report:** "The talks yielded enough progress to get the peace process moving, but as



expected, there was no major breakthrough. 'We haven't found the magic wand, but we have relaunched talks,' said French President Emmanuel Macron, who convened the gathering. He said the talks had made 'practical, tangible progress.' **The parties agreed to meet again in four months to discuss one of the stumbling blocks: conditions for elections in eastern Ukraine**, which would then lead to special status for the regions. The Ukrainian president has declared that there can be no elections in those regions until all military formations have withdrawn. ... **This is a lonely moment for Zelensky. Once-ironclad U.S. support for Ukraine is shrinking under Trump.** German Chancellor Angela Merkel helped mediate Monday's meetings, but she is distracted by her own roiling domestic politics."

**-- Trump will meet with Russian Foreign Minister Sergey Lavrov today in the Oval Office for a conversation that could include the extension of the last major nuclear treaty between the U.S. and Russia. Lavrov will also meet with Secretary of State Mike Pompeo.** [From the Times](#): "Considerable evidence suggests any conversation with Mr. Lavrov would include the last major nuclear arms control treaty still in force between the United States and Russia: the Obama-era New START treaty, which in recent days [Putin] has said he wants to extend for another five years. In any other presidency that would seem uncontroversial. Democrats and Republicans on Capitol Hill have largely agreed that extending the accord would be good, avoiding a nuclear arms race at a time of heightened tension with Mr. Putin's government ... The result is that Mr. Trump, until recently, has dismissed the agreement as a 'one-sided deal,' and a failure by President Barack Obama. ... At the same time, Mr. Trump

has said he wants to avoid a nuclear arms race ... If Mr. Trump can pull off an extension, it would be the first diplomatic breakthrough of his presidency with Russia.”

**-- Russia called the Olympic committee’s ban “anti-Russia hysteria” that is politically motivated. [Isabelle Khurshudyan reports](#):**

“Russia’s reaction to being banned Monday from the next two Olympics in the wake of one of the biggest international sports doping scandals has been to claim it’s the world’s punching bag. ... Just as Moscow has repeatedly denied interfering in the 2016 U.S. presidential election, claiming allegations were part of an anti-Russian narrative, the official reaction since the sports scandal first surfaced in 2015 has been to complain that this too was political. ‘It’s obvious in this case that there are still significant doping problems on the Russian side — I mean our sports community. This can’t be denied,’ Russian Prime Minister Dmitry Medvedev said at a conference Monday with deputy prime ministers in Moscow.”

**-- The behavior of the trainee who killed three classmates at a Florida Navy base changed after a trip to his native Saudi Arabia, friends said. [Souad Mekhennet, T.S. Strickland and Joby Warrick report](#):**

“Ahmed Mohammed al-Shamrani was described as ‘strange’ and ‘angry’ in the weeks leading up to Friday’s shooting rampage, but schoolmates and other acquaintances said he showed no outward sign that he was preparing to open fire inside a classroom building where he had been training to become a military aviator. The shooting, which also left eight people injured, is being treated by the FBI as a possible terrorist attack.”

**-- The White House blocked a U.N. meeting on North Korean**



**atrocities in an attempt to salvage the faltering diplomatic effort to convince Kim Jong Un to abandon his nuclear weapons program.** [From Foreign Policy](#): “Once again, the U.S. has prevented the U.N. Security Council from scrutinizing North Korea’s abysmal human rights record, apparently because of President Trump’s special relationship with Kim Jong Un,” said Louis Charbonneau, the U.N. director for Human Rights Watch. ‘By blocking this meeting, which was set to go ahead on Human Rights Day..., the Trump administration is sending a message to Kim that the U.S. no longer considers arbitrary detention, starvation, torture, summary executions, sexual violence and other crimes against the North Korean people a priority,’ Charbonneau added. ‘North Korea and many other abusive governments can now rest assured that they have little to fear from the Trump administration when it comes to human rights.’ In response to a request for comment, a State Department spokesman said that the U.S. still plans to press for a council meeting on North Korea this week, but did not say human rights would be discussed.”

**-- Trump and Pelosi are ready to pass a new NAFTA.** [From Politico](#): “The deal remains unofficial until Tuesday, when the top trade officials from the U.S., Mexico and Canada are expected to meet in Mexico City for an afternoon ceremony. Pelosi is also holding off on making a public announcement until she has briefed her caucus on the policy details of the pact, which replaces the 25-year-old North American Free Trade Agreement. ... AFL-CIO President Richard Trumka, whose support is crucial to getting Democrats’ approval, briefed his executive council Monday afternoon on changes to the pact and is now willing to let the agreement move forward ... The new trade deal keeps tariff-free trade among the three countries.”

**-- Poll numbers in the U.K. show Tories maintaining the lead over the Labour Party as the campaign enters its final days.** ([The Guardian](#))

**-- Jonathan Ashworth, the U.K.'s shadow health secretary, dismissed as “banter” a leaked tape showing him saying Labour, his party, will lose the election.** In the recording, Ashworth also says Jeremy Corbyn is a serious problem for the party. ([The Guardian](#))

**-- After two elections in less than a year, Israeli leaders have less than 48 hours to stop a third.** [Ruth Eglash reports](#): “There had been a flurry of attempts to find a solution or form a new government over the past week, but as the clock ticked toward the final deadline, the only thing the sides appeared to agree upon was a date for the next election: March 2, 2020. After two rounds of voting, in April and September, and two 28-day stretches where Prime Minister Benjamin Netanyahu and his political rival, former military chief Benny Gantz, attempted and failed to cobble together a coalition, Israel’s parliament, the Knesset, was given a final 21 days to find someone who might be able to solve the stalemate. If none among the Knesset’s 120 lawmakers comes forward with backing from 61 fellow parliamentarians by midnight on Wednesday, the next election cycle will automatically be underway.”

**-- Ethiopia’s Abiy Ahmed won’t answer any questions when he receives his Nobel Prize, highlighting the Nobel Committee’s awareness that his victory would generate controversy.** [Max Bearak reports](#): “Abiy is refusing to engage with the international media when he receives the prize Tuesday in Oslo — refusing even to



field questions from the young students who traditionally are offered that opportunity at an event hosted by Save the Children — and the Nobel Committee is scrambling to get him to change his mind and spare it a major embarrassment. ... Although Abiy has soaked up public adoration during morale-raising events such as rallies and tree-planting drives, he has often stayed silent for weeks after incidences of ethnic tension, which have been frequent and often bloody over the past two years.”

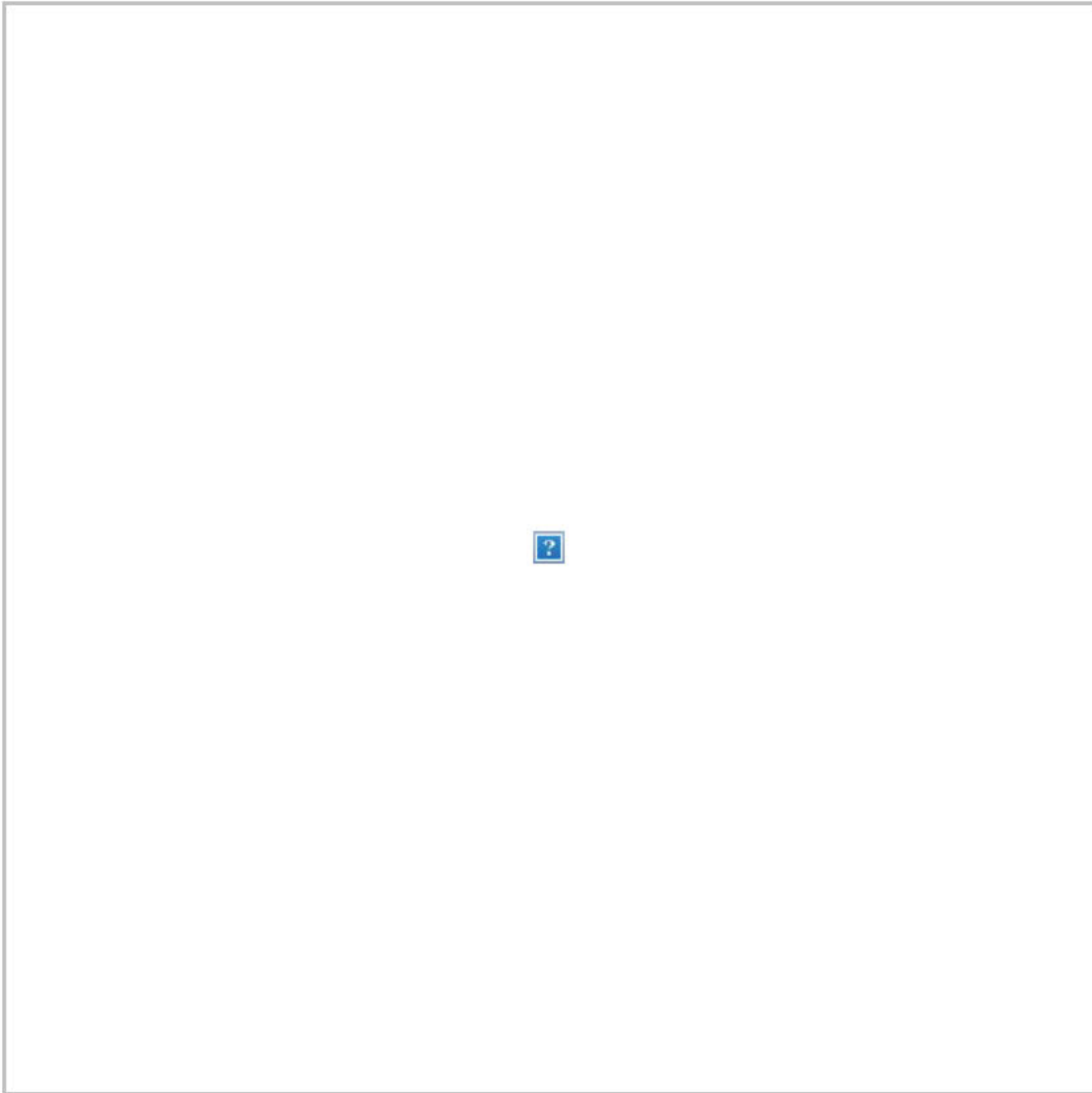
**-- A Chilean Air Force plane carrying 38 went missing on its way to Antarctica. Authorities believe it crashed.** [From CNN](#): “Its last known position was about 390 nautical miles from Punta Arenas and 280 nautical miles from the Antarctic base ... There were 17 crew members and 21 other passengers on board, who were on their way to perform ‘logistical support tasks’ such as repairing the floating oil pipeline that provides fuel for the base, said the Air Force. In addition to crew members, the plane was also carrying personnel from the armed forces, an engineering firm, and the University of Magallanes.”

**-- At least six people were shot dead in a Czech Republic hospital last night before the gunman escaped and then shot himself.** [Loveday Morris reports](#): “Police hunted for the 42-year-old suspect for several hours before they tracked him to his vehicle, where he shot himself in the head as the police helicopter hovered overhead, according to regional police head Tomas Kuzel. He added that the gunman was using an illegal 9mm handgun.”

**SOCIAL MEDIA SPEED READ:**



These were this year's most popular politicians on Twitter:



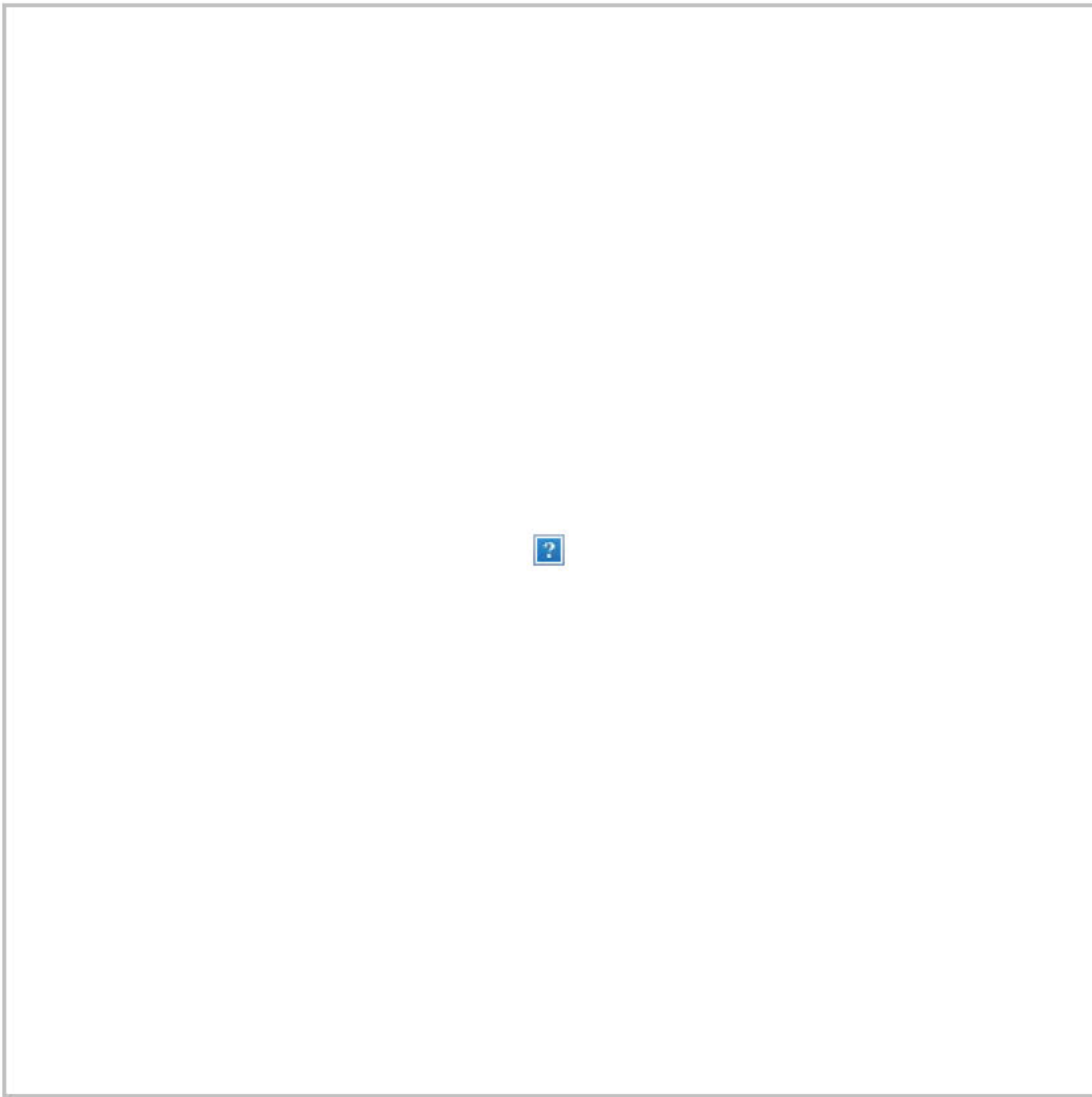
A CNN host noted that, for many, yesterday's big news didn't come from the Inspector General's report or from the impeachment hearing:



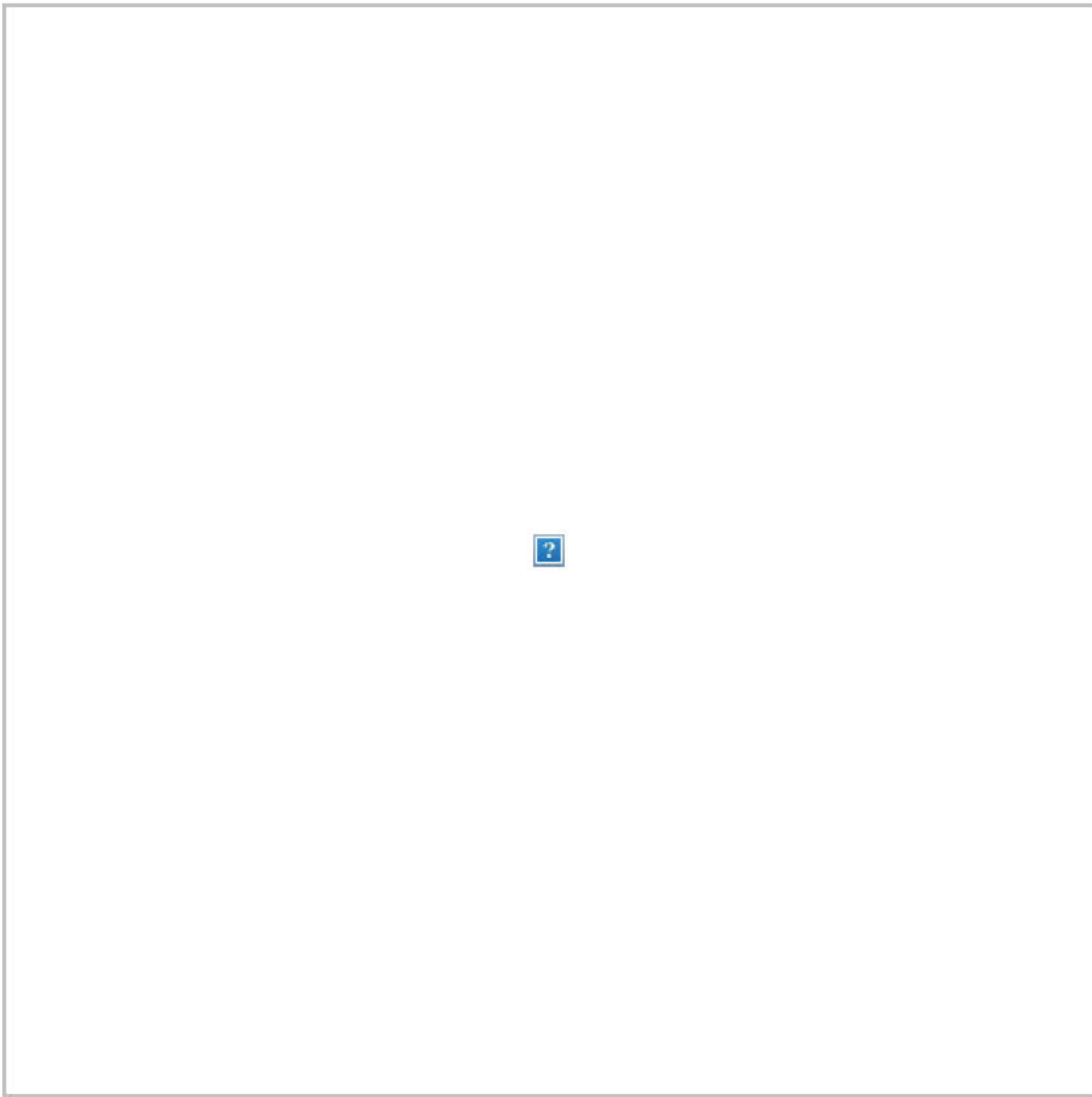
Jim Comey said he agreed to go on Fox News this morning, but the network canceled. Fox responded that his appearance was never confirmed:



Comey's agent, Keith Urbahn of Javelin, replied to a conservative commentator who took Fox's denial at face value:

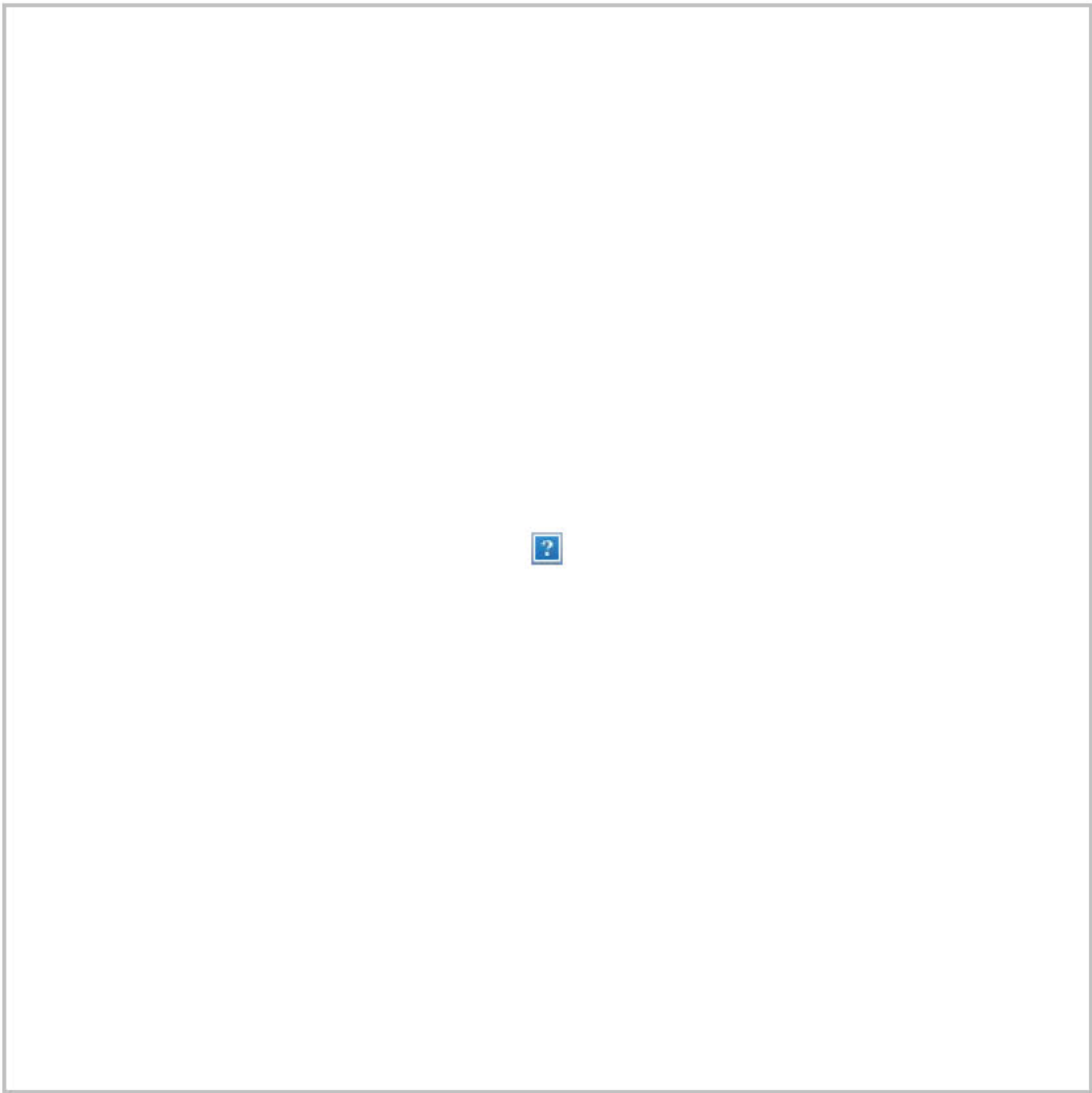


A former director of the Office of Government Ethics highlighted the IG's disclosure that FBI agents were also exchanging pro-Trump messages:

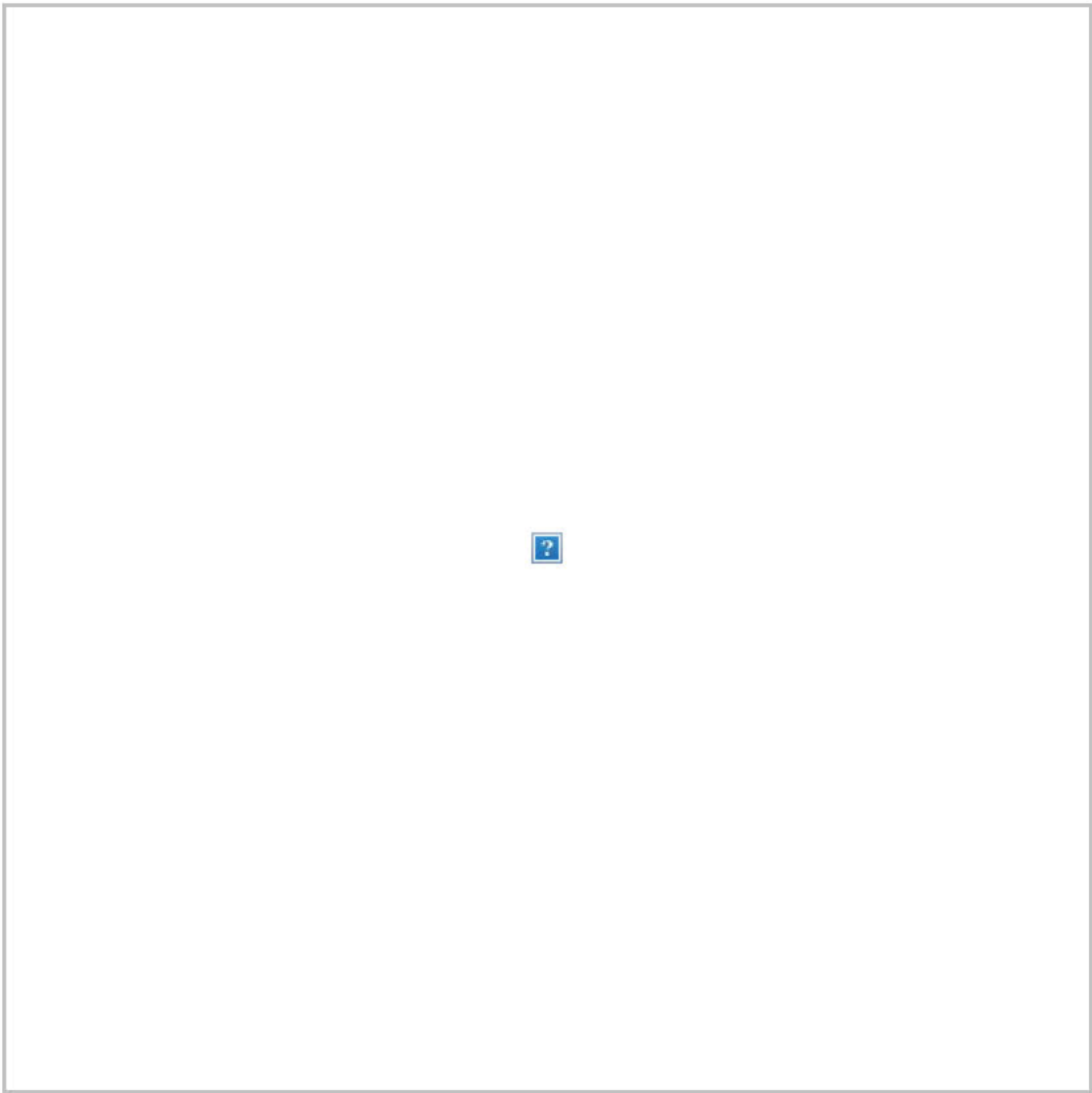


The former FBI lawyer, whose texts were publicized by Trump appointees at the DOJ and who has been a frequent target of the president, claimed vindication from the IG report:

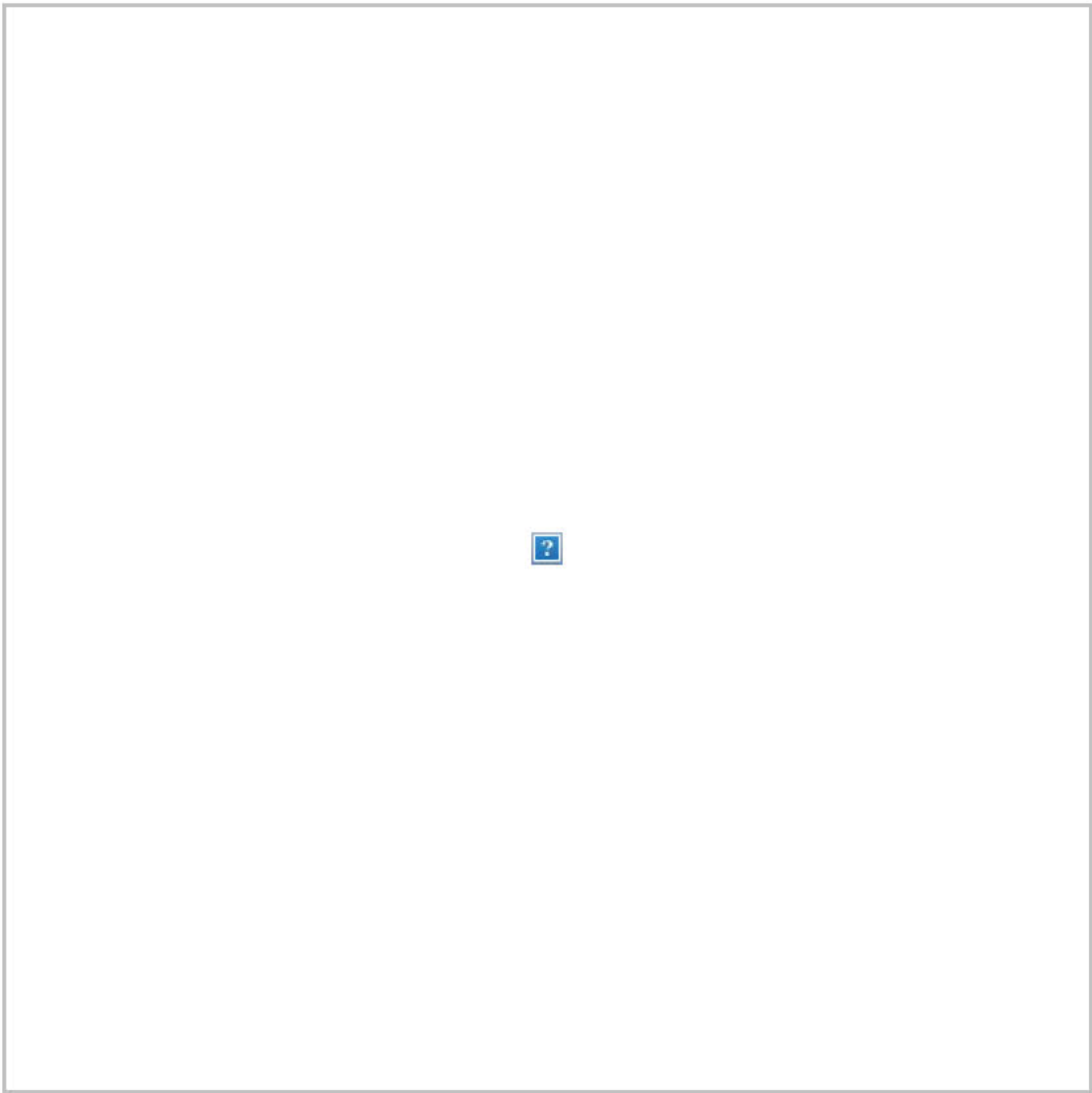




Imagine what's going on in this young man's head:

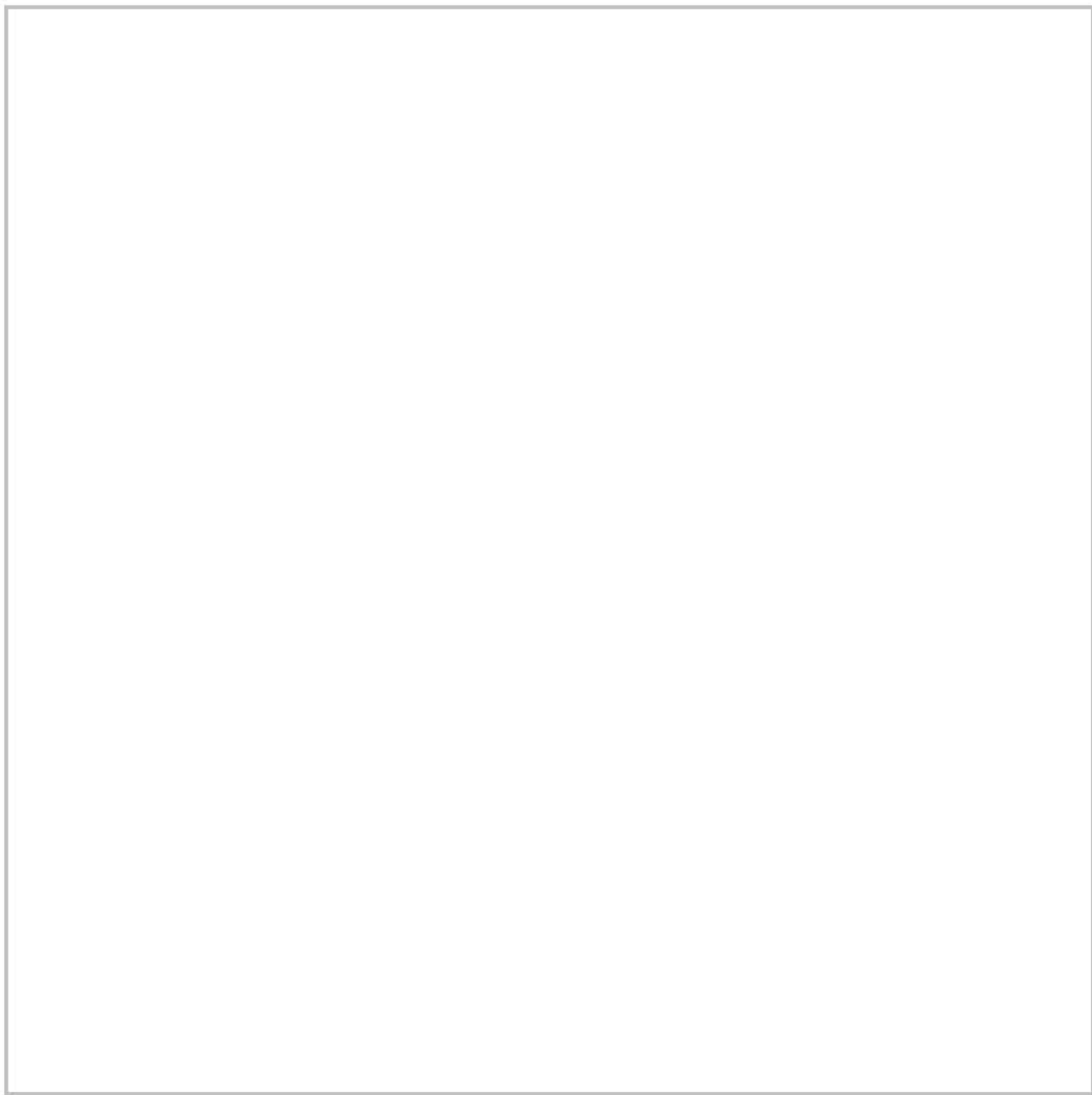


A University of Texas law professor asked Americans to read the IG report after a top Republican shared a misleading tweet about it:



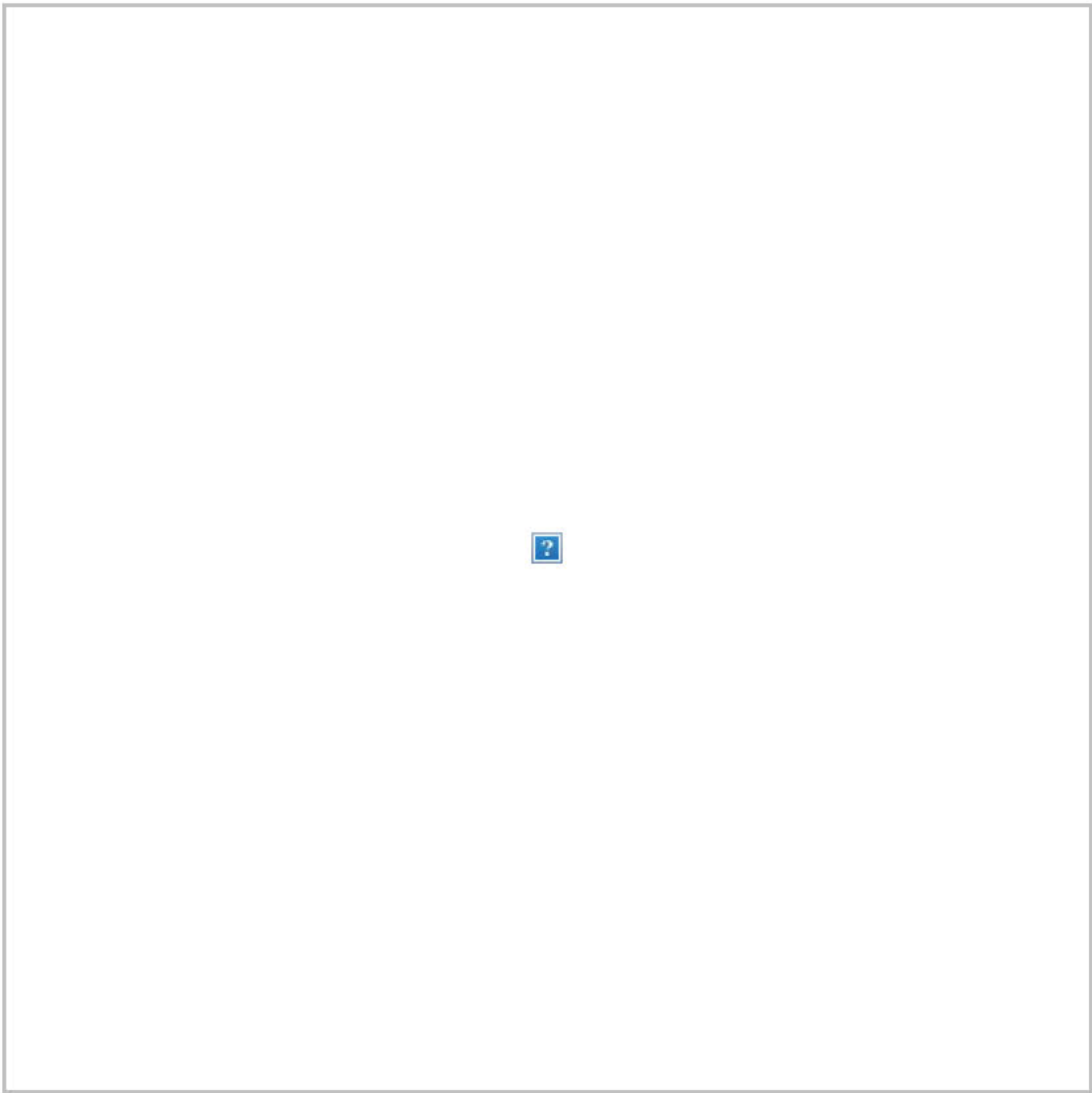
Can't say the latest impeachment hearing was boring, not with these posters:





Rep. Tulsi Gabbard (D-Hawaii) announced she won't participate in a debate that she has not qualified for:

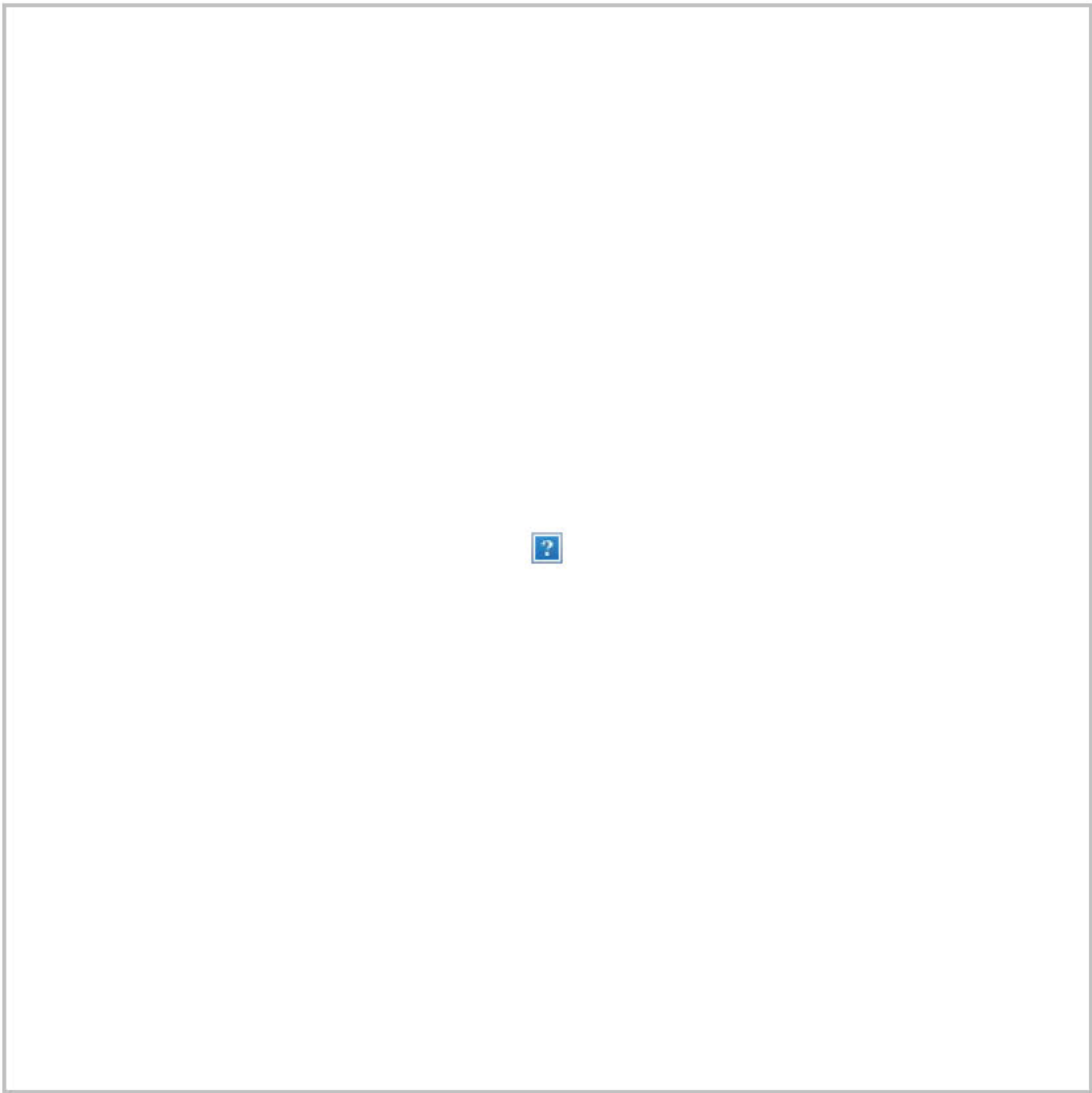




Elizabeth Warren's new campaign spokesman might have to update his Twitter bio:



Pete Buttigieg's term as mayor is ending:



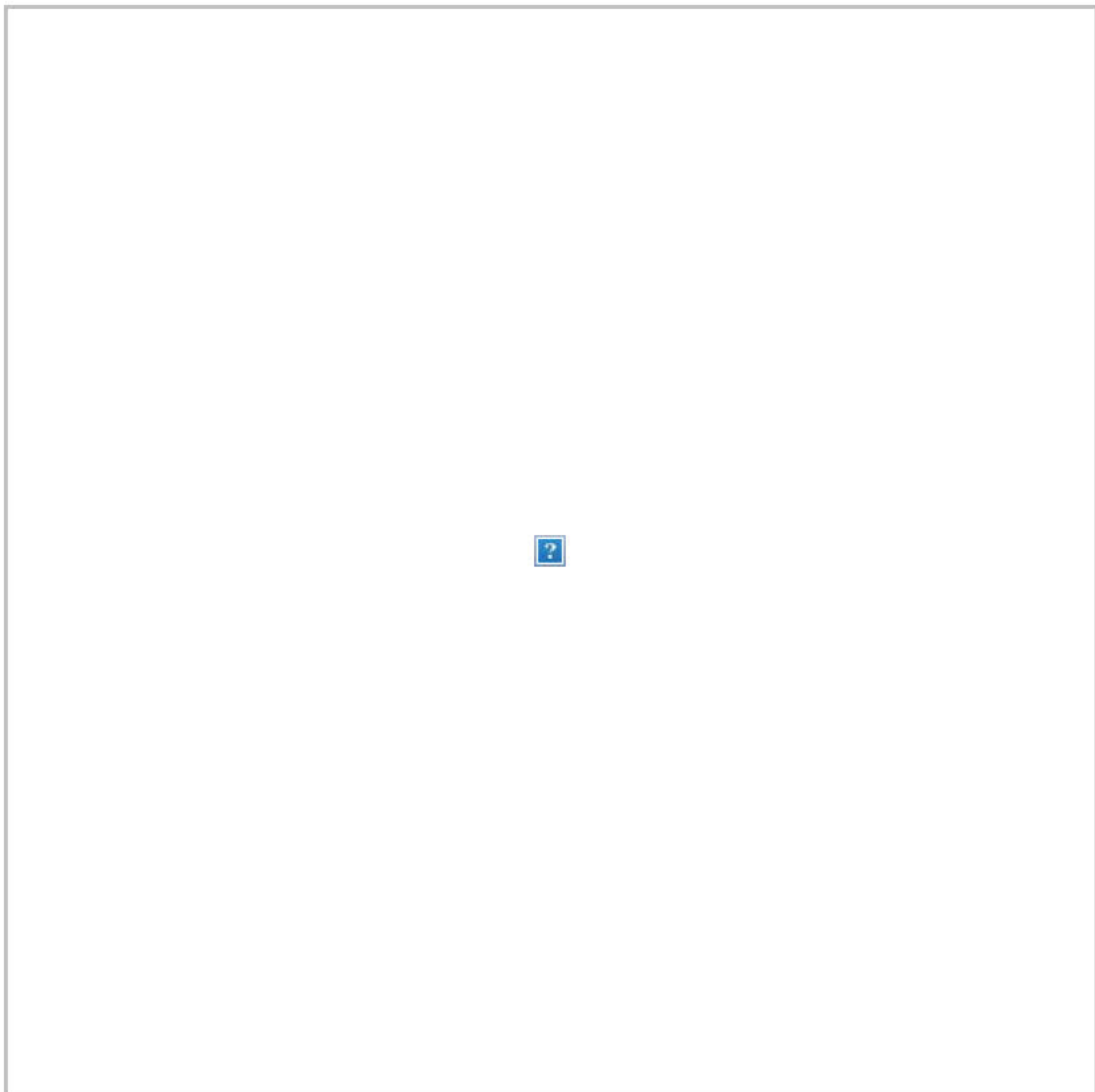
And Monica Lewinsky had some life advice to share:



**QUOTE OF THE DAY:** "The most traumatic experiences of our lives didn't have to happen, our friends didn't have to die on the other side of the planet," said Marine Corps veteran Dustin Kelly, who said The Post's report on the U.S. government's distortion over the prosecution of the Afghanistan War reignites the agony of not knowing precisely what comrades gave their lives for. (Alex Horton)

## VIDEOS OF THE DAY:

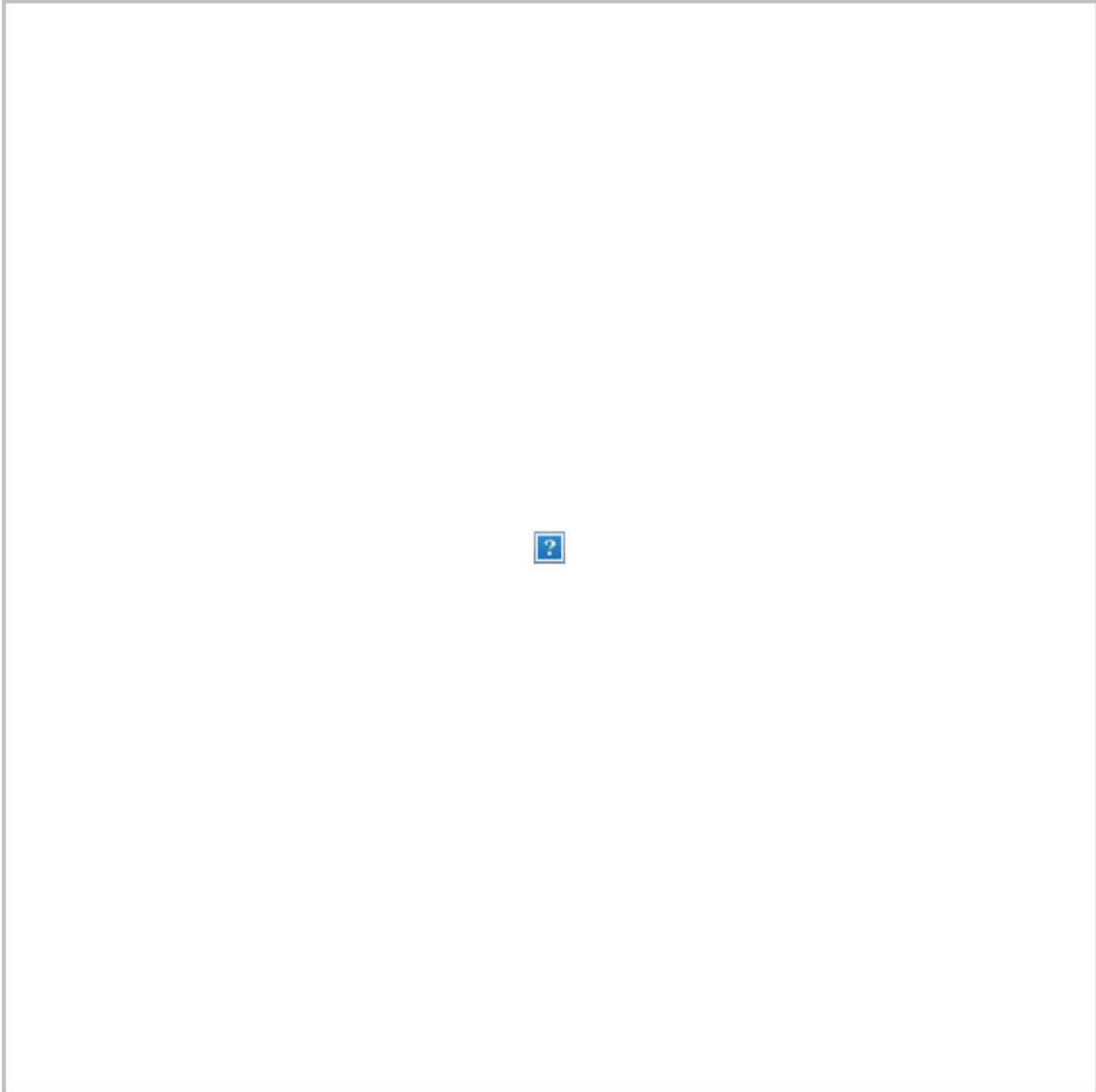
Houston Police Chief Art Acevedo lashed out at three top Republican lawmakers, including two from his state, for not reauthorizing the Violence Against Women Act. One of his officers, Sgt. Chris Brewster, was fatally shot this weekend after responding to reports of a domestic disturbance:



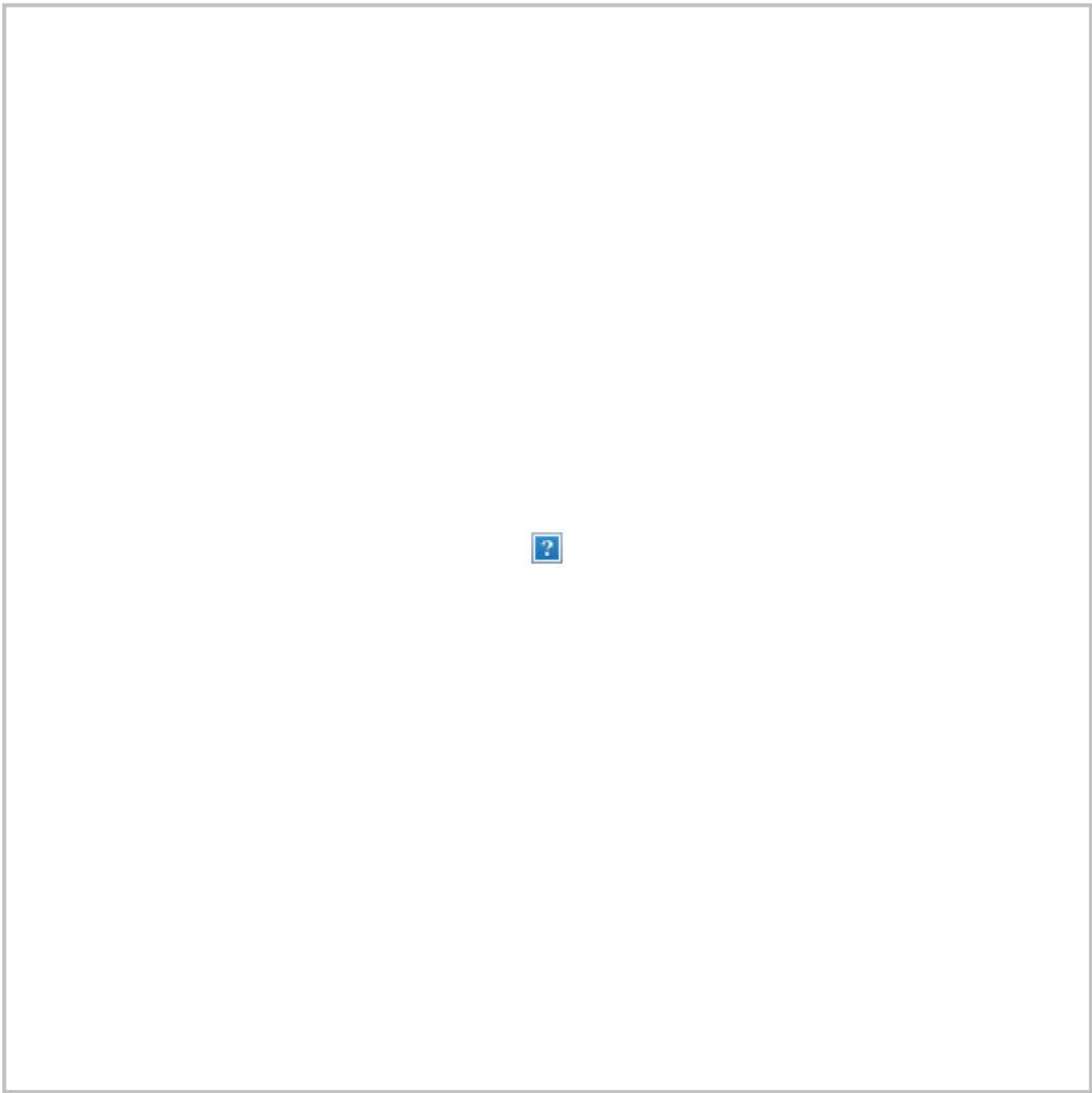


'Whose side are you on?': Houston police chief blasts NRA, senators over inaction on gun legislation

British Prime Minister Boris Johnson remade a famous scene from “Love Actually” to create a viral ad for his reelection:



John Weigel, the veteran who told Bernie Sanders at a rally earlier this year that he was considering suicide because he could not afford his medical bills, told the candidate on Monday that he's received help and tried to offer Sanders his flight jacket:



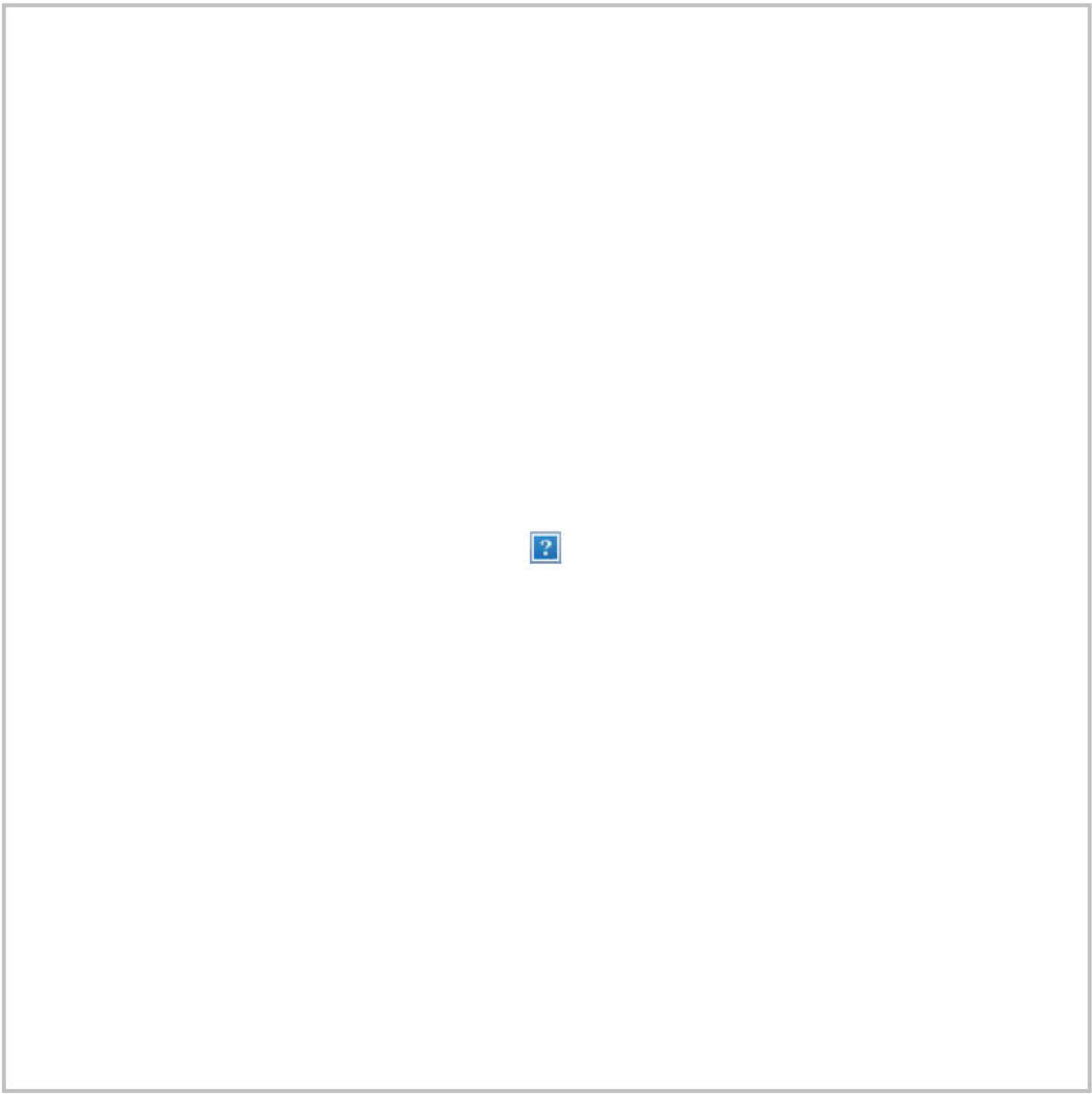
GOP counsel Steve Castor walked into Monday's House Judiciary Committee hearing not with a briefcase but a reusable grocery bag:



Seth Meyers really, really wants Rudy Giuliani to testify before Congress:



Stephen Colbert thinks Trump's understanding of the Inspector General report is further proof he lives in an alternate reality:



You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)

---

©2019 The Washington Post | 1301 K St NW, Washington DC 20071





**From:** [Association of Deputy District Attorneys](#)  
**To:** [fggurina@sunnyvale.ca.gov](mailto:fggurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for December 9, 2019  
**Date:** Monday, December 09, 2019 5:03:24 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)



### **Police officers breached due process by intensifying peril**

A police officer who took a woman's statement in confidence as to physical and sexual abuse by her boyfriend in a hotel and then repeated the substance in the presence of the abuser - prompting the woman to recant her accusations and resulting in the physical abuse of her that night - violated the woman's right to due process, the Ninth U.S. Circuit Court of Appeals held yesterday.

[Metropolitan News-Enterprise](#)

### **Four Ninth Circuit judges say colleagues are skirting the law**

Four judges of the Ninth U.S. Circuit Court of Appeals have chastised their colleagues, accusing them of ignoring U.S. Supreme Court precedent on qualified immunity of police officers in excessive-force cases. The reproach came in a dissent by Judge Carlos T. Bea to an order denying en banc review in a case decided June 20 in a memorandum opinion. That opinion reversed a grant of immunity by District Court Judge John F. Walter of the Central District of California.

[Metropolitan News-Enterprise](#)

### **Supreme Court confronts homeless crisis and whether there's a right to sleep on the sidewalk**

Four judges of the Ninth U.S. Circuit Court of Appeals have chastised their colleagues, accusing them of ignoring U.S. Supreme Court precedent on qualified immunity of police officers in excessive-force cases. The reproach came in a dissent by Judge Carlos T. Bea to an order denying en banc review in a case decided June 20 in a memorandum opinion.

[Los Angeles Times](#)

### **Oxnard man's 1988 murder convictions thrown out, ordered released under new law**

A judge on Tuesday vacated an Oxnard man's two murder convictions under a new law restricting accomplice liability and ordered his release from custody. David Cerda Jr., now 51, became the first Ventura County prisoner ordered released under the law known as state Senate Bill 1437, said Ventura County Public Defender Todd Howeth. It took effect Jan. 1.

[Ventura County Star](#)

### **Federal-state split over cameras in courtrooms**

California's Supreme Court has been televising its hearings for years, hoping to make the sometimes-obscure legal process more accessible to the public. So have the high courts of Canada, Great Britain and Brazil, and the largest U.S. appeals court, the Ninth Circuit in San Francisco.

"The public tuning in and learning about the workings of the court, I think that's essential," former California Chief Justice Ronald George said in a recent interview.

[San Francisco Chronicle](#)

## **Ventura County judge rescinds order to send rapist to Joshua Tree**

After strong opposition from San Bernardino County law enforcement and Morongo Basin residents, a Ventura County superior court judge decided on Nov. 8 not to relocate a convicted rapist and child molester to Joshua Tree. The decision prolongs the nearly yearlong process to find a home for Ross Leo Wollschlager, 56, who had been convicted in the 1980s of raping two women and sexually assaulting a 10-year-old girl while she slept in her home in Ventura County.

[San Bernardino District Attorney's Office](#)

## **San Jose, other charter cities can't flout state housing law, appellate court finds**

San Jose and 120 other charter cities must follow a state law that reserves surplus public land for affordable housing, a California appellate court has found - a ruling that could have broad implications in the ongoing battle between legislators pushing statewide housing fixes and city officials fighting to retain local control.

[Lake County Record-Bee](#)

## **Justice Dept. asks Supreme Court to let federal executions proceed after appeals court denial**

The Trump administration on Monday asked the U.S. Supreme Court to let it resume federal executions next week by "setting aside" a district court's injunction blocking it from carrying out lethal injections as planned. This request, which came hours after an appeals court blocked a similar application, marked an escalation of the administration's push to restart federal executions after a nearly two-decade hiatus.

[Washington Post](#)

## **'Judge Mike Cummins' is unfit for service on Los Angeles Superior Court**

What would the natural assumption be as to the occupation of someone known as "Judge Mike Cummins"? Unless someone followed last year's race for district attorney in San Luis Obispo County and knows that Cummins - who sat 12 years earlier on the bench in Stanislaus County and recently changed his first name to "Judge" - or has seen coverage here on his current bid for the Los Angeles Superior Court under his altered name, the impression would be that Cummins is a "judge."

[Metropolitan News-Enterprise](#)

## **Appellate court gives Fairfield convict big sentencing win**

A law that goes into effect in January will significantly reduce the time a convicted Fairfield man will be in prison after a state appellate court ruled that his felony convictions must be reclassified as misdemeanors and his past four prison terms used as enhancements in sentencing be stricken. The First Appellate District of the state Court of Appeal rejected Joshua N. Harrell's assertion that his conviction on "three felony counts

of fraudulent possession of the personal identification of another after having been previously convicted of this offense," should be reversed because the trial court wrongfully denied his motion to suppress evidence.

[Daily Republic](#)

### **9th Circuit grapples with nationwide injunctions in 2 cases**

A federal appeals court panel wrestled Monday with how to handle two immigration-related legal disputes that triggered howls of protest from the Trump administration after district court judges issued nationwide injunctions to enforce their rulings. The suits - argued back-to-back in San Francisco before three judges of the 9th U.S. Circuit Court of Appeals - highlight the intense legal controversy that has erupted over the authority of individual judges to block U.S. government policies across the country.

[Politico](#)

### **Attorneys question presence of tech industry insiders on California bar task force for reforming legal industry**

A California state bar task force crafting proposals to overhaul regulation of the state's legal marketplace has drawn criticism from attorneys who believe some of its members evaluating whether to open up the legal industry to nonlawyer ownership and greater technology-driven legal services have conflicts of interest.

[ABA Journal](#)

### **Federal appeals court to hear Florida transgender bathroom lawsuit**

A federal appeals court will reportedly decide whether a Florida school district must allow students to use the bathroom assigned to the gender with which they identify rather than the gender they were born. The case before the 11th U.S. Circuit Court of Appeals began Thursday after district officials from the St. Johns County school district appealed the lower court victory won by Drew Adams, a transgender former student of Nease High School in Ponte Vedra, Fla., NBC News reported.

[The Hill](#)

## **Prosecutors/ Prosecutions**

### **With state executions on hold, death penalty foes rethink ballot strategy**

California advocates of abolishing the death penalty got a jolt of momentum in March, when Gov. Gavin Newsom announced that he would not allow any executions to take place while he was in office. But after trying twice this decade to persuade voters to end capital punishment, they have no plans to go to the ballot again in 2020. Rather than seeking to build on Newsom's temporary reprieve for Death Row inmates, activists are taking their own pause.

[San Francisco Chronicle](#)

**Car burglaries in some California cities are at crisis levels.  
Prosecutors say their hands are tied**

An epidemic of car burglaries in San Francisco over the last few years has led one Democratic lawmaker to propose plugging a loophole in state law that allows some break-ins to go unpunished, but the Legislature has balked at prosecutors' requests to make obtaining convictions easier. The proposal, which would eliminate a requirement that prosecutors prove a car's doors were locked at the time of a break-in, has been shelved two years in a row in legislative committees.

[Los Angeles Times](#)

**Justice Department sues City of Hesperia, California and San Bernardino County Sheriff's Department for discriminating against African American and Latino renters through the enactment and enforcement of a rental ordinance**

The Justice Department today announced it has filed a lawsuit alleging that the City of Hesperia, California, and the San Bernardino County Sheriff's Department in California discriminated against African American and Latino renters in violation of the Fair Housing Act.

[Department of Justice](#)

**NewsConference: LA DA Lacey running for re-election (Video)**

Jackie Lacey is the 42nd district attorney for the county of Los Angeles. She acts as the chief law enforcement officer for the nation's most populous county with 10 million residents. And is now seeking re-election. NBC4's Conan Nolan asks her why she is seeking a third term?

[NBC4](#)

**Gigi and Bella Hadid's dad files bankruptcy petition over Bel-Air mega mansion dubbed 'most illegal structure' in Los Angeles**

The developer dad of supermodels Gigi and Bella Hadid filed a bare-bones bankruptcy petition just hours before the Thanksgiving holiday. Mohamed Hadid, 71, sought the Chapter 11 protection for his Bel-Air mega-mansion dubbed the "Starship Enterprise" after fed-up neighbors called it "the most illegal structure ever constructed" in Los Angeles, court paperwork reveals.

[New York Daily News](#)

**SF prosecutors weigh retrial in Kate Steinle shooting**

San Francisco prosecutors have an opportunity to decide whether to retry the undocumented immigrant who fatally shot Kate Steinle after an appeals court overturned his conviction for illegal gun possession. The case of Jose Ines Garcia Zarate is back in San Francisco Superior Court on Tuesday with defense attorneys calling on the District Attorney's Office to not seek a second trial.

[San Francisco Examiner](#)

**13-year-old student charged with conspiracy to commit murder**



### **in school threat**

A 13-year-old boy who allegedly threatened to shoot fellow students and staff at Animo Mae Jemison Charter Middle School in the Willowbrook area is set to appear in juvenile court next week on more than a dozen charges, including conspiracy to commit murder. The unidentified student also faces nine counts of criminal threats, and one count each of possession of an assault weapon, possession of a large-capacity magazine and minor in possession of ammunition, according to Greg Risling, a spokesman for the Los Angeles County District Attorney's Office.

[My News LA](#)

### **More USC staff accepted bribes and helped admissions scam, feds say**

Additional employees at the University of Southern California were involved in the "Varsity Blues" admissions scandal beyond the four indicted so far, according to court documents and prosecutors' statements. USC already has more employees charged - three coaches and an athletics administrator - than any other university caught up in the nationwide admissions scam. But in addition to those four employees, prosecutors allege that "others at USC" also took bribes in order to facilitate getting the children of wealthy parents admitted to the school.

[LAist](#)

### **Santana: DA Todd Spitzer and Sheriff Don Barnes clash over secret booking audits**

Orange County District Attorney Todd Spitzer and Sheriff Don Barnes continued to take aim at each other this week, in the wake of an evidence-booking scandal that has already triggered four fired and seven disciplined deputy sheriffs along with four ongoing probes inside the Sheriff's department. Last month, it was revealed that the Sheriff's officials face huge challenges booking evidence according to policy, with deputies holding on to evidence like cash, drugs and guns for longer than is allowed.

[Voice of OC](#)

## **Policy Legal Issues**

### **Another showdown over crime looms**

No California ballot would be complete without at least one measure about crime and punishment and 2020 will be no exception. A referendum seeking to overturn California's landmark ban on cash bail in criminal cases will once again test voters' sentiments about the treatment of accused lawbreakers.

[CalMatters](#)

### **Ex CHP officer claims PTSD affected his mental state in alleged shooting of Ventura neighbor**

A former California Highway Patrol officer claims he was suffering from post-traumatic stress disorder when he allegedly shot his Ventura neighbor two years ago. Court documents unsealed last month provide insight into Trevor Dalton's state of mind during the Dec. 5, 2017, shooting. The documents were filed in support of Dalton's request for treatment in a mental health diversion program rather than criminal prosecution.

[Ventura County Star](#)

### **LAPD tests device to snare people from distance**

The Los Angeles Police Department will begin testing a device designed to snare a person from a distance. Officers will start testing the tool for free for 90 days beginning in January. A training video put out by the company that makes it demonstrates how it works. The device, called the "Bola-Wrap 100," fires a Kevlar cord that wraps around a person 10 to 25 feet away. It's an alternative to firing a taser or a gun and may be particularly useful when dealing with mentally ill individuals.

[ABC7](#)

### **Racial divide shrinks in US criminal justice system, report**

Racial disparities have narrowed across the U.S. criminal justice system over 16 years, though black people are still significantly more likely to be behind bars than white people, new federal figures show. Racial gaps broadly declined in local jails, state prisons, and among people on probation and parole, according to the study released Tuesday by the nonpartisan Council on Criminal Justice.

[AP](#)

### **How California funds DUI prevention by local police**

Every year, millions of dollars pour into local agencies for one purpose: reducing the number of traffic accidents. The money is distributed by the California Office of Traffic Safety, a state agency in charge of allocating funds from the National Highway Traffic Safety Administration in the form of grants. According to Sgt. Ricardo Vazquez, an officer with the Oxnard Police Department's Traffic Unit, not all of the money goes toward DUI checkpoints during holiday weekends - although that is certainly a major component.

[Ventura County Star](#)

### **Editorial: Hey, California lawmakers: Stop tolerating car burglaries**

The San Diego Union-Tribune Editorial Board has long advocated for criminal justice reforms, arguing an archly punitive legal system can ruin the lives of people who could be redeemed. A part of that reform effort is realizing that when poorly written laws help crime flourish, they should be fixed. Which brings us to the report printed Monday in the Los Angeles Times about the state law that says people can't be prosecuted for breaking into a vehicle unless prosecutors can prove a car's doors were locked.

## **Prop 47 & 57 & AB 109**

### **State law reportedly causing car burglary epidemic in some CA cities**

A surge in car break-ins throughout California in recent years has one state lawmaker trying to close a loophole in the current law that he and many in law enforcement see as a big part of the problem. Senator Scott Wiener is a Democrat from Francisco. He introduced legislation this year to amend the state law that requires prosecutors to prove a car was locked before they can file charges against a suspected car burglar.

[iHeart Media](#)

### **Is this Santa Monica watchdog group doing more harm than good?**

A 7-foot-tall, bearded homeless man landed in the heart of Santa Monica in late November, and no one knew why. Most people knew who put him there - artist and activist Ed Massey dropped the sculptural portrait, titled "In the Image," at the corner of 26th Street and Wilshire Boulevard. "Good people - progressive to conservative, secular to religious - are confronted by the issue every day," the sculpture's description reads.

[Los Angeleno](#)

### **Victim-turned-advocate Lenora Claire's warning about celebrity stalker: 'He is going to kill somebody'**

In 2011, casting director and art curator Lenora Claire was living her best life. She'd already led several colorful lives, in fact, as an original Hot Topic model, child actress, radio and TV host, nightlife figure, performance artist, and entertainment journalist. And now her underground art gallery, Pop tART - which showcased exhibits like "Golden Gals Gone Wild" (erotic depictions of the Golden Girls) and "Bettie Page: Heaven Bound" - had just earned her a feature as one of Los Angeles's most interesting people in L.A. Weekly's annual best-of issue.

[Yahoo Music](#)

## **Los Angeles County**

### **L.A. County moves to oppose higher fees for asylum, citizenship requests**

The Los Angeles County Board of Supervisors voted Tuesday to express its opposition to a proposed federal rule that would increase application fees for U.S. citizenship and charge a fee to asylum seekers for the first time in the country's history. Supervisor Hilda Solis recommended sending a letter to Department of Homeland Security Acting Secretary Chad Wolf.

[City News Service](#)

### **Sad ceremony: L.A. County buries 1,460 unclaimed dead in mass grave**

Los Angeles County will hold a ceremony Wednesday to mark the burial of 1,460 people who died in 2016 but whose remains went unclaimed by relatives or loved ones. Supervisor Janice Hahn called for a moment of silence in memory of the dead during Tuesday's Board of Supervisors meeting. While acknowledging that she knew little about the people who will be buried in a mass grave on Wednesday, she said, "We do know that they mattered."

[My News LA](#)

### **LA County places 6 cent parcel tax for fire department on March ballot**

The Board of Supervisors agreed Tuesday to place a parcel tax on the March ballot that would provide funding for more staffing and upgraded equipment for the Los Angeles County Fire Department. Fire Chief Daryl Osby, who has held that job for nearly nine years, said calls for emergency medical assistance have jumped by more than 50% since 2008, while the number of paramedic units has increased by only 5%.

[City News Service](#)

## **Consumer**

### **Real or fake? How to avoid counterfeit products while shopping online**

A few years ago, I needed a new pair of Apple EarPods. I found a pair on Amazon that were labeled as a genuine Apple product. It even showed Apple as the seller. The price was about \$3 less than I knew they sold for on Apple's website - and in Target and Walmart. But hey, this was Amazon. It's got to be the real thing. The EarPods were fake - a counterfeit Apple product that lasted a few weeks before one of the ear pods fell off.

[WPSD](#)

### **One in four U.S. consumers have been conned into purchasing counterfeit goods in past 12 months according to Incopro survey**

Consumers are looking for the best holiday deals on fashion items, electronics, and more, but not always from reputable sellers. Online brand protection software provider Incopro, in partnership with Sapio Research, conducted a survey with 1,059 U.S. respondents in October 2019 to understand how consumers are influenced online, and whether they know - or care - that they are being tricked.

[Incopro Press Release](#)

### **California stops insurance companies from pulling policies in areas hit by wildfires**

California on Thursday ordered insurance companies to stop dropping customers who live in areas affected by recent wildfires, invoking a new

law for the first time to stabilize the state's volatile market. The order from Insurance Commissioner Ricardo Lara will only last for one year. And it only covers people who live within the perimeter of one of 16 different wildfires that raged across the state in October.

[AP](#)

## Crime

### **LAPD union will not defend officer accused of fondling dead woman's breasts**

Leaders of the Los Angeles Police Protective League, the union that represents rank-and-file cops, said it would not criminally defend an officer who allegedly fondled a dead woman's breasts. The officer's body-worn camera recorded the incident. Lt. Craig Lally, a 39-year officer and union president, said he has never heard of any similar incident in policing. He called the allegation "reprehensible, repugnant" and said, if true, the officer "has no place in law enforcement."

[Los Angeles Times](#)

### **Charges filed against woman accused of spitting on food being served to police officer**

Prosecutors on Tuesday filed charges against a woman accused of spitting on food being served to an officer at the restaurant where she worked. A charge of attempting to mingle substances with food or drink - a felony - and a misdemeanor battery charge have been filed against Tatyana Hargrove in connection with the Nov. 15, 2019, incident. Hargrove, 21, was an employee of a west Bakersfield McDonald's where a fellow employee said he saw her fill the order of a uniformed Bakersfield police officer.

[KGET](#)

### **Two more women come forward to LAPD with Danny Masterson rape allegations**

The Underground Bunker has learned that two additional women have identified themselves as rape victims of Scientologist celebrity Danny Masterson and have spoken to the Los Angeles Police Department as part of its ongoing investigation of the That '70s Show actor, bringing to six the number of women who are cooperating with the three-year police probe.

[The Underground Bunker](#)

### **Video and witnesses help detectives arrest man accused in more than 20 SoCal armed robberies**

Deputies arrested a man who they say is responsible for a series of armed robberies spanning several weeks at retail stores across Southern California, the Los Angeles County Sheriff's Department announced in a news release on Monday. Darryle Samuel, 26, was arrested Nov. 20 on suspicion of committing several armed robberies between early October and Nov. 19, in both Los Angeles and Orange counties.



## Public Safety

### **LAPD asks for money to prevent communicable diseases for cops working in filthy conditions**

The LAPD plans to ask for hundreds of thousands of dollars in new funding to pay for equipment, building upgrades, and landscaping - all aimed at reducing the spread of communicable diseases among officers who often work in filthy conditions. The Department's proposed 2020-2021 budget includes requests for more than \$2 million in facilities improvements, including \$325,000 to purchase 50 boot sanitizers that use ultraviolet light to kill microbes and bacteria on the soles of officers' shoes.

[NBC4](#)

### **Cheap automatic license plate readers are creeping into neighborhoods.**

Clayton Burnett seems like an unlikely candidate to run a cutting-edge surveillance system. He is not an FBI agent, nor does he investigate homicides for the NYPD. Burnett is the director of innovation and new technology at Watchtower Security, a private company that contracts with property managers-hundreds of them-in low-income communities across the U.S.

[Slate](#)

### **Long Beach police have seized over 940 firearms in 2019**

The Long Beach Police Department's (LBPD) Gang Investigations Detail has been working to proactively investigate the illegal possession of firearms in an effort to decrease firearm related crime in the city. Year to date, over 940 firearms have been seized citywide. Through the utilization of "Neighborhood Safe Streets" funding available through Measure A, detectives assigned to a Prohibited Possessor Team are identifying prohibited possessors of firearms and following up on all leads involving crimes of gun violence.

[Orange County Breeze](#)

### **New boxing program in Watts seeks to show at-risk kids a different path**

Evana Catalan said bullies had been picking on her for a while at school, but the 9-year-old couldn't do anything about it. Her classmates, she said, would make fun of her for her nice demeanor and because she didn't know how to fight. She felt sad and frustrated but couldn't channel those feelings because she didn't know what to do. Then, on a Friday afternoon when she came home from school, things changed.

[Los Angeles Times](#)

### **California gets #1 rating in gun safety laws**

California has strengthened its gun safety laws over the past 25 years and is now generally considered to have the strongest gun safety laws in the nation, reports the Juvenile Justice Information Exchange. Giffords Law Center, which evaluates the strength of state gun laws, gave California the top rank on its Annual Gun Law Scorecard. The state's legislative changes have been associated with significant declines in overall gun deaths and homicides.

[The Crime Report](#)

### **FBI: 4 dead, including UPS driver, after police chase ends in gunfire after Coral Gables armed robbery**

Four people, including a UPS driver, have died after a police chase that spanned more than 30 miles across highways and surface streets ended with gunfire in Miramar after officers pursued alleged armed robbery subjects from Coral Gables, according to the FBI. Coral Gables Police first responded to a shooting outside of a jewelry store along the 300 block of Miracle Mile at around 4:15 p.m., Thursday.

[WSVN](#)

### **Greater privacy, fewer births, a gun case, and UC admissions**

Come Jan. 1, Californians will gain greater control over their personal data, when a landmark privacy law takes effect. CalMatters' Laurel Rosenhall breaks down what it means for you. California in 2018 became the first state in the nation to pass a law giving consumers more control of their digital data. Companies are spending \$55 billion to comply.

[CalMatters](#)

### **Oklahoma officer indicted for murder in killing of active shooter**

On Thursday, Blackwell police officer Lt. John Mitchell was indicted by a grand jury for his role in a May officer-involved shooting. Monday at his bond hearing a Kay County Judge set his bond at \$10,000 but allowed Mitchell to be released on his own recognizance. Mitchell was then processed at the Kay County Detention Center and able to go home.

[KFOR](#)

### **Lawmakers approved \$4.4 billion in new taxes and fees while swimming in revenue**

State lawmakers and the governor approved more than \$4.4 billion a year in higher taxes and fees this year, even as the state was experiencing a revenue windfall from existing taxes, according to the new Tax and Fee Report published by the California Tax Foundation. The increases enacted this year include a renewal of California's Managed Care Organization tax, two cellphone surcharges and a renewal of a surcharge on electricity ratepayers.

[Fox & Hounds](#)

### **One mistake trapped a desperate dad in a Mexican drug cartel's web. Then he vanished.**

Oscar Macias gripped his cellphone and quickly hammered out a text message to his childhood friend Tommy Cantu. It was 7:38 p.m. on July 20, 2014. A Sunday. Twenty miles away in Whittier, California, Tommy's phone buzzed as he sat down to dinner with his wife and two children. He glanced at the message on his screen, then scanned it again to make sure he read it right. He called Oscar. No one answered.

[Louisville Courier Journal](#)

### **New privacy law could bring big changes to companies doing business in California**

A long-awaited consumer privacy law goes into effect in January, with broad implications for companies doing business across the United States. The California Consumer Privacy Act was passed by the California State Legislature back in 2018, but lawmakers delayed its implementation until this coming Jan. 1. While the law targets companies doing business in the state, it casts a wide net.

[Washington Examiner](#)

### **One of California's most powerful labor unions is feuding with Gov. Gavin Newsom**

A young girl dressed as a newsie walked up to Gov. Gavin Newsom at the California Democratic Party convention in Long Beach last month, handing him a copy of a paper with his image splashed across the front page. Alongside an unflattering photo of the Democratic governor, a headline on the Building Trades News read: "Gov. Newsom Vetoes Fair Wages for Construction Workers."

[Los Angeles Times](#)

### **Starbucks should forgive barista in 'PIG' cup flap: chief**

An Oklahoma police chief is asking Starbucks to have mercy on a barista who plastered "PIG" on a police officer's coffee order. "I just recently learned that the employee was terminated, and this may be a bit surprising, but I would like Starbucks to reconsider," Keifer, Oklahoma, Police Chief Johnny O'Mara told Fox News. "I'm asking for civility." O'Mara took to Facebook Thursday after one of his officers made a Thanksgiving coffee run as a treat for the department's dispatchers - and came away with the insult.

[New York Post](#)

### **Lisa Page, ex-FBI lawyer targeted by Trump, breaks silence**

Roughly two years after her anti-Donald Trump text messages were released to Congress and she became a public target of the President's ire, Lisa Page said it's time to break her silence. The embattled former FBI lawyer resurfaced her Twitter account Sunday night, tweeting, "I'm done being quiet," along with a link to a new interview with The Daily Beast.

[CNN](#)

### **Federal background check and state gun laws together reduce**

### **teen gun carrying: Study**

As the Supreme Court hears its first firearms case since 2010 this week, new research indicates there's one area in which strong gun laws have proved effective. Adolescents in states that require universal background checks were less likely to report carrying a firearm than teenagers living in states that rely entirely on checks during gun sales at federally licensed gun dealers, a study published Monday in the journal of Pediatrics found.

[ABC News](#)

### **Drug cartels muscle into Mexican town packed with Americans**

San Miguel de Allende oozes old Mexico charm. There are the cobblestone streets, the colonial-era buildings and wrought-iron balconies, the neo-Gothic steeples soaring high above the pink-sandstone church anchoring a corner of the main plaza. Travel and Leisure magazine has twice named it the best city in the world, a ratification of how beloved it is with tourists and retirees from the U.S., Canada and beyond.

[Bloomberg](#)

### **Leave California, keep paying California taxes...really**

If you leave California, can the state say you really didn't and keep taxing you? Yes, and it happens more than you might think. California taxes have always been high, and for that reason, many people do their best to try to avoid paying them. This is especially true for someone expecting a big spike in income. Some people vote with their feet, although in some cases, California can assess taxes no matter where you live. How high are California taxes?

[Forbes](#)

## **Articles of Interest**

### **Cell phone detection cameras rolled out in Australia**

The Australian state of New South Wales rolled out "high definition detection cameras" on Sunday, designed to catch drivers using cell phones behind the wheel. Andrew Constance, New South Wales' minister for roads, said the "world-first" technology would target illegal cell phone use through "fixed and mobile trailer-mounted cameras." The cameras will use artificial intelligence to review images and detect illegal use of cell phones, according to Transport for NSW.

[CNN](#)

### **Why TV networks may be afraid of investigative stories**

This has been the autumn of discontent for investigative TV journalists. Ronan Farrow's bestselling book "Catch and Kill" detailed his frustration with former bosses at NBC News over his failed attempt to break the story on the sexual assault and harassment allegations against movie mogul Harvey Weinstein.

[Los Angeles Times](#)

## **New FBI audio reveals chaotic moments after deadly 2011 Tucson shooting**

The Federal Bureau of Investigation released dozens of new audio files on the 2011 Tucson mass shooting that left six people dead and former Arizona Rep. Gabrielle Giffords with serious injuries. The files are between dispatchers and police following initial 911 calls regarding the shooting that happened outside a Safeway in Casa Adobes.

[KOLD](#)

## **How to speak LA: Your guide to the city's most debated and mispronounced words**

The question of how to pronounce some of L.A.'s most quintessential names - the streets, neighborhoods and destinations that make up our everyday vocabulary - is much more complicated than it should be. That's because there's no "right" way to say a lot of them. Is Los Feliz lahs-FEE-luss or lohs-feh-LEEZ? Is Angeleno an-jeh-LEE-noh or an-jeh-LAY-noh? Ask around and you're not likely to find much consensus.

[LAist](#)

## **Is California a 'permanently blue' state?**

"The very rapid decline of California's Republican Party," writes Dan Walters of CALmatters, "from near-dominance in the 1980s and early 1990s to its current irrelevance has been one of the state's most dramatic political events." Walters has been writing on the Golden State since the 1970s and on some points shows a keen memory. California Republican Ronald Reagan served two terms as president during the 1980s.

[California Globe](#)

## **Medical professors are supposed to share their outside income with the University of California. But many don't.**

For nearly two decades, Dr. Neal Hermanowicz has led the movement disorders program at the University of California's Irvine campus, where he earns more than \$380,000 a year in salary and bonuses. The widely respected expert on Parkinson's and Huntington's diseases adds to his income by consulting for drug companies. Since 2014, 11 pharmaceutical companies have paid him a total of at least \$588,000 for consulting, speaking and honoraria, according to federal data.

[ProPublica](#)

## **Sentences/Convictions**

### **California man tells court he served as agent for China**

A former San Francisco Bay Area tour operator agreed Monday to plead guilty to serving as an unregistered agent for China in exchange for a possible reduced prison sentence. Xuehua Edward Peng agreed in court to a four-year prison term and a fine of \$30,000 in a plea deal



negotiated with prosecutors after they charged him with being an illegal foreign agent who delivered U.S. national security information to officials in China.

[NBC4](#)

### **Fontana woman sentenced to prison for distributing powerful opioid**

A Fontana woman who was part of a drug-trafficking organization that distributed carfentanil, a powerful fentanyl analogue that is sometimes used to sedate elephants and other large animals, was sentenced Monday in Los Angeles to three years in federal prison. Alejandra Romero-Agredano, 50, pleaded guilty in January to one count of distribution of more than 100 grams of carfentanil.

[My News LA CBS LA](#)

## **Corrections/Parole**

### **California prison inmate killed; 2 separated had weapons**

Two California prison inmates serving extended sentences because of crimes they committed in custody allegedly killed another inmate on Wednesday, according to the Department of Corrections and Rehabilitation. The department has not yet released the name of the inmate who was killed in the attack at High Desert State Prison in Susanville. The department said the victim was assaulted before 3 p.m. on Wednesday in between general population yards.

[Sacramento Bee](#)

## **Homeless**

### **Violence and the homeless - the reality**

Whenever there are suggestions or efforts to aggressively abate street encampments, the cry goes out: "don't criminalize the homeless". This ignores the fact that the homeless are committing a disproportionate amount of serious and violent crime. It is also true that the homeless are disproportionately the victims of such crimes. The LAPD tracks crimes committed by and against the homeless and the statistics for 2018 are stunning.

[Medium](#)

### **More subsidies can better help those experiencing mental illnesses, homelessness**

Homelessness is a vicious cycle. And for those without support, it can be both a cause and effect of mental illness. In 2015, according to the U.S. Department of Housing and Urban Development, Los Angeles County had the second-highest rate of unsheltered homeless people in the country, at 70.3%. Additionally, 26.2% of sheltered people who were homeless are estimated to experience a severe mental illness.

[Daily Bruin](#)

### **Leader of L.A.'s top homeless agency quits after a 'long five years,' rising public anger**

In a major change for the team tasked with addressing rising homelessness in the region, Peter Lynn announced Monday that he is stepping down as head of the Los Angeles Homeless Services Authority. Chief Program Officer Heidi Marston will fill in as interim director during a national search for a replacement when Lynn officially leaves at the end of this month.

[Los Angeles Times](#)

### **As Trump officials target California's homeless crisis, state officials brace for fight**

As the Trump administration looks to replace a recently fired Obama appointee tasked with battling homelessness, California officials and advocates are in the dark and bracing for battle. The abrupt nature of the dismissal Nov. 15 of Matthew Doherty, executive director of the U.S. Interagency Council on Homelessness, has suggested to many who work on homelessness that the White House is poised to deliver a new agenda as early as next week.

[USA Today](#)

### **Redefining homelessness could help homeless kids & families on the edge, advocates say**

With many cities seeing a spike in homelessness, there's a renewed state and federal effort to pass laws that would make it easier to help homeless children and youth, from getting them food and housing to connecting them with counseling. Utah enacted legislation earlier this year allowing homeless minors to enter shelters without parental consent. This week, Wisconsin Democratic Gov. Tony Evers signed a similar bill.

[Witness LA](#)

### **How homeless services differ in LA and New York**

One of LA's biggest homeless encampments is nestled below the 405 Freeway overpass at Venice Boulevard. Dylan Brumley rummages through trash there, looking for food. He and about 40 others call the encampment home. Most of the people living here say they're struggling with drug addiction or mental illness. Outreach workers with the LA's Homeless Services Authority, or LAHSA, sometimes visit the site. But Brumley said he sees them mostly just handing out snacks.

[NBC4](#)

### **Homeless hearing on Skid Row: Millions spent, but no improvement, officials say**

There are almost 59,000 homeless people in Los Angeles County as of this year, and the numbers continue to grow. Even as 123 people get off the streets every day, another 154 become homeless. "We are bailing water out of this boat faster than ever before, but the hole on the

bottom of the boat is so large that we are at risk of this boat sinking," says Phil Ansell from the Los Angeles County Homeless Initiative.

[ABC7](#)

## Pensions

### **Gavin Newsom's climate order focuses on pensions and roads. What does it mean for taxpayers?**

On his way to an international climate forum two months ago, Gov. Gavin Newsom handed down an executive order meant to sharpen the state's focus - and its spending - on global warming. Government agencies have been struggling to explain it ever since. Newsom's order directs the state's Transportation Agency, pension funds and the department that manages government contracts to reconsider how they spend the public's money with an eye toward investing in projects that could help Californians prepare for climate change.

[Sacramento Bee](#)

### **Pension reform waits for California Supreme Court**

With markets fitfully advancing after a nearly two year pause, the need for pension reform again fades from public discussion. And it's easy for pension reformers to forget that even when funds are obviously imperiled, with growing unfunded liabilities and continuously increasing demands from the pension funds, hardly anyone understands what's going on.

[California Globe](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Los Angeles Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [The Washington Post](#)  
**To:** [aaquino@sunnyvale.ca.gov](mailto:aaquino@sunnyvale.ca.gov)  
**Subject:** The Daily 202: Ousted Navy secretary warns Trump that 'the rule of law is what sets us apart from our adversaries'  
**Date:** Monday, November 25, 2019 7:49:10 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you're having trouble reading this, [click here](#).

---

# The Daily 202

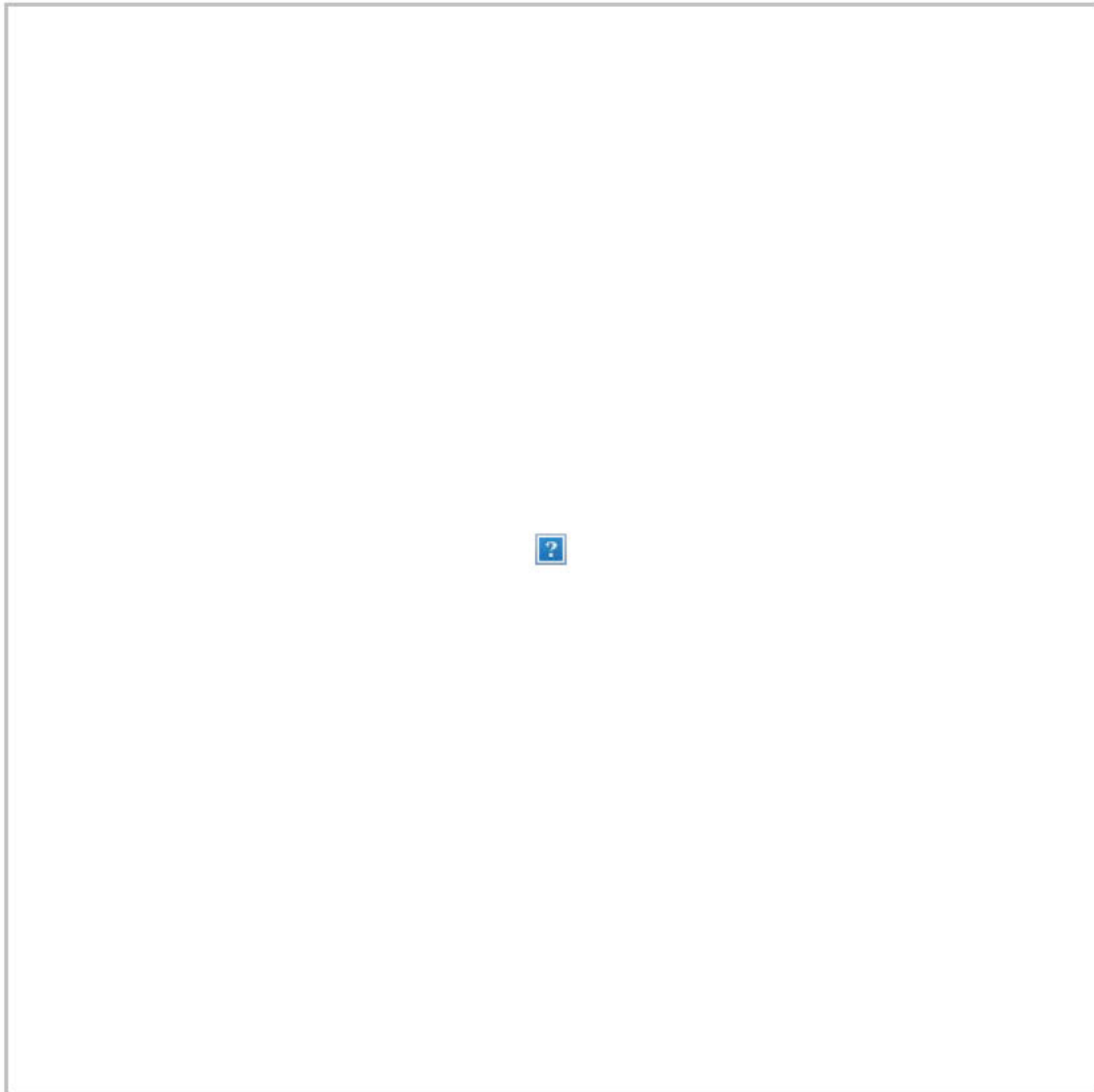


Share:  

 Listen to The Big Idea



## Ousted Navy secretary warns Trump that ‘the rule of law is what sets us apart from our adversaries’



Richard V. Spencer visits the Blue Angels at the squadron's hangar in Pensacola, Fla., on Nov. 5. He was forced out on Sunday as secretary of the Navy. (Timothy Schumaker/Navy/EPA-EFE/Rex)





**BY JAMES HOHMANN**

*with Mariana Alfaro*

**THE BIG IDEA: What makes America [exceptional](#) isn't any arsenal. It's moral authority.**

That's the upshot of Richard V. Spencer's Sunday letter to President Trump, acknowledging his "termination" as secretary of the navy. The messy circumstances surrounding Spencer's exit should not overshadow another damning resignation letter from another Trump appointee.

Spencer explained that he has strived over two-plus years on the job to ensure judicial proceedings are "fair, transparent and consistent," from ensigns to admirals. "Unfortunately, it has become apparent that in this respect, I no longer share the same understanding with the Commander in Chief who appointed me, in regards to the key principle of good order and discipline," he [wrote](#). "I cannot in good conscience obey an order that I believe violates the sacred oath I took in the presence of my family, my flag and my faith to support and defend the Constitution of the United States."

His language goes further than [Jim Mattis's letter](#) last December when he [resigned](#) as secretary of defense to protest Trump ordering U.S. troops to withdraw from Syria, but there are echoes. Both Spencer and Mattis said Trump deserves someone whose views are better aligned with his own.

**Spencer was ousted over his efforts to resolve a dispute between the White House and Navy commanders who wanted to strip**

**Edward Gallagher of the Trident pin that makes him a Navy SEAL.** Gallagher's was one of three cases in the military justice system that Trump intervened in 10 days ago. The chief petty officer was accused of committing war crimes during a 2017 deployment in Iraq. He was acquitted of murder but convicted in July of posing with the corpse of an Islamic State prisoner. Trump reinstated Gallagher's rank after he was demoted as part of his punishment. The president tweeted on Thursday that he doesn't want Gallagher, who has become a cause celebre on Fox News, kicked out of the SEALs.

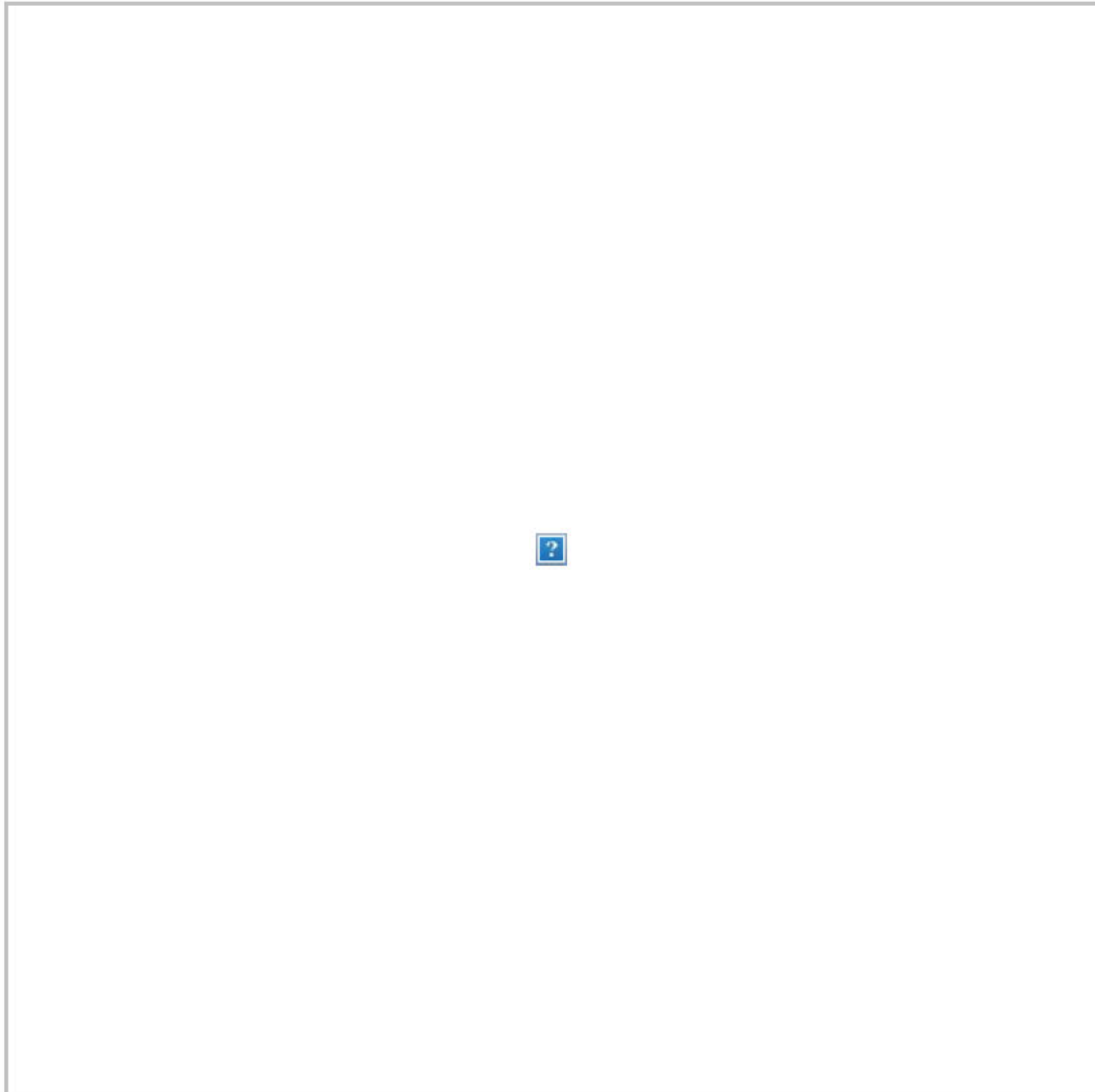
**"The rule of law is what sets us apart from our adversaries," Spencer told Trump, offering a brief history lesson.** "Good order and discipline is what has enabled our victory against foreign tyranny time and again, from Captain Lawrence's famous order 'Don't Give up the Ship,' to the discipline and determination that propelled our flag to the highest point on Iwo Jima. The Constitution, and the Uniform Code of Military Justice, are the shields that set us apart, and the beacons that protect us all."

**-- Disdain for the rule of law has been a recurring feature of Trumpism.**

**-- Spencer, 65, served in the Marines as an aviator from 1976 to 1981, separating as a captain, before making a fortune on Wall Street.** He has been secretary of the Navy since the Senate confirmed him in August 2017. In his letter, he praised the troops who will soon miss their Thanksgiving dinners at home so that they can continue the watch beyond the curve of the horizon.

"As Secretary of the Navy, one of the most important responsibilities I

have to our people is to maintain good order and discipline throughout the ranks,” Spencer wrote. “I regard this as deadly serious business. The lives of our Sailors, Marines and civilian teammates quite literally depend on the professional execution of our many missions, and they also depend on the ongoing faith and support of the people we serve and the allies we serve alongside.”



Edward Gallagher and his wife, Andrea Gallagher, celebrate in July after a military jury in San Diego acquitted the Navy SEAL of premeditated murder in the killing of a wounded Islamic State captive under his care in Iraq. (Gregory Bull/AP)



**-- Pentagon spokespeople said Defense Secretary Mark Esper asked for Spencer's resignation after losing confidence in him.**

Their explanation is that Esper became "deeply troubled" when he discovered Spencer was backchanneling with the White House to offer a secret deal in which a review board would decide to let Gallagher keep his Trident pin – and affiliation with the SEALs – if Trump didn't directly meddle in the official peer-review process, thereby maintaining the appearance of independence.

**-- "Spencer had tried to find a compromise," David Ignatius reports in his column,** "after Trump tweeted Thursday, 'The Navy will NOT be taking away Warfighter and Navy Seal Eddie Gallagher's Trident Pin.' Spencer feared that a direct order from Trump to protect Gallagher, who is represented by two former partners of Trump's personal attorney Rudolph W. Giuliani, would be seen as subverting military justice. After that Trump tweet, Spencer cautioned acting White House Chief of Staff Mick Mulvaney that he would not overturn the planned SEAL peer review of Gallagher without a direct presidential order; he privately told associates that if such an order came, he might resign rather than carry it out. ...

**"It was a hold-your-nose solution,' said a source close to Spencer about his effort to broker an arrangement** that would allow Gallagher to retire at the end of November with his former rank, an honorable discharge and his Trident pin, as Trump wanted, but without direct presidential interference in the SEAL review process. **As so often happens with attempts to work with Trump's erratic demands, this one ended in disaster.** 'The president wants you to go,' Esper told Spencer on Sunday ... Esper then toed the White

House line and announced Spencer's dismissal. ...

**"Trump began lobbying Spencer to exempt Gallagher from Navy discipline back in March,** when he ordered the Navy secretary in an early-morning phone call to release Gallagher from the brig and give him more comfortable quarters. Presidential pressure has been relentless, ever since. ... While Gallagher is celebrated on Fox, current and former senior officers of the SEALs and other elite units told me this weekend that his case has little support within the community of Special Operations forces. One former SEAL commander noted that maintaining discipline among these elite units is so important that the SEAL peer-review panels have removed more than 150 Trident pins since 2011, or more than one a month."

**-- Trump now gets the outcome he wanted:** Esper's aides said he will let Gallagher keep his Trident pin without even the pretense of a review board. And Trump has rid himself of someone he came to disregard as disloyal, based on his threat to resign.

**-- Spencer joins a growing list of former Trump appointees who have spoken critically, to varying degrees, about the president after leaving his employ.** This includes, among others, [John Bolton](#), [Rex Tillerson](#), [John Kelly](#), [Tom Bossert](#), [Fiona Hill](#) and [Gary Cohn](#).

**-- Spencer took the sting out of this punch by vigorously denying well-sourced press reports on Saturday that he had threatened to resign.** In the version of his letter distributed to media outlets last night, the date "24 Nov 19" has been scrawled by hand on the top right of a letter that was reportedly drafted last week. The denial of accurate media accounts muddies the narrative around the



secretary's departure.

-- This appears to be the coda of a contentious chapter in a civilian-military relationship that has **grown increasingly fraught**.

Trump avoided military service by claiming bone spurs. He has stated that avoiding sexually transmitted infections while bedding models in New York during the 1970s was "my personal Vietnam." **Trump has insulted several war heroes**, as well as their families, and never apologized.



CONTENT FROM GOLDMAN SACHS 10,000 SMALL BUSINESSES

**What are the key issues impacting small**

## businesses?

Explore the “voice of small business” in our new infographic, which covers a range of small business perspectives on everything from the economy and healthcare to hiring and minimum wage.



Gen. Mark Milley arrives in Bahrain on Monday. (Idrees Ali/Reuters)

**-- The top U.S. military officer voiced public support today for Esper's decision to allow Gallagher to remain a Navy SEAL and**

**to fire Spencer.** “As far as I’m concerned, it’s case closed now,” Gen. Mark Milley, chairman of the Joint Chiefs of Staff, told reporters traveling with him in the Middle East, [including Missy Ryan](#). “It’s time to move on and address the national security of the United States. ... Esper made decisions for good reasons that are within his power. I’ll support the secretary of defense in those decisions.”

**-- Senate Minority Leader Chuck Schumer (D-N.Y.) said he spoke by phone with Spencer on Sunday night:** “I told him he’s a patriot, that he served the Navy and the nation well and he will be missed,” Schumer said in a statement. “Secretary Spencer did the right thing and he should be proud of standing up to President Trump when he was wrong, something too many in this administration and the Republican Party are scared to do. Good order, discipline, and morale among the Armed Services must transcend politics, and Secretary Spencer’s commitment to these principles will not be forgotten.”

**-- Senate Armed Services Committee Chairman Jim Inhofe (R-Okla.) said Trump notified him personally that Spencer was being fired.** “Both Secretary Esper and President Trump deserve to have a leadership team who has their trust and confidence,” Inhofe said in a statement, adding: “It is no secret that I had my own disagreements with Secretary Spencer over the management of specific Navy programs.”

**-- Other lawmakers offered praise for Spencer:**



-- Trump **tweeted** that he will nominate Kenneth Braithwaite, a retired Navy rear admiral who is currently the ambassador to Norway, to be Spencer's replacement. Esper recommended him.

-- In an interview Sunday morning on "**Fox & Friends**," Gallagher said the Navy was only trying to take his Trident pin away as "retaliation" for Trump intervening on his behalf. "They could have taken my Trident at any time they wanted," he said on a show the president often watches. "Now they're trying to take it after the president restored my rank." Speaking of Rear Adm. Collin Green, who is in charge of the SEAL program as commander of the Naval



Special Warfare Command, Gallagher said: “What the admiral is doing is showing complete insubordination.”

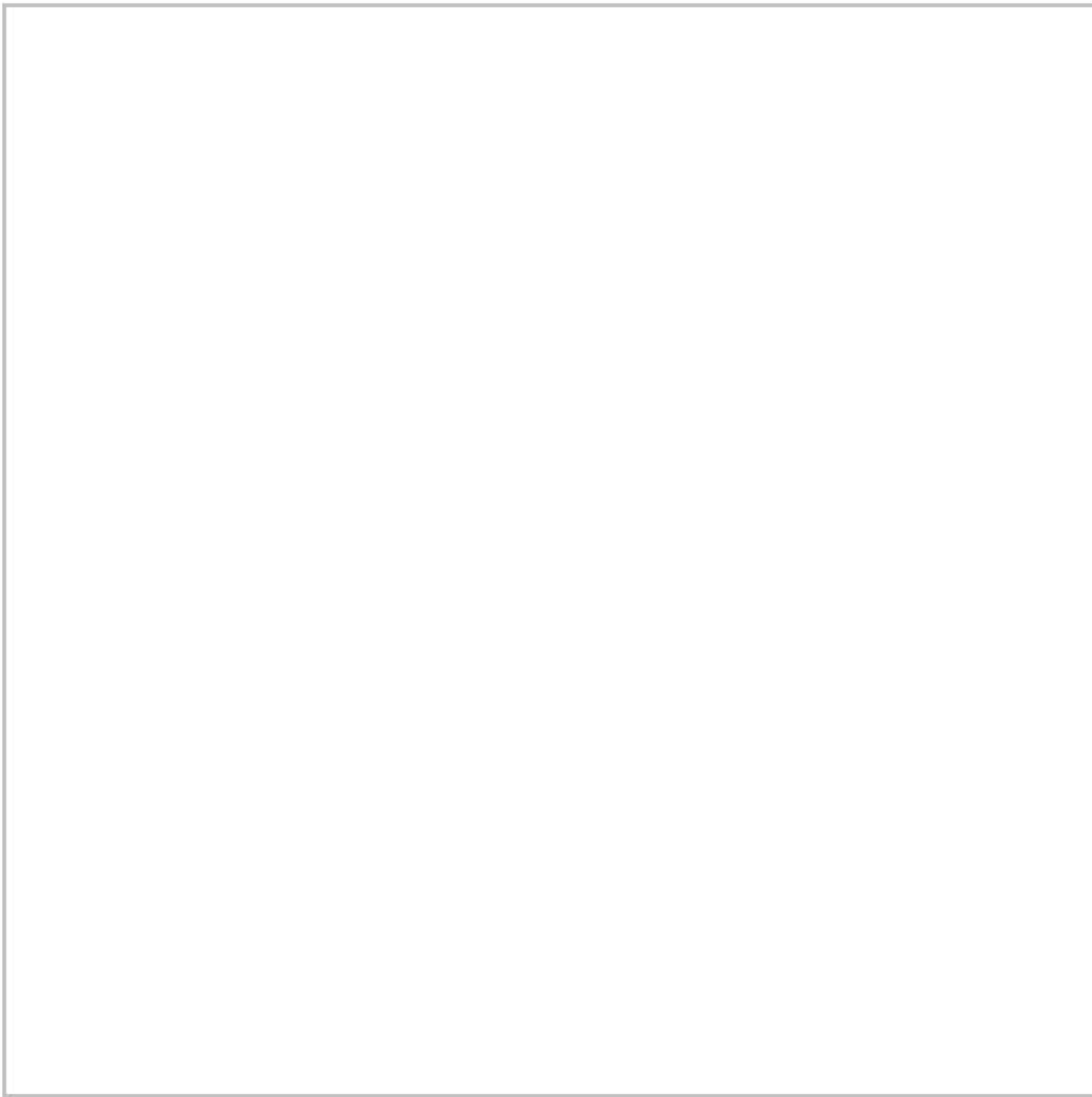
**-- Ray Mabus, who served as Navy secretary under Barack Obama, said on MSNBC that he's been stunned that a sailor on active duty is going on cable television to criticize his commanding officers.** “It's so dangerous for good order and discipline ... to get this politicized,” Mabus said Sunday [on MSNBC](#). “You simply cannot have good order and discipline. You simply cannot hold people accountable. You simply cannot have the elite fighting force if you allow things like this to happen. If you set this sort of precedent, then how do you tell the next SEAL that is up on charges not to go public, not to try to undermine their superiors, not to try to change a military judgment and make it a political one?”

**-- The Post's Editorial Board says Trump's intervention in the Gallagher case, including Spencer's ouster, [dishonors the troops who uphold American values](#):** “Restoring to service someone who was turned in by members of his unit who wouldn't tolerate his behavior sends precisely the wrong message. ... Most offensive is what Mr. Trump's actions say about his view of the military. ‘We train our boys to be killing machines, then prosecute them when they kill!’ he tweeted in October when he announced he would review these cases. Perhaps Mr. Trump has watched too many bad war movies, but if he were to consult with his military leaders or talk to the many fine men and women in uniform, they would tell him they are trained to engage in combat while following the laws of war and upholding the country's ideals.”



### **QUOTE OF THE DAY:**

A lawyer for Gallagher, Tim Parlatore, welcomed last night's news and expressed amazement at the turn of events that led to Spencer's ouster. "This case is bananas," he said. "Yes, you can quote that." (Ashley Parker and Dan Lamothe)



Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



Lawmakers react after a week of impeachment inquiry hearings

## **THE IMPEACHMENT INQUIRY:**

**-- A confidential White House review of Trump's decision to place a hold on military aid to Ukraine has turned up hundreds of documents that reveal extensive efforts to generate an after-the-fact justification for the decision and a debate over whether the delay was legal, according to three people familiar with the records. [Josh Dawsey, Carol D. Leonnig and Tom Hamburger scoop](#): "The research by the White House Counsel's Office ... includes early**



August email exchanges between acting chief of staff Mick Mulvaney and White House budget officials seeking to provide an explanation for withholding the funds after the president had already ordered a hold in mid-July on the nearly \$400 million in security assistance ... White House lawyers are expressing concern that the review has turned up some unflattering exchanges and facts that could at a minimum embarrass the president. ...

**“In the early August email exchanges, Mulvaney asked acting OMB director Russell Vought for an update on the legal rationale for withholding the aid and how much longer it could be delayed.**

Trump had made the decision the prior month without an assessment of the reasoning or legal justification ... Emails show Vought and OMB staffers arguing that withholding aid was legal, while officials at the National Security Council and State Department protested. OMB lawyers said that it was legal to withhold the aid, as long as they deemed it a ‘temporary’ hold ...

**“Mulvaney’s request for information came days after the White House Counsel’s Office was put on notice that an anonymous CIA official had made a complaint to the agency’s general counsel** about Trump’s July 25 call to [Volodymyr] Zelensky ... This official would later file a whistleblower complaint with the intelligence community’s inspector general ...

**“The document research has only exacerbated growing tension between [White House Counsel Pat] Cipollone and Mulvaney and their offices,** with Cipollone tightly controlling access to his findings, and Mulvaney’s aides complaining Cipollone isn’t briefing other White House officials or sharing important material they need to respond to



public inquiries ... The emails revealed by White House lawyers include some in which Mulvaney urges Vought to immediately focus on Ukraine's aid package, making clear it was a top priority for the administration. [Mulvaney's lawyer, Robert Driscoll, declined to comment.]

**“The legal office launched this fact-finding review of internal records in a protective mode**, both to determine what the records might reveal about internal administration conversations and also to help the White House produce a timeline for defending Trump's decision and his public comments. Along with examining documents, **the review has also involved interviewing some key White House officials** involved in handling Ukraine aid and dealing with complaints and concerns in the aftermath of the call between Trump and Zelensky. **Cipollone's office has focused closely on correspondence that could be subject to public records requests**, those which involve discussions between staff at the White House and at other agencies. Internal White House records are not subject to federal public records law, but messages that include officials at federal agencies are.”

**-- Follow the money: Lev Parnas and Igor Fruman, the Rudy Giuliani associates who have been indicted, tried to recruit a Ukrainian energy executive to join them in a proposed takeover of the state oil-and-gas company.** [From the Wall Street Journal](#): The two men described the “company's chief executive and [Marie Yovanovitch] as part of ‘this Soros cartel’ working against [Trump.] ‘You're a Republican, right?’ Andrew Favorov, the head of natural gas for state-run Naftogaz, recalled the men ... asking him, after their

reference to investor and Democratic donor George Soros. 'We want you to be our guy.' ... **Mr. Favorov described the efforts of Messrs. Fruman and Parnas to enlist his help in an effort to oust Naftogaz CEO Andriy Kobolyev. Naftogaz is the most important company in Ukraine, representing nearly 10% of the country's gross domestic product and supplying virtually all of the country's natural gas.** Mr. Favorov said he was bewildered by Messrs. Parnas and Fruman's pitch to stage a takeover of Naftogaz and put Mr. Favorov in place as CEO. On one hand, **the pair appeared to know little about the natural gas business;** on the other it was clear to him they had significant political connections. 'They don't teach you how to deal with this in business school,' Mr. Favorov said."

**-- So many potential conflicts: Giuliani also discussed representing a state-owned Ukrainian bank in a legal dispute over the summer, even as he publicly pressed Ukraine on behalf of Trump.** [From Bloomberg News](#): "Though he ultimately did not take on the client, the talks expose his enthusiasm for foreign business and his willingness to insert himself in matters rife with potential conflicts. In fact, **the Ukrainian bank is entangled in a legal dispute with its former owner who has ties to Ukraine's president and is the subject of a federal investigation in the U.S.** ... [Giuliani] said he was approached by lawyers for Privatbank seeking to recover assets linked to the previous owner. They wanted to know if Giuliani -- who had written tweets critical of the man -- could assist their civil suit, Giuliani confirmed by phone on Thursday."

**-- "What we still don't know about the Ukraine affair,"** [by deputy editorial page editor Jackson Diehl](#): "Let's start with the distinct



possibility that Trump's demand that [Zelensky] launch politicized investigations in exchange for military aid and a White House meeting was only the last of a series of quid pro quos he forced on Ukrainians." **Giuliani met with Zelensky's predecessor at least twice in 2017 as Ukraine's former chief prosecutor Yuri Lutsenko transferred an investigation into secret payments to Paul Manafort, effectively stalling it, and the U.S. released the sale of Javelin missiles to Ukraine.** "Let's see: a White House meeting and weapons ... for favorable actions on an investigation? There's no proof. But no wonder Trump complained to Zelensky in their July 25 phone call that 'I heard you had a prosecutor who was very good and he was shut down and that's really unfair.' One of Zelensky's first acts had been to fire Lutsenko.

**"The prosecutor has also been blamed for Trump's recall of [Yovanovitch]. But the full story behind her dismissal is still not known.** ... Trump began demanding Yovanovitch's removal a year earlier, after meeting with [Parnas and Fruman]. Why did Parnas and Fruman want the ambassador out? It's still not clear. ... One person who probably could shed light on this is Rick Perry.

**... According to testimony by U.S. Embassy staffer David Holmes, Perry used a meeting with Zelensky to give him a list of 'people he trusts' on energy matters. The Times reported that these included a couple of Texas businessmen whom Perry wanted appointed to the supervisory board of the Ukrainian state gas company.** That's the same company Parnas and Fruman were trying to deal with. ... We may eventually learn more about Ukraine from federal prosecutors in New York, who have already indicted Parnas and Fruman and are said to be looking at Giuliani. But you

have to wonder if Democrats are making a mistake by not pursuing these matters themselves.”

**-- Rep. Devin Nunes (R-Calif.), the ranking member on the House Intelligence Committee, said reports that he met with ex-Ukrainian prosecutor general Viktor Shokin in Vienna to obtain information about the Bidens were false.** [Elise Viebeck and Felicia Sonmez report](#): “The allegation ... was made by the attorney for [Parnas]. ... **On Fox News, Nunes declined to answer further questions about the accusation** ... A person close to Shokin also has denied the claim. ... Nunes has also threatened to sue two of the news outlets that reported Parnas’s accusation. On Fox News, Nunes claimed that CNN and the Daily Beast were ‘likely conspiring to obstruct justice’ by basing their reporting on interviews with a lawyer for Parnas. ... **House Armed Services Committee Chairman Adam Smith (D-Wash.) said Saturday that it was ‘quite likely, without question’ that Nunes would face an ethics investigation** following media reports of a meeting with Shokin. ... Several other Democratic lawmakers have said that Parnas’s testimony could be helpful to impeachment investigators or that Nunes should face an ethics probe.”

**-- Lordy, there are tapes? Parnas has provided the House Intelligence Committee with audio, photos and video recordings, but what these records show is unclear.** [From ABC News](#): “[The] tapes were provided as part of that congressional subpoena issued to Parnas, and the former Giuliani ally also provided a number of documents both in English and Ukrainian to the committee in two separate productions ... However, some of the material sought by



congressional investigators is already in possession of federal investigators within the Southern District of New York and thus held up from being turned over, according to sources familiar with the matter.”

**-- House Intelligence Committee Chairman Adam Schiff (D-Calif.) said his panel will press ahead with preparing its impeachment report, even though several key witnesses have refused to testify.** [Felicia Sonmez and Elise Vlebeck report](#): “In an interview on CNN’s ‘State of the Union,’ Schiff said the evidence against Trump is ‘already overwhelming,’ although he stopped short of saying whether he would support impeachment himself. ‘Yes, we’d love to have these witnesses come in,’ Schiff said. ‘But we’re not willing to simply allow them to wait us out — to stall this proceeding — when the facts are already overwhelming.’ ... Several key figures, including [Mulaney], Vice President Pence, Secretary of State Mike Pompeo, former national security adviser John Bolton and [Giuliani], have declined to cooperate with the impeachment inquiry. A federal judge is expected to rule [today] on whether [former White House counsel Don McGahn] must testify under subpoena. ...

**"Schiff said Sunday that time is of the essence and that Democrats will continue to investigate even after they have submitted their report to the House Judiciary Committee. ...** 'The investigation isn't going to end,' he said, adding that 'we may have other depositions and hearings to do.' He took particular aim at Bolton, arguing that the former national security adviser will have to explain why he chose to give his account of events 'in a book' rather than show the 'courage' that Fiona Hill, the former National Security



Council Russia adviser, did in testifying before lawmakers last week. Schiff declined to say how long it might take impeachment investigators to finish their report, saying only that ‘we’ll take the time that’s necessary.’”

**-- Amid tensions between the Trump administration and Democrats, Pelosi and Treasury Secretary Steve Mnuchin must work out a spending deal. Luckily, they appear to maintain a good rapport. From the Journal:** “While the Office of Management and Budget leads the administration’s efforts on spending, Mr. Mnuchin has emerged as the public face of the administration on Capitol Hill in the spending talks, which took a positive turn this weekend even as [impeachment strains](#) the broader relationship between the two branches. Mr. Mnuchin’s role speaks to the rapport and goodwill he has built up with lawmakers and, in particular, Mrs. Pelosi ... Mrs. Pelosi has clashed with two of the administration’s other top negotiators, [Mulaney] and [Vought], with whom she refused to negotiate last summer’s budget deal. ... **House Budget Committee Chairman John Yarmuth (D., Ky.) said ... that Mr. Mulvaney would normally play a more visible role in the negotiations, ‘but I think Mick, he has other distractions.’”**





Record numbers vote in Hong Kong elections

## **THE NEW WORLD ORDER:**

**-- Hong Kong's pro-democracy parties swept aside the pro-Beijing establishment during local council elections in a significant endorsement of the protest movement that's shaken the territory. [Shibani Mahtani](#), [Simon Denyer](#), [Tiffany Liang](#) and [Anna Kam report](#):** "Voters took to the polls in record numbers to cast ballots in the only fully democratic election in the Chinese territory, an early sign that they wanted to send a strong message to their government

and to the Communist Party in Beijing. Early results compiled by the South China Morning Post showed pro-democracy parties winning 278 of the first 344 seats to be declared, pro-Beijing parties taking 42, and independents 24. Many prominent figures in the protest movement won, and many leading pro-establishment figures were unseated. Pro-democrats look to be able to secure 12 of 18 district councils available in Hong Kong — before this vote, they did not have a majority in any. ... The turnout — 2.94 million, or more than 71 percent of the 4.13 million eligible voters — was more than double the 1.4 million who voted in local elections in 2015. Voter registration was also a record high, driven in part by 390,000 first-time voters.”

**-- The election's results will pressure Beijing to rethink its approach.** [Shibani, Simon and Tiffany report](#): “With this rebuke of its affiliates in the city, Beijing faces a choice among opening up politics as promised in Hong Kong’s mini-constitution, extending a crackdown on the pro-democracy protesters by the city’s police force and government, or trying to navigate a delicate middle path. Beijing can continue to dig in, but it would risk escalating and prolonging the conflict now that the electorate has spoken, said Ho-Fung Hung, an expert on the Chinese political economy and Hong Kong politics at the Johns Hopkins University’s School of Advanced International Studies. .... Reacting to the outcome on Monday, Chinese state media accused foreign forces, particularly the United States, of interfering. ... [Carrie] Lam, Hong Kong’s embattled leader, said in a statement Monday that her government respects the election results and acknowledged ‘various analyses and interpretations.’ ... Susan Shirk, a China expert and former official in the Clinton administration who is now at the University of California at San Diego, said it was possible



that Chinese leader Xi Jinping had not been receiving accurate information from lower-level officials on the public dissatisfaction in Hong Kong, despite months of protests.”

**-- A growing body of evidence from former detainees, human rights groups and reporters details the Chinese government's efforts to detain more than 1 million ethnic minorities in camps.**

[Hannah Knowles, Kim Bellware and Lateshia Beachum report:](#)

“Papers released Sunday pierce a culture of intense secrecy to add a new piece of corroboration: the government's own classified directives. Provided to the International Consortium of Investigative Journalists by an anonymous source, the documents lay bare a crackdown in Xinjiang that has sought to stamp out minority culture, language and religion — with a particular focus on the Muslim Uighurs, whom the government blames for regional unrest. A manual, the first of its kind to be made public, details the inner workings of the three-year-old detention camps, while four intelligence briefings illuminate the mass surveillance that identifies people for internment on merely the suspicion that they may cause trouble. ...

**“Camps are heavily secured and full of surveillance, according to the manual signed by Zhu Hailun, who used to be in charge of security in Xinjiang. ...** Some communication with outsiders is allowed to put family ‘at ease.’ Detainees are supposed to have phone conversations with relatives at least once a week and video chats every month.”

**-- A “phase two” trade deal between the U.S. and China is looking less likely.** [From Reuters:](#) “Officials in Beijing say they don’t anticipate sitting down to discuss a phase two deal before the U.S.

election, in part because they want to wait to see if Trump wins a second term. 'It's Trump who wants to sign these deals, not us. We can wait,' one Chinese official told Reuters.... Trump's main priority at the moment is to secure a big phase one announcement, locking in big-ticket Chinese purchases of U.S. agricultural goods that he can tout as an important win during his re-election campaign, according to a Trump administration official."

**-- Pope Francis called for the abolition of nuclear weapons while visiting Nagasaki and Hiroshima. [Akiko Kashiwagi and Chico Harlan](#) report:**

"Pope Francis called Sunday for a 'world without nuclear weapons,' which he said are 'immoral' for war or deterrence. 'We will be judged on this,' Francis said. In Hiroshima, the pope met with bomb survivors and spoke vividly of the 'black hole of death and destruction' atomic weapons could cause. Earlier, in a somber address in Nagasaki delivered in the driving rain, he spoke about the weapons in policy terms and expressed concern that a 'climate of distrust' was endangering international arms control efforts. ... Francis used the first papal trip to Japan since 1981 to emphasize one of his signature issues in cities that remain lasting symbols of atomic destruction (though both have been fully rebuilt in the decades since the 1945 attacks). ... After laying a wreath to the Nagasaki bombing's victims, the pope said the arms race creates a false sense of security, poisoning international relationships. He described nuclear weapons as wasteful and environmentally damaging. ... By saying that weapons shouldn't be held for deterrence — a stance he first outlined in 2017 — Francis has gone further than his predecessors. The only other pope to visit Japan, John Paul II, said during the Cold War that deterrence could be 'morally acceptable,' so long as it was a step



toward disarmament."

**-- A couple kidnapped by Islamists was rescued in the Philippines during a military operation. [Regine Cabato reports](#):**

"Allan Hyrons, 71, and Wilma Hyrons, 59, were abducted last month by Abu Sayyaf fighters at a beach resort the couple owned in the southern Philippines. They were rescued around 8 a.m. Monday in the island province of Sulu after a 20-minute firefight, said regional military commander Lt. Gen. Cirilito Sobejana, who attributed the operation's success to support from the public. ... The rescue of the Hyrons came at the end of a three-day operation, which the military said left six militant fighters dead."

**-- The White House asked Sen. Lindsey Graham (R-S.C.) to block the resolution that would have formally recognized Turkey's genocide of the Armenian people. [From Axios](#):**

Graham was leaving the Oval Office after he joined a meeting with Turkish President Recep Tayyip Erdogan when a senior White House staff asked him to object on the floor to the resolution that had passed the House to avoid upsetting Erdogan. "Graham confirmed this in a phone interview on Saturday. ... A White House legislative affairs official told Graham that Bob Menendez (D-N.J.) was going to bring up his Armenian genocide resolution and asked if Graham could 'please object.' 'I said sure,' Graham said. 'The only reason I did it is because he [Erdogan] was still in town. ... That would've been poor timing. I'm trying to salvage the relationship if possible.' Asked whether he felt uncomfortable blocking the Armenian genocide resolution, Graham replied: 'Yeah. ... I'm not going to object next time,' Graham added." The White House prodded Sen. David Perdue (R-Ga.) to object the

next time, and he obliged.

**-- Threatening more arrests, Iran restored Internet access in large parts of the country after a weeklong shutdown aimed at nationwide protests.**

**From the Journal:** "Tehran's response to the unrest indicates its willingness to resort to deadly force to push back against what it sees as U.S. attempts to weaken and eventually oust the country's leaders. It also comes amid a growing pushback in the region, where Iraqi and Lebanese protesters have railed against the influence of Iran and its local allies. ... Iranian authorities haven't released an official number of arrests, but state media said authorities had arrested 180 'ringleaders' and 'rioters' connected with such disparate groups as Islamic State, the MeK and Kurdish militants. Iran's internet blackout stemmed the sharing of videos and photos of the demonstrations, helping contain coverage to inside Iran, while making it difficult for those outside the country to assess the state of the protests and the brutal crackdown."

**-- Reuters chronicles the role Iran's leaders had in plotting the September attacks on the world's biggest oil processing facility in Saudi Arabia.**

"This account [was] described to Reuters by three officials familiar with the meetings and a fourth close to Iran's decision making ... These people said Iran's Supreme Leader Ayatollah Ali Khamenei approved the operation, but with strict conditions: Iranian forces must avoid hitting any civilians or Americans. ... The plan by Iranian military leaders to strike Saudi oil installations developed over several months, according to the official close to Iran's decision making. ... The official close to Iran's decision making said the group settled on the plan to attack Saudi Arabia's oil installations because it



could grab big headlines, inflict economic pain on an adversary and still deliver a strong message to Washington.”

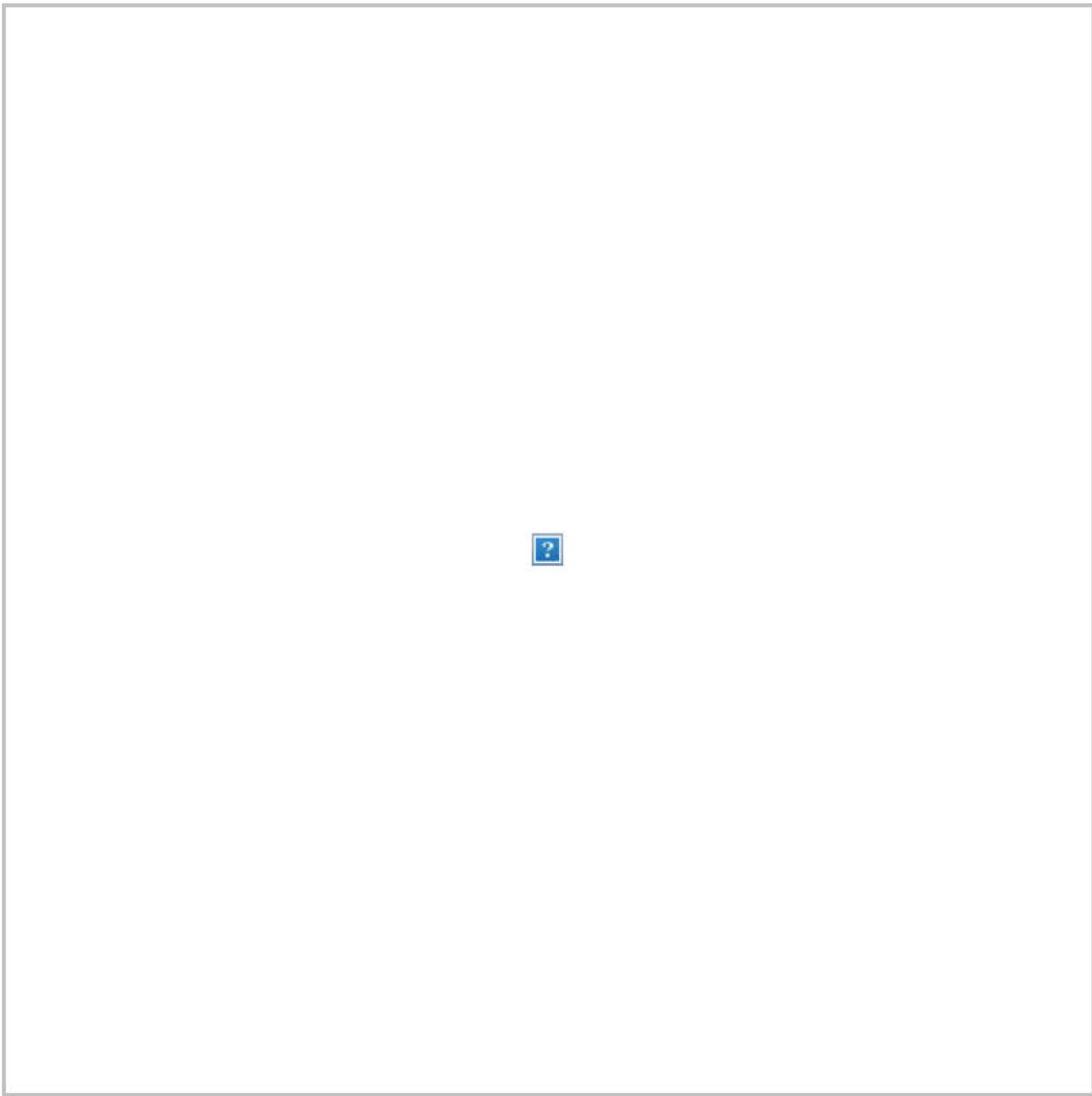
**-- Israeli Prime Minister Benjamin Netanyahu faces his first serious leadership challenge from his own party.** [Ruth Eglash reports](#): “The first public cracks in [Netanyahu]’s Likud party appeared over the weekend, days after the country’s attorney general indicted the longtime leader on charges of bribery and fraud in three criminal cases. The move comes after a year of political limbo that could send Israelis back to the polls for an unprecedented third general election in less than a year. Gideon Saar, Netanyahu’s most outspoken challenger within Likud, told an Israeli news show Saturday that it was time for the party to hold primaries to decide its leader and keep it from losing power. Saar, a 52-year-old former minister who returned to politics last year after a four-year hiatus, said he himself could end the political crisis. On Sunday, he submitted a request to the party’s central committee calling for a leadership vote to be held in the next three weeks — the deadline for the country’s lawmakers to form a long-elusive government before another general election must be called.”

**-- Uber lost its license to operate in London after authorities discovered that more than 14,000 trips were taken with uninsured drivers.** [From the Guardian](#): “Transport for London announced the decision not to renew the global ride-hailing firm’s licence at the end of a two-month probationary extension granted in September. Uber was then told it needed to address issues with checks on drivers, insurance and safety, but has apparently failed to satisfy the capital’s transport authorities. ... The decision is unlikely to see Uber cars

disappear from London, as the firm is expected to appeal, and can continue to operate pending the outcome, provided it launches official proceedings within 21 days.”

**-- Not only will England's Prince Andrew stand aside from all of his 230 patronages after a scandalous interview about his relationship with sex offender Jeffrey Epstein, he also won't be able to throw a birthday bash next year, under orders from the Queen. From the Guardian:** “The blanket move represents a key step in Buckingham Palace's attempts to limit the damage to the British monarchy from the prince's association with Epstein and his interview with BBC Two's Newsnight last weekend in which he was widely thought to have shown insufficient concern for Epstein's victims. ... **Andrew's withdrawal from public life coincides with Charles's wish for a more streamlined and cost-effective monarchy when he becomes king.** Sources close to the Prince of Wales, who is on an official visit to the Solomon Islands, denied reports that he was ‘angry and frustrated’ by the publicity his younger brother was attracting. It was also reported that the Queen has cancelled a planned 60th birthday party for Andrew in February and has downsized it to a small family gathering.”

**-- A small plane crashed in eastern Congo, killing at least 27 people. From Reuters:** “The propeller plane, which was operated by local company Busy Bee, crashed shortly after take-off en route to the city of Beni.”



Mike Bloomberg announces Democratic presidential run | Campaign 2020

## **2020 WATCH:**

**-- Former New York City mayor Mike Bloomberg officially announced his bid for the Democratic presidential nomination.**

[Michael Scherer reports](#): "Bloomberg has promised a disruptive campaign that could break spending records with a massive advertising buy aimed at states that vote in March and April. ...

Without offering specifics, the announcement video says he will push for the wealthy to pay more in taxes and to guarantee health care to



all Americans without removing private insurance from anyone who wants it. His campaign has made more than \$30 million in television advertising reservations to help introduce him as a candidate. The ads will start [today]. ... Bloomberg has also announced a \$100 million ad campaign to criticize Trump in key battleground states and a \$15 million voter registration effort in those same places. Those initial spending plans are already double the amount raised by the top fundraiser in the Democratic field, Sen. Bernie Sanders (I-Vt.), through September.”

**-- The billionaire’s news outlet, Bloomberg News, announced it will stop writing unsigned editorials about its founder and its reporters will avoid investigating him or his Democratic rivals as long as he stays in the race. [Paul Farhi reports](#):** “In an extraordinary memo to his newsroom on Sunday, Bloomberg News Editor in Chief John Micklethwait outlined steps designed to steer his reporters through a potential journalistic minefield: how to cover the campaign of the man who owns the news organization that is covering him. ... Bloomberg operates one of the world’s largest media organizations, with about 2,700 journalists in TV, radio, magazine and digital operations ... Micklethwait’s memo Sunday laid out what he called ‘basic principles’ in covering Bloomberg’s political aspirations. Most notably, he said his newsroom would continue ‘our tradition’ of not investigating Bloomberg, his family and his wealth, ‘and we will extend the same policy to his rivals in the Democratic primaries.’ A Bloomberg News spokeswoman, Kerri Chyka, also said the company won’t initiate stories about Bloomberg L.P., following a long-standing policy. The hands-off policy puts Bloomberg News in the awkward position of passing on such critical stories as Trump’s unfounded

allegations of corruption against [Biden] and his son Hunter. At the same time, Micklethwait said Bloomberg News would continue to investigate the Trump administration.”

**-- “America already elected a builder,” White House adviser Kellyanne Conway said of Bloomberg’s announcement, which uses the tagline “Rebuild America.”** “His new ad that he put millions behind is all unicorns and rainbows. Keep your health care if you’d like to — and if you don’t, I have something better. Rebuild America. We heard that from Obama-Biden,” Conway said. ([Politico](#))

**-- Biden is struggling in Iowa and his supporters blame a lack of enthusiasm and a spotty campaign operation.** [From the Times](#): “Voters at Mr. Biden’s events, along with county chairs and party strategists, characterize his on-the-ground organization as scattershot, visibly present in some counties but barely detectable in others. His events are often relatively small and sometimes subdued affairs, and in a state where enthusiasm can make or break a candidate on caucus night — a big part of caucusing centers on persuading friends and neighbors — Mr. Biden’s operation has found it difficult to build contagious excitement, these Democrats say. ... ‘This is prime political season in Iowa and most candidates are spending a good deal of time visiting Iowa,’ said Joey Norris, the Democratic chair in Montgomery County, Iowa, where [Pete] Buttigieg plans to campaign on Monday. ‘The Biden campaign has been notably absent.’”

**-- Sanders’s loyal voters could keep him in the race for months.** [From the Journal](#): “Sanders’s campaign has made it clear that to win the nomination, he would have to pull off an ambitious expansion of



the electorate. His campaign says it is banking on turning out a coalition of young, working-class and minority voters. But polls show the Vermont independent's base is more loyal than that of any other 2020 Democrat, and in interviews over the last four months, Mr. Sanders's supporters [have said] that they wouldn't support any other candidate as long as he is running. Those backers—and his massive fundraising—mean that, unlike many of his rivals, Mr. Sanders might not need a marquee win in an early state to stay in the presidential race for months.”

**-- Sen. Cory Booker keeps winning praise for his presidential campaign. What he's not winning is much support. [Cleve R.](#)**

[Wootson Jr. and Michael Scherer report](#): “As he struggles with low-single-digit polling and the prospect of missing the cut for next month's debate, Booker has become a symbol for the harsh reality of this year's nominating process. It is just not enough to win plaudits for performance, as he has after multiple events, or to execute a clear campaign strategy. In the shadow of Trump's potential reelection, Democratic voters have become focused on winning and are unforgiving with their doubts. Booker has sought to answer that concern by preaching the power of empathy. He appeals to white Iowa and New Hampshire voters by talking about the problems of inner cities and poverty. He has confronted Trump by explaining his compassion for his supporters. And unlike other campaigns that have pivoted on message and policy, he has made clear he will not change his strategy to win.”

**-- Sarah Sanders left Washington less than six months ago. Now the former White House press secretary has returned to**

**Arkansas in search for a new political role. [From the Times:](#)**

“‘There are two types of people who run for office,’ Ms. Sanders said over breakfast tacos at a diner in downtown Little Rock last week. ‘People that are called and people that just want to be a senator or governor. I feel like I’ve been called.’ ... As the daughter of Mike Huckabee, who served as governor from 1996 to 2007 and twice ran for president, she is seen as political royalty in Arkansas, and Mr. Trump himself urged her to run for governor when she left the West Wing. That job will open in 2023, when Gov. Asa Hutchinson’s term is up, and Ms. Sanders is giving every indication that she plans to run.

...

“In the 23 months that Ms. Sanders served as Mr. Trump’s chief spokeswoman, her battles with the White House press corps were epic. ... Ms. Sanders’s relationship with reporters reached a nadir in April after it was revealed that she had admitted under oath to investigators working for the special counsel, Robert S. Mueller III, that her claim at a press briefing that ‘countless members of the F.B.I.’ told her they had lost confidence in the bureau’s director, James B. Comey, was a ‘slip of the tongue’ that was not based on any facts. ... ‘I was attacked for everything, not just my performance,’ she said of her time in Washington. ‘I was called a fat soccer mom, my kids were threatened, my life was threatened. It was a lot. I hate harping on it, but to be in the position I’m in and to have Secret Service, that’s not normal.’ Ms. Sanders paused. ‘I don’t like being called a liar,’ she said.”

**-- Doctors who previously worked at the White House and those who are currently in touch with the White House said the**



**mysterious and unannounced visit Trump made to the hospital last weekend was highly unusual.** [From CNN's Dr. Sanjay Gupta:](#)

“Given that the White House had previously given plenty of advance notice about the President's past physical exams, last weekend's visit to Walter Reed reportedly took everyone by surprise, including much of the staff at the hospital itself. Whenever the President is planning a visit to Walter Reed, an institution-wide notice goes out, making staff aware of certain road and corridor closings. According to a person familiar with the matter, that didn't happen last weekend. **Also striking: the fact that the president's physician, Dr. Sean Conley, rode with Trump in the presidential motorcade. Typically, the doctor rides separately from the President for security reasons.**

A former White House doctor [said] it had never happened during their time there. ...

**"All tests Conley described could've been performed at the White House instead of the hospital.** Many blood tests require the patient to fast overnight and are thus performed first thing in the morning -- not in the middle of the afternoon, as apparently happened with the President. And remember, the President had these tests just nine months ago. One of the reasons doctors wait a year to order labs for a routine physical is to better assess the impact of medication and lifestyle changes over a consistent interval of time. There is no benefit to drawing the blood early, unless there is a concern about something. Finally, there is no such thing as a phased physical exam, as Trump had described it in his tweet from last weekend.”

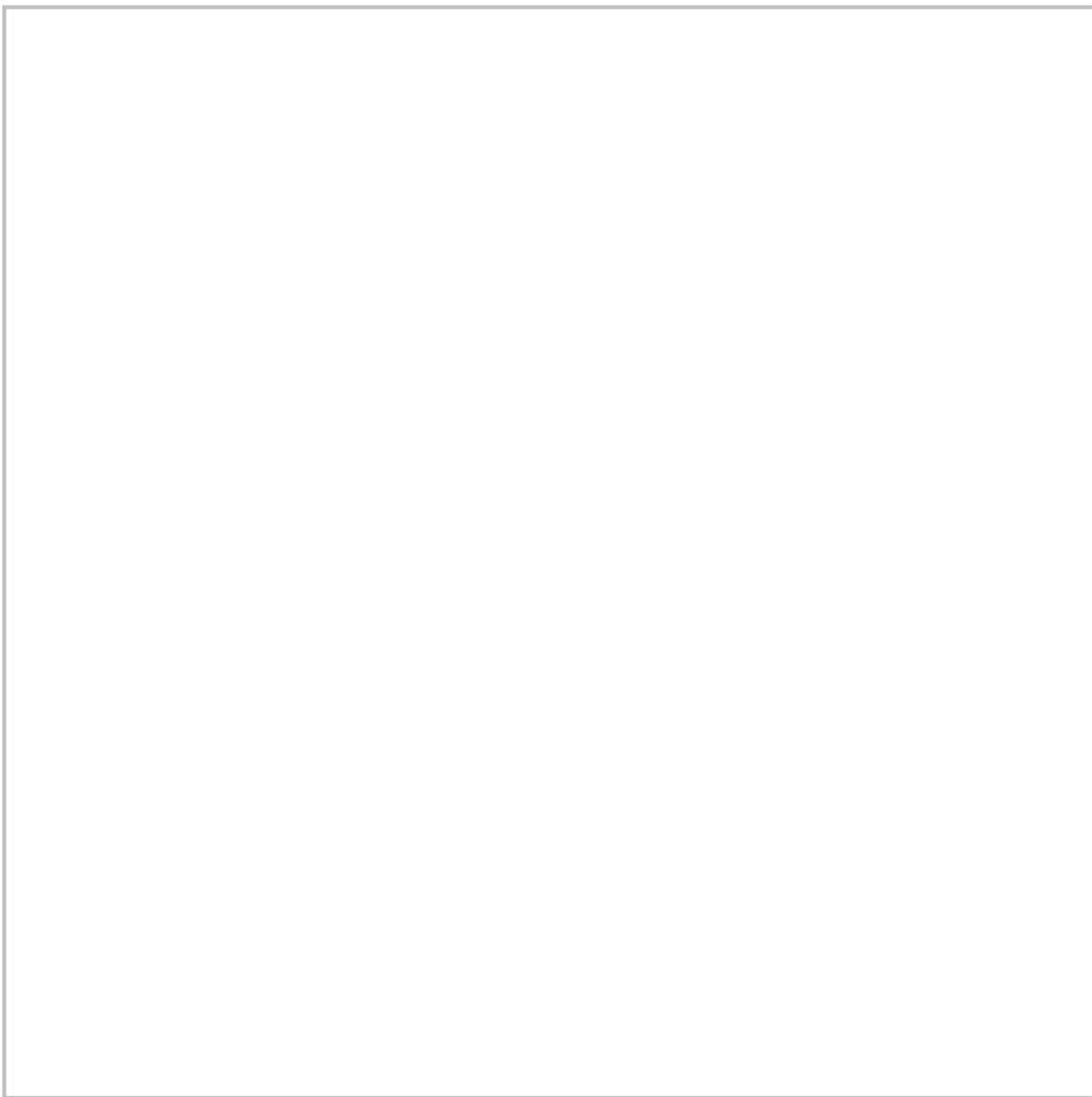
**-- Another health scare: Justice Ruth Bader Ginsburg was released from the hospital on Sunday after going in with chills**



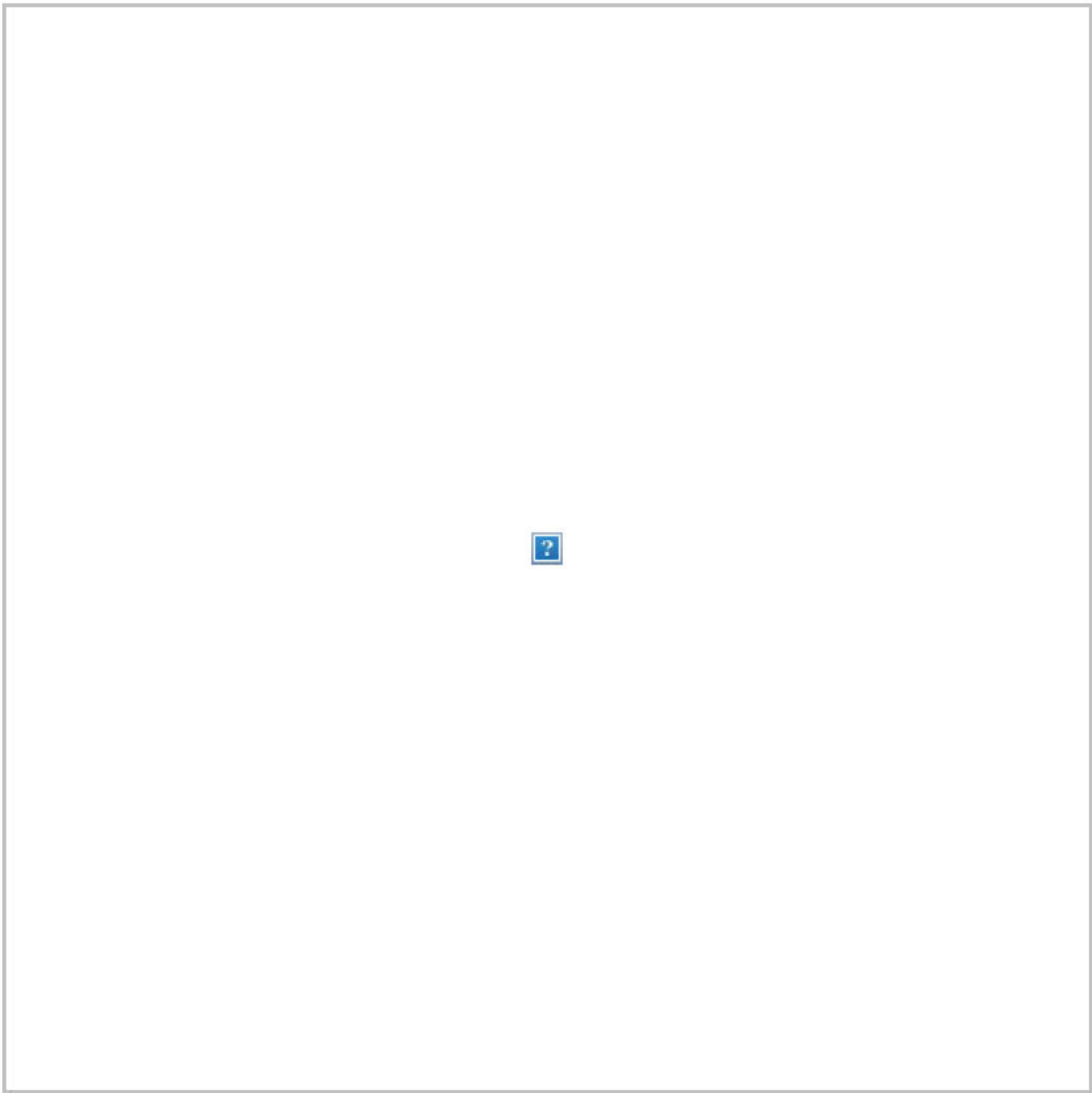
**and a fever.** [Robert Barnes reports](#): “The court announced in a news release Saturday evening that the 86-year-old had been seen at Sibley Memorial Hospital in Washington and then transferred to Johns Hopkins Hospital in Baltimore, where doctors were more familiar with her medical history. She was treated for a possible infection. 'With intravenous antibiotics and fluids, her symptoms have abated,' the court said in the Saturday release. The court provided no other details.”

### **SOCIAL MEDIA SPEED READ:**

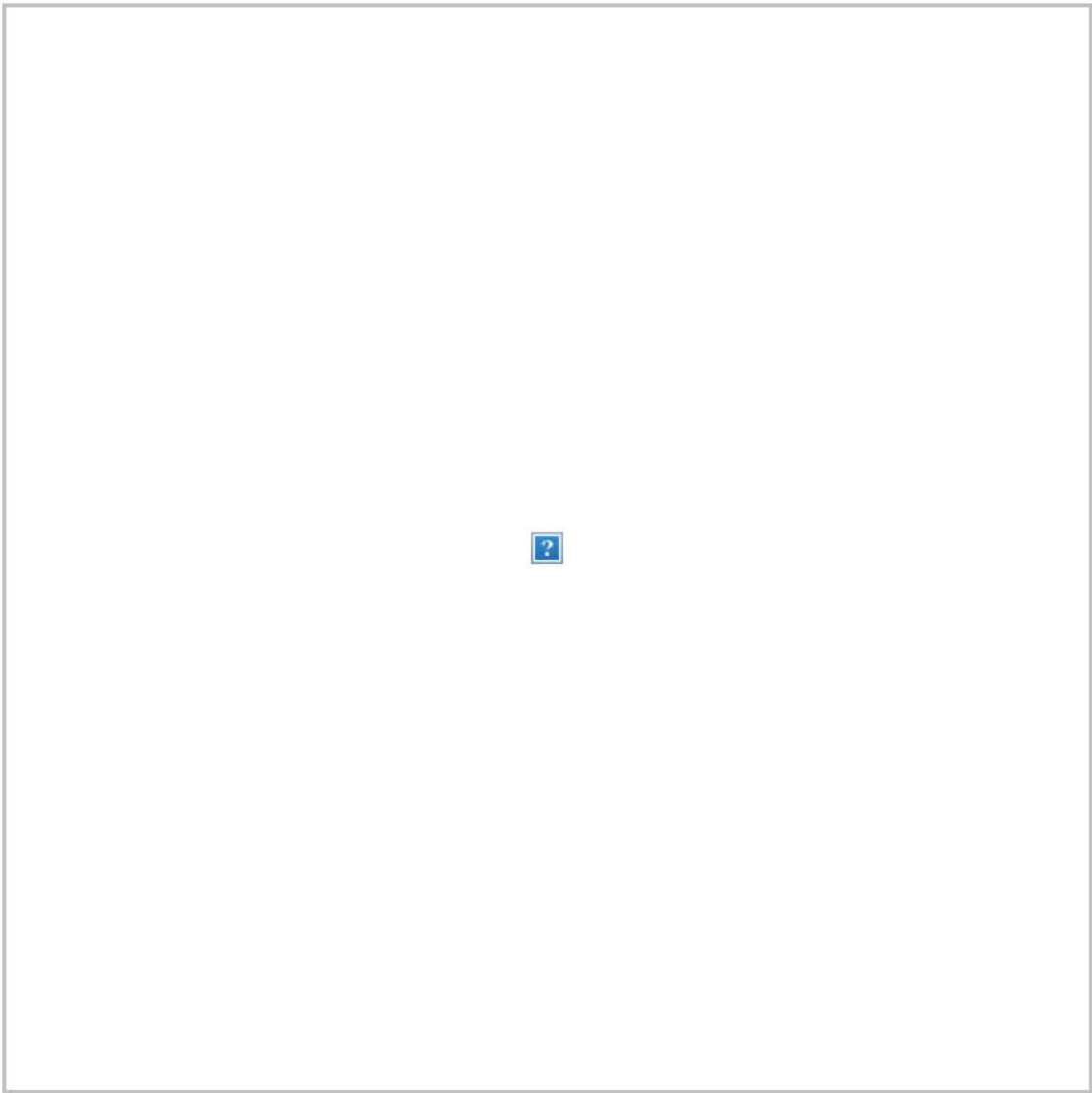
The Intelligence chairman reacted to The Post's scoop:



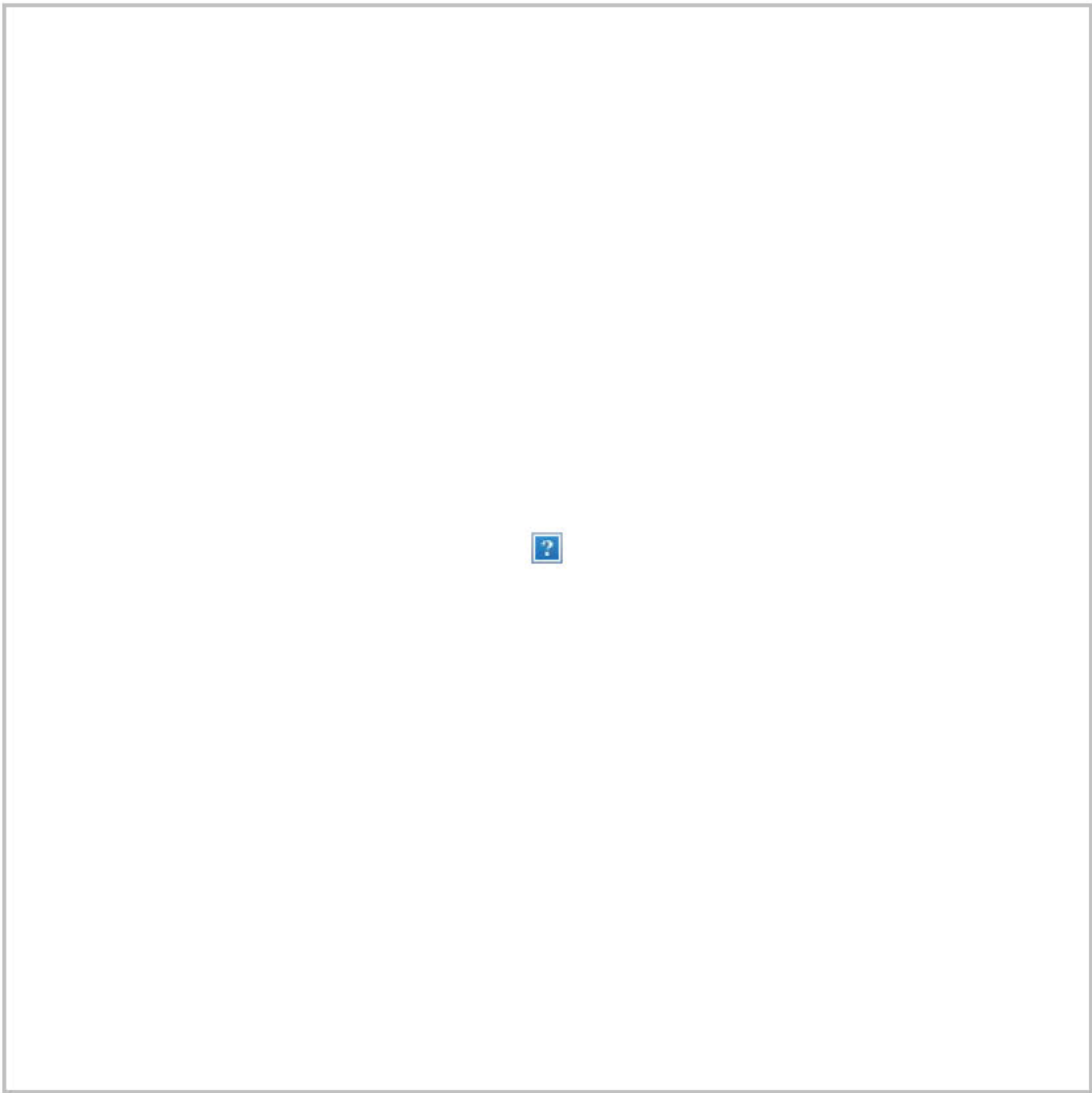
The Post's Shane Harris had this reminder after an assertion by Sen. John Neely Kennedy (R-La.) on "Fox News Sunday":



On Saturday, Rudy Giuliani made this comparison:

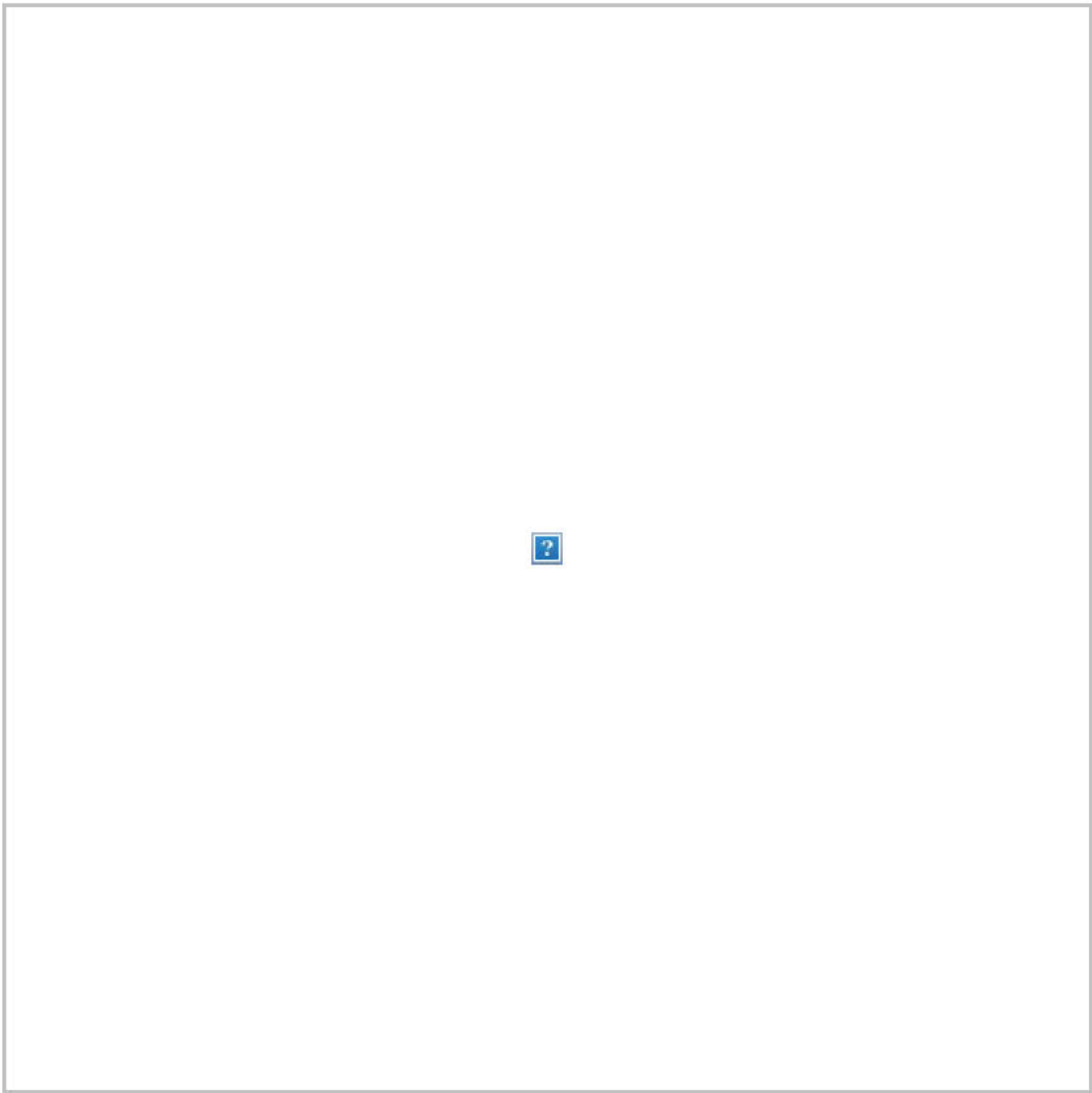


This scandal from a decade ago [seems so quaint](#):

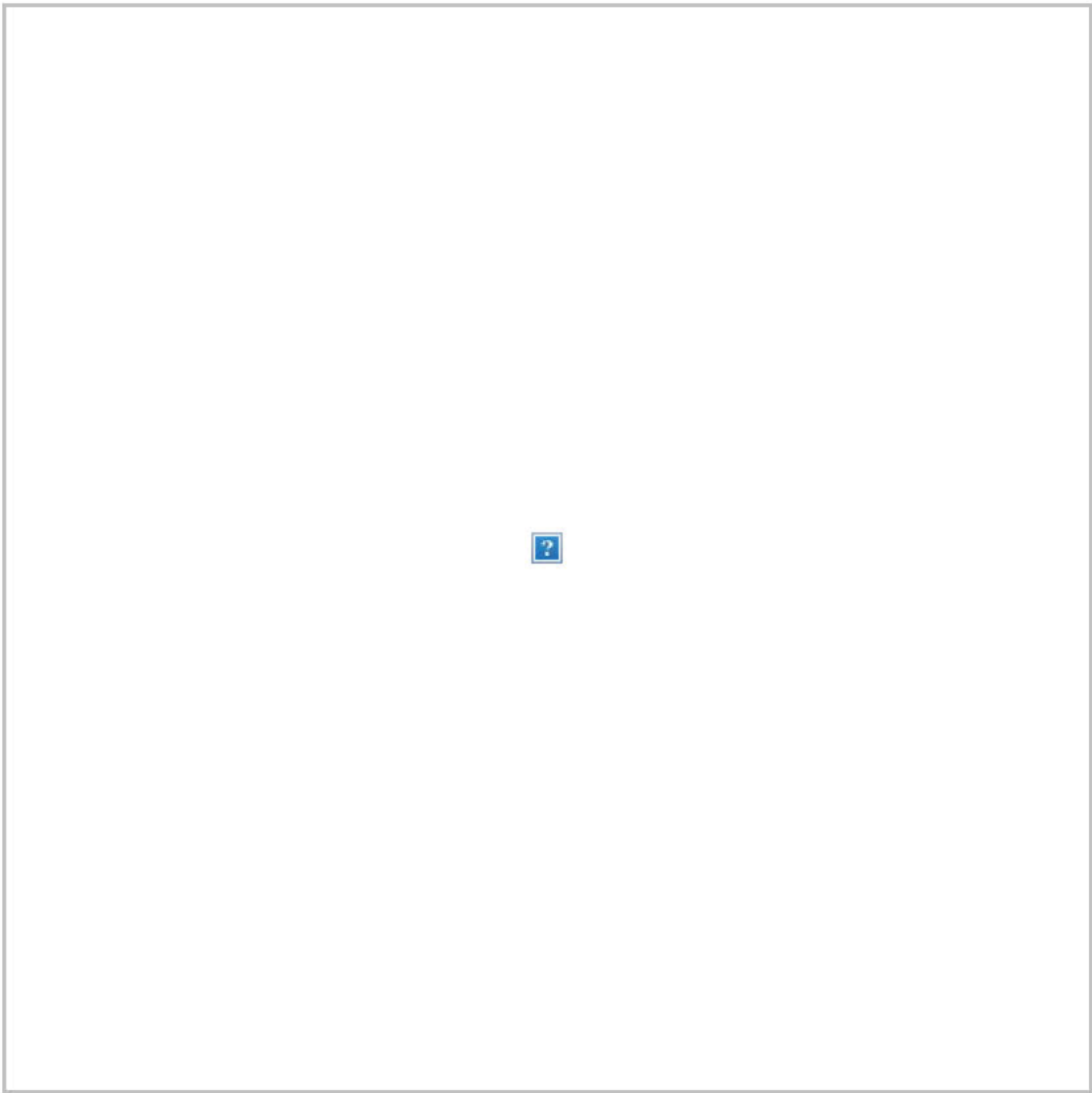


Bernie Sanders went out dancing:

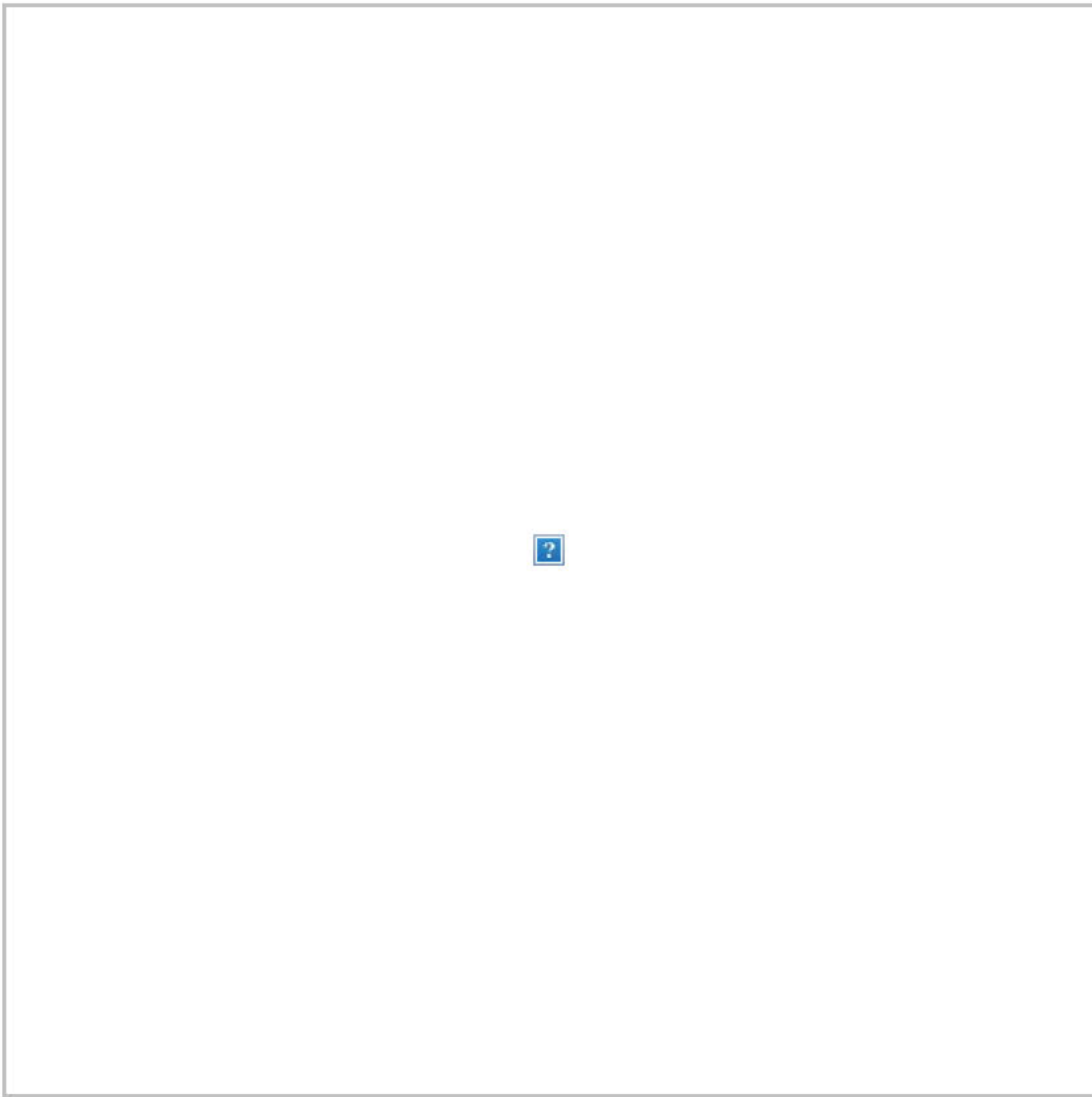




It's almost Thanksgiving, which means a pair of turkeys are having the time of their lives in D.C.:

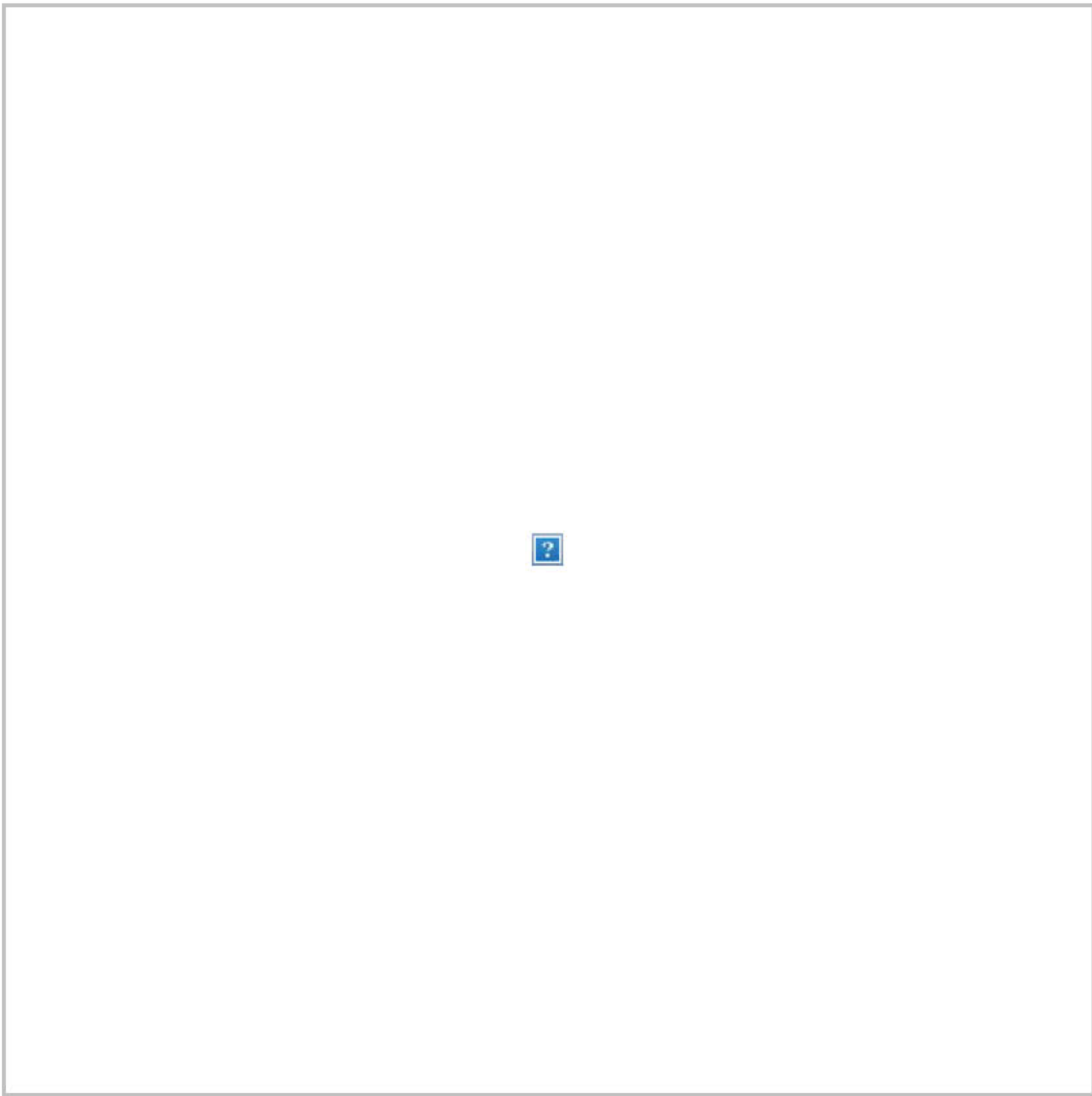


And border officials detained a shipment of illegal cold cuts, which led to this killer lede:



### **VIDEOS OF THE DAY:**

Taylor Swift broke Michael Jackson's record for winning the most American Music Awards of all time. Jackson won 24. Swift has 29 after last night:



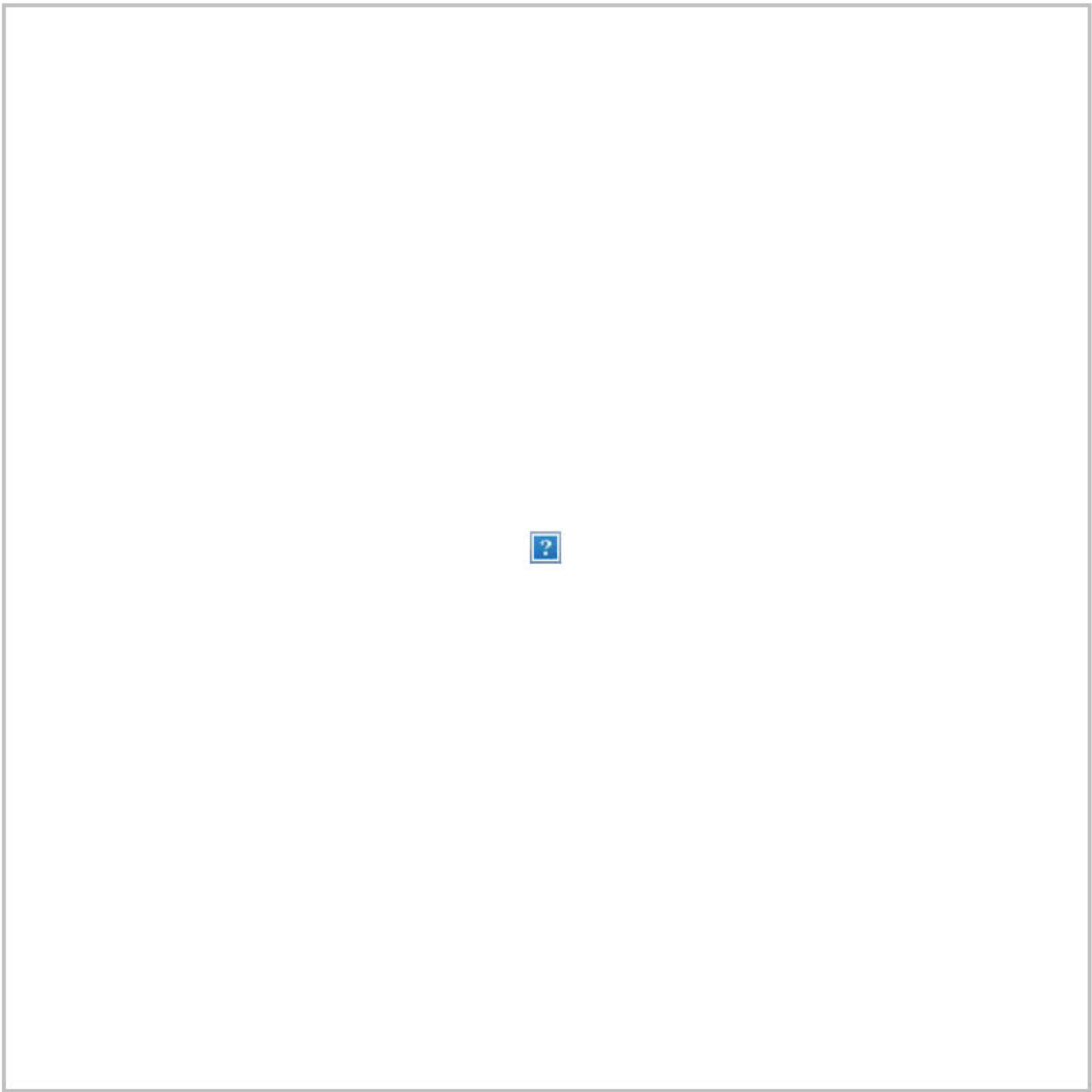
(Find the complete list of winners [here](#).)

“Saturday Night Live” spoofed last week’s Democratic debate:



“Weekend Update” pointed out that testimony on impeachment concluded in the House last week and “now the debate will shift to your house for Thanksgiving”:

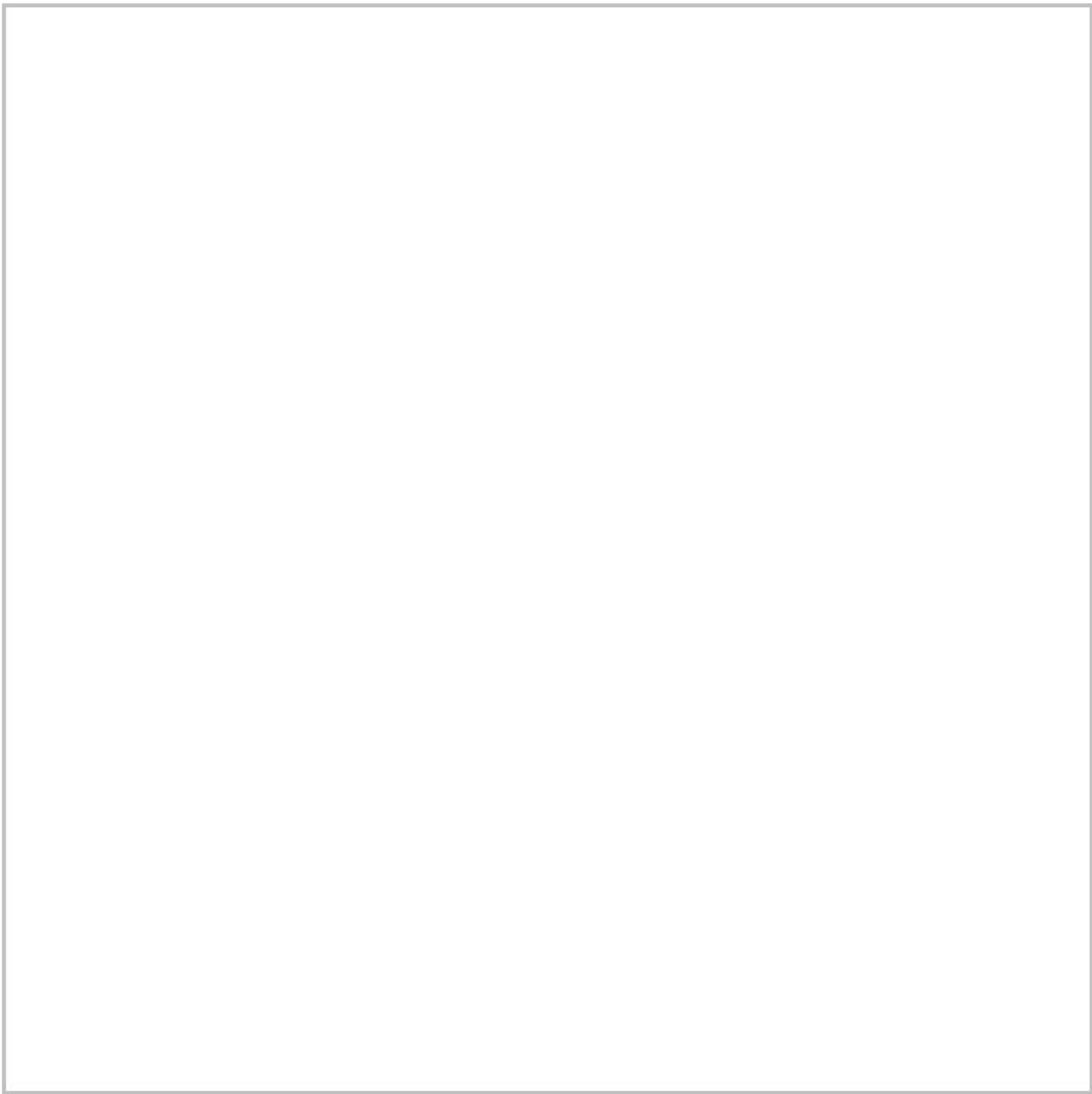




“The Daily Show” set out to investigate who will win the black vote in 2020:



And Trevor Noah interviewed Hillary and Chelsea Clinton:



You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)

---

©2019 The Washington Post | 1301 K St NW, Washington DC 20071



**From:** [The Washington Post](#)  
**To:** [achu@sunnyvale.ca.gov](mailto:achu@sunnyvale.ca.gov)  
**Subject:** The Daily 202: Ousted Navy secretary warns Trump that 'the rule of law is what sets us apart from our adversaries'  
**Date:** Monday, November 25, 2019 7:48:21 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

If you're having trouble reading this, [click here](#).

---

# The Daily 202

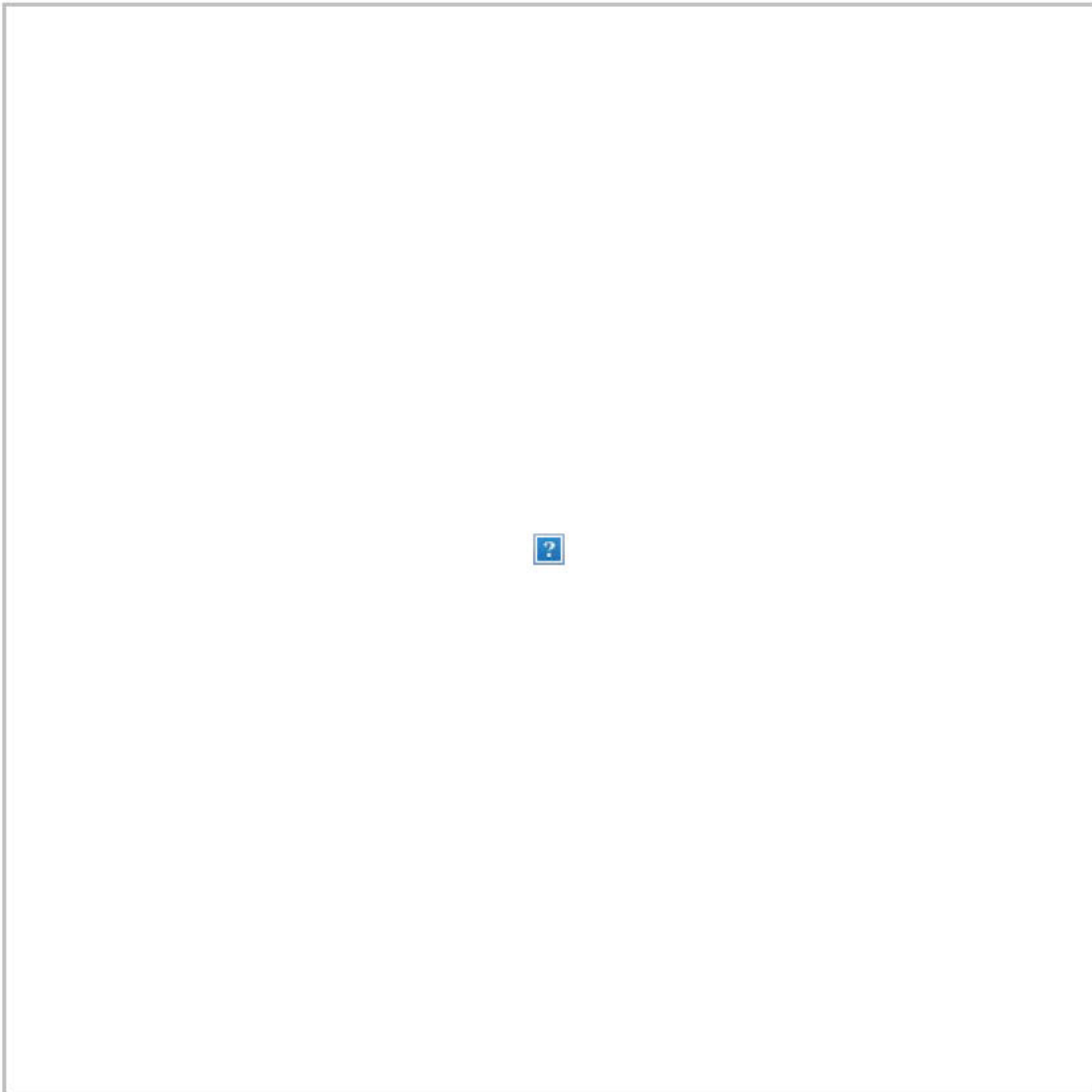


Share:  

 Listen to The Big Idea



## Ousted Navy secretary warns Trump that ‘the rule of law is what sets us apart from our adversaries’



Richard V. Spencer visits the Blue Angels at the squadron's hangar in Pensacola, Fla., on Nov. 5. He was forced out on Sunday as secretary of the Navy. (Timothy Schumaker/Navy/EPA-EFE/Rex)





**BY JAMES HOHMANN**

*with Mariana Alfaro*

**THE BIG IDEA: What makes America [exceptional](#) isn't any arsenal. It's moral authority.**

That's the upshot of Richard V. Spencer's Sunday letter to President Trump, acknowledging his "termination" as secretary of the navy. The messy circumstances surrounding Spencer's exit should not overshadow another damning resignation letter from another Trump appointee.

Spencer explained that he has strived over two-plus years on the job to ensure judicial proceedings are "fair, transparent and consistent," from ensigns to admirals. "Unfortunately, it has become apparent that in this respect, I no longer share the same understanding with the Commander in Chief who appointed me, in regards to the key principle of good order and discipline," he [wrote](#). "I cannot in good conscience obey an order that I believe violates the sacred oath I took in the presence of my family, my flag and my faith to support and defend the Constitution of the United States."

His language goes further than [Jim Mattis's letter](#) last December when he [resigned](#) as secretary of defense to protest Trump ordering U.S. troops to withdraw from Syria, but there are echoes. Both Spencer and Mattis said Trump deserves someone whose views are better aligned with his own.

**Spencer was ousted over his efforts to resolve a dispute between the White House and Navy commanders who wanted to strip**

**Edward Gallagher of the Trident pin that makes him a Navy SEAL.** Gallagher's was one of three cases in the military justice system that Trump intervened in 10 days ago. The chief petty officer was accused of committing war crimes during a 2017 deployment in Iraq. He was acquitted of murder but convicted in July of posing with the corpse of an Islamic State prisoner. Trump reinstated Gallagher's rank after he was demoted as part of his punishment. The president tweeted on Thursday that he doesn't want Gallagher, who has become a cause celebre on Fox News, kicked out of the SEALs.

**"The rule of law is what sets us apart from our adversaries," Spencer told Trump, offering a brief history lesson.** "Good order and discipline is what has enabled our victory against foreign tyranny time and again, from Captain Lawrence's famous order 'Don't Give up the Ship,' to the discipline and determination that propelled our flag to the highest point on Iwo Jima. The Constitution, and the Uniform Code of Military Justice, are the shields that set us apart, and the beacons that protect us all."

**-- Disdain for the rule of law has been a recurring feature of Trumpism.**

**-- Spencer, 65, served in the Marines as an aviator from 1976 to 1981, separating as a captain, before making a fortune on Wall Street.** He has been secretary of the Navy since the Senate confirmed him in August 2017. In his letter, he praised the troops who will soon miss their Thanksgiving dinners at home so that they can continue the watch beyond the curve of the horizon.

"As Secretary of the Navy, one of the most important responsibilities I

have to our people is to maintain good order and discipline throughout the ranks,” Spencer wrote. “I regard this as deadly serious business. The lives of our Sailors, Marines and civilian teammates quite literally depend on the professional execution of our many missions, and they also depend on the ongoing faith and support of the people we serve and the allies we serve alongside.”



Edward Gallagher and his wife, Andrea Gallagher, celebrate in July after a military jury in San Diego acquitted the Navy SEAL of premeditated murder in the killing of a wounded Islamic State captive under his care in Iraq. (Gregory Bull/AP)



**-- Pentagon spokespeople said Defense Secretary Mark Esper asked for Spencer's resignation after losing confidence in him.**

Their explanation is that Esper became "deeply troubled" when he discovered Spencer was backchanneling with the White House to offer a secret deal in which a review board would decide to let Gallagher keep his Trident pin – and affiliation with the SEALs – if Trump didn't directly meddle in the official peer-review process, thereby maintaining the appearance of independence.

**-- "Spencer had tried to find a compromise," David Ignatius reports in his column,** "after Trump tweeted Thursday, 'The Navy will NOT be taking away Warfighter and Navy Seal Eddie Gallagher's Trident Pin.' Spencer feared that a direct order from Trump to protect Gallagher, who is represented by two former partners of Trump's personal attorney Rudolph W. Giuliani, would be seen as subverting military justice. After that Trump tweet, Spencer cautioned acting White House Chief of Staff Mick Mulvaney that he would not overturn the planned SEAL peer review of Gallagher without a direct presidential order; he privately told associates that if such an order came, he might resign rather than carry it out. ...

**"It was a hold-your-nose solution,' said a source close to Spencer about his effort to broker an arrangement** that would allow Gallagher to retire at the end of November with his former rank, an honorable discharge and his Trident pin, as Trump wanted, but without direct presidential interference in the SEAL review process. **As so often happens with attempts to work with Trump's erratic demands, this one ended in disaster.** 'The president wants you to go,' Esper told Spencer on Sunday ... Esper then toed the White

House line and announced Spencer's dismissal. ...

**"Trump began lobbying Spencer to exempt Gallagher from Navy discipline back in March,** when he ordered the Navy secretary in an early-morning phone call to release Gallagher from the brig and give him more comfortable quarters. Presidential pressure has been relentless, ever since. ... While Gallagher is celebrated on Fox, current and former senior officers of the SEALs and other elite units told me this weekend that his case has little support within the community of Special Operations forces. One former SEAL commander noted that maintaining discipline among these elite units is so important that the SEAL peer-review panels have removed more than 150 Trident pins since 2011, or more than one a month."

**-- Trump now gets the outcome he wanted:** Esper's aides said he will let Gallagher keep his Trident pin without even the pretense of a review board. And Trump has rid himself of someone he came to disregard as disloyal, based on his threat to resign.

**-- Spencer joins a growing list of former Trump appointees who have spoken critically, to varying degrees, about the president after leaving his employ.** This includes, among others, [John Bolton](#), [Rex Tillerson](#), [John Kelly](#), [Tom Bossert](#), [Fiona Hill](#) and [Gary Cohn](#).

**-- Spencer took the sting out of this punch by vigorously denying well-sourced press reports on Saturday that he had threatened to resign.** In the version of his letter distributed to media outlets last night, the date "24 Nov 19" has been scrawled by hand on the top right of a letter that was reportedly drafted last week. The denial of accurate media accounts muddies the narrative around the



secretary's departure.

-- This appears to be the coda of a contentious chapter in a civilian-military relationship that has **grown increasingly fraught**.

Trump avoided military service by claiming bone spurs. He has stated that avoiding sexually transmitted infections while bedding models in New York during the 1970s was "my personal Vietnam." **Trump has insulted several war heroes**, as well as their families, and never apologized.



CONTENT FROM GOLDMAN SACHS 10,000 SMALL BUSINESSES

**What are the key issues impacting small**

## businesses?

Explore the “voice of small business” in our new infographic, which covers a range of small business perspectives on everything from the economy and healthcare to hiring and minimum wage.



Gen. Mark Milley arrives in Bahrain on Monday. (Idrees Ali/Reuters)

**-- The top U.S. military officer voiced public support today for Esper’s decision to allow Gallagher to remain a Navy SEAL and**

**to fire Spencer.** “As far as I’m concerned, it’s case closed now,” Gen. Mark Milley, chairman of the Joint Chiefs of Staff, told reporters traveling with him in the Middle East, [including Missy Ryan](#). “It’s time to move on and address the national security of the United States. ... Esper made decisions for good reasons that are within his power. I’ll support the secretary of defense in those decisions.”

**-- Senate Minority Leader Chuck Schumer (D-N.Y.) said he spoke by phone with Spencer on Sunday night:** “I told him he’s a patriot, that he served the Navy and the nation well and he will be missed,” Schumer said in a statement. “Secretary Spencer did the right thing and he should be proud of standing up to President Trump when he was wrong, something too many in this administration and the Republican Party are scared to do. Good order, discipline, and morale among the Armed Services must transcend politics, and Secretary Spencer’s commitment to these principles will not be forgotten.”

**-- Senate Armed Services Committee Chairman Jim Inhofe (R-Okla.) said Trump notified him personally that Spencer was being fired.** “Both Secretary Esper and President Trump deserve to have a leadership team who has their trust and confidence,” Inhofe said in a statement, adding: “It is no secret that I had my own disagreements with Secretary Spencer over the management of specific Navy programs.”

**-- Other lawmakers offered praise for Spencer:**



-- Trump **tweeted** that he will nominate Kenneth Braithwaite, a retired Navy rear admiral who is currently the ambassador to Norway, to be Spencer's replacement. Esper recommended him.

-- In an interview Sunday morning on "**Fox & Friends**," Gallagher said the Navy was only trying to take his Trident pin away as "retaliation" for Trump intervening on his behalf. "They could have taken my Trident at any time they wanted," he said on a show the president often watches. "Now they're trying to take it after the president restored my rank." Speaking of Rear Adm. Collin Green, who is in charge of the SEAL program as commander of the Naval



Special Warfare Command, Gallagher said: “What the admiral is doing is showing complete insubordination.”

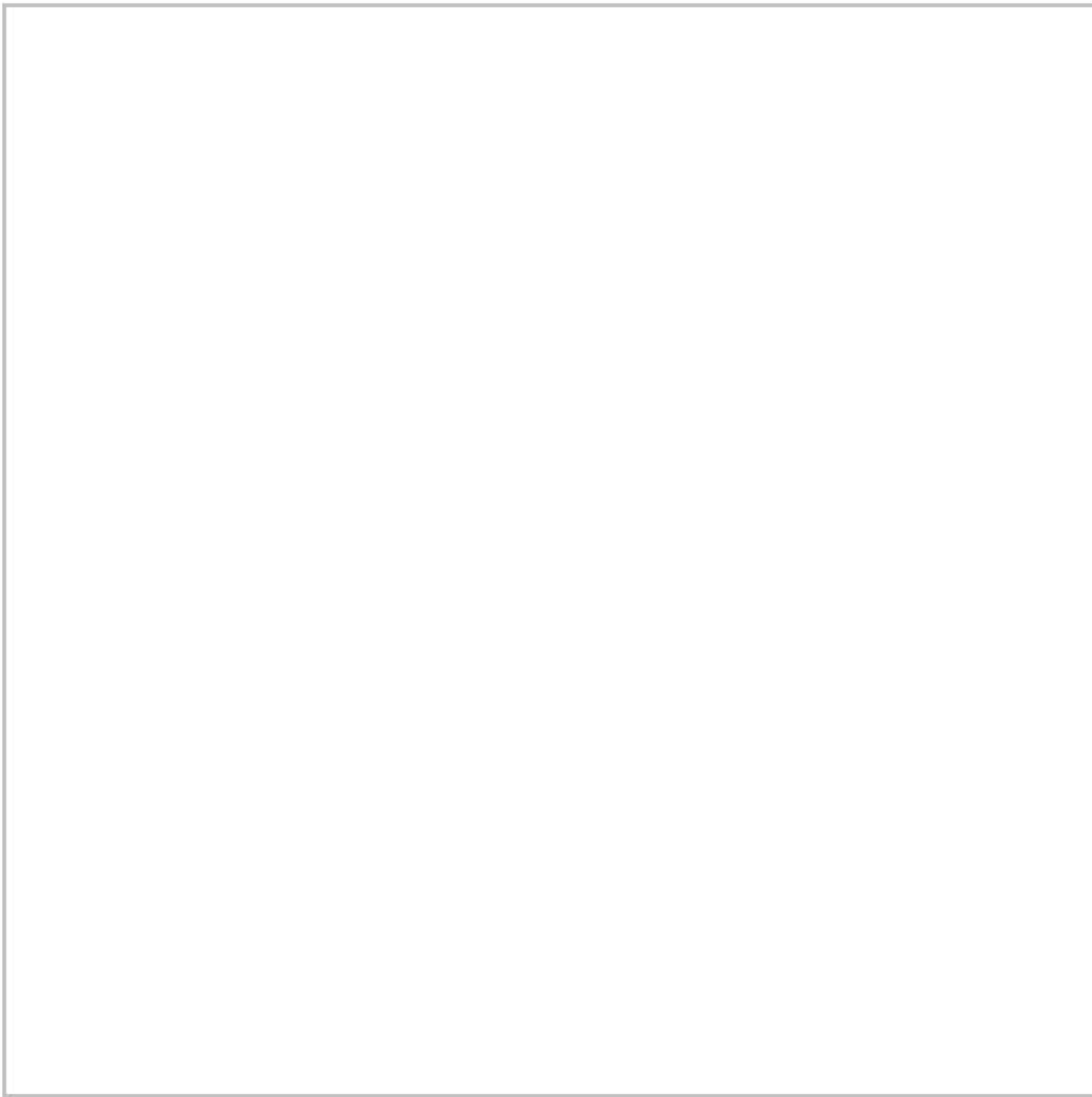
**-- Ray Mabus, who served as Navy secretary under Barack Obama, said on MSNBC that he's been stunned that a sailor on active duty is going on cable television to criticize his commanding officers.** “It's so dangerous for good order and discipline ... to get this politicized,” Mabus said Sunday [on MSNBC](#). “You simply cannot have good order and discipline. You simply cannot hold people accountable. You simply cannot have the elite fighting force if you allow things like this to happen. If you set this sort of precedent, then how do you tell the next SEAL that is up on charges not to go public, not to try to undermine their superiors, not to try to change a military judgment and make it a political one?”

**-- The Post's Editorial Board says Trump's intervention in the Gallagher case, including Spencer's ouster, [dishonors the troops who uphold American values](#):** “Restoring to service someone who was turned in by members of his unit who wouldn't tolerate his behavior sends precisely the wrong message. ... Most offensive is what Mr. Trump's actions say about his view of the military. ‘We train our boys to be killing machines, then prosecute them when they kill!’ he tweeted in October when he announced he would review these cases. Perhaps Mr. Trump has watched too many bad war movies, but if he were to consult with his military leaders or talk to the many fine men and women in uniform, they would tell him they are trained to engage in combat while following the laws of war and upholding the country's ideals.”



### **QUOTE OF THE DAY:**

A lawyer for Gallagher, Tim Parlatore, welcomed last night's news and expressed amazement at the turn of events that led to Spencer's ouster. "This case is bananas," he said. "Yes, you can quote that." (Ashley Parker and Dan Lamothe)



Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



Lawmakers react after a week of impeachment inquiry hearings

## **THE IMPEACHMENT INQUIRY:**

**-- A confidential White House review of Trump's decision to place a hold on military aid to Ukraine has turned up hundreds of documents that reveal extensive efforts to generate an after-the-fact justification for the decision and a debate over whether the delay was legal, according to three people familiar with the records. [Josh Dawsey, Carol D. Leonnig and Tom Hamburger scoop](#): "The research by the White House Counsel's Office ... includes early**



August email exchanges between acting chief of staff Mick Mulvaney and White House budget officials seeking to provide an explanation for withholding the funds after the president had already ordered a hold in mid-July on the nearly \$400 million in security assistance ... White House lawyers are expressing concern that the review has turned up some unflattering exchanges and facts that could at a minimum embarrass the president. ...

**“In the early August email exchanges, Mulvaney asked acting OMB director Russell Vought for an update on the legal rationale for withholding the aid and how much longer it could be delayed.**

Trump had made the decision the prior month without an assessment of the reasoning or legal justification ... Emails show Vought and OMB staffers arguing that withholding aid was legal, while officials at the National Security Council and State Department protested. OMB lawyers said that it was legal to withhold the aid, as long as they deemed it a ‘temporary’ hold ...

**“Mulvaney’s request for information came days after the White House Counsel’s Office was put on notice that an anonymous CIA official had made a complaint to the agency’s general counsel** about Trump’s July 25 call to [Volodymyr] Zelensky ... This official would later file a whistleblower complaint with the intelligence community’s inspector general ...

**“The document research has only exacerbated growing tension between [White House Counsel Pat] Cipollone and Mulvaney and their offices,** with Cipollone tightly controlling access to his findings, and Mulvaney’s aides complaining Cipollone isn’t briefing other White House officials or sharing important material they need to respond to



public inquiries ... The emails revealed by White House lawyers include some in which Mulvaney urges Vought to immediately focus on Ukraine's aid package, making clear it was a top priority for the administration. [Mulvaney's lawyer, Robert Driscoll, declined to comment.]

**“The legal office launched this fact-finding review of internal records in a protective mode**, both to determine what the records might reveal about internal administration conversations and also to help the White House produce a timeline for defending Trump's decision and his public comments. Along with examining documents, **the review has also involved interviewing some key White House officials** involved in handling Ukraine aid and dealing with complaints and concerns in the aftermath of the call between Trump and Zelensky. **Cipollone's office has focused closely on correspondence that could be subject to public records requests**, those which involve discussions between staff at the White House and at other agencies. Internal White House records are not subject to federal public records law, but messages that include officials at federal agencies are.”

**-- Follow the money: Lev Parnas and Igor Fruman, the Rudy Giuliani associates who have been indicted, tried to recruit a Ukrainian energy executive to join them in a proposed takeover of the state oil-and-gas company.** [From the Wall Street Journal](#): The two men described the “company's chief executive and [Marie Yovanovitch] as part of ‘this Soros cartel’ working against [Trump.] ‘You're a Republican, right?’ Andrew Favorov, the head of natural gas for state-run Naftogaz, recalled the men ... asking him, after their

reference to investor and Democratic donor George Soros. 'We want you to be our guy.' ... **Mr. Favorov described the efforts of Messrs. Fruman and Parnas to enlist his help in an effort to oust Naftogaz CEO Andriy Kobolyev. Naftogaz is the most important company in Ukraine, representing nearly 10% of the country's gross domestic product and supplying virtually all of the country's natural gas.** Mr. Favorov said he was bewildered by Messrs. Parnas and Fruman's pitch to stage a takeover of Naftogaz and put Mr. Favorov in place as CEO. On one hand, **the pair appeared to know little about the natural gas business**; on the other it was clear to him they had significant political connections. 'They don't teach you how to deal with this in business school,' Mr. Favorov said."

**-- So many potential conflicts: Giuliani also discussed representing a state-owned Ukrainian bank in a legal dispute over the summer, even as he publicly pressed Ukraine on behalf of Trump.** [From Bloomberg News](#): "Though he ultimately did not take on the client, the talks expose his enthusiasm for foreign business and his willingness to insert himself in matters rife with potential conflicts. In fact, **the Ukrainian bank is entangled in a legal dispute with its former owner who has ties to Ukraine's president and is the subject of a federal investigation in the U.S.** ... [Giuliani] said he was approached by lawyers for Privatbank seeking to recover assets linked to the previous owner. They wanted to know if Giuliani -- who had written tweets critical of the man -- could assist their civil suit, Giuliani confirmed by phone on Thursday."

**-- "What we still don't know about the Ukraine affair,"** [by deputy editorial page editor Jackson Diehl](#): "Let's start with the distinct



possibility that Trump's demand that [Zelensky] launch politicized investigations in exchange for military aid and a White House meeting was only the last of a series of quid pro quos he forced on Ukrainians." **Giuliani met with Zelensky's predecessor at least twice in 2017 as Ukraine's former chief prosecutor Yuri Lutsenko transferred an investigation into secret payments to Paul Manafort, effectively stalling it, and the U.S. released the sale of Javelin missiles to Ukraine.** "Let's see: a White House meeting and weapons ... for favorable actions on an investigation? There's no proof. But no wonder Trump complained to Zelensky in their July 25 phone call that 'I heard you had a prosecutor who was very good and he was shut down and that's really unfair.' One of Zelensky's first acts had been to fire Lutsenko.

**"The prosecutor has also been blamed for Trump's recall of [Yovanovitch]. But the full story behind her dismissal is still not known.** ... Trump began demanding Yovanovitch's removal a year earlier, after meeting with [Parnas and Fruman]. Why did Parnas and Fruman want the ambassador out? It's still not clear. ... One person who probably could shed light on this is Rick Perry.

**... According to testimony by U.S. Embassy staffer David Holmes, Perry used a meeting with Zelensky to give him a list of 'people he trusts' on energy matters. The Times reported that these included a couple of Texas businessmen whom Perry wanted appointed to the supervisory board of the Ukrainian state gas company.** That's the same company Parnas and Fruman were trying to deal with. ... We may eventually learn more about Ukraine from federal prosecutors in New York, who have already indicted Parnas and Fruman and are said to be looking at Giuliani. But you

have to wonder if Democrats are making a mistake by not pursuing these matters themselves.”

**-- Rep. Devin Nunes (R-Calif.), the ranking member on the House Intelligence Committee, said reports that he met with ex-Ukrainian prosecutor general Viktor Shokin in Vienna to obtain information about the Bidens were false. [Elise Viebeck and Felicia Sonmez report](#): “The allegation ... was made by the attorney for [Parnas]. ... On Fox News, Nunes declined to answer further questions about the accusation ... A person close to Shokin also has denied the claim. ... Nunes has also threatened to sue two of the news outlets that reported Parnas’s accusation. On Fox News, Nunes claimed that CNN and the Daily Beast were ‘likely conspiring to obstruct justice’ by basing their reporting on interviews with a lawyer for Parnas. ... House Armed Services Committee Chairman Adam Smith (D-Wash.) said Saturday that it was ‘quite likely, without question’ that Nunes would face an ethics investigation following media reports of a meeting with Shokin. ... Several other Democratic lawmakers have said that Parnas’s testimony could be helpful to impeachment investigators or that Nunes should face an ethics probe.”**

**-- Lordy, there are tapes? Parnas has provided the House Intelligence Committee with audio, photos and video recordings, but what these records show is unclear. [From ABC News](#): “[The] tapes were provided as part of that congressional subpoena issued to Parnas, and the former Giuliani ally also provided a number of documents both in English and Ukrainian to the committee in two separate productions ... However, some of the material sought by**



congressional investigators is already in possession of federal investigators within the Southern District of New York and thus held up from being turned over, according to sources familiar with the matter.”

**-- House Intelligence Committee Chairman Adam Schiff (D-Calif.) said his panel will press ahead with preparing its impeachment report, even though several key witnesses have refused to testify.** [Felicia Sonmez and Elise Vlebeck report](#): “In an interview on CNN’s ‘State of the Union,’ Schiff said the evidence against Trump is ‘already overwhelming,’ although he stopped short of saying whether he would support impeachment himself. ‘Yes, we’d love to have these witnesses come in,’ Schiff said. ‘But we’re not willing to simply allow them to wait us out — to stall this proceeding — when the facts are already overwhelming.’ ... Several key figures, including [Mulaney], Vice President Pence, Secretary of State Mike Pompeo, former national security adviser John Bolton and [Giuliani], have declined to cooperate with the impeachment inquiry. A federal judge is expected to rule [today] on whether [former White House counsel Don McGahn] must testify under subpoena. ...

**"Schiff said Sunday that time is of the essence and that Democrats will continue to investigate even after they have submitted their report to the House Judiciary Committee. ...** 'The investigation isn't going to end,' he said, adding that 'we may have other depositions and hearings to do.' He took particular aim at Bolton, arguing that the former national security adviser will have to explain why he chose to give his account of events 'in a book' rather than show the 'courage' that Fiona Hill, the former National Security



Council Russia adviser, did in testifying before lawmakers last week. Schiff declined to say how long it might take impeachment investigators to finish their report, saying only that ‘we’ll take the time that’s necessary.’”

**-- Amid tensions between the Trump administration and Democrats, Pelosi and Treasury Secretary Steve Mnuchin must work out a spending deal. Luckily, they appear to maintain a good rapport.** [From the Journal](#): “While the Office of Management and Budget leads the administration’s efforts on spending, Mr. Mnuchin has emerged as the public face of the administration on Capitol Hill in the spending talks, which took a positive turn this weekend even as [impeachment strains](#) the broader relationship between the two branches. Mr. Mnuchin’s role speaks to the rapport and goodwill he has built up with lawmakers and, in particular, Mrs. Pelosi ... Mrs. Pelosi has clashed with two of the administration’s other top negotiators, [Mulaney] and [Vought], with whom she refused to negotiate last summer’s budget deal. ... **House Budget Committee Chairman John Yarmuth (D., Ky.) said ... that Mr. Mulvaney would normally play a more visible role in the negotiations, ‘but I think Mick, he has other distractions.’”**





Record numbers vote in Hong Kong elections

## **THE NEW WORLD ORDER:**

**-- Hong Kong's pro-democracy parties swept aside the pro-Beijing establishment during local council elections in a significant endorsement of the protest movement that's shaken the territory. [Shibani Mahtani](#), [Simon Denyer](#), [Tiffany Liang](#) and [Anna Kam report](#):** "Voters took to the polls in record numbers to cast ballots in the only fully democratic election in the Chinese territory, an early sign that they wanted to send a strong message to their government

and to the Communist Party in Beijing. Early results compiled by the South China Morning Post showed pro-democracy parties winning 278 of the first 344 seats to be declared, pro-Beijing parties taking 42, and independents 24. Many prominent figures in the protest movement won, and many leading pro-establishment figures were unseated. Pro-democrats look to be able to secure 12 of 18 district councils available in Hong Kong — before this vote, they did not have a majority in any. ... The turnout — 2.94 million, or more than 71 percent of the 4.13 million eligible voters — was more than double the 1.4 million who voted in local elections in 2015. Voter registration was also a record high, driven in part by 390,000 first-time voters.”

**-- The election's results will pressure Beijing to rethink its approach.** [Shibani, Simon and Tiffany report](#): “With this rebuke of its affiliates in the city, Beijing faces a choice among opening up politics as promised in Hong Kong’s mini-constitution, extending a crackdown on the pro-democracy protesters by the city’s police force and government, or trying to navigate a delicate middle path. Beijing can continue to dig in, but it would risk escalating and prolonging the conflict now that the electorate has spoken, said Ho-Fung Hung, an expert on the Chinese political economy and Hong Kong politics at the Johns Hopkins University’s School of Advanced International Studies. .... Reacting to the outcome on Monday, Chinese state media accused foreign forces, particularly the United States, of interfering. ... [Carrie] Lam, Hong Kong’s embattled leader, said in a statement Monday that her government respects the election results and acknowledged ‘various analyses and interpretations.’ ... Susan Shirk, a China expert and former official in the Clinton administration who is now at the University of California at San Diego, said it was possible



that Chinese leader Xi Jinping had not been receiving accurate information from lower-level officials on the public dissatisfaction in Hong Kong, despite months of protests.”

**-- A growing body of evidence from former detainees, human rights groups and reporters details the Chinese government's efforts to detain more than 1 million ethnic minorities in camps.**

[Hannah Knowles, Kim Bellware and Lateshia Beachum report:](#)

“Papers released Sunday pierce a culture of intense secrecy to add a new piece of corroboration: the government's own classified directives. Provided to the International Consortium of Investigative Journalists by an anonymous source, the documents lay bare a crackdown in Xinjiang that has sought to stamp out minority culture, language and religion — with a particular focus on the Muslim Uighurs, whom the government blames for regional unrest. A manual, the first of its kind to be made public, details the inner workings of the three-year-old detention camps, while four intelligence briefings illuminate the mass surveillance that identifies people for internment on merely the suspicion that they may cause trouble. ...

**“Camps are heavily secured and full of surveillance, according to the manual signed by Zhu Hailun, who used to be in charge of security in Xinjiang. ...** Some communication with outsiders is allowed to put family ‘at ease.’ Detainees are supposed to have phone conversations with relatives at least once a week and video chats every month.”

**-- A “phase two” trade deal between the U.S. and China is looking less likely.** [From Reuters:](#) “Officials in Beijing say they don’t anticipate sitting down to discuss a phase two deal before the U.S.

election, in part because they want to wait to see if Trump wins a second term. 'It's Trump who wants to sign these deals, not us. We can wait,' one Chinese official told Reuters.... Trump's main priority at the moment is to secure a big phase one announcement, locking in big-ticket Chinese purchases of U.S. agricultural goods that he can tout as an important win during his re-election campaign, according to a Trump administration official."

**-- Pope Francis called for the abolition of nuclear weapons while visiting Nagasaki and Hiroshima. [Akiko Kashiwagi and Chico Harlan report](#):**

"Pope Francis called Sunday for a 'world without nuclear weapons,' which he said are 'immoral' for war or deterrence. 'We will be judged on this,' Francis said. In Hiroshima, the pope met with bomb survivors and spoke vividly of the 'black hole of death and destruction' atomic weapons could cause. Earlier, in a somber address in Nagasaki delivered in the driving rain, he spoke about the weapons in policy terms and expressed concern that a 'climate of distrust' was endangering international arms control efforts. ... Francis used the first papal trip to Japan since 1981 to emphasize one of his signature issues in cities that remain lasting symbols of atomic destruction (though both have been fully rebuilt in the decades since the 1945 attacks). ... After laying a wreath to the Nagasaki bombing's victims, the pope said the arms race creates a false sense of security, poisoning international relationships. He described nuclear weapons as wasteful and environmentally damaging. ... By saying that weapons shouldn't be held for deterrence — a stance he first outlined in 2017 — Francis has gone further than his predecessors. The only other pope to visit Japan, John Paul II, said during the Cold War that deterrence could be 'morally acceptable,' so long as it was a step



toward disarmament."

**-- A couple kidnapped by Islamists was rescued in the Philippines during a military operation. [Regine Cabato reports](#):**

"Allan Hyrons, 71, and Wilma Hyrons, 59, were abducted last month by Abu Sayyaf fighters at a beach resort the couple owned in the southern Philippines. They were rescued around 8 a.m. Monday in the island province of Sulu after a 20-minute firefight, said regional military commander Lt. Gen. Cirilito Sobejana, who attributed the operation's success to support from the public. ... The rescue of the Hyrons came at the end of a three-day operation, which the military said left six militant fighters dead."

**-- The White House asked Sen. Lindsey Graham (R-S.C.) to block the resolution that would have formally recognized Turkey's genocide of the Armenian people. [From Axios](#):** Graham was leaving the Oval Office after he joined a meeting with Turkish President Recep Tayyip Erdogan when a senior White House staff asked him to object on the floor to the resolution that had passed the House to avoid upsetting Erdogan. "Graham confirmed this in a phone interview on Saturday. ... A White House legislative affairs official told Graham that Bob Menendez (D-N.J.) was going to bring up his Armenian genocide resolution and asked if Graham could 'please object.' 'I said sure,' Graham said. 'The only reason I did it is because he [Erdogan] was still in town. ... That would've been poor timing. I'm trying to salvage the relationship if possible.' Asked whether he felt uncomfortable blocking the Armenian genocide resolution, Graham replied: 'Yeah. ... I'm not going to object next time,' Graham added." The White House prodded Sen. David Perdue (R-Ga.) to object the

next time, and he obliged.

**-- Threatening more arrests, Iran restored Internet access in large parts of the country after a weeklong shutdown aimed at nationwide protests.**

**From the Journal:** “Tehran’s response to the unrest indicates its willingness to resort to deadly force to push back against what it sees as U.S. attempts to weaken and eventually oust the country’s leaders. It also comes amid a growing pushback in the region, where Iraqi and Lebanese protesters have railed against the influence of Iran and its local allies. ... Iranian authorities haven’t released an official number of arrests, but state media said authorities had arrested 180 ‘ringleaders’ and ‘rioters’ connected with such disparate groups as Islamic State, the MeK and Kurdish militants. Iran’s internet blackout stemmed the sharing of videos and photos of the demonstrations, helping contain coverage to inside Iran, while making it difficult for those outside the country to assess the state of the protests and the brutal crackdown.”

**-- Reuters chronicles the role Iran’s leaders had in plotting the September attacks on the world’s biggest oil processing facility in Saudi Arabia.**

“This account [was] described to Reuters by three officials familiar with the meetings and a fourth close to Iran’s decision making ... These people said Iran’s Supreme Leader Ayatollah Ali Khamenei approved the operation, but with strict conditions: Iranian forces must avoid hitting any civilians or Americans. ... The plan by Iranian military leaders to strike Saudi oil installations developed over several months, according to the official close to Iran’s decision making. ... The official close to Iran’s decision making said the group settled on the plan to attack Saudi Arabia’s oil installations because it



could grab big headlines, inflict economic pain on an adversary and still deliver a strong message to Washington.”

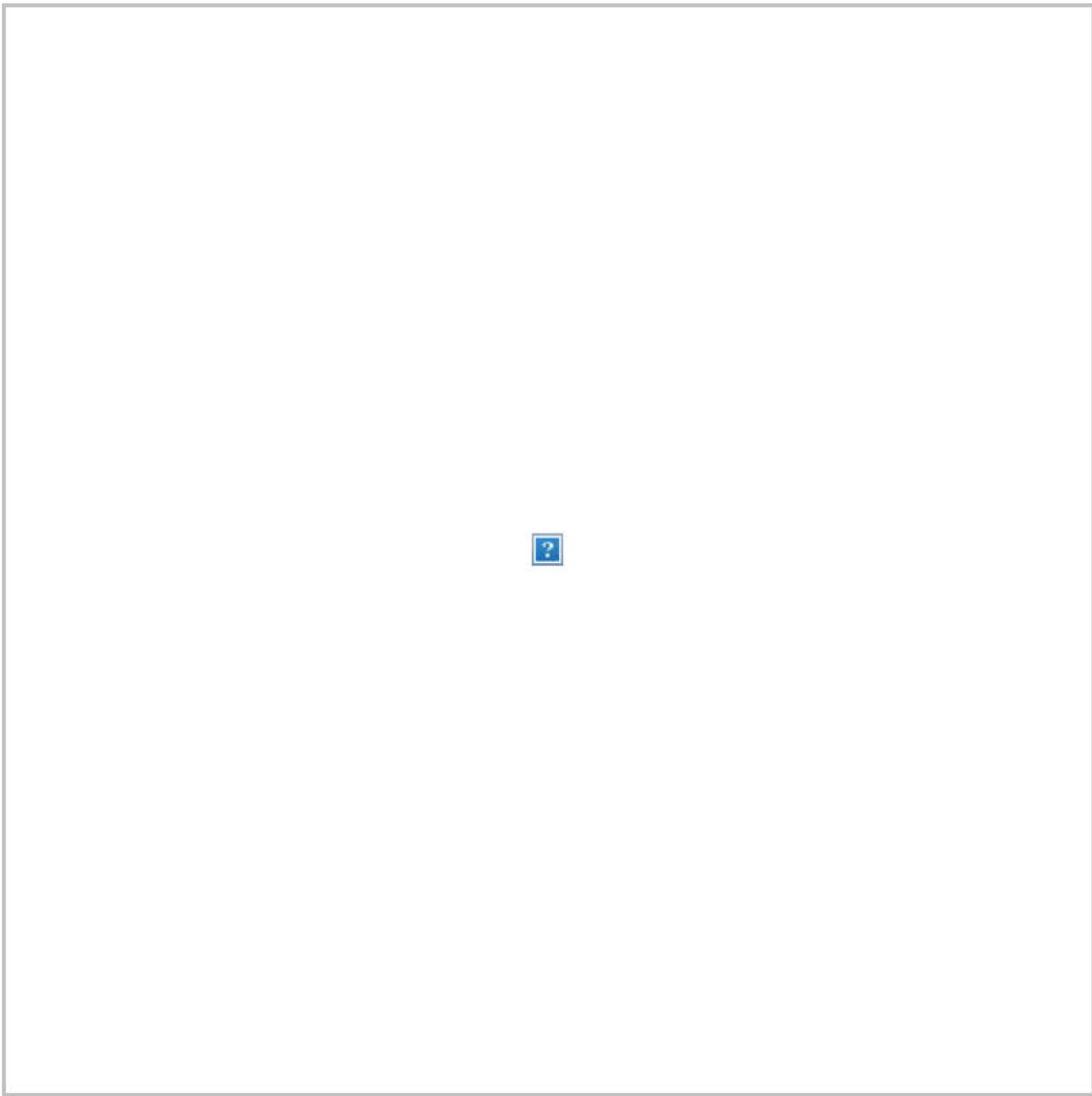
**-- Israeli Prime Minister Benjamin Netanyahu faces his first serious leadership challenge from his own party.** [Ruth Eglash reports](#): “The first public cracks in [Netanyahu]’s Likud party appeared over the weekend, days after the country’s attorney general indicted the longtime leader on charges of bribery and fraud in three criminal cases. The move comes after a year of political limbo that could send Israelis back to the polls for an unprecedented third general election in less than a year. Gideon Saar, Netanyahu’s most outspoken challenger within Likud, told an Israeli news show Saturday that it was time for the party to hold primaries to decide its leader and keep it from losing power. Saar, a 52-year-old former minister who returned to politics last year after a four-year hiatus, said he himself could end the political crisis. On Sunday, he submitted a request to the party’s central committee calling for a leadership vote to be held in the next three weeks — the deadline for the country’s lawmakers to form a long-elusive government before another general election must be called.”

**-- Uber lost its license to operate in London after authorities discovered that more than 14,000 trips were taken with uninsured drivers.** [From the Guardian](#): “Transport for London announced the decision not to renew the global ride-hailing firm’s licence at the end of a two-month probationary extension granted in September. Uber was then told it needed to address issues with checks on drivers, insurance and safety, but has apparently failed to satisfy the capital’s transport authorities. ... The decision is unlikely to see Uber cars

disappear from London, as the firm is expected to appeal, and can continue to operate pending the outcome, provided it launches official proceedings within 21 days.”

**-- Not only will England's Prince Andrew stand aside from all of his 230 patronages after a scandalous interview about his relationship with sex offender Jeffrey Epstein, he also won't be able to throw a birthday bash next year, under orders from the Queen. From the Guardian:** “The blanket move represents a key step in Buckingham Palace's attempts to limit the damage to the British monarchy from the prince's association with Epstein and his interview with BBC Two's Newsnight last weekend in which he was widely thought to have shown insufficient concern for Epstein's victims. ... **Andrew's withdrawal from public life coincides with Charles's wish for a more streamlined and cost-effective monarchy when he becomes king.** Sources close to the Prince of Wales, who is on an official visit to the Solomon Islands, denied reports that he was ‘angry and frustrated’ by the publicity his younger brother was attracting. It was also reported that the Queen has cancelled a planned 60th birthday party for Andrew in February and has downsized it to a small family gathering.”

**-- A small plane crashed in eastern Congo, killing at least 27 people. From Reuters:** “The propeller plane, which was operated by local company Busy Bee, crashed shortly after take-off en route to the city of Beni.”



Mike Bloomberg announces Democratic presidential run | Campaign 2020

## **2020 WATCH:**

**-- Former New York City mayor Mike Bloomberg officially announced his bid for the Democratic presidential nomination.**

[Michael Scherer reports](#): "Bloomberg has promised a disruptive campaign that could break spending records with a massive advertising buy aimed at states that vote in March and April. ...

Without offering specifics, the announcement video says he will push for the wealthy to pay more in taxes and to guarantee health care to



all Americans without removing private insurance from anyone who wants it. His campaign has made more than \$30 million in television advertising reservations to help introduce him as a candidate. The ads will start [today]. ... Bloomberg has also announced a \$100 million ad campaign to criticize Trump in key battleground states and a \$15 million voter registration effort in those same places. Those initial spending plans are already double the amount raised by the top fundraiser in the Democratic field, Sen. Bernie Sanders (I-Vt.), through September.”

**-- The billionaire’s news outlet, Bloomberg News, announced it will stop writing unsigned editorials about its founder and its reporters will avoid investigating him or his Democratic rivals as long as he stays in the race. [Paul Farhi reports](#):** “In an extraordinary memo to his newsroom on Sunday, Bloomberg News Editor in Chief John Micklethwait outlined steps designed to steer his reporters through a potential journalistic minefield: how to cover the campaign of the man who owns the news organization that is covering him. ... Bloomberg operates one of the world’s largest media organizations, with about 2,700 journalists in TV, radio, magazine and digital operations ... Micklethwait’s memo Sunday laid out what he called ‘basic principles’ in covering Bloomberg’s political aspirations. Most notably, he said his newsroom would continue ‘our tradition’ of not investigating Bloomberg, his family and his wealth, ‘and we will extend the same policy to his rivals in the Democratic primaries.’ A Bloomberg News spokeswoman, Kerri Chyka, also said the company won’t initiate stories about Bloomberg L.P., following a long-standing policy. The hands-off policy puts Bloomberg News in the awkward position of passing on such critical stories as Trump’s unfounded

allegations of corruption against [Biden] and his son Hunter. At the same time, Micklethwait said Bloomberg News would continue to investigate the Trump administration.”

**-- “America already elected a builder,” White House adviser Kellyanne Conway said of Bloomberg’s announcement, which uses the tagline “Rebuild America.”** “His new ad that he put millions behind is all unicorns and rainbows. Keep your health care if you’d like to — and if you don’t, I have something better. Rebuild America. We heard that from Obama-Biden,” Conway said. ([Politico](#))

**-- Biden is struggling in Iowa and his supporters blame a lack of enthusiasm and a spotty campaign operation.** [From the Times](#): “Voters at Mr. Biden’s events, along with county chairs and party strategists, characterize his on-the-ground organization as scattershot, visibly present in some counties but barely detectable in others. His events are often relatively small and sometimes subdued affairs, and in a state where enthusiasm can make or break a candidate on caucus night — a big part of caucusing centers on persuading friends and neighbors — Mr. Biden’s operation has found it difficult to build contagious excitement, these Democrats say. ... ‘This is prime political season in Iowa and most candidates are spending a good deal of time visiting Iowa,’ said Joey Norris, the Democratic chair in Montgomery County, Iowa, where [Pete] Buttigieg plans to campaign on Monday. ‘The Biden campaign has been notably absent.’”

**-- Sanders’s loyal voters could keep him in the race for months.** [From the Journal](#): “Sanders’s campaign has made it clear that to win the nomination, he would have to pull off an ambitious expansion of



the electorate. His campaign says it is banking on turning out a coalition of young, working-class and minority voters. But polls show the Vermont independent's base is more loyal than that of any other 2020 Democrat, and in interviews over the last four months, Mr. Sanders's supporters [have said] that they wouldn't support any other candidate as long as he is running. Those backers—and his massive fundraising—mean that, unlike many of his rivals, Mr. Sanders might not need a marquee win in an early state to stay in the presidential race for months.”

**-- Sen. Cory Booker keeps winning praise for his presidential campaign. What he's not winning is much support. [Cleve R.](#)**

[Wootson Jr. and Michael Scherer report](#): “As he struggles with low-single-digit polling and the prospect of missing the cut for next month's debate, Booker has become a symbol for the harsh reality of this year's nominating process. It is just not enough to win plaudits for performance, as he has after multiple events, or to execute a clear campaign strategy. In the shadow of Trump's potential reelection, Democratic voters have become focused on winning and are unforgiving with their doubts. Booker has sought to answer that concern by preaching the power of empathy. He appeals to white Iowa and New Hampshire voters by talking about the problems of inner cities and poverty. He has confronted Trump by explaining his compassion for his supporters. And unlike other campaigns that have pivoted on message and policy, he has made clear he will not change his strategy to win.”

**-- Sarah Sanders left Washington less than six months ago. Now the former White House press secretary has returned to**

**Arkansas in search for a new political role. [From the Times:](#)**

“‘There are two types of people who run for office,’ Ms. Sanders said over breakfast tacos at a diner in downtown Little Rock last week. ‘People that are called and people that just want to be a senator or governor. I feel like I’ve been called.’ ... As the daughter of Mike Huckabee, who served as governor from 1996 to 2007 and twice ran for president, she is seen as political royalty in Arkansas, and Mr. Trump himself urged her to run for governor when she left the West Wing. That job will open in 2023, when Gov. Asa Hutchinson’s term is up, and Ms. Sanders is giving every indication that she plans to run.

...

“In the 23 months that Ms. Sanders served as Mr. Trump’s chief spokeswoman, her battles with the White House press corps were epic. ... Ms. Sanders’s relationship with reporters reached a nadir in April after it was revealed that she had admitted under oath to investigators working for the special counsel, Robert S. Mueller III, that her claim at a press briefing that ‘countless members of the F.B.I.’ told her they had lost confidence in the bureau’s director, James B. Comey, was a ‘slip of the tongue’ that was not based on any facts. ... ‘I was attacked for everything, not just my performance,’ she said of her time in Washington. ‘I was called a fat soccer mom, my kids were threatened, my life was threatened. It was a lot. I hate harping on it, but to be in the position I’m in and to have Secret Service, that’s not normal.’ Ms. Sanders paused. ‘I don’t like being called a liar,’ she said.”

**-- Doctors who previously worked at the White House and those who are currently in touch with the White House said the**



**mysterious and unannounced visit Trump made to the hospital last weekend was highly unusual.** [From CNN's Dr. Sanjay Gupta:](#)

“Given that the White House had previously given plenty of advance notice about the President's past physical exams, last weekend's visit to Walter Reed reportedly took everyone by surprise, including much of the staff at the hospital itself. Whenever the President is planning a visit to Walter Reed, an institution-wide notice goes out, making staff aware of certain road and corridor closings. According to a person familiar with the matter, that didn't happen last weekend. **Also striking: the fact that the president's physician, Dr. Sean Conley, rode with Trump in the presidential motorcade. Typically, the doctor rides separately from the President for security reasons.** A former White House doctor [said] it had never happened during their time there. ...

**"All tests Conley described could've been performed at the White House instead of the hospital.** Many blood tests require the patient to fast overnight and are thus performed first thing in the morning -- not in the middle of the afternoon, as apparently happened with the President. And remember, the President had these tests just nine months ago. One of the reasons doctors wait a year to order labs for a routine physical is to better assess the impact of medication and lifestyle changes over a consistent interval of time. There is no benefit to drawing the blood early, unless there is a concern about something. Finally, there is no such thing as a phased physical exam, as Trump had described it in his tweet from last weekend.”

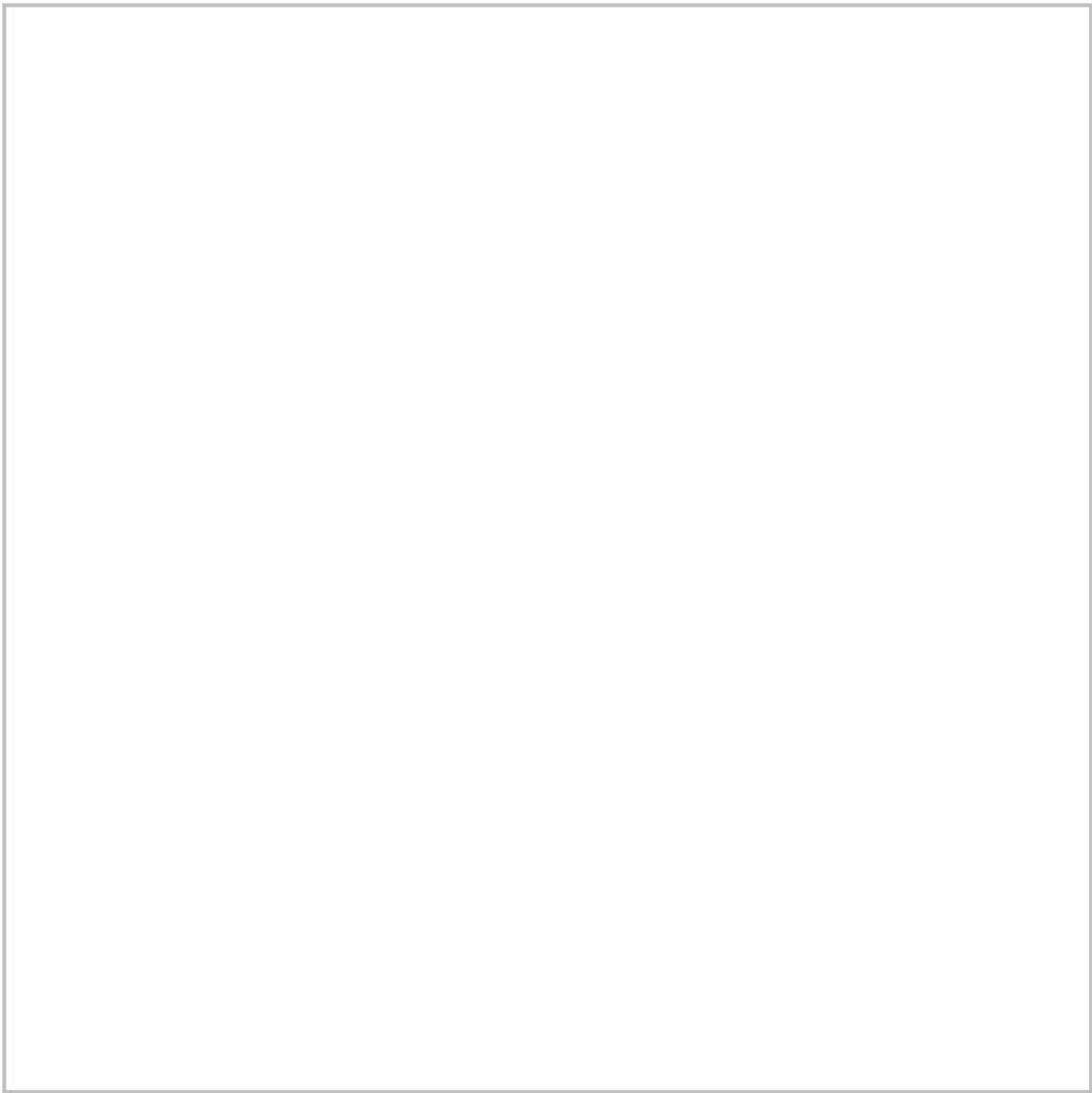
**-- Another health scare: Justice Ruth Bader Ginsburg was released from the hospital on Sunday after going in with chills**



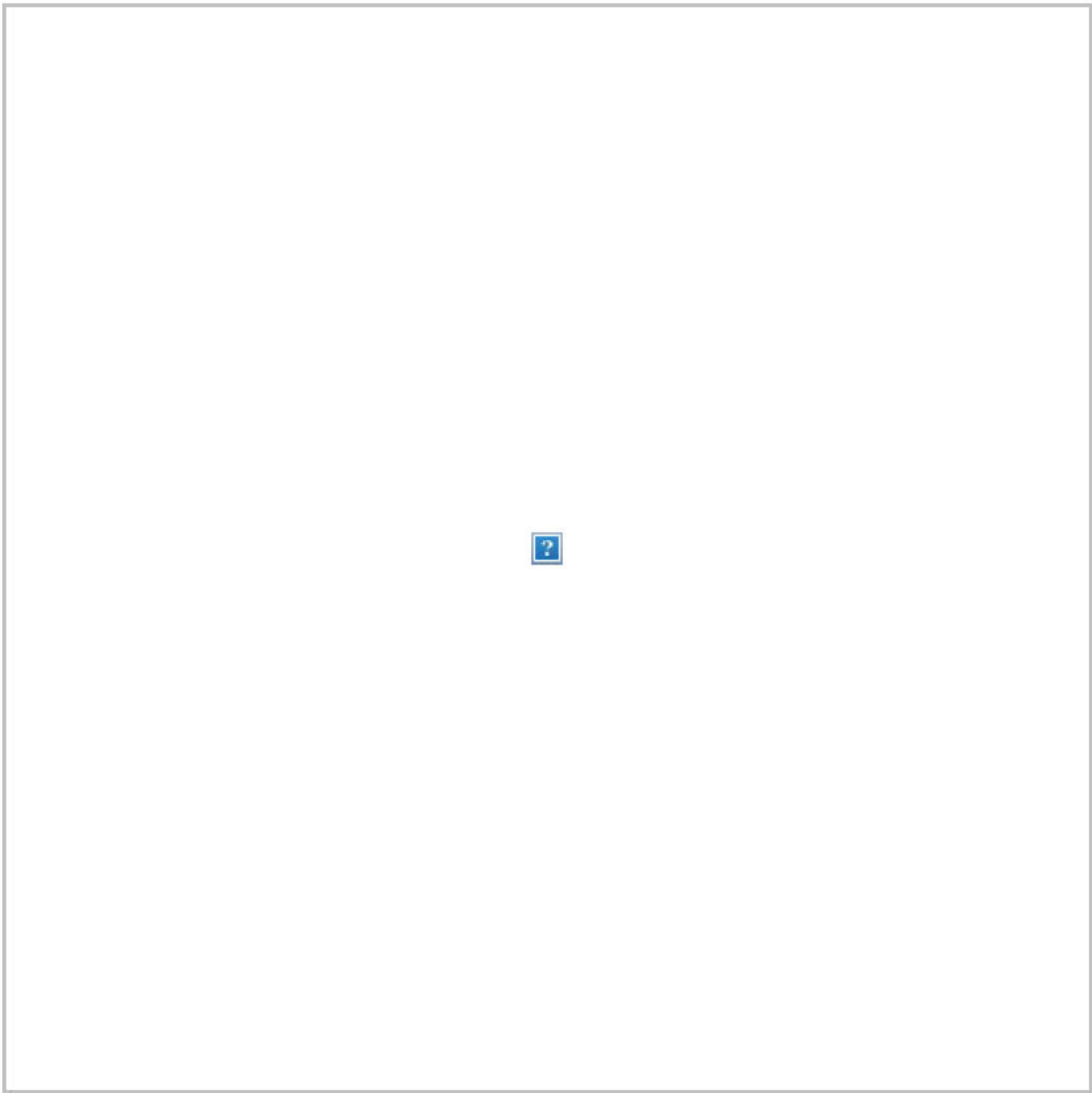
**and a fever.** [Robert Barnes reports](#): “The court announced in a news release Saturday evening that the 86-year-old had been seen at Sibley Memorial Hospital in Washington and then transferred to Johns Hopkins Hospital in Baltimore, where doctors were more familiar with her medical history. She was treated for a possible infection. 'With intravenous antibiotics and fluids, her symptoms have abated,' the court said in the Saturday release. The court provided no other details.”

### **SOCIAL MEDIA SPEED READ:**

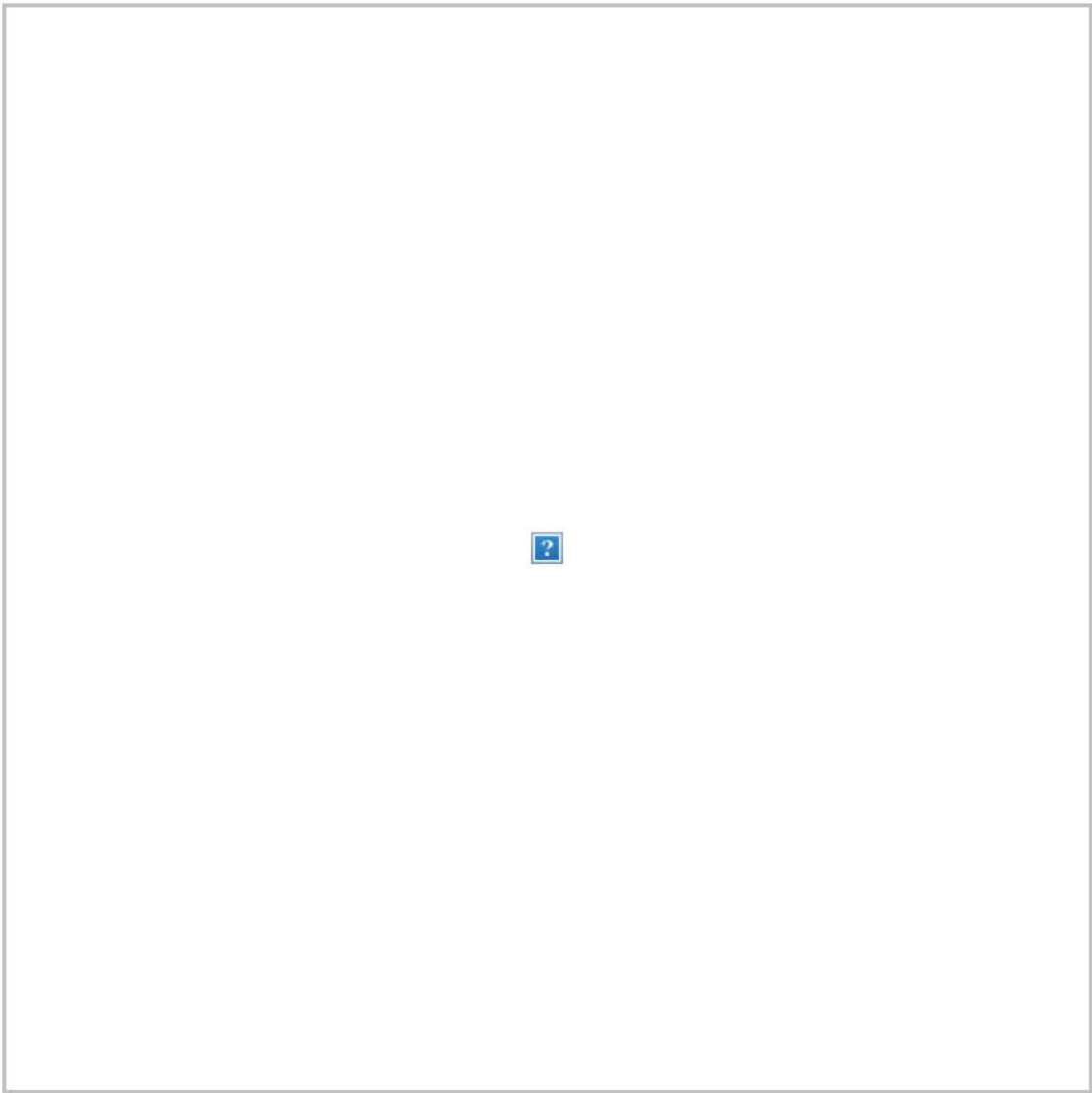
The Intelligence chairman reacted to The Post's scoop:



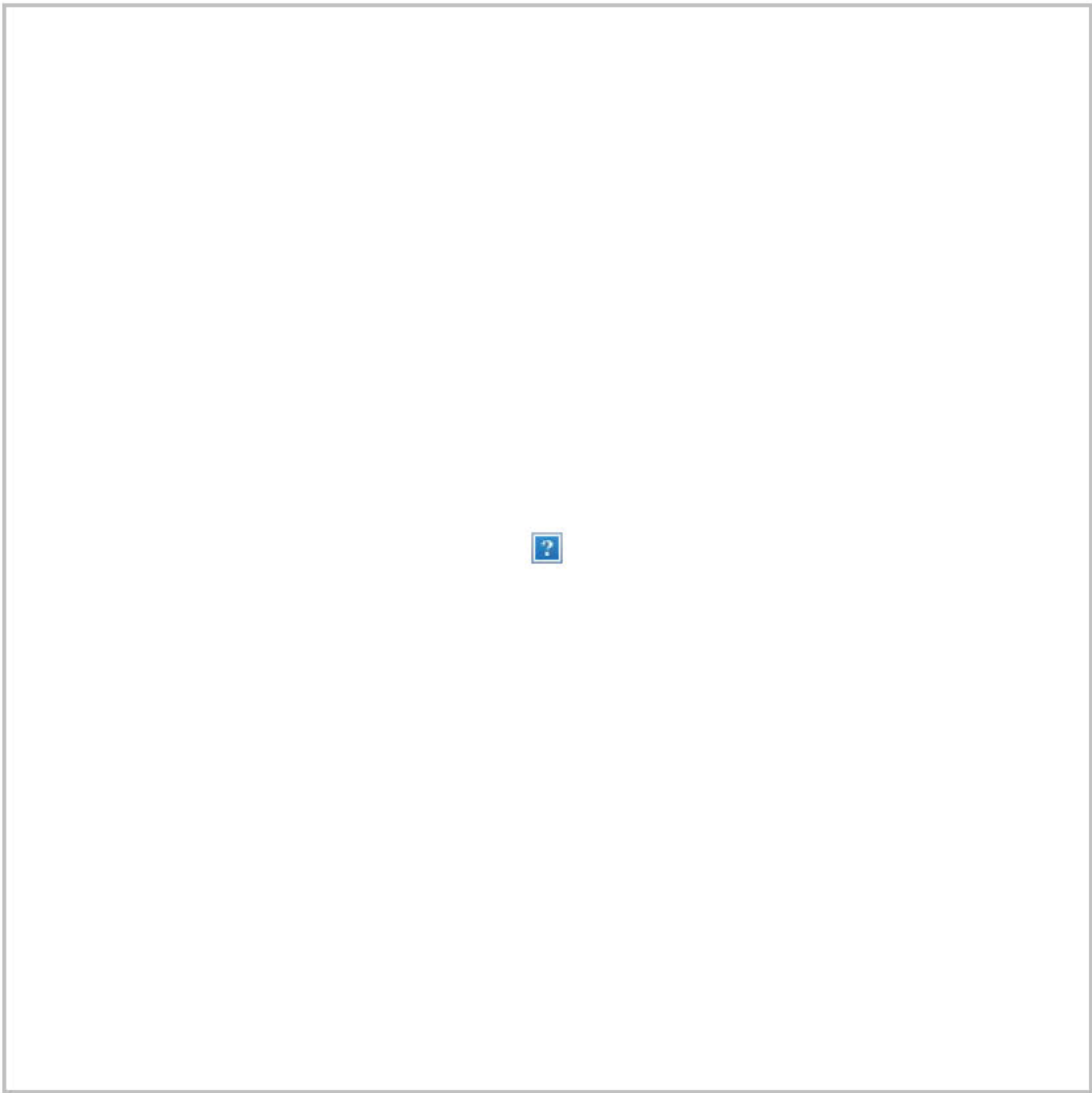
The Post's Shane Harris had this reminder after an assertion by Sen. John Neely Kennedy (R-La.) on "Fox News Sunday":



On Saturday, Rudy Giuliani made this comparison:

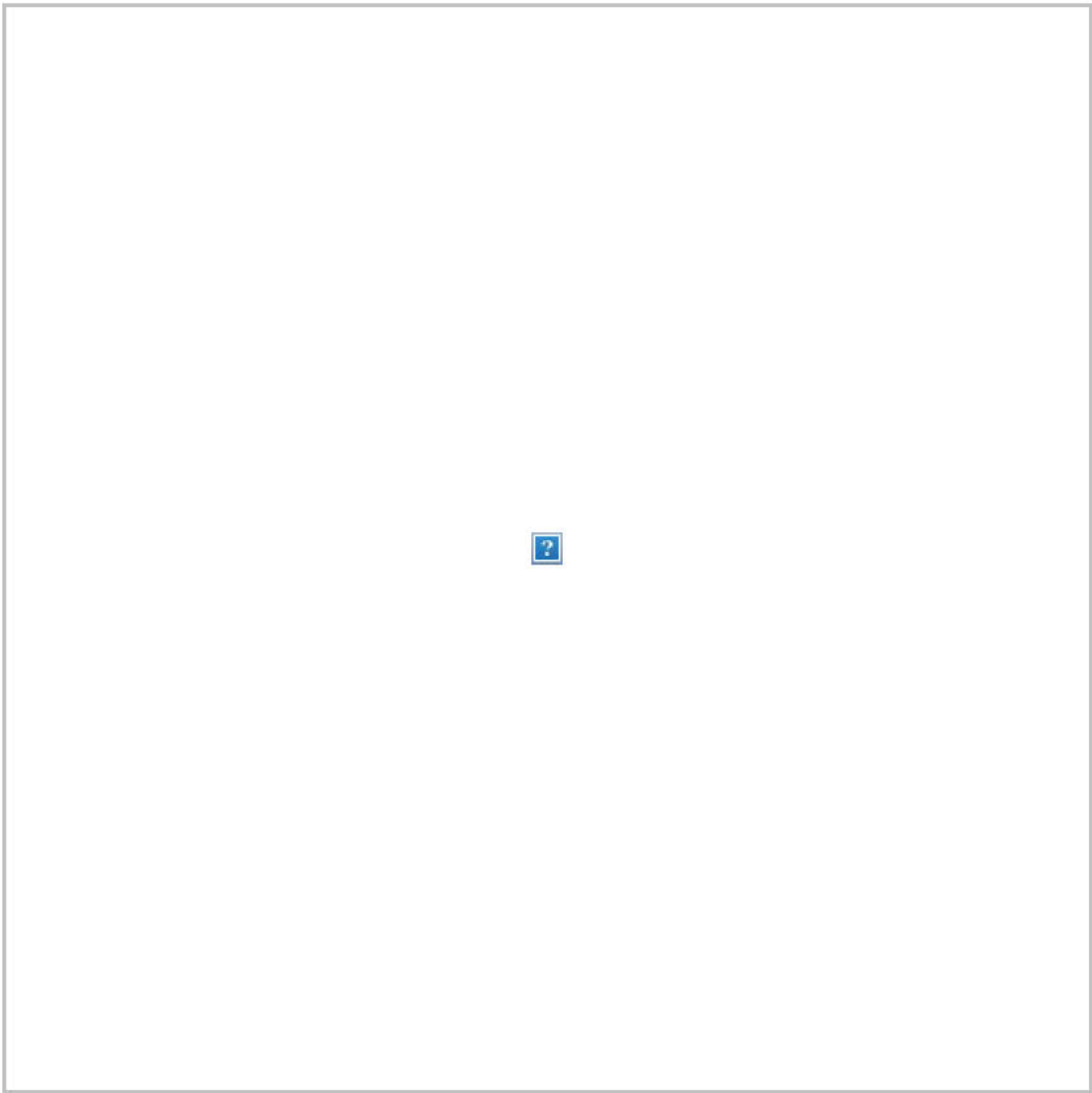


This scandal from a decade ago [seems so quaint](#):

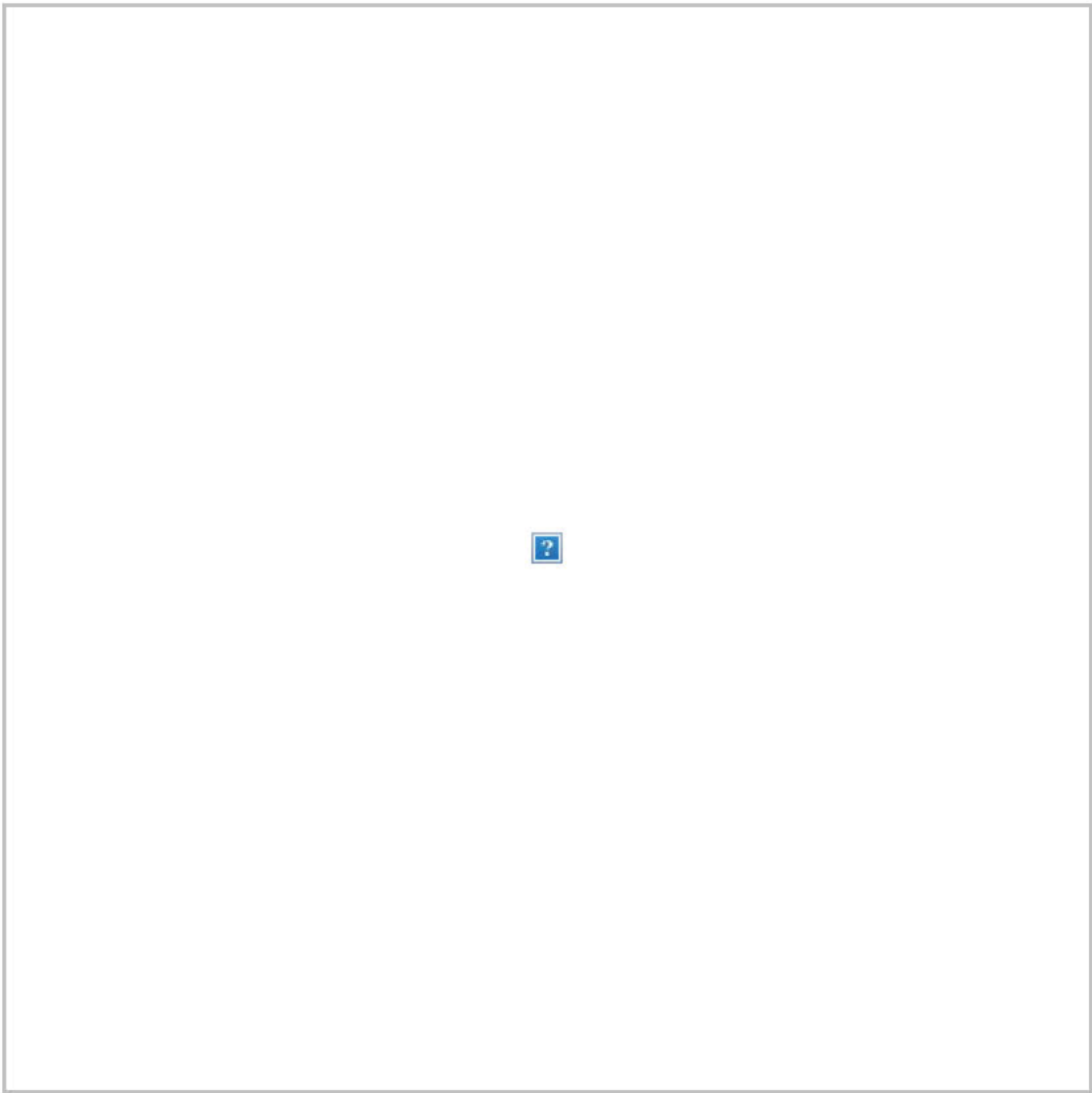


Bernie Sanders went out dancing:

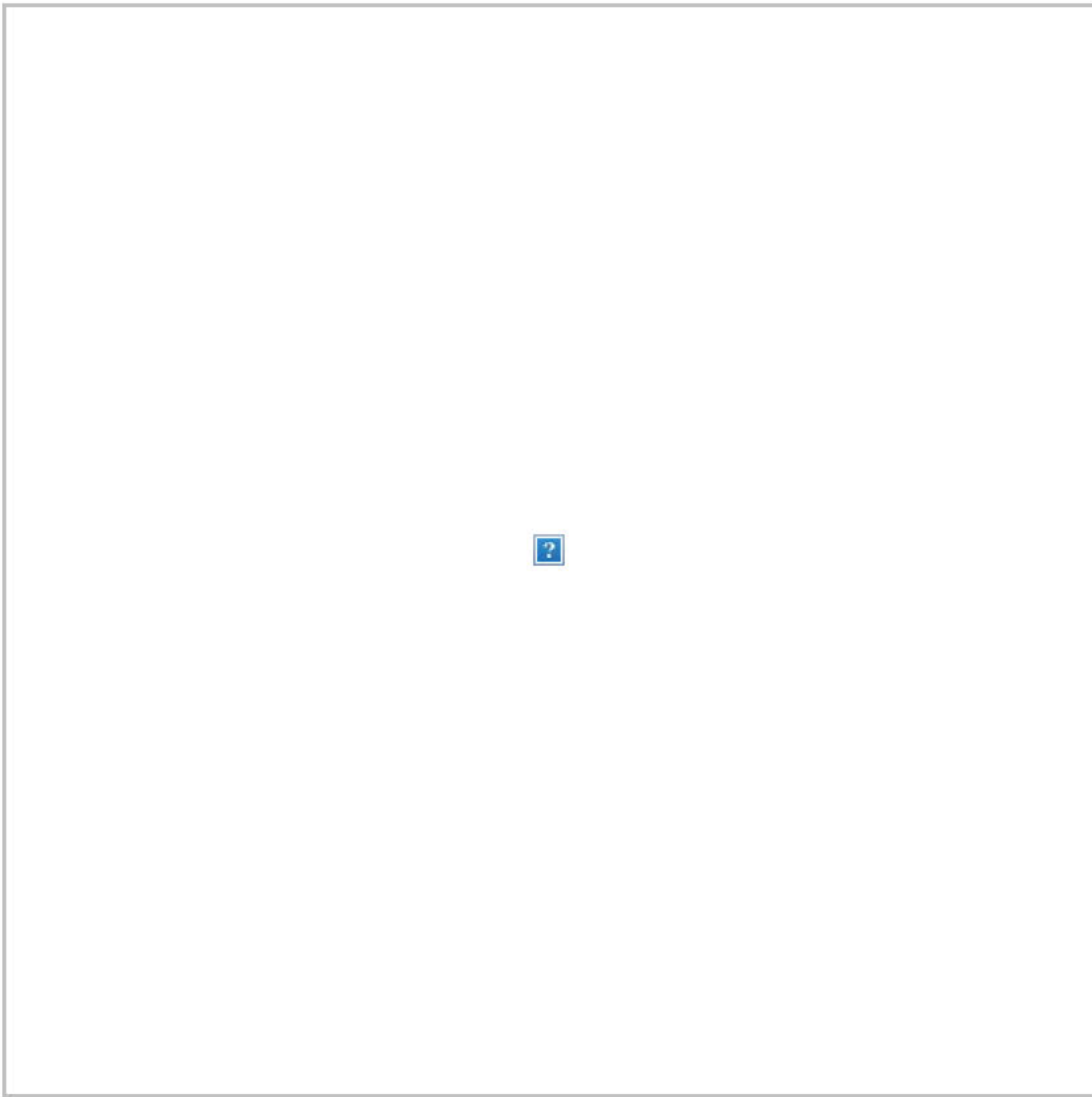




It's almost Thanksgiving, which means a pair of turkeys are having the time of their lives in D.C.:

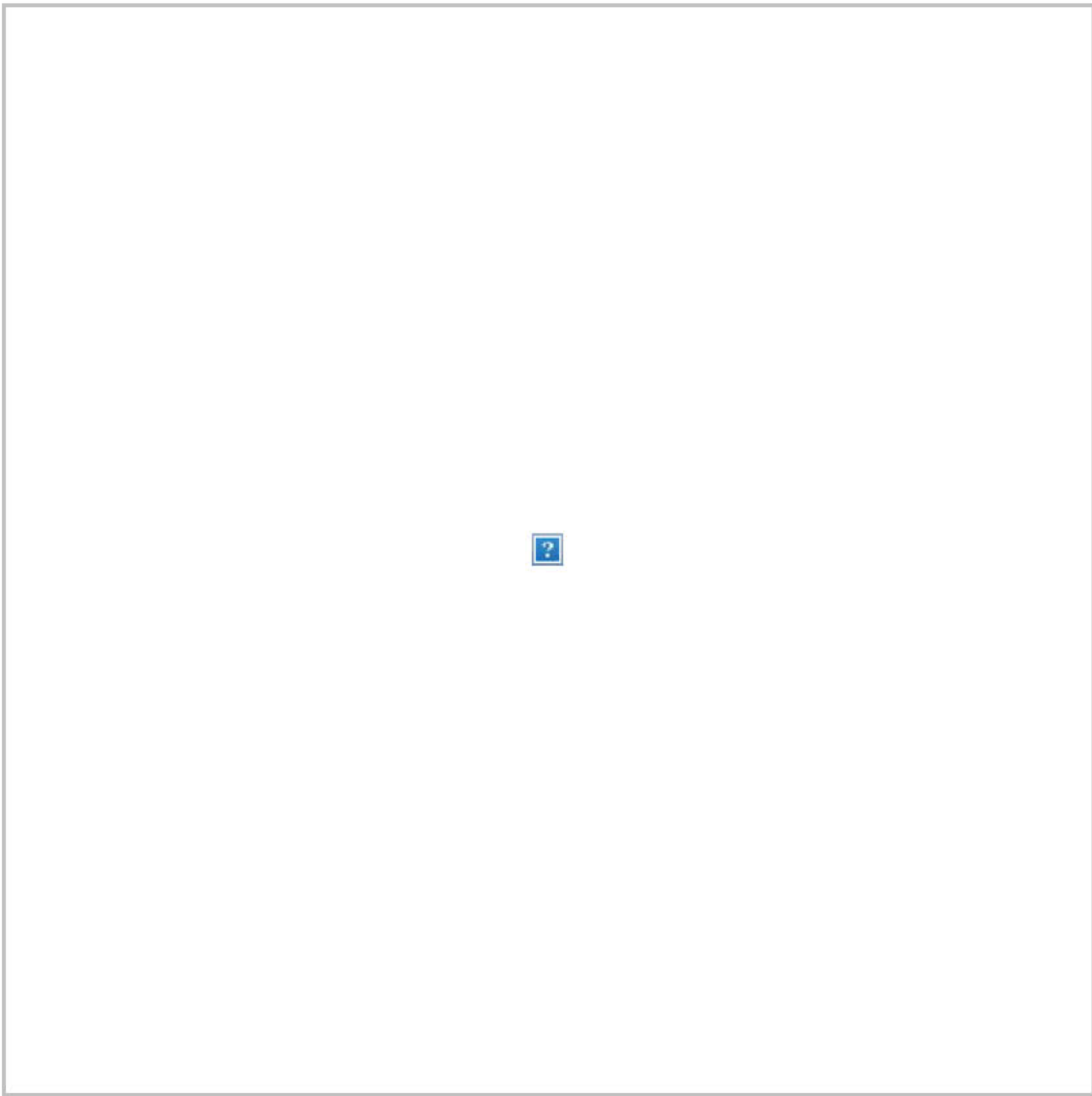


And border officials detained a shipment of illegal cold cuts, which led to this killer lede:



### **VIDEOS OF THE DAY:**

Taylor Swift broke Michael Jackson's record for winning the most American Music Awards of all time. Jackson won 24. Swift has 29 after last night:



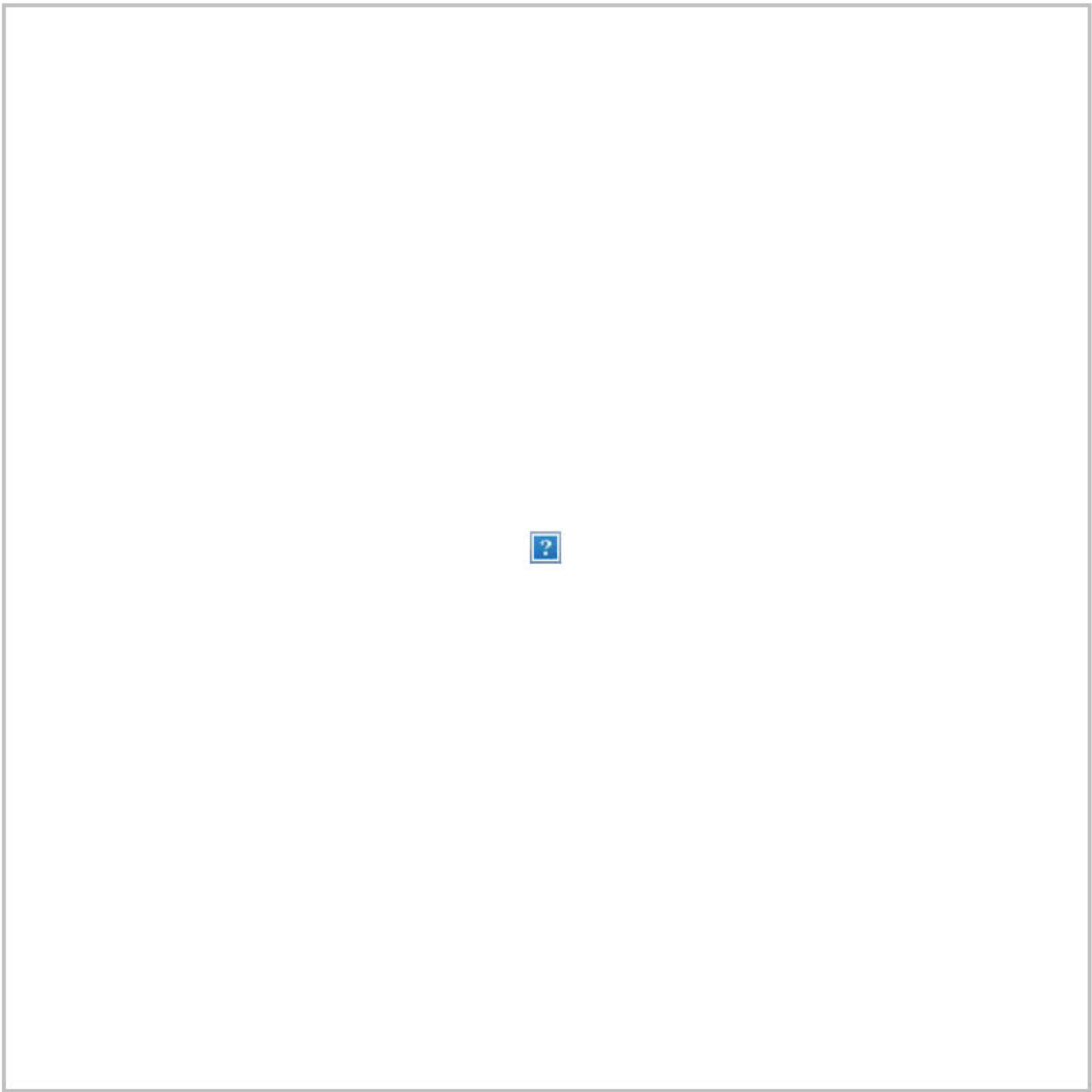
(Find the complete list of winners [here](#).)

“Saturday Night Live” spoofed last week’s Democratic debate:



“Weekend Update” pointed out that testimony on impeachment concluded in the House last week and “now the debate will shift to your house for Thanksgiving”:

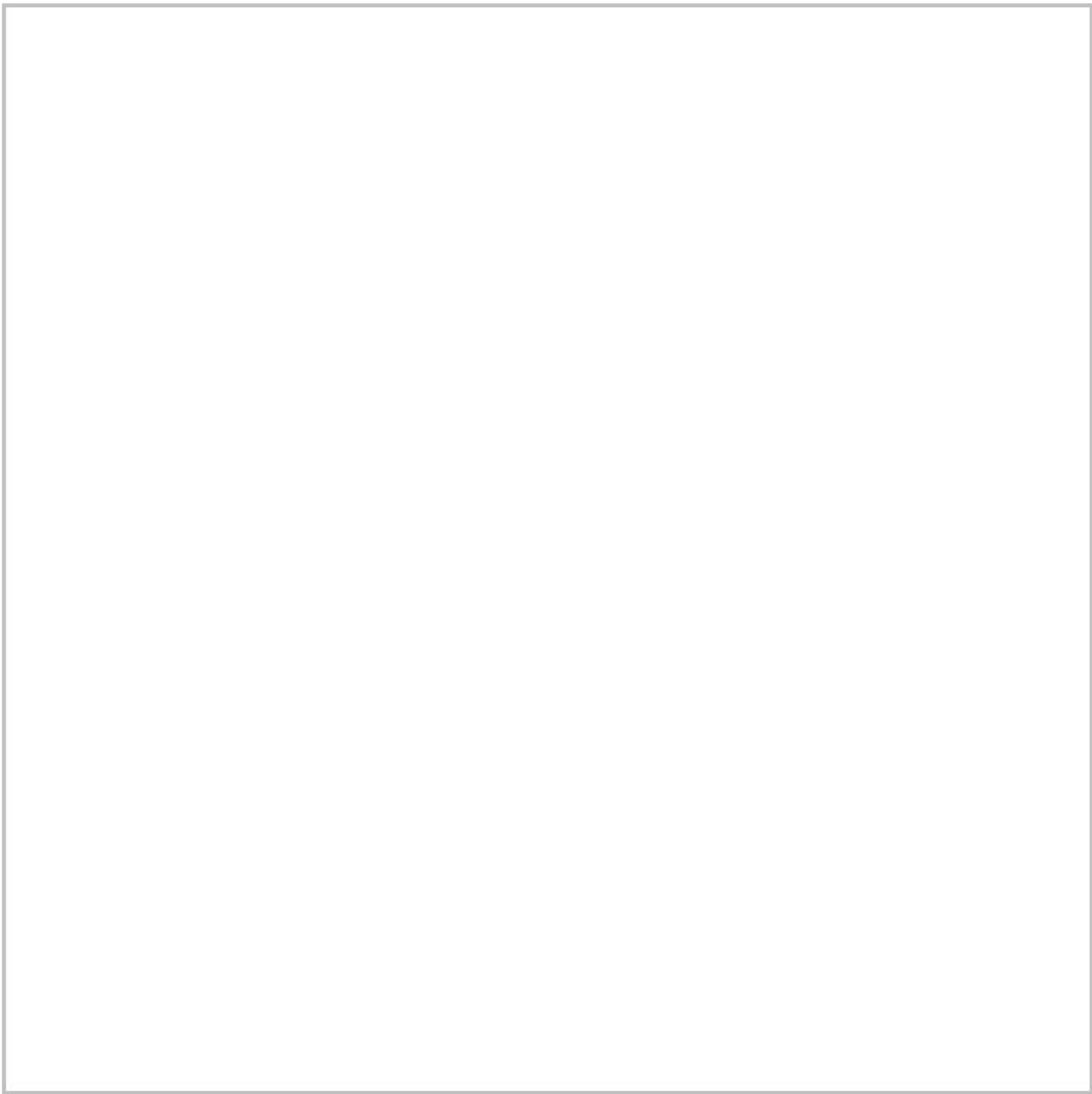




“The Daily Show” set out to investigate who will win the black vote in 2020:



And Trevor Noah interviewed Hillary and Chelsea Clinton:



You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)

---

©2019 The Washington Post | 1301 K St NW, Washington DC 20071



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fgrgurina@sunnyvale.ca.gov](mailto:fgrgurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for November 11, 2019  
**Date:** Monday, November 11, 2019 5:04:53 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)



### **Justices appear split over police power in traffic stops**

The Supreme Court was sharply divided Monday as the justices considered whether a police officer can pull a car over based solely on the knowledge that it is registered to a person with a suspended license. To some justices, a Kansas sheriff's deputy was perfectly justified in pulling over Charles Glover as he was driving his 1995 Chevy pickup truck based solely on the fact that the deputy ran the car's plates and found Glover's license was suspended.

[Courthouse News Service](#)

### **Order for forfeiture of nearly \$2 million did not violate Eighth Amendment**

The Ninth U.S. Circuit Court of Appeals has rejected the contention of a drug kingpin that an order to forfeit nearly \$2 million violates the Eighth Amendment's ban on "excessive fines" because it was grossly disproportional to the tame financial offense to which he pled guilty. Affirmance of the order was tied to defendant Lakhwinder Singh's drug trafficking - of which he does not stand convicted, but which he does not deny - rather than the trickery to which he pled guilty in connection with deterring the filing by third parties of financial reports.

[Metropolitan News-Enterprise](#)

### **Federal judge shreds fired deputy's lawsuit claiming political retaliation, in the latest chapter of the never-ending Carl Mandoyan drama**

Last Thursday, October 31, United States District Judge John F. Walter handed down the latest chapter in the seemingly never-ending saga of the firing, re-hiring, and then un-hiring of former Los Angeles County Sheriff's deputy Caren Carl Mandoyan. In a ten-page order, Judge Walter, an appointee of George W. Bush, ruled to dismiss with prejudice the federal civil rights lawsuit filed by Carl Mandoyan on March 4, of this year claiming that he has been subjected to retaliation based on his constitutionally protected right to free speech, and his political associations.

[Witness LA](#)

### **Qualified immunity properly granted in white supremacist's suit**

California prison officials were properly granted qualified immunity in a case in which racist materials were seized from the plaintiff's cell - materials he declares to be religious - "holy books" of his white supremacist creed were banned, a "fruitarian" diet was denied him while dietary requirements of other faiths were accommodated, the Ninth U.S. Circuit Court of Appeals has held.

[Metropolitan News-Enterprise](#)

### **Another 13-year confinement**

A man who was civilly confined in a state hospital for over 13 years claims the Los Angeles Public County Defender mishandled his case so



badly it amounts to deliberate indifference - nearly identical to a recently settled lawsuit.

[Courthouse News Service](#)

### **Ninth Circuit takes new swipe at ex-mayor's fight of voting districts**

A Ninth Circuit panel scrutinized a former Southern California mayor's challenge to the state's Voting Rights Act on Tuesday, seeming to doubt his claim that a change in the way the city elects its council members had unconstitutional consequences. "How is your client worse off?" U.S. Circuit Judge Andrew Hurwitz asked Jeffrey Harris, attorney for ex-Poway mayor Don Higginson.

[Courthouse News Service](#)

### **Woman accused in Rolling Hills Estates stabbing murder wins legal victory in Federal Court**

The woman who says she was falsely accused of killing a retired nurse in the parking lot of a shopping mall in Rolling Hills Estates has won an unusual legal ruling in federal court that may allow a wrongful arrest lawsuit to begin even though the murder case is unresolved. U.S. District Court Judge R. Gary Klausner lifted a stay that had delayed the lawsuit while the Los Angeles County Sheriff's Department investigates the May 3, 2018 stabbing murder of retired nurse Susan Leeds.

[NBC4](#)

### **Online access to court records remains elusive in Kern**

It frustrates Bakersfield attorney Jeff Wise that he can't simply download local court records any time of day in exchange for a modest fee.

Federal courts allow it. So does Los Angeles County's court system. But if Wise wants immediate access to Kern County Superior Court's full library of digital records, he has to stand at one of three computerized public terminals in the lobby of the courthouse on Truxtun Avenue in downtown Bakersfield.

[Bakersfield.com](#)

### **Contra Costa judge ordered removed from office for 'significant' misconduct**

The Commission on Judicial Performance has voted to oust Contra Costa County Superior Court Judge John Laettner from office for "a significant amount of misconduct," including "a pattern" of inappropriate behavior toward women.

[Law.com](#)

### **Judge expands injunction in self-driving car trade secrets case**

A federal judge tipped his hand on how he views a case involving corporate espionage in the hypercompetitive industry of self-driving cars. In short, he thinks something foul is afoot. In an order issued Tuesday, U.S. District Judge Edward Davila granted the most important parts of WeRide's request to expand a preliminary injunction against a

bevy of corporate actors, multinational companies replete with puppet CEOs and a few shadow companies allegedly created to dodge liability.  
[Courthouse News Service](#)

### **University of California a part of upcoming DACA fight in SCOTUS**

The University of California is one of the parties involved in the upcoming Deferred Action for Childhood Arrivals (DACA) case at the Supreme Court. The Justices will hear arguments on Nov. 12. The outcome could have a big impact on the lives of the nearly 800,000 people currently protected under DACA and their families. DACA was created by the Department of Homeland Security in 2012 during the Obama Administration.

[ABC10 Sacramento](#)

### **Ninth Circuit judge confirmed with little pushback from Democrats**

The Senate on Wednesday confirmed an Oregon state court judge to a seat on the Ninth Circuit, while also setting up a vote that will likely make a quarter of all federal appeals court judges President Donald Trump's appointees. Judge Danielle Hunsaker currently serves as the presiding judge on the Washington County Circuit Court in Oregon and has held a seat on the court since 2017, when she was appointed by Oregon Governor Kate Brown, a Democrat.

[Courthouse News Service](#)

### **State Bar of California looking into rule change on attorneys sharing fees with non-lawyers**

The State Bar of California is looking at a rule change that would end a general ban on attorneys sharing fees with non-lawyers so non-attorneys could eventually hold financial interests in law firms. However, opponents say this would increase third-party litigation funding, leading to more third-party pressures on civil litigation that might do a disservice to clients.

[Northern California Record](#)

## **Prosecutors/Prosecutions**

### **Los Angeles ADAs endorse incumbent Jackie Lacey over San Francisco DA Gascón**

The Association of Deputy District Attorney's announced their endorsement of Jackie Lacey for Los Angeles County District Attorney. Lacey is being challenged by San Francisco DA George Gascón, who recently announced he was leaving San Francisco to run for District Attorney in Los Angeles. Lacey has been Los Angeles District Attorney since 2012 and is a native of Southern California.

[California Globe](#)

### **From car break-ins to meth possession, interim DA Loftus signals tougher approach**

Ten days in a new job is usually just enough time to get through orientation and ensure your email account is working. But for interim District Attorney Suzy Loftus, the past two weeks have been a high-profile trial run for the permanent gig she desperately wants - and she's packed a lot in. Her flurry of appearances and news conferences has grabbed headlines and given voters an idea of how she'd perform if she wins Tuesday's race against three strong competitors.

[San Francisco Chronicle](#)

### **Bel-Air mega-mansion should be torn down, city officials say**

Los Angeles city prosecutors are calling for an unfinished mega-mansion in Bel-Air to be torn down to its foundation, the latest twist in the saga over a colossal building at the center of criminal charges, court battles and an FBI investigation. Until recently, city officials had been working with real estate developer Mohamed Hadid to bring the building in line with city codes, requiring only parts of the building to be removed.

[Los Angeles Times](#)

### **SF DA's race foreshadows coming LA DA's fight and continuing battle over the criminal justice system**

Today's vote in San Francisco will not merely fill the District Attorney position but provide insight on where California stands in the national movement to change the criminal justice system. That effort, spurred on by progressives, will extend to Los Angeles next year when the county's voters will likely decide between two candidates who will represent different views on how rapidly the criminal justice is changed with public safety the key question in the debate.

[Fox & Hounds](#)

### **What punishment could the driver suspected of killing a family of 3 face?**

A 20-year-old driver suspected of being under the influence of drugs or alcohol when he allegedly killed a Long Beach couple and their 3-year-old son in a crash on Halloween could face charges ranging from manslaughter to murder, legal experts said. Police said Carlo Navarro was behind the wheel of an SUV when he plowed into Joseph Awaida, 30, his wife Raihan Dakhil, 32, and their son Omar as the family was trick-or-treating in the Los Cerritos Park neighborhood on Thursday.

[Long Beach Post](#)

### **L.A.-based U.S. Attorney's office to participate in Procurement Collusion Strike Force that will combat antitrust crimes and related schemes in government procurement, grant and program funding**

The Justice Department announced today the formation of the new Procurement Collusion Strike Force (PCSF) focusing on deterring, detecting, investigating and prosecuting antitrust crimes, such as bid-rigging conspiracies and related fraudulent schemes, which undermine

competition in government procurement, grant and program funding.  
[Department of Justice/District of Colorado](#)

### **California probing Facebook's privacy practices**

California is investigating Facebook Inc.'s privacy practices, the state's attorney general revealed Wednesday in a lawsuit that accuses the Silicon Valley tech giant of failing to adequately comply with information requests. Attorney General Xavier Becerra said he has asked the San Francisco Superior Court to force Facebook to comply with investigators' subpoenas, the latest of which were issued in June.

[Wall Street Journal](#)

### **Prosecutors charge man with hate crime in acid attack**

A 61-year-old white Milwaukee man accused of throwing acid on a Hispanic man's face will be charged with a hate crime, increasing the possible sentence he may receive if convicted, prosecutors announced Wednesday. Prosecutors filed one charge against Clifton Blackwell - first-degree reckless injury - but added the sentencing enhancers of hate crime and use of a dangerous weapon.

[NBC4](#)

### **US prosecutors: Saudis recruited Twitter employees to get personal account information of critics**

The Saudi government, frustrated by growing criticism of its leaders and policies on social media, recruited two Twitter employees to gather confidential personal information on thousands of accounts that included prominent opponents, prosecutors alleged Wednesday. The complaint unsealed in U.S. District Court in San Francisco detailed a coordinated effort by Saudi government officials to recruit employees at the social media giant to look up the private data of Twitter accounts, including email addresses linked to the accounts and internet protocol addresses that can give up a user's location.

[AP](#)

### **Porn site owner charged with child sex trafficking amid fraud trial**

GirlsDoPorn owner Michael Pratt, a fugitive believed to be in New Zealand, was charged Thursday for allegedly producing child porn and sex trafficking related to a 2012 incident involving a 16-year-old. The new criminal indictment was unsealed in the Southern District of California Thursday at a hearing attended by Pratt's co-defendants, GirlsDoPorn videographer Matthew Wolfe, actor Andre Garcia and administrative assistant Valorie Moser.

[Courthouse News Service](#)

## **Policy & Legal Issues**

**Marijuana breathalyzers: Could new testing methods help employers and employees?**

Employers are grappling with the wave of marijuana laws sweeping the nation, some of which provide very employee-friendly protections. While no state requires an employer to tolerate employees' use of marijuana or impairment while they are working, present drug testing methodologies cannot determine whether an employee used marijuana two hours or two weeks ago.

[Seyfarth](#)

### **These machines can put you in jail: Don't trust them**

A million Americans a year are arrested for drunken driving, and most stops begin the same way: flashing blue lights in the rearview mirror, then a battery of tests that might include standing on one foot or reciting the alphabet. What matters most, though, happens next. By the side of the road or at the police station, drivers blow into a miniature science lab that estimates the concentration of alcohol in their blood.

[New York Times](#)

### **Bill Bratton talks about why upcoming criminal justice reforms will make New Yorkers less safe (Audio)**

[Cops Count - Police Matter](#)

### **Defining prison abolitionism in a time of progressive prosecutors**

In a time where progressive prosecutors are becoming a national movement, several organizations came together to create a document outlining abolitionist principles and strategies titled "Abolitionist Principles & Campaign Strategies for Prosecutor Organizing." Community Justice Exchange presented the document at a webinar on Nov. 11, 2019. The presentation began with words from Mariame Kaba, the founder and director of Project NIA and co-founder organizer with Survived and Punished New York.

[The Davis Vanguard](#)

### **Internet increasingly used for government surveillance**

Freedom House issued its annual report Tuesday, warning that social media is an increasingly dangerous tool for mass surveillance and manipulation of elections. Global internet freedom also declined for the ninth straight year, the nonpartisan, U.S.-government-supported organization found. "What was once a liberating technology has become a conduit for surveillance and electoral manipulation," begins the 32-page report, "Freedom on the Net 2019 - The Crisis of Social Media."

[Courthouse News Service](#)

### **California DAs need to utilize police transparency law**

After decades of secrecy surrounding police misconduct, California has a new law that is designed to restore trust in our criminal justice system. And what we've seen since Senate Bill 1421 took effect in January has been both illuminating and deeply concerning, demonstrating why the measure was necessary to ensure that law enforcement is both transparent and accountable.



[Sacramento Bee](#)

### **Nothing prepared sheriffs on duty for the horror of borderline**

The former sheriff of Ventura County, and the current sheriff whose first days on the job were spent dealing with the Borderline Bar mass shooting and the explosive Woolsey Fire, have a combined 75 years in law enforcement, but nothing prepared them for that evening in Thousand Oaks one year ago Thursday. "You have a great playbook until the first shot's fired," former Ventura County Sheriff Geoff Dean said.

[NBC4](#)

## **Public Safety**

### **Additional victims of Chilean 'tourist' burglary ring come forward after FOX 11 investigation**

New victims of a Chilean "tourist" burglary ring have come forward after a FOX 11 investigation revealed that Chilean nationals are exploiting the ESTA visa waiver system to come to Southern California and commit hundreds of burglaries. After the story aired, FOX 11 was contacted by Marya Ortiz, the owner of Luxmary Handbags in Burbank. She said her luxury handbag store had been burglarized for \$450,000 by the same Chilean crime ring in August.

[Fox11 LA](#)

### **Mayor Lori Lightfoot appoints retired LAPD Chief Charlie Beck as Chicago's interim top cop**

Interim police superintendents are typically caretakers, seasoned insiders who step in to provide continuity while the search for a permanent leader takes place. But Friday's unusual appointment of an outsider - retired Los Angeles police Chief Charlie Beck, a nationally recognized leader - as Chicago's interim police superintendent suggests that Mayor Lori Lightfoot is intent on pushing reform efforts even in the months before a successor to outgoing Eddie Johnson can take office.

[Chicago Tribune](#)

### **Airbnb bans 'party houses' after five die in California**

Airbnb is taking actions against unauthorized parties after a deadly shooting at a Halloween party at an Airbnb rental home in California, the Associated Press reports. CEO Brian Chesky said Saturday the San Francisco-based company is expanding manual screening of "high risk" reservations and will remove guests who fail to comply with policies banning parties at Airbnb rental homes.

[The Crime Report](#)

### **Freelance videographer alleges assault, battery by Beverly Hills Police Chief**

A freelance videographer Tuesday began the process to sue Beverly Hills and Police Chief Sandra Spagnoli, alleging she ran over his foot when he tried to interview her in April. Jacob Rogers alleges in the Los Angeles

Superior Court lawsuit, whose filing has not been completed, that at about noon on April 16, he approached Spagnoli for comment about an internal investigation regarding a Beverly Hills Police Department officer who had allegedly slandered a photojournalist by calling him a "child molester" and a "rapist."

[My News LA](#)

### **California 'awash in guns,' feds say as they target illegal firearms and violent crime**

Last June, a police officer in the Shasta County city of Anderson pulled over a pickup truck driven by Jim David Travis, a 72-year-old convicted felon who was on searchable probation. By the time Officer Michael Hallagan finished searching, police seized a loaded .22-caliber Ruger pistol from his truck, a loaded Colt AR-15 rifle from under his bed and a loaded Mauser handgun tucked between a mattress and box spring at his home, court records say.

[Sacramento Bee](#)

### **Prop 47 & 57 & AB 109**

#### **California referendum has led to more shoplifting, report says**

Five years ago, California passed Proposition 47, a referendum that reduced various theft and drug possession crimes from felonies to misdemeanors. But in the years since the referendum passed, critics say the law has resulted in an increase of theft. Fox News reported that the referendum "effectively gives shoplifters and addicts the green light to commit crimes as long as the merchandise they steal or the drugs they take are less than \$950 in value."

[The Daily Wire](#)

#### **Santa Maria City Council to consider resolution about ballot initiative aimed at reducing crime**

The Santa Maria City Council is considering a Resolution in support of a 2020 statewide initiative aimed at reducing crime. Santa Maria Police report an uptick in crime over the last few years. The department attributes recent trends to two California laws approved by voters in 2014, and in 2016. The 2020 ballot initiative would partly roll back those measures.

[KEYT/KCOY/KKFX](#)

#### **A California retail group says proposition 47 is bad for business**

Thefts in stores are becoming a bigger problem, according to a trade group, because of prop 47. The California Retailers Association tells Fox News thefts of items worth under 950-dollars are getting worse because thieves are not as worried about being prosecuted. Passed by voters in 2014, prop 47 reclassifies some crimes as misdemeanors. Supporters say it focuses resources on bigger crimes. Critics maintain it gives crooks a green light to steal.

[790 KABC](#)

### **Retailers worry about shoplifting during holiday season**

'Tis the season - for a five-finger discount. Retailers are on the lookout for shoplifters as the holiday season gets underway - the first since Suffolk District Attorney Rachael Rollins declared she would decline to prosecute the crime. "Going into the holiday season, we're going to need to take a close look at what's going to happen," said Jon Hurst, president of the Retailers Association of Massachusetts.

[Boston Herald](#)

### **Sacramento's latest reckless law will give lighter sentences to 10,000 repeat felons**

Jerry Dewayne Williams, if popular folklore is to be believed, should be coming up for parole soon. This spring marks the silver anniversary since Williams, better known as the "pizza thief," received 25-years-to-life for shoplifting a slice of pizza at the Redondo Beach pier. Ever since, he's been "the patron saint of unfair sentencing." His story is featured in ongoing efforts by the ACLU to erode tough-on-crime laws.

[CalMatters](#)

## **Los Angeles County**

### **Shia LaBeouf thanks cop who arrested him for 'changing my life'**

Shia LaBeouf's 2017 arrest may have been "mortifying," but he's grateful that it helped turn his life around. While accepting an award for the script of his new autobiographical film Honey Boy at the Hollywood Film Awards in Los Angeles on Sunday, the actor extended a warm message to the police officer who arrested him for public drunkenness.

"I want to thank the police officer who arrested me in Georgia for changing my life," said LaBeouf, 33.

[People](#)

### **Wildfires: Inside Los Angeles' remote fire base**

Perched atop the Santa Monica Mountains is a prime chunk of real estate with stunning ocean views that's owned by a wealthy former radio executive. You won't find a palatial mansion or an infinity pool there, however. Instead, the former exec and county firefighters have transformed the picturesque property into a remote base for helicopters to refill their water tanks - a spot that's helping prevent small fires from turning catastrophic.

[Los Angeles Times](#)

## **Consumer**

### **DEA warns of counterfeit pills containing deadly doses of fentanyl**

Federal authorities in San Diego issued a warning to the public Monday regarding the severe dangers posed by counterfeit prescription pills containing the extremely potent and often deadly synthetic opioid

fentanyl. Since the beginning of this year, there have been 92 local deaths involving the drug, according to the U.S. Drug Enforcement Administration.

[City News Service & NBC7 San Diego](#)

### **Amazon is a safe haven for counterfeit sales**

Amazon is a company the world can't trust. Amazon built its global empire, in part, by flooding the consumer marketplace with an inexhaustible supply of counterfeit, fraudulent, and replica merchandise, OTC drugs, and books. The global giant is both a direct retailer of the fraudulent goods, e.g., "ships from and sold by Amazon.com" while also enabling and facilitating global criminals, counterfeiters, and scammers to manipulate its hyper-competitive environment with scams, fakes, and fraud.

[The Counterfeit Report](#)

### **Why cell phones failed in PG&E outages, and how to prevent a repeat**

As the lights flickered out and wildfires flared, PG&E's blackouts also cut off thousands of Californians from cell phone service, leaving them unable to get emergency alerts or call 911. It exposed a troubling gap in the state's readiness for mass outages that could, according to PG&E, keep happening for a decade. And it's left regulators scrambling to find a fix - though it will be difficult.

[San Francisco Chronicle](#)

### **Impostor marijuana vapes flood California as health crisis expands**

A short walk from police headquarters in the heart of downtown Los Angeles, a cluster of bustling shops are openly selling packaging and hardware that can be used to produce counterfeit marijuana vapes that have infected California's cannabis market. Bootleggers eager to profit off unsuspecting consumers are mimicking popular, legal vape brands, pairing replica packaging churned out in Chinese factories with untested, possibly dangerous cannabis oil produced in the state's vast underground market.

[AP](#)

### **Luggage tracking apps aren't 100% accurate. People are the weak link**

On a September vacation to celebrate their wedding anniversary, Marci and Eric Rose landed in Greece on an American Airlines flight and were notified by the airline's smartphone app that their baggage was waiting for them at the baggage carousel. The app was wrong. The luggage made the first leg of the trip, from Los Angeles International Airport to Chicago's O'Hare International Airport, but had not been loaded into the plane to Greece, despite what the app said.

[Los Angeles Times](#)

---

### **And now, the legal battle: Will California's pioneering 'revenge porn' law really help Rep. Katie Hill?**

Now former Rep. Katie Hill is quitting Congress - but she isn't going down without a fight. "I am leaving because I didn't want to be peddled by papers and blogs and websites, used by shameless operatives for the dirtiest gutter politics that I've ever seen and (by) the right-wing media to drive clicks and expand their audience by distributing intimate photos of me - taken without my knowledge, let alone my consent - for the sexual entertainment of millions," the San Fernando Valley lawmaker said in her final speech on the House floor.

[CalMatters](#)

### **This California firefighter nearly died. Then voters laid him off - in fight for lower taxes**

Firefighter Scott Wager was battling a wildfire in rural El Dorado County this summer when he and his partner were unexpectedly surrounded by roaring flames and flying embers. Wager and Capt. Chris Schwegler ran to their engine and got inside. The truck wouldn't move. The cab filled with thick black smoke as it began to catch fire. Wager's thoughts turned to his fiancée and the baby girl she's carrying.

[Sacramento Bee](#)

### **Some California governments sought to punish Alabama; state hardly noticed**

When the Alabama Legislature voted to ban nearly all abortions earlier this year, some California jurisdictions aimed to hit the Heart of Dixie in the pocketbook. The state hardly noticed. "There hasn't been any falling off that I've seen in tourism dollars or anything else from their moratorium at all," said State Sen. Greg Albritton (R-Atmore), who sponsored Alabama's tough abortion crackdown.

[WALA Mobile](#)

### **Newsom vows to step in if PG&E cannot restructure itself, as Trump trolls California over fires**

Gov. Gavin Newsom is summoning Pacific Gas and Electric Co.'s leaders to Sacramento this week, and says the state will step in if California's largest utility cannot resolve its leadership structure quickly. With PG&E mired in bankruptcy, different factions of investors - hedge funds that hold equity and hedge funds that hold corporate bonds - are battling for control of PG&E.

[CalMatters](#)

### **Petition to help refugees from deportation to Cambodia**

Family members, advocates and supporters gathered Friday at the state Capitol in Sacramento to urge Gov. Gavin Newsom to stop the deportation of Cambodian refugees with criminal convictions living in California. The coalition delivered a petition with 40,000 signatures to



the governor's office, asking for Newsom to pardon Saman Pho, who is being held by federal authorities, and to grant parole to Tith Ton, in an effort to prevent him from being transferred to immigration officials.

[Sacramento Bee](#)

### **California DMV data breach exposed thousands of drivers' social security information**

The California Department of Motor Vehicles said Tuesday that a data breach improperly shared social security information of more than 3,000 drivers with seven governmental agencies. According to the DMV, the data breach happened over the past four years, and the information could have been used in criminal, tax or child support investigations. The DMV said it discovered the data breach in August and sent a letter to all affected drivers informing them of the breach.

[CBS LA](#)

## **Crime**

### **California announces 148 arrests in illegal marijuana planting enforcement program**

State Attorney General Xavier Becerra Monday announced the arrests of 148 people so far this year during the Campaign Against Marijuana Planting Program enforcement effort, the nation's largest such multi-agency eradication program. During this year's effort, CAMP personnel also eradicated 953,459 marijuana plants from 345 raided grow sites across the state and seized 168 weapons, Becerra announced at a downtown Los Angeles news conference.

[City News Service](#)

### **Officials to investigate how a Nazi flag ended up hanging in state government building**

State officials sought to quell fears this week about racism in the ranks of state correctional officers after two Nazi flags were seen hanging inside a California Department of Corrections and Rehabilitation office in Sacramento. First published by local TV news stations on Monday, the troubling footage of the flags - one red with a black swastika in the center, another black with SS bolts, hanging on the wall next to a bulletin board - spread quickly, with national media coverage by the Washington Post, Newsweek, the Daily Beast and other outlets.

[The Jewish News of Northern California](#)

### **Off-duty California deputy threatens teen at gunpoint for playing music too loud**

A "big bully" Orange County sheriff's deputy as one witness described him is on administrative leave after threatening a group of teens with a handgun for playing their music too loudly last month. The officer was off duty and didn't immediately identify himself as a cop when he pulled up on the group on October 12 at a skate park in San Clemente, California.

[News Maven](#)

### **10 arrested for recycling fraud in alleged Vegas-to-LA smuggling ring**

Ten people have been arrested for allegedly smuggling tons of empty beverage containers from Nevada and Arizona into California in an effort to defraud the California Redemption Value fund, authorities announced Wednesday. Eight of the suspects allegedly participated in a scheme to bring large amounts of recyclables from Las Vegas to a dozen Los Angeles-area recycling centers, according to the California Department of Resources Recycling and Recovery, known as CalRecycle.

[City News Service](#)

## **Sentences/Convictions**

### **Sex offender who assaulted 6-year-old girl is sentenced**

A 32-year-old registered sex offender was sentenced Monday to 15 years to life in prison for sexually assaulting a 6-year-old girl on a Torrance elementary school playground. Dalan Anthony Johnson of Torrance pleaded no contest to one count of forcible lewd act on a child under the age of 14, according to the District Attorney's Office. The assault occurred March 28, after the girl was dropped off at Lincoln Elementary School.

[City News Service](#)

### **Man sentenced for fatally stabbing college student on public bus**

A man convicted of repeatedly stabbing a fellow passenger in the head with a knife in a random attack aboard a Montebello Public Transit bus was sentenced Wednesday to 26 years to life in state prison. Manuel Ortiz Jr. of Montebello, 29, was initially charged with attempted murder and aggravated mayhem, but he was subsequently charged with and convicted of first-degree murder after 22-year-old Austin Angelo Zavala died about two months after he was attacked on April 9, 2018.

[City News Service](#)

### **Man convicted for multiple burglaries of schools and homes in Ventura County**

Ventura County District Attorney's Office announced the conviction of a former local businessman on Wednesday in Ventura County. A jury convicted Cory Fletcher, 47, of Oxnard for 12 counts of felony burglary, including four first-degree residential burglaries, one burglary of an uninhabited house and seven burglaries of schools throughout Ventura County. From February 1, 2016 to March 31, 2016, Fletcher executed a series of residential and school burglaries with the aid of his 19-year-old employee and a 17-year-old relative of Fletcher's fiancé.

[KCOY/KEYT/KKFX](#)

### **Ex-NFL player Kellen Winslow Jr pleads guilty to rape**

Former NFL player Kellen Winslow Jr. pleaded guilty Monday to raping

an unconscious teen in 2003 and to sexual battery involving a 54-year-old hitchhiker in a deal that spared him the possibility of life in prison. Winslow initially hesitated and seemed to agonize over his decision. "I'm sorry. I'm just not thinking very clearly," Winslow told the judge at one point.

[Courthouse News Service](#)

### **Gang member sentenced to life in prison for series of murders and attempted murders in Baldwin Park**

A judge sentenced a 26-year-old gang member to life in prison without the possibility of parole Friday for orchestrating a series of two deadly shootings, two other shootings and a stabbing in Baldwin Park in 2013, authorities said. A Los Angeles County Superior Court jury convicted Ulises Jose Gutierrez of Baldwin Park in September of two counts of murder and three counts of attempted murder, according to Los Angeles County District Attorney's Office spokesman Paul Eakins.

[KTLA](#)

### **Armenian Power gang leader to be sentenced on 30 counts, including \$1 million 99 Cents Only debit card skimming scam**

The co-leader of an Armenian street gang was sentenced Monday to nearly 18 years behind bars for multiple federal racketeering crimes, including a debit-card-skimming operation that siphoned more than \$1 million from customers of 99 Cents Only stores across the Southland. Mher "Mike" Darbinyan, 44, formerly of Valencia, was also ordered by U.S. District Judge R. Gary Klausner to pay \$170,000 in fines and restitution to the victimized financial institutions.

[City News Service](#)

### **Arsonist portrayed in victims' drawings is sentenced to three years in prison**

A 37-year-old man, who was tracked down after victims made hand-drawn pictures of their attacker, pleaded guilty Wednesday and was immediately sentenced to three years in prison for setting fire to a tent occupied by two homeless people in Santa Ana. James Anthony Lawlor of Santa Ana pleaded guilty to arson of an inhabited structure, possession of flammable material, criminal threats and assault with force likely to produce great bodily injury, all felonies.

[City News Service](#)

## **Corrections/Parole**

### **Monterey County Jail escapees captured by U.S. Customs and Border Protection**

The two inmates charged with murder who broke out of a California jail over the weekend are back in custody, the Monterey County Sheriff's Office said Wednesday. Santos Fonseca, 21, and Jonathan Salazar, 20, broke free from the jail after climbing through a hole they made in a

bathroom ceiling of their housing unit. The inmates then squeezed through a wall before finding an escape hatch, authorities said.

[NBC Bay Area](#)

### **A California prisoner ripped out her eye and ate it. It's a sign of a bigger crisis that the state tried to downplay**

In July 2018, Dr. Michael Golding, the chief psychiatrist for California's correctional department, visited a maximum-security prison near Sacramento to shadow a couple of psychiatrists there. At least three-quarters of their scheduled patients missed their morning appointments. That afternoon, he and one of the psychiatrists went to a cell block, trying to find the no-shows among a huddle of towel-clad inmates returning from the shower, to talk at least for a minute or two with people struggling with issues like manic episodes and suicidal thoughts.

[Mother Jones](#)

## **Homeless**

### **L.A. voided millions of old tickets and warrants. Here's why it won't help homeless people**

When Los Angeles officials decided to toss out millions of citations and warrants in early October, they hailed it as a boon for homeless people. The purge, they said, would "unclog" the court system and stop the cycle of debt and arrests that has made it harder for the poorest Angelenos to land jobs and housing. But weeks after the announcement by L.A. City Atty. Mike Feuer, L.A. County Dist. Atty. Jackie Lacey and LAPD Chief Michel Moore, it has become clear that their amnesty program is unlikely to lead to a total end to criminal consequences for low-level offenses by people who live outdoors.

[Los Angeles Times](#)

### **These homes keep L.A.'s most vulnerable from becoming homeless. Now they're closing**

The news came in September: Long Beach Residential, a 49-bed home for adults who are mentally ill, was being sold. The residents of the converted apartment building, some of whom had lived there for decades, would have 60 days to move. It's a scenario that is becoming increasingly common across California, brought on by a combination of an inadequate state funding system and California's red hot real estate market.

[Los Angeles Times](#)

### **AIDS Healthcare Foundation sues city over Skid Row project**

A Los Angeles advocacy group has taken the city to court over a mammoth affordable housing program that is already under fire. AIDS Healthcare Foundation, or AHF, filed a complaint in Los Angeles County Superior Court last week demanding the city undo its denial of a \$24.8 million loan request under Measure HHH, money AHF planned to use to build 262 units of affordable housing in the Skid Row neighborhood.

## Articles of Interest

### **Saving L.A. by the numbers**

When I came to Los Angeles in 1970, I couldn't figure it out. The city and its environs were exhaustingly big and complicated. Eventually, I saw it's just a place of distinctive neighborhoods. If I learned about L.A. neighborhood by neighborhood, I'd understand the city. That experience came back to me recently when I visited Crosstown, a non-profit news organization run out of the USC Annenberg School of Journalism, in cooperation with the Integrated Media Systems Center at the university's Viterbi School of Engineering and mappers from SC's Spatial Sciences Institute.

[LA Observed](#)

### **My Herald Examiner days**

I had just accepted a job offer from the Los Angeles Herald Examiner to become an editorial writer and op-ed columnist when I realized I might be making a terrible mistake. It was late in the day on January 22, 1987 when I left the office after a promising first interview. On my way to my car, I spotted a Herald newsrack featuring the paper's "afternoon wrap," which was the morning edition with an added four-page wraparound section for late-breaking news.

[LA Observed](#)

### **The Government protects our food and cars. Why not our data?**

After Apple discovered in June that certain MacBook laptops could overheat, posing a fire hazard, the Consumer Product Safety Commission quickly issued a warning, along with information about consumer burns and smoke inhalation. But after Apple learned that its FaceTime video chat app was enabling consumers to listen in on the conversations of people they called - even when the recipients did not answer their phones - there was no designated federal protection agency to warn Americans or collect reports of privacy invasions.

[New York Times](#)

### **Universal says it owes artists nothing for fire that destroyed masters**

An attorney for Universal Music Group told a federal judge Monday that artists seeking a cut of an insurance settlement from a 2008 fire that destroyed their master recordings have no stake in the matter since recordings belong solely to the label. After the blaze at Universal Studios Hollywood destroyed 100,000 recordings, videos and other media, Soundgarden and other artists filed a federal class action against the label claiming it failed to properly store and protect the tapes.

[Courthouse News Service](#)



## **Study shows pension funds' refusal to divest from fossil fuels cost retired teachers, firefighters, and public workers \$19 billion**

Amid global demands for immediate and bold climate action, a new economic analysis released Tuesday reveals that the pensions of working-class people are paying the price for continued investments in the same fossil fuel companies that are ruining the planet. Toronto-based firm Corporate Knights revealed in a new study that three major state pension funds in California and Colorado lost over \$19 billion collectively as a result of investments in fossil fuel industries over ten years.

[Nation of Change](#)

## **'Public Safety Employees' hit hard by CA pension costs**

Stanislaus Consolidated Fire Protection District came into being 14 years ago when four small fire departments serving farms and small towns east of Modesto merged. The district now flirts with insolvency, a case study in how rapidly growing costs for pensions and other employee benefits are clobbering local governments. Four years ago, Stanislaus Consolidated had 80 employees, most of them firefighters, and more than \$13 million in revenues.

[CalMatters](#)

## **How Calif. public agencies can reform pension benefits**

In 2011, in a report that led to the enactment of the California Public Employees' Pension Reform Act, or PEPPRA, the Little Hoover Commission - an independent oversight agency in California - gave a dire warning: California's pension plans are dangerously underfunded, the result of overly generous benefit promises, wishful thinking and an unwillingness to plan prudently.

[Law360](#)

---

***For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).***

---



Los Angeles Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

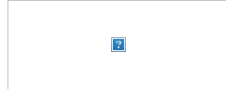
[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

From: [US-CERT](mailto:US-CERT)  
To: [mcg.mie@sunnyvale.ca.gov](mailto:mcg.mie@sunnyvale.ca.gov)  
Subject: Vulnerability Summary for the Week of October 28, 2019  
Date: Monday, November 04, 2019 2:44:17 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## Vulnerability Summary for the Week of October 28, 2019

11/04/2019 02:07 AM EST

Original release date: November 4, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-10-25	7.5	<a href="#">CVE-2019-8088 CONFIRM</a>
apache -- thrift	In Apache Thrift all versions up to and including 0.12.0, a server or client may run into an endless loop when feed with specific input data. Because the issue had already been partially fixed in version 0.11.0, depending on the installed version it affects only certain language bindings.	2019-10-29	7.8	<a href="#">CVE-2019-0205 MISC</a>
bitlbee -- bitlbee	Bitlbee does not drop extra group privileges correctly in unix.c	2019-10-29	7.5	<a href="#">CVE-2012-1187 MISC MISC MISC MISC</a>
cisco -- video_communications_server	Cisco Video Communications Server (VCS) before X7.0.3 contains a command injection vulnerability which allows remote, authenticated attackers to execute arbitrary commands.	2019-10-29	9	<a href="#">CVE-2011-2538 CONFIRM</a>
codesys -- eni_server	CODESYS V2.3 ENI server up to V3.2.2.24 has a Buffer Overflow.	2019-10-25	7.5	<a href="#">CVE-2019-16265 CONFIRM MISC</a>
d-link -- dir-865	D-Link DIR-865L has PHP File Inclusion in the router xml file.	2019-10-25	7.5	<a href="#">CVE-2013-4857 MISC MISC</a>
d-link -- dir-865l_devices	D-Link DIR-865L has SMB Symlink Traversal due to misconfiguration in the SMB service allowing symbolic links to be created to locations outside of the Samba share.	2019-10-25	7.9	<a href="#">CVE-2013-4855 MISC MISC MISC</a>
debian_project -- qtpartd	qtpartd has insecure library loading which may allow arbitrary code execution	2019-10-29	7.5	<a href="#">CVE-2010-3375 DEBIAN MISC MISC</a>
google -- chrome	browser/extensions/api/dial/dial_registry.cc in Google Chrome before 54.0.2840.98 on macOS, before 54.0.2840.99 on Windows, and before 54.0.2840.100 on Linux neglects to copy a device ID before an erase() call, which causes the erase operation to access data that that erase operation will destroy.	2019-10-25	7.5	<a href="#">CVE-2016-5202 MISC MISC MISC MISC MISC</a>
hot-world -- repetier-server	A directory traversal vulnerability was discovered in RepetierServer.exe in Repetier-Server 0.8 through 0.91 that allows for the creation of a user controlled XML file at an unintended location. When this is combined with CVE-2019-14451, an attacker can upload an "external command" configuration as a printer configuration, and achieve remote code execution. After exploitation, loading of the external command configuration is dependent on a system reboot or service restart.	2019-10-28	10	<a href="#">CVE-2019-14450 CONFIRM MISC</a>
hot-world -- repetier-server	RepetierServer.exe in Repetier-Server 0.8 through 0.91 does not properly validate the XML data structure provided when uploading a new printer configuration. When this is combined with CVE-2019-14450, an attacker can upload an "external command" configuration as a printer configuration, and achieve remote code execution. After exploitation, loading of the external command configuration is dependent on a system reboot or service restart.	2019-10-25	10	<a href="#">CVE-2019-14451 CONFIRM MISC</a>
intrasrv -- intrasrv	A remote SEH buffer overflow has been discovered in IntraSrv 1.0 (2007-06-03). An attacker may send a crafted HTTP GET or HEAD request that can result in a compromise of the hosting system.	2019-10-28	10	<a href="#">CVE-2019-17181 MISC MISC</a>
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.4, insecure Java Deserialization could potentially allow remote code execution.	2019-10-31	7.5	<a href="#">CVE-2019-18364 CONFIRM</a>
k7_computing -- antivirus_premium_and_total_security_and_ultimate_security	In K7 Antivirus Premium 16.0.xxx through 16.0.0120; K7 Total Security 16.0.xxx through 16.0.0120; and K7 Ultimate Security 16.0.xxx through 16.0.0120, the module K7TSHlpr.dll improperly validates the administrative privileges of the user, allowing arbitrary registry writes in the K7AVOptn.dll module to facilitate escalation of privileges via inter-process communication with a service process.	2019-10-28	7.5	<a href="#">CVE-2019-16897 MISC</a>
labf -- nfsaxe_ftp_client	Buffer overflow in LabF nfsAxe FTP client 3.7 allows an attacker to execute code remotely.	2019-10-25	7.5	<a href="#">CVE-2017-14742 EXPLOIT-DB</a>
linksys -- ea6500_router	Linksys EA6500 has SMB Symlink Traversal allowing symbolic links to be created to locations outside of the Samba share.	2019-10-25	10	<a href="#">CVE-2013-4658 MISC MISC MISC</a>
medoo -- medoo	columnQuote in medoo before 1.7.5 allows remote attackers to perform a SQL Injection due to improper escaping.	2019-10-30	7.5	<a href="#">CVE-2019-10762 MISC MISC</a>
mikrotik -- routeros	RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below insufficiently validate where upgrade packages are download from when using the autoupgrade feature. Therefore, a remote attacker can trick the router into "upgrading" to an older version of RouterOS and possibly	2019-10-29	8.5	<a href="#">CVE-2019-3977 MISC</a>

	resetting all the system's usernames and passwords.			
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a buffer overflow in a web application via a long username or password.	2019-10-25	7.5	<a href="#">CVE-2016-2356</a> MISC MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 allow remote attackers to bypass authentication and access a protected resource by simultaneously making a request for the unprotected vb.htm resource.	2019-10-25	7.5	<a href="#">CVE-2016-2359</a> MISC MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Undocumented hard-coded user passwords for root, ineaadmin, mitsadmin, and maint could allow an attacker to gain unauthorised access to the RTU. (Also, the accounts ineaadmin and mitsadmin are able to escalate privileges to root without supplying a password due to insecure entries in /etc/sudoers on the RTU.)	2019-10-28	10	<a href="#">CVE-2019-14930</a> MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote OS Command Injection vulnerability allows an attacker to execute arbitrary commands on the RTU due to the passing of unsafe user supplied data to the RTU's system shell. Functionality in mobile.php provides users with the ability to ping sites or IP addresses via Mobile Connection Test. When the Mobile Connection Test is submitted, action.php is called to execute the test. An attacker can use a shell command separator (;) in the host variable to execute operating system commands upon submitting the test data.	2019-10-28	10	<a href="#">CVE-2019-14931</a> MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Hard-coded SSH keys allow an attacker to gain unauthorised access or disclose encrypted data on the RTU due to the keys not being regenerated on initial installation or with firmware updates. In other words, these devices use private-key values in /etc/ssh/ssh_host_rsa_key, /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_dsa_key files that are publicly available from the vendor web sites.	2019-10-28	7.5	<a href="#">CVE-2019-14926</a> MISC MISC
philips -- intellispace_perinatal	In IntelliSpace Perinatal, Versions K and prior, a vulnerability within the IntelliSpace Perinatal application environment could enable an unauthorized attacker with physical access to a locked application screen, or an authorized remote desktop session host application user to break-out from the containment of the application and access unauthorized resources from the Windows operating system as the limited-access Windows user. Due to potential Windows vulnerabilities, it may be possible for additional attack methods to be used to escalate privileges on the operating system.	2019-10-25	7.2	<a href="#">CVE-2019-13546</a> MISC
php -- php	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.	2019-10-28	7.5	<a href="#">CVE-2019-11043</a> REDHAT REDHAT REDHAT REDHAT CONFIRM MISC FEDORA FEDORA FEDORA CONFIRM CONFIRM UBUNTU UBUNTU DEBIAN DEBIAN
pixelpost -- pixelpost	pixelpost 1.7.1 has SQL injection	2019-10-28	7.5	<a href="#">CVE-2009-4899</a> MISC DEBIAN MISC
rconfig -- rconfig	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to search.crud.php because the catCommand parameter is passed to the exec function without filtering, which can lead to command execution.	2019-10-28	9	<a href="#">CVE-2019-16663</a> MISC MISC MISC MISC MISC
rconfig -- rconfig	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to ajaxServerSettingsChk.php because the rootUname parameter is passed to the exec function without filtering, which can lead to command execution.	2019-10-28	10	<a href="#">CVE-2019-16662</a> MISC MISC MISC MISC MISC MISC
rittal -- rittal_chiller_sk_3232_series	Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems is configured using hard-coded credentials. These credentials could allow attackers to influence the primary operations of the affected systems, namely turning the cooling unit on and off and setting the temperature set point.	2019-10-25	10	<a href="#">CVE-2019-13553</a> FULLDISC MISC
sequelize -- sequelize	Sequelize all versions prior to 3.35.1, 4.44.3, and 5.8.11 are vulnerable to SQL Injection due to JSON path keys not being properly escaped for the MySQL/MariaDB dialects.	2019-10-29	7.5	<a href="#">CVE-2019-10748</a> MISC MISC MISC
sequelize -- sequelize	sequelize before version 3.35.1 allows attackers to perform a SQL Injection due to the JSON path keys not being properly sanitized in the Postgres dialect.	2019-10-29	7.5	<a href="#">CVE-2019-10749</a> MISC MISC
snoopy -- snoopy e	Snoopy before 2.0.0 has a security hole in exec cURL	2019-10-28	7.5	<a href="#">CVE-2002-2444</a> MISC DEBIAN MISC
sugarcrm -- sugarcrm	SugarCRM CE <= 6.3.1 contains scripts that use "unserialize()" with user controlled input which allows remote attackers to execute arbitrary PHP code.	2019-10-29	7.5	<a href="#">CVE-2012-0694</a> MISC MISC EXPLOIT-DB
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains global buffer overflow in HandleCORREBBP macro function, which can potentially result code execution. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	<a href="#">CVE-2019-8287</a> MLIST
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains heap buffer overflow in InitialiseRFBConnection function, which can potentially result code execution. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	<a href="#">CVE-2019-15679</a> MLIST
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains heap buffer overflow in			<a href="#">CVE-2019-15678</a>

	rfbServerCutText handler, which can potentially result code execution.. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	MLIST
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has Local File Inclusion	2019-10-28	7.5	CVE-2010-4239 MISC MISC MISC MISC
tp-link -- tl-wdr4300_devices	TP-Link TL-WDR4300 version 3.13.31 has multiple CSRF vulnerabilities.	2019-10-25	9.3	CVE-2013-4848 MISC MISC MISC MISC MISC
transmission -- transmission	Transmission before 1.92 allows an attacker to cause a denial of service (crash) or possibly have other unspecified impact via a large number of tr arguments in a magnet link.	2019-10-30	7.5	CVE-2010-0748 MISC CONFIRM MISC CONFIRM MLIST
youphtube -- youphtube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Uri in /objects/getImage.php is vulnerable to a command injection attack.	2019-10-25	7.5	CVE-2019-5127 MISC
youphtube -- youphtube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Uri in /objects/getImageMP4.php is vulnerable to a command injection attack.	2019-10-25	7.5	CVE-2019-5128 MISC
youphtube -- youphtube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Uri in /objects/getSpiritsFromVideo.php is vulnerable to a command injection attack.	2019-10-25	7.5	CVE-2019-5129 MISC
ytnef -- ytnef	ytnef has directory traversal	2019-10-29	7.5	CVE-2009-3887 MISC MISC MISC MISC MISC
zend_framework -- zend_framework	Zend Framework before 2.2.10 and 2.3.x before 2.3.5 has Potential SQL injection in PostgreSQL Zend\Db adapter.	2019-10-25	7.5	CVE-2015-0270 MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8087 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4 and 6.3 have a cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8083 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8084 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8085 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a cross-site request forgery vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	CVE-2019-8234 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have an authentication bypass vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8081 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8082 CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	CVE-2019-8086 CONFIRM
apache -- hadoop	Hadoop 1.0.3 contains a symlink vulnerability.	2019-10-29	5	CVE-2012-2945 MISC MISC
apache -- thrift	In Apache Thrift 0.9.3 to 0.12.0, a server implemented in Go using TJSONProtocol or TSimpleJSONProtocol may panic when feed with invalid input data.	2019-10-29	5	CVE-2019-0210 CONFIRM
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows directory traversal by issuing a special HTTP POST request with ../ characters. This could lead to create malicious HTML file, because they can inject a content with crafted template. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	CVE-2019-17324 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows remote attacker to upload arbitrary local file via the ActiveX method in RexViewerCtrl30.ocx. That could lead to disclosure of sensitive information. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	CVE-2019-17325 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows remote attacker to arbitrary file deletion by issuing a HTTP GET request with a specially crafted parameter. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	5.8	CVE-2019-17326 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows arbitrary file creation via a POST request with the parameter set to the file path to be written. This can be an executable file that is written to in the arbitrary directory. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	CVE-2019-17322 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version have an information disclosure issue. When requesting web page associated with session, could leak username via session file path of HTTP response data. No authentication is required.	2019-10-30	5	CVE-2019-17321 MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows arbitrary file creation and execution via report print function of rexpert viewer with modified XML document. User	2019-10-30	6.8	CVE-2019-17323

	interaction is required to exploit this vulnerability in that the target must visit a malicious web page.			MISC
corehr -- core_portal	CoreHR Core Portal before 27.0.7 allows stored XSS.	2019-10-25	4.3	<a href="#">CVE-2019-18221</a> MISC MISC
debian_project -- mercurial	Mercurial before 1.6.4 fails to verify the Common Name field of SSL certificates which allows remote attackers who acquire a certificate signed by a Certificate Authority to perform a man-in-the-middle attack.	2019-10-29	4.3	<a href="#">CVE-2010-4237</a> MISC CONFIRM CONFIRM MISC
debian_project -- pootle	pootle 2.0.5 has XSS via 'match_names' parameter	2019-10-28	4.3	<a href="#">CVE-2010-4245</a> MISC DEBIAN MISC MISC
debian_project -- xpdf	In xpdf, the xref table contains an infinite loop which allows remote attackers to cause a denial of service (application crash) in xpdf-based PDF viewers.	2019-10-30	4.3	<a href="#">CVE-2010-0207</a> MISC MISC
debian_project -- xpdf	xpdf allows remote attackers to cause a denial of service (NULL pointer dereference and crash) in the way it processes JBIG2 PDF stream objects.	2019-10-30	4.3	<a href="#">CVE-2010-0206</a> MISC MISC
debian_project -- zoo	Zoo 2.10 has Directory traversal	2019-10-28	5	<a href="#">CVE-2005-2349</a> MISC MISC
devada -- dzone_and_answerhub	An XML External Entity Injection vulnerability exists in Dzone AnswerHub.	2019-10-28	5	<a href="#">CVE-2017-15725</a> MISC
digium -- asterisk	asterisk allows calls on prohibited networks	2019-10-29	5	<a href="#">CVE-2009-3723</a> MISC MISC MISC
fabrik -- fabrik	Reflected Cross-Site Scripting (XSS) vulnerability in the fabrik_referrer hidden field in the Fabrikar Fabrik component through v3.8.1 for Joomla! allows remote attackers to inject arbitrary web script via the HTTP Referer header.	2019-10-29	4.3	<a href="#">CVE-2018-10727</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of Javascript in the HTML2PDF plugin. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8692.	2019-10-25	6.8	<a href="#">CVE-2019-17139</a> MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9276.	2019-10-25	6.8	<a href="#">CVE-2019-17145</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DWG files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9274.	2019-10-25	6.8	<a href="#">CVE-2019-17144</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of script within a Keystroke action of a listbox field. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9081.	2019-10-25	6.8	<a href="#">CVE-2019-17142</a> MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of script within a Calculate action of a text field. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9044.	2019-10-25	6.8	<a href="#">CVE-2019-17141</a> MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9273.	2019-10-25	4.3	<a href="#">CVE-2019-17143</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the OnFocus event. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9091.	2019-10-25	6.8	<a href="#">CVE-2019-17140</a> MISC MISC
foxit -- studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion from JPEG to EPS. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8809.	2019-10-25	4.3	<a href="#">CVE-2019-17138</a> MISC MISC
gnuboard -- gnuboard5	GNUBOARD5 before 5.3.2.0 has XSS that allows remote attackers to inject arbitrary web script or HTML via the "board group extra contents" parameter, aka the admn/boardgroup_form_update.php gr_1~10 parameter.	2019-10-30	4.3	<a href="#">CVE-2018-18678</a> MISC MISC MISC
gpw -- gpw	gpw generates shorter passwords than required	2019-10-29	5	<a href="#">CVE-2011-4931</a> MISC MISC MISC MISC
honeywell -- ip-ak2	In IP-AK2 Access Control Panel Version 1.04.07 and prior, the integrated web server of the affected devices could allow remote attackers to obtain web configuration data, which can be accessed without authentication over the network.	2019-10-25	5	<a href="#">CVE-2019-13525</a> MISC
ibm -- api_connect	IBM API Connect version V5.0.0.0 through 5.0.8.7 could reveal sensitive information to			<a href="#">CVE-2019-4600</a>



	an attacker using a specially crafted HTTP request. IBM X-Force ID: 167883.	2019-10-29	5	XF <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 162260.	2019-10-25	5	<a href="#">CVE-2019-4399</a> XF <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 162261.	2019-10-25	4	<a href="#">CVE-2019-4400</a> XF <a href="#">CONFIRM</a>
ibm -- maximo_asset_management	After installing the IBM Maximo Health- Safety and Environment Manager 7.6.1, a user is granted additional privileges that they are not normally allowed to access. IBM X-Force ID: 165948.	2019-10-29	6.5	<a href="#">CVE-2019-4546</a> XF <a href="#">CONFIRM</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance could allow unauthenticated attacker to cause a denial of service in the reverse proxy component. IBM X-Force ID: 156159.	2019-10-25	5	<a href="#">CVE-2019-4036</a> XF <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 161418.	2019-10-29	5	<a href="#">CVE-2019-4339</a> XF <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 specifies permissions for a security-critical resource which could lead to the exposure of sensitive information or the modification of that resource by unintended parties. IBM X-Force ID: 160986.	2019-10-29	6.4	<a href="#">CVE-2019-4306</a> XF <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores sensitive information in cleartext within a resource that might be accessible to another control sphere. IBM X-Force ID: 1610141.	2019-10-29	5	<a href="#">CVE-2019-4314</a> XF <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 does not set the secure attribute for cookies in HTTPS sessions, which could cause the user agent to send those cookies in plaintext over an HTTP session. IBM X-Force ID: 161210.	2019-10-29	4.3	<a href="#">CVE-2019-4330</a> XF <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 161209.	2019-10-29	4	<a href="#">CVE-2019-4329</a> XF <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161037.	2019-10-29	5	<a href="#">CVE-2019-4311</a> XF <a href="#">CONFIRM</a>
ikiwiki -- ikiwiki	A cross-site scripting (XSS) vulnerability in ikiwiki before 3.20101112 allows remote attackers to inject arbitrary web script or HTML via a comment.	2019-10-30	4.3	<a href="#">CVE-2010-1673</a> CONFIRM MISC
ikiwiki -- ikiwiki	Cross Site Scripting (XSS) in ikiwiki before 3.20110122 could allow remote attackers to insert arbitrary JavaScript due to insufficient checking in comments.	2019-10-29	4.3	<a href="#">CVE-2011-0428</a> CONFIRM MISC
jetbrains -- teamcity	In JetBrains YouTrack before 2019.2.55152, removing tags from the issues list without the corresponding permission was possible.	2019-10-31	5	<a href="#">CVE-2019-18369</a> CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.2, access could be gained to the history of builds of a deleted build configuration under some circumstances.	2019-10-31	5	<a href="#">CVE-2019-18363</a> CONFIRM
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. It is possible to force a logged-in administrator to execute code through a /reports-viewScriptReport.view CSRF vulnerability.	2019-10-29	6.8	<a href="#">CVE-2019-9926</a> MISC MISC
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. Sending an SVG containing an XXE payload to the endpoint visualization-exportImage.view or visualization-exportPDF.view allows local files to be read.	2019-10-29	5	<a href="#">CVE-2019-9757</a> MISC MISC
libpod -- libpod	An issue was discovered in Podman in libpod before 1.6.0. It resolves a symlink in the host context during a copy operation from the container to the host, because an undesired glob operation occurs. An attacker could create a container image containing particular symlinks that, when copied by a victim user to the host filesystem, may overwrite existing files with others from the host.	2019-10-28	5.8	<a href="#">CVE-2019-18466</a> MISC MISC MISC MISC
mcafee -- mcafee_total_protection	A File Masquerade vulnerability in McAfee Total Protection (MTP) version 16.0.R21 and earlier in Windows client allowed an attacker to read the plaintext list of AV-Scan exclusion files from the Windows registry, and to possibly replace excluded files with potential malware without being detected.	2019-10-28	4.6	<a href="#">CVE-2019-3636</a> CONFIRM
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension through 1.34 for MediaWiki. Previously hidden (restricted) AbuseFilter filters were viewable (or their differences were viewable) to unprivileged users, thus disclosing potentially sensitive information.	2019-10-29	5	<a href="#">CVE-2019-18612</a> MISC MISC
mediawiki -- mediawiki	A cross-site scripting (XSS) vulnerability in MediaWiki before 1.19.5 and 1.20.x before 1.20.4 and allows remote attackers to inject arbitrary web script or HTML via Lua function names.	2019-10-31	4.3	<a href="#">CVE-2013-1951</a> MISC MISC MISC MISC MISC MISC MISC CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in the CheckUser extension through 1.34 for MediaWiki. Certain sensitive information within oversighted edit summaries made available via the MediaWiki API was potentially visible to users with various levels of access to this extension. Said users should not have been able to view these oversighted edit summaries via the MediaWiki API.	2019-10-29	4	<a href="#">CVE-2019-18611</a> MISC MISC
mediawiki -- mediawiki	mediawiki allows deleted text to be exposed	2019-10-29	5	<a href="#">CVE-2012-0046</a> MISC MISC MISC
mikrotik -- routers	RouterOS versions 6.45.6 Stable, 6.44.5 Long-term, and below are vulnerable to a DNS unrelated data attack. The router adds all A records to its DNS cache even when the records are unrelated to the domain that was queried. Therefore, a remote attacker controlled DNS server can poison the router's DNS cache via malicious responses with additional and untrue records.	2019-10-29	5	<a href="#">CVE-2019-3979</a> MISC
mikrotik -- routers	RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below are vulnerable to an arbitrary directory creation vulnerability via the upgrade package's name field. If an authenticated user installs a malicious package then a directory could be created and the developer shell could be enabled.	2019-10-29	6.5	<a href="#">CVE-2019-3976</a> MISC
mikrotik -- routers	RouterOS versions 6.45.6 Stable, 6.44.5 Long-term, and below allow remote unauthenticated attackers to trigger DNS queries via port 8291. The queries are sent from the router to a server of the attacker's choice. The DNS responses are cached by the router, potentially resulting in cache poisoning	2019-10-29	5	<a href="#">CVE-2019-3978</a> MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a default set of 10 privileged accounts with hardcoded credentials. They are accessible if the customer has not configured 10 actual user accounts.	2019-10-25	5	<a href="#">CVE-2016-2358</a> MISC MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a default root password in /etc/shadow that is the same across different customers' installations.	2019-10-25	5	<a href="#">CVE-2016-2360</a> MISC MISC MISC

milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a hardcoded SSL private key under the /etc/config directory.	2019-10-25	5	<a href="#">CVE-2016-2357</a> MISC MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A world-readable /usr/smarttu/init/settings.xml configuration file on the file system allows an attacker to read sensitive configuration settings such as usernames, passwords, and other sensitive RTU data due to insecure permission assignment.	2019-10-28	4	<a href="#">CVE-2019-14925</a> MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Stored cleartext passwords could allow an unauthenticated attacker to obtain configured username and password combinations on the RTU due to the weak credentials management on the RTU. An unauthenticated user can obtain the exposed password credentials to gain access to the following services: DDNS service, Mobile Network Provider, and OpenVPN service.	2019-10-28	5	<a href="#">CVE-2019-14929</a> MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote configuration download vulnerability allows an attacker to download the smartRTU's configuration file (which contains data such as usernames, passwords, and other sensitive RTU data).	2019-10-28	5	<a href="#">CVE-2019-14927</a> MISC MISC
netapp -- clustered_data_ontap	Clustered Data ONTAP versions 9.2 through 9.6 are susceptible to a vulnerability which allows an attacker to use IPping to cause a Denial of Service (DoS).	2019-10-25	5	<a href="#">CVE-2019-5508</a> MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to an information disclosure vulnerability because uninitialized scalars are sent over the network to a peer.	2019-10-29	5	<a href="#">CVE-2019-18602</a> MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to information leakage upon certain error conditions because uninitialized RPC output variables are sent over the network to a peer.	2019-10-29	4.3	<a href="#">CVE-2019-18603</a> MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to denial of service from unserialized data access because remote attackers can make a series of VOTE_Debug RPC calls to crash a database server within the SVOTE_Debug RPC handler.	2019-10-29	5	<a href="#">CVE-2019-18601</a> MISC
pimcore -- pimcore	Pimcore 6.2.3 has XSS in the translations grid because bundles/AdminBundle/Resources/public/js/pimcore/settings/translations.js mishandles certain HTML elements.	2019-10-31	4.3	<a href="#">CVE-2019-18656</a> MISC
pixelpost -- pixelpost	pixelpost 1.7.1 has XSS	2019-10-28	4.3	<a href="#">CVE-2009-4900</a> MISC DEBIAN MISC
python_keyring_lib -- python_keyring_lib	Python keyring lib before 0.10 created keyring files with world-readable permissions.	2019-10-28	5	<a href="#">CVE-2012-5577</a> MISC CONFIRM MISC MISC MISC
rittal -- rittal_chiller_sk_3232_series	Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems does not provide a sufficient level of protection against unauthorized configuration changes. Primary operations, namely turning the cooling unit on and off and setting the temperature set point, can be modified without authentication.	2019-10-25	5	<a href="#">CVE-2019-13549</a> FULLDISC MISC
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the firmware with no firmware image inside the package using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6841</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the firmware with a missing web server image inside the package using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6842</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the controller with an empty firmware package using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6843</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the controller with a firmware package containing an invalid web server image using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6844</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the FTP service when upgrading the firmware with a version incompatible with the application in the controller using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6847</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-200: Information Exposure vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause the disclosure of sensitive information when using specific Modbus services provided by the REST API of the controller/communication module.	2019-10-29	5	<a href="#">CVE-2019-6849</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause a Denial of Service attack on the PLC when sending specific data on the REST API of the controller/communication module.	2019-10-29	5	<a href="#">CVE-2019-6848</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-200: Information Exposure vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause the disclosure of sensitive information when reading specific registers with the REST API of the controller/communication module.	2019-10-29	5	<a href="#">CVE-2019-6850</a> CONFIRM
terramaster -- fs-210_devices	An issue was discovered on TerraMaster FS-210 4.0.19 devices. Normal users can use 1.user.php for privilege elevation.	2019-10-28	6.5	<a href="#">CVE-2019-18195</a> MISC
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains null pointer dereference in HandleZlibBPP function, which results Denial of System (DoS). This attack appear to be exploitable via network connectivity.	2019-10-29	5	<a href="#">CVE-2019-15680</a> MLIST
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has XSS	2019-10-28	4.3	<a href="#">CVE-2010-4240</a> MISC MISC MISC MISC
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has CSRF	2019-10-28	6.8	<a href="#">CVE-2010-4241</a> MISC MISC MISC MISC
total_defense -- anti-virus	The malware scan function in Total Defense Anti-virus 11.5.2.28 is vulnerable to a TOCTOU bug; consequently, symbolic link attacks allow privileged files to be deleted.	2019-10-31	5.8	<a href="#">CVE-2019-18644</a> MISC
transmission -- transmission	Transmission before 1.92 allows attackers to prevent download of a file by corrupted data during the endgame.	2019-10-30	5	<a href="#">CVE-2010-0749</a> MISC CONFIRM MISC CONFIRM

				<a href="#">MLIST</a>
trend_micro -- apex_one	Trend Micro Apex One could be exploited by an attacker utilizing a command injection vulnerability to extract files from an arbitrary zip file to a specific folder on the Apex One server, which could potentially lead to remote code execution (RCE). The remote process execution is bound to the IUSR account, which has restricted permission and is unable to make major system changes. An attempted attack requires user authentication.	2019-10-28	5	<a href="#">CVE-2019-18188</a> <a href="#">N/A</a>
trend_micro -- office_scan	Trend Micro OfficeScan versions 11.0 and XG (12.0) could be exploited by an attacker utilizing a directory traversal vulnerability to extract files from an arbitrary zip file to a specific folder on the OfficeScan server, which could potentially lead to remote code execution (RCE). The remote process execution is bound to a web service account, which depending on the web platform used may have restricted permissions. An attempted attack requires user authentication.	2019-10-28	5	<a href="#">CVE-2019-18187</a> <a href="#">N/A</a>
youshphptube -- youshphptube	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5120</a> <a href="#">MISC</a>
youshphptube -- youshphptube	SQL injection vulnerabilities exist in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter name in /objects/pluginSwitch.json.php.	2019-10-25	6.5	<a href="#">CVE-2019-5122</a> <a href="#">MISC</a>
youshphptube -- youshphptube	SQL injection vulnerabilities exist in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter uuid in /objects/pluginSwitch.json.php	2019-10-25	6.5	<a href="#">CVE-2019-5121</a> <a href="#">MISC</a>
youshphptube -- youshphptube	An exploitable SQL injection vulnerability exist in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5119</a> <a href="#">MISC</a>
youshphptube -- youshphptube	Exploitable SQL injection vulnerabilities exist in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5117</a> <a href="#">MISC</a>
youshphptube -- youshphptube	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause a SQL injection. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5116</a> <a href="#">MISC</a>
youshphptube -- youshphptube	An exploitable SQL injection vulnerability exists in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5114</a> <a href="#">MISC</a>
youshphptube -- youshphptube	Specially crafted web requests can cause SQL injections in YouPHPTube 7.6. An attacker can send a web request with Parameter dir in /objects/pluginSwitch.json.php.	2019-10-25	6.5	<a href="#">CVE-2019-5123</a> <a href="#">MISC</a>
zucchetti -- infobusiness	Multiple Reflected Cross-site Scripting (XSS) vulnerabilities exist in Zucchetti InfoBusiness before and including 4.4.1. The browsing component did not properly sanitize user input (encoded in base64). This also applies to the search functionality for the searchKey parameter.	2019-10-30	4.3	<a href="#">CVE-2019-18205</a> <a href="#">MISC</a>
zucchetti -- infobusiness	Zucchetti InfoBusiness before and including 4.4.1 allows any authenticated user to upload .php files in order to achieve code execution.	2019-10-30	6.5	<a href="#">CVE-2019-18204</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- airflow	A malicious admin user could edit the state of objects in the Airflow metadata database to execute arbitrary javascript on certain page views. This also presented a Local File Disclosure vulnerability to any file readable by the webserver process.	2019-10-30	3.5	<a href="#">CVE-2019-12417</a> <a href="#">MLIST</a>
d-link -- dir-865L_devices	D-Link DIR-865L has Information Disclosure.	2019-10-25	2.9	<a href="#">CVE-2013-4856</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
debian_project -- mailscanner	mailscanner can allow local users to prevent virus signatures from being updated	2019-10-28	2.1	<a href="#">CVE-2010-3293</a> <a href="#">MISC</a> <a href="#">DEBIAN</a> <a href="#">MISC</a> <a href="#">MISC</a>
debian_project -- paxtext	paxtext handles temporary files insecurely	2019-10-29	2.1	<a href="#">CVE-2010-3373</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gmer -- gmer	A stack based buffer overflow vulnerability exists in the method receiving data from SysTreeView32 control of the GMER 2.1.19357 application. A specially created long path can lead to a buffer overflow on the stack resulting in code execution. An attacker needs to create path longer than 99 characters to trigger this vulnerability.	2019-10-29	2.1	<a href="#">CVE-2016-4289</a> <a href="#">MISC</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a local user to obtain sensitive information from temporary script files. IBM X-Force ID: 162333.	2019-10-25	2.1	<a href="#">CVE-2019-4395</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 is vulnerable to HTTP response splitting attacks, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject arbitrary HTTP headers and cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning or cross-site scripting, and possibly obtain sensitive information. IBM X-Force ID: 162236.	2019-10-25	3.5	<a href="#">CVE-2019-4396</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 is vulnerable to HTTP Response Splitting caused by improper caching of content. This would allow the attacker to perform further attacks, such as Web Cache poisoning, cross-site scripting and possibly obtain sensitive information. IBM X-Force ID: 163682.	2019-10-25	3.5	<a href="#">CVE-2019-4461</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 contain APIs that could be used by a local user to send email. IBM X-Force ID: 162232.	2019-10-25	2.1	<a href="#">CVE-2019-4394</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 160987.	2019-10-29	2.1	<a href="#">CVE-2019-4307</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses hard coded credentials which could allow a local user to obtain highly sensitive information. IBM X-Force ID: 161035.	2019-10-29	2.1	<a href="#">CVE-2019-4309</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. The display name of a user is vulnerable to stored XSS that can execute on administrators from security/permissions.view, security/addUsers.view, or wiki/Administration/page.view in the admin panel, leading to privilege escalation.	2019-10-29	3.5	<a href="#">CVE-2019-9758</a> MISC MISC
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the configuration report page (adm_config_report.php) in MantisBT 1.2.0rc1 before 1.2.14 allows remote authenticated users to inject arbitrary web script or HTML via a complex value.	2019-10-31	3.5	<a href="#">CVE-2013-1934</a> MISC MISC MISC CONFIRM MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A number of stored cross-site script (XSS) vulnerabilities allow an attacker to inject malicious code directly into the application. An example input variable vulnerable to stored XSS is SerialInitialModemString in the index.php page.	2019-10-28	3.5	<a href="#">CVE-2019-14928</a> MISC
postgresql -- postgresql	Postgresql, versions 11.x before 11.5, is vulnerable to a memory disclosure in cross-type comparison for hashed subplan.	2019-10-29	3.5	<a href="#">CVE-2019-10209</a> CONFIRM CONFIRM
postgresql -- postgresql_windows_installer	Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.	2019-10-29	1.9	<a href="#">CVE-2019-10210</a> CONFIRM CONFIRM
total_defense -- antivirus	The quarantine restoration function in Total Defense Anti-virus 11.5.2.28 is vulnerable to symbolic link attacks, allowing files to be written to privileged directories.	2019-10-31	2.1	<a href="#">CVE-2019-18645</a> MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published Score	Source & Patch Info
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. Lack of sanitization of user-supplied input cause SQL injection vulnerabilities. An attacker can leverage these vulnerabilities to disclose information.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18229</a> MISC MISC MISC MISC MISC MISC MISC MISC MISC
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. There is an unsecured function that allows anyone who can access the IP address to use the function without authentication.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-13547</a> MISC MISC
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. XXE vulnerabilities exist that may allow disclosure of sensitive data.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18227</a> MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. Path traversal vulnerabilities are caused by a lack of proper validation of a user-supplied path prior to use in file operations. An attacker can leverage these vulnerabilities to remotely execute code while posing as an administrator.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-13551</a> MISC MISC MISC MISC
amd -- atidxx64.dll_driver	An exploitable memory corruption vulnerability exists in AMD ATIDXX64.DLL driver, versions 25.20.15031.5004 and 25.20.15031.9002. A specially crafted pixel shader can cause an out-of-bounds memory write. An attacker can provide a specially crafted shader file to trigger this vulnerability. This vulnerability can be triggered from VMware guest, affecting VMware host.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5049</a> MISC
apache -- struts	Apache Struts before 2.3.1.2 allows remote attackers to bypass security protections in the ParameterInterceptor class and execute arbitrary commands.	2019- r/bt yet calculated 01	<a href="#">CVE-2011-3923</a> MISC EXPLOIT-DB BID MISC MISC XF MISC
apak -- wholesale_floorplanning_finance	Apak Wholesale Floorplanning Finance 6.31.8.3 and 6.31.8.5 allows XSS via the mainForm:loanNotesnotes:0:rich_text_editor_note_text parameter to WFS/agreementView.faces in the Notes section. Although versions 6.31.8.3 and 6.31.8.5 are confirmed to be affected, all versions with the vulnerable WYSIWYG ?Notes? section are likely affected.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-17551</a> MISC
archiver -- archiver	All versions of archiver allow attacker to perform a Zip Slip attack via the "unarchive" functions. It is exploited using a specially crafted zip archive, that holds path traversal filenames. When exploited, a filename in a malicious archive is concatenated to the target extraction directory, which results in the final path ending up outside of the target folder. For instance, a zip may hold a file with a ". /./file.exe" location and thus break out of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-10743</a> MISC MISC MISC
archos -- safe-t_devices	On Archos Safe-T devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. In other words, the side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-14358</a> MISC
aruba -- instant	Aruba Instant 4.x prior to 6.4.4.8-4.2.4.12, 6.5.x prior to 6.5.4.11, 8.3.x prior to 8.3.0.6, and 8.4.x prior to 8.4.0.1 allows Command injection.	2019- r/bt yet calculated 30	<a href="#">CVE-2018-16417</a> BID CONFIRM MISC CONFIRM MISC
	An exploitable uninitialized pointer vulnerability exists in the Word document parser of the the		

atlantis_word_processor -- atlantis_word_processor	Atlantis Word Processor. A specially crafted document can cause an array fetch to return an uninitialized pointer and then performs some arithmetic before writing a value to the result. Usage of this uninitialized pointer can allow an attacker to corrupt heap memory resulting in code execution under the context of the application. An attacker must convince a victim to open a document in order to trigger this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2018-3983</a> MISC
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app before 1.6.14_J8 for Jira. It is possible to obtain a list of all Jira projects without authentication/authorization via the plugins/servlet/nfj/ProjectFilter?searchQuery= URI.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-16908</a> MISC MISC
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app before 1.6.14_J8 for Jira. It is possible to obtain a list of all Jira projects (with authentication as a Jira user, but without authorization for specific projects) via the plugins/servlet/nfj/NotificationSettings URI.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-16909</a> MISC MISC
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app 1.6.13_J8 for Jira. It is possible to obtain a list of all valid Jira usernames without authentication/authorization via the plugins/servlet/nfj/UserFilter?searchQuery=@ URI.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16907</a> MISC BUGTRAQ
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app 1.6.13_J8 for Jira. By using plugins/servlet/nfj/PushNotification?username= with a modified username, a different user's notifications can be read without authentication/authorization. These notifications are then no longer displayed to the normal user.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16906</a> MISC BUGTRAQ
atlassian -- jira	An issue summary information disclosure vulnerability exists in Atlassian Jira Tempo plugin, version 4.10.0. Authenticated users can obtain the summary for issues they do not have permission to view via the Tempo plugin.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5095</a> MISC
autojump -- autojump	autojump before 21.5.8 allows local users to gain privileges via a Trojan horse custom_install directory in the current working directory.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-2012</a> MISC MISC MISC CONFIRM CONFIRM MISC
avast -- antivirus	A Cross Site Scripting (XSS) issue exists in Avast AntiVirus (Free, Internet Security, and Premiere Edition) 19.3.2369 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-18653</a> MISC MISC
avg_technologies -- avg_antivirus	A Cross Site Scripting (XSS) issue exists in AVG AntiVirus (Internet Security Edition) 19.3.3084 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-18654</a> MISC MISC
axohelp -- axohelp	In axohelp.c before 1.3 in axohelp in axodraw2 before 2.1.1b, as distributed in TeXLive and other collections, sprintf is mishandled.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-18604</a> MISC
bitdefender -- box_firmware	An issue was discovered in Bitdefender BOX firmware versions before 2.1.37.37-34 that allows an attacker to pass arbitrary code to the BOX appliance via the web API. In order to exploit this vulnerability, an attacker needs presence in Bitdefender BOX setup network and Bitdefender BOX be in setup mode.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-12612</a> CONFIRM
centos-webpanel -- centos_web_panel	Stored XSS in filemanager2.php in CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.885 exists via the cmd_arg parameter. This can be exploited by a local attacker who supplies a crafted filename within a directory visited by the victim.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16295</a> MISC CONFIRM
cezerin -- cezerin	Cezerin v0.33.0 allows unauthorized order-information modification because certain internal attributes can be overwritten via a conflicting name when processing order requests. Hence, a malicious customer can manipulate an order (e.g., its payment status or shipping fee) by adding additional attributes to user-input during the PUT /ajax/cart operation for a checkout, because of getValidDocumentForUpdate in api/server/services/orders/orders.js.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-18608</a> MISC
chicken -- chicken	OS command injection vulnerability in the "qs" procedure from the "utils" module in Chicken before 4.9.0.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-2024</a> MISC MISC MISC MISC CONFIRM MISC MISC
chicken -- chicken	Multiple buffer overflows in the (1) R5RS char-ready, (2) tcp-accept-ready, and (3) file-select procedures in Chicken through 4.8.0.3 allows attackers to cause a denial of service (crash) by opening a file descriptor with a large integer value. NOTE: this issue exists because of an incomplete fix for CVE-2012-6122.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-2075</a> CONFIRM CONFIRM CONFIRM MISC MISC MISC CONFIRM MISC
chicken -- chicken	A casting error in Chicken before 4.8.0 on 64-bit platform caused the random number generator to return a constant value. NOTE: the vendor states "This function wasn't used for security purposes (and is advertised as being unsuitable)."	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6124</a> MISC MISC CONFIRM MISC
chicken -- chicken	Chicken before 4.8.0 does not properly handle NUL bytes in certain strings, which allows an attacker to conduct "poisoned NUL byte attack."	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6123</a> MISC MISC MISC
chicken -- chicken	Chicken before 4.8.0 is susceptible to algorithmic complexity attacks related to hash table collisions.	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6125</a> MISC MISC CONFIRM CONFIRM MISC
chicken -- chicken	Buffer overflow in the thread scheduler in Chicken before 4.8.0.1 allows attackers to cause a denial of service (crash) by opening a file descriptor with a large integer value.	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6122</a> MISC MISC MISC MISC MISC CONFIRM CONFIRM MISC
compal -- ch7465lg_modem	The web interface of the Compal Broadband CH7465LG modem (version CH7465LG-NCIP-6.12.18.25-2p6-NOSH) is vulnerable to a %62f/ path traversal attack, which can be exploited in order to test for the existence of a file pathname outside of the web root directory. If a file exists but is not part of the product, there is a 404 error. If a file does not exist, there is a 302 redirect to index.html.	2019- r/bt yet calculated 28	<a href="#">CVE-2019-17224</a> MISC MISC
cujo -- smart_firewall	An exploitable vulnerability exists in the safe browsing function of the CUJO Smart Firewall, version 7003. The flaw lies in the way the safe browsing function parses HTTP requests. The server hostname is extracted from captured HTTP/HTTPS requests and inserted as part of a Lua statement without prior sanitization, which results in arbitrary Lua script execution in the kernel. An attacker could send an HTTP request to exploit this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2018-4031</a> MISC
cujo -- smart_firewall	An exploitable denial-of-service vulnerability exists in the mdnscap binary of the CUJO Smart Firewall running firmware 7003. When parsing labels in mDNS packets, the firewall unsafely handles label compression pointers, leading to an uncontrolled recursion that eventually	2019- r/bt yet calculated	<a href="#">CVE-2018-4002</a> MISC



	exhausts the stack, crashing the mdnscap process. An unauthenticated attacker can send an mDNS message to trigger this vulnerability.	31	
debian_project -- autokey	The init script in autokey before 0.61.3-2 allows local attackers to write to arbitrary files via a symlink attack.	2019- r/bt yet calculated 30	<a href="#">CVE-2010-0398</a> MISC MISC
debian_project -- burn	burn allows file names to escape via mishandled quotation marks	2019- r/bt yet calculated 31	<a href="#">CVE-2009-5043</a> MISC
debian_project -- debian	The Debian backport of the fix for CVE-2017-3137 leads to assertion failure in validator.c:1858; Affects Debian versions 9.9.5.dfs-g-9+deb8u15; 9.9.5.dfs-g-9+deb8u18; 9.10.3.dfs-g-P4-12.3+deb9u5; 9.11.5.P4+dfs-g-5.1 No ISC releases are affected. Other packages from other distributions who did similar backports for the fix for 2017-3137 may also be affected.	2019- r/bt yet calculated 30	<a href="#">CVE-2018-5735</a> CONFIRM
debian_project -- mumble	Mumble: murmur-server has DoS due to malformed client query	2019- r/bt yet calculated 31	<a href="#">CVE-2010-2490</a> MISC MISC MISC
debian_project -- overkill	overkill has buffer overflow via long player names that can corrupt data on the server machine	2019- r/bt yet calculated 31	<a href="#">CVE-2009-5041</a> MISC
debian_project -- python-docutils	python-docutils allows insecure usage of temporary files	2019- r/bt yet calculated 31	<a href="#">CVE-2009-5042</a> MISC
debian_project -- drbd8	drbd8 allows local users to bypass intended restrictions for certain actions via netlink packets, similar to CVE-2009-3725.	2019- r/bt yet calculated 30	<a href="#">CVE-2010-0747</a> MISC CONFIRM
debian_project -- mutt	Mutt before 1.5.20 patch 7 allows an attacker to cause a denial of service via a series of requests to mutt temporary files.	2019- r/bt yet calculated 01	<a href="#">CVE-2005-2351</a> MISC MISC
elastic -- elasticsearch	Elasticsearch versions 7.0.0-7.3.2 and 6.7.0-6.8.3 contain a username disclosure flaw was found in the API Key service. An unauthenticated attacker could send a specially crafted request and determine if a username exists in the Elasticsearch native realm.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-7619</a> CONFIRM CONFIRM CONFIRM
elastic -- logstash	Logstash versions before 7.4.1 and 6.8.4 contain a denial of service flaw in the Logstash Beats input plugin. An unauthenticated user who is able to connect to the port the Logstash beats input could send a specially crafted network packet that would cause Logstash to stop responding.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-7620</a> CONFIRM CONFIRM CONFIRM
european_commission -- eidas_node_integration_package	European Commission eIDAS-Node Integration Package before 2.3.1 has Missing Certificate Validation because a certain ExplicitKeyTrustEvaluator return value is not checked. NOTE: only 2.1 is confirmed to be affected.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-18633</a> MISC
european_commission -- eidas_node_integration_package	European Commission eIDAS-Node Integration Package before 2.3.1 allows Certificate Faking because an attacker can sign a manipulated SAML response with a forged certificate.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-18632</a> MISC
f5 -- big-ip	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-6657</a> CONFIRM
f5 -- big-ip_afm	On BIG-IP AFM 15.0.0-15.0.1, 14.0.0-14.1.2, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, a vulnerability in the AFM configuration utility may allow any authenticated BIG-IP user to run an SQL injection attack.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-6658</a> CONFIRM
facebook -- whatsapp	The Wireless Emergency Alerts (WEA) protocol allows remote attackers to spoof a Presidential Alert because cryptographic authentication is not used, as demonstrated by MessageIdentifier 4370 in LTE System Information Block 12 (aka SIB12). NOTE: testing inside an RF-isolated shield box suggested that all LTE phones are affected by design (e.g., use of Android versus iOS does not matter); testing in an open RF environment is, of course, contraindicated.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18659</a> MISC
fastweb -- fastgate_devices	Fastweb FASTGate 1.0.1b devices allow partial authentication bypass by changing a certain check_pwd return value from 0 to 1. An attack does not achieve administrative control of a device; however, the attacker can view all of the web pages of the administration console.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18661</a> MISC MISC
fortinet -- fortitxtender	An OS command injection vulnerability in FortiExtender 4.1.1 and below under CLI admin console may allow unauthorized administrators to run arbitrary system level commands via specially crafted "execute date" commands.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-15710</a> CONFIRM
foswiki -- foswiki	Foswiki before 1.1.8 contains a code injection vulnerability in the MAKETEXT macro.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-1666</a> CONFIRM MISC MISC MISC
freebsd -- freebsd	/usr/local/www/freeradius_view_config.php in the freeradius3 package before 0.15.7_3 for pfSense on FreeBSD has XSS via a filename.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18667</a> MISC
freebsd -- freebsd	FreeBSD NSD before 3.2.13 allows remote attackers to crash a NSD child server process (SIGSEGV) and cause a denial of service in the NSD server.	2019- r/bt yet calculated 01	<a href="#">CVE-2012-2979</a> MISC CONFIRM MISC
freetds -- freetds	FreeTDS through 1.1.11 has a Buffer Overflow.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-13508</a> MISC
glpi_project -- glpi	GLPI 0.83.7 has Local File Inclusion in common.tabs.php.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2227</a> MISC MISC MISC MISC MISC
gnome -- evince	evince is missing a check on number of pages which can lead to a segmentation fault	2019- r/bt yet calculated 01	<a href="#">CVE-2013-3718</a> MISC MISC MISC MISC
google -- nest_cam_iq_indoor	An exploitable denial-of-service vulnerability exists in the Weave daemon of the Nest Cam IQ Indoor, version 4620002. A set of TCP connections can cause unrestricted resource allocation, resulting in a denial of service. An attacker can connect multiple times to trigger this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5043</a> MISC
grsecurity -- pax	An exploitable vulnerability exists in the grsecurity PaX patch for the function read_kmem, in PaX from version pax-linux-4.9.8-test1 to 4.9.24-test7, grsecurity official from version grsecurity-3.1-4.9.8-201702060653 to grsecurity-3.1-4.9.24-201704252333, grsecurity unofficial from version v4.9.25-unofficialgrsec to v4.9.74-unofficialgrsec. PaX adds a temp buffer to the read_kmem function, which is never freed when an invalid address is supplied. This results in a memory leakage that can lead to a crash of the system. An attacker needs to induce a read to /dev/kmem using an invalid address to exploit this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5023</a> MISC
gs-gpl -- gs-gpl	I race condition in Temp files was found in gs-gpl before 8.56 addons scripts.	2019- r/bt yet calculated 01	<a href="#">CVE-2005-2352</a> MISC MISC
honeywell -- equip_and_performance_series_ip_cameras	Honeywell equipP and Performance series IP cameras, multiple versions, A vulnerability exists where the affected product allows unauthenticated access to audio streaming over HTTP.	2019- r/bt yet calculated	<a href="#">CVE-2019-18230</a> MISC

		31	
honeywell -- equip_and_performance_series_ip_cameras_and_recorders	Honeywell equip series and Performance series IP cameras and recorders. A vulnerability exists in the affected products where IP cameras and recorders have a potential replay attack vulnerability as a weak authentication method is retained for compatibility with legacy products.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18226</a> MISC
honeywell -- equip_ip_and_multipleequip_series_cameras	Honeywell equip series IP cameras Multiple equip Series Cameras, A vulnerability exists in the affected products where a specially crafted HTTP packet request could result in a denial of service.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18228</a> MISC
hunt_cctv -- multiple_cctv_devices	Authentication bypass vulnerability in the web interface in Hunt CCTV, Capture CCTV, Hachi CCTV, NoVus CCTV, and Well-Vision Inc DVR systems allows a remote attacker to retrieve the device configuration.	2019- r/bt yet calculated 30	<a href="#">CVE-2013-1391</a> MISC MISC BID
hyundai -- pay_kasse_hk-1000_devices	On Hyundai Pay Kasse HK-1000 devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. In other words, the side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-14360</a> MISC
icedtea6 -- icedtea6	IcedTea6 before 1.7.4 allow unsigned apps to read and write arbitrary files, related to Extended JNLP Services.	2019- r/bt yet calculated 31	<a href="#">CVE-2010-2783</a> CONFIRM MISC MISC MISC
icedtea6 -- icedtea6	IcedTea6 before 1.7.4 does not properly check property access, which allows unsigned apps to read and write arbitrary files.	2019- r/bt yet calculated 31	<a href="#">CVE-2010-2548</a> CONFIRM MISC MISC
ikiwiki -- ikiwiki	ikiwiki before 3.20110608 allows remote attackers to hijack root's tty and run symlink attacks.	2019- r/bt yet calculated 29	<a href="#">CVE-2011-1408</a> CONFIRM MISC MISC MISC
internet_systems_consortium -- bind	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-6470</a> CONFIRM CONFIRM CONFIRM CONFIRM
ipswitch -- progress_movieit_transfer	In Progress MOVEit Transfer 11.1 before 11.1.3, a vulnerability has been found that could allow an attacker to sign in without full credentials via the SSH (SFTP) interface. The vulnerability affects only certain SSH (SFTP) configurations, and is applicable only if the MySQL database is being used.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18465</a> CONFIRM CONFIRM
ipswitch -- progress_movieit_transfer	In Progress MOVEit Transfer 10.2 before 10.2.6 (2018.3), 11.0 before 11.0.4 (2019.0.4), and 11.1 before 11.1.3 (2019.1.3), multiple SQL Injection vulnerabilities have been found in the REST API that could allow an unauthenticated attacker to gain unauthorized access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database or may be able to alter the database.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18464</a> CONFIRM CONFIRM CONFIRM CONFIRM
jetbrains -- hub	In JetBrains Hub versions earlier than 2019.1.11738, username enumeration was possible through password recovery.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18360</a> CONFIRM
jetbrains -- intellij_idea	JetBrains IntelliJ IDEA before 2019.2 allows local user privilege escalation, potentially leading to arbitrary code execution.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18361</a> CONFIRM
jetbrains -- mps	JetBrains MPS before 2019.2.2 exposed listening ports to the network.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18362</a> CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.2, a non-destructive operation could be performed by a user without the corresponding permissions.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18367</a> CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.4, reverse tabnabbing was possible on several pages.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18365</a> CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.2, secure values could be exposed to users with the "View build runtime parameters and data" permission.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18366</a> CONFIRM
jetbrains -- toolbox_app	In JetBrains Toolbox App before 1.15.5666 for Windows, privilege escalation was possible.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18368</a> CONFIRM
jitbit -- jitbit	A cross-site scripting (XSS) vulnerability in Jitbit .NET Forum (aka ASP.NET forum) 8.3.8 allows remote attackers to inject arbitrary web script or HTML via the gravatar URL parameter.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-18636</a> MISC MISC
libvnc -- libvnc	LibVNC commit before d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a contains a memory leak (CWE-655) in VNC server code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appear to be exploitable via network connectivity. These vulnerabilities have been fixed in commit d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-15681</a> MISC MLIST MLIST
linux -- linux_kernel	ovirt-engine 3.2 running on Linux kernel 3.1 and newer creates certain files world-writeable due to an upstream kernel change which impacted how python's os.chmod() works when passed a mode of '-1'.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-4367</a> MISC MISC
magento -- magento	An insecure direct object reference (IDOR) vulnerability exists in Magento 2.3 prior to 2.3.1, 2.2 prior to 2.2.8, and 2.1 prior to 2.1.17 versions. An authenticated user may be able to view personally identifiable shipping details of another user due to insufficient validation of user controlled input.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-8235</a> CONFIRM
manageiq -- manageiq_evm	Multiple cross-site scripting (XSS) vulnerabilities in ManageIQ EVM allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-0186</a> CONFIRM MISC
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in MantisBT 1.2.14 allows remote attackers to inject arbitrary web script or HTML via a version, related to deleting a version.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-1931</a> MISC MISC MISC MISC CONFIRM

			MISC
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the configuration report page (adm_config_report.php) in MantisBT 1.2.13 allows remote authenticated users to inject arbitrary web script or HTML via a project name.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-1932</a> MISC MISC MISC CONFIRM MISC
mantisbt -- mantisbt	MantisBT 1.2.12 before 1.2.15 allows authenticated users to by the workflow restriction and close issues.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-1930</a> MISC MISC MISC MISC MISC MISC MISC MISC
mapserver -- mapserver	Mapserver 5.2, 5.4 and 5.6 before 5.6.5-2 improperly validates symbol index values during Mapfile parsing.	2019- r/bt yet calculated 29	<a href="#">CVE-2010-1678</a> MISC MISC CONFIRM
maxthon -- maxthon_browser_for_windows	Unquoted Search Path in Maxthon 5.1.0 to 5.2.7 Browser for Windows.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-16647</a> MISC MISC
minidlna -- minidlna	MiniDLNA has heap-based buffer overflow	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2739</a> MISC MISC
minidlna -- minidlna	minidlna has SQL Injection that may allow retrieval of arbitrary files	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2738</a> MISC MISC MISC MISC MISC
miniupnpd -- miniupnpd	MiniUPnPd has information disclosure use of snprintf()	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2600</a> MISC MISC MISC MISC MISC MISC
mooltipass -- moolticute	An issue was discovered in Mooltipass Moolticute through v0.42.1 and v0.42.x-testing through v0.42.5-testing. There is a NULL pointer dereference in MPDevice_win.cpp.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-18635</a> MISC MISC
opera -- opera_mini_for_android	Opera Mini for Android allows attackers to bypass intended restrictions on .apk file download/installation via an RTLO (aka Right to Left Override) approach, as demonstrated by misinterpretation of malicious%E2%80%AEtxt.apk as maliciouskpa.txt. This affects 44.1.2254.142553, 44.1.2254.142659, and 44.1.2254.143214.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-18624</a> MISC MISC
phoenix_contact -- pc_works_and_pc_worx_express_and_config+	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to an Out-of-bounds Read and remote code execution. The attacker needs to get access to an original PC Worx or Config+ project to be able to manipulate data inside. After manipulation, the attacker needs to exchange the original files with the manipulated ones on the application programming workstation.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16675</a> MISC MISC MISC MISC
postgresql -- postgresql	A flaw was discovered in postgresql versions 9.4.x before 9.4.24, 9.5.x before 9.5.19, 9.6.x before 9.6.15, 10.x before 10.10 and 11.x before 11.5 where arbitrary SQL statements can be executed given a suitable SECURITY DEFINER function. An attacker, with EXECUTE permission on the function, can execute arbitrary SQL as the owner of the function.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-10208</a> CONFIRM CONFIRM
postgresql -- postgresql_windows_installer	Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via bundled OpenSSL executing code from unprotected directory.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-10211</a> CONFIRM CONFIRM CONFIRM
project_jupyter -- jupyter_notebook	Jupyter Notebook before 5.5.0 does not use a CSP header to treat served files as belonging to a separate origin. Thus, for example, an XSS payload can be placed in an SVG document.	2019- r/bt yet calculated 31	<a href="#">CVE-2018-21030</a> MISC MISC
python -- python	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 / 3.6.6. A specially crafted X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initiate or accept TLS connections using crafted certificates to trigger this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5010</a> MISC
qtum -- qtum	qtum through 0.16 (a chain-based proof-of-stake cryptocurrency) allows a remote denial of service. The attacker sends invalid headers/blocks. The attack requires no stake and can fill the victim's disk and RAM.	2019- r/bt yet calculated 29	<a href="#">CVE-2018-19151</a> MISC MISC MISC
rainbow_pdf -- office_server_document_converter	A buffer overflow vulnerability exists in the PowerPoint document conversion function of Rainbow PDF Office Server Document Converter V7.0 Pro MR1 (7.0.2019.0220). While parsing a document text info container, the TxMasterStyleAtom::parse function is incorrectly checking the bounds corresponding to the number of style levels, causing a vtable pointer to be overwritten, which leads to code execution.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5030</a> MISC
rdesktop -- rdesktop	RDesktop version 1.8.4 contains multiple out-of-bound access read vulnerabilities in its code, which results in a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. These issues have been fixed in version 1.8.5	2019- r/bt yet calculated 30	<a href="#">CVE-2019-15682</a> MISC
red_hat -- jboss_operations_network	A missing permission check was found in The CLI in JBoss Operations Network before 2.3.1 does not properly check permissions, which allows JBoss ON users to perform management tasks and configuration changes with the privileges of the administrator user.	2019- r/bt yet calculated 30	<a href="#">CVE-2010-0737</a> MISC
red_hat -- openshift	cartridges/openshift-origin-cartridge-mongodb-2.2/info/bin/dump.sh in OpenShift does not properly create files in /tmp.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-0165</a> MISC
red_hat -- openstack	HTTPSConnections in OpenStack Keystone 2013, OpenStack Compute 2013.1, and possibly other OpenStack components, fail to validate server-side SSL certificates.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2255</a> MISC MISC MISC MISC MISC MISC MISC MISC
red_hat -- red_hat_enterprise_linux	While backporting a feature for a newer branch of BIND9, RedHat introduced a path leading to an assertion failure in buffer.c:420. Affects RedHat versions bind-9.9.4-65.el7 -> bind-9.9.4-72.el7. No ISC releases are affected. Other packages from other distributions who made the same error may also be affected.	2019- r/bt yet calculated 30	<a href="#">CVE-2018-5742</a> CONFIRM
redis -- redis	Insecure temporary file vulnerability in Redis 2.6 related to /tmp/redis.ds.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-0180</a> MLIST MISC
redis -- redis	Insecure temporary file vulnerability in Redis before 2.6 related to /tmp/redis-%p.vm.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-0178</a> MISC MISC MISC MISC MISC MISC MISC

rpcbind -- rpcbind	rpcbind 0.2.0 does not properly validate (1) /tmp/portmap.xdr and (2) /tmp/rpcbind.xdr, which can be created by an attacker before the daemon is started.	2019- r/bt yet calculated 29	<a href="#">CVE-2010-2061</a> MISC MISC MISC MISC MLIST
rpcbind -- rpcbind	rpcbind 0.2.0 allows local users to write to arbitrary files or gain privileges via a symlink attack on (1) /tmp/portmap.xdr and (2) /tmp/rpcbind.xdr.	2019- r/bt yet calculated 29	<a href="#">CVE-2010-2064</a> MISC MISC MISC MISC MLIST
ruby193 -- ruby193	ruby193 uses an insecure LD_LIBRARY_PATH setting.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-1945</a> MISC
sahi_pro -- sahi_pro	Sahi Pro 8.0.0 has a script manager arena located at _s_dyn/pro/DBReports with many different areas that are vulnerable to reflected XSS, by updating a script's Script Name, Suite Name, Base URL, Android, iOS, Scripts Run, Origin Machine, or Comment field. The sql parameter can be used to trigger reflected XSS.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-13066</a> MISC MISC
schneider_electric -- multiple_modicon_products	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists in Modicon M580, Modicon M340, Modicon Premium , Modicon Quantum (all firmware versions), which could cause the disclosure of information when transferring applications to the controller using Modbus TCP protocol.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-6845</a> CONFIRM
schneider_electric -- multiple_modicon_products	A CWE-538: File and Directory Information Exposure vulnerability exists in Modicon M580, Modicon M340, Modicon Premium , Modicon Quantum (all firmware versions), which could cause the disclosure of information from the controller when using TFTP protocol.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-6851</a> CONFIRM
schneider_electric -- multiple_modicon_products	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause information disclosure when using the FTP protocol.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-6846</a> CONFIRM
secudos -- domos	The Log module in SECUDOS DOMOS before 5.6 allows XSS.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18664</a> MISC
secudos -- domos	The Log module in SECUDOS DOMOS before 5.6 allows local file inclusion.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18665</a> MISC
sensiolabs -- php-symphony2-validator	php-symfony2-Validator has loss of information during serialization	2019- r/bt yet calculated 01	<a href="#">CVE-2013-4751</a> MISC MISC MISC MISC MISC MISC
shift_cryptosecurity -- bitbox02	On SHIFT BitBox02 devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. Note: BIP39 secrets are not displayed by default on this device. The side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18673</a> MISC
sierra_wireless -- airlink_es450_fw	An exploitable unverified password change vulnerability exists in the ACEManager upload.cgi functionality of Sierra Wireless AirLink ES450 FW 4.9.3. A specially crafted HTTP request can cause a unverified device configuration change, resulting in an unverified change of the user password on the device. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2018-4064</a> MISC
smokeping -- smokeping	Cross-site scripting (XSS) vulnerability in SmokePing 2.6.9 in the start and end time fields.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-4168</a> MISC MISC MISC MISC MISC MISC
sonatype -- nexus_repository_manager	There is an OS Command Injection in Nexus Repository Manager <= 2.14.14 (bypass CVE-2019-5475) that could allow an attacker a Remote Code Execution (RCE). All instances using CommandLineExecutor.java with user-supplied data is vulnerable, such as the Yum Configuration Capability.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-15588</a> MISC CONFIRM
symantec -- sonar	The Symantec SONAR component, prior to 12.0.2, may be susceptible to a tamper protection bypass vulnerability which could potentially allow an attacker to circumvent the existing tamper protection in use on the resident system.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-12752</a> CONFIRM
systemd -- systemd	systemd 239 through 243 accepts any certificate signed by a trusted certificate authority for DNS Over TLS. Server Name Indication (SNI) is not sent, and there is no hostname validation with the GnuTLS backend.	2019- r/bt yet calculated 30	<a href="#">CVE-2018-21029</a> MISC MISC MISC
technicolor -- td5130v2_devices	An issue was discovered in certain Oi third-party firmware that may be installed on Technicolor TD5130v2 devices. A Command Injection in the Ping module in the Web Interface in Oi_Fw_V20 allows remote attackers to execute arbitrary OS commands in the pingAddr parameter to mnt_ping.cgi. NOTE: This may overlap CVE-2017?14127.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18396</a> MISC MISC MISC
tightrope_media_systems -- carousel	The Tightrope Media Carousel Seneca HDn Windows-based appliance 7.0.4.104 is shipped with a default local administrator username and password. This can be found by a limited user account in an "unattend.xml" file left over on the C: drive from the Sysprep process. An attacker with this username and password can leverage it to gain administrator-level access on the system.	2019- r/bt yet calculated 29	<a href="#">CVE-2018-18929</a> MISC
tightrope_media_systems -- carousel	An issue was discovered in the Tightrope Media Carousel digital signage product 7.0.4.104. Due to insecure default permissions on the C:\TRMS\Services directory, an attacker who has gained access to the system can elevate their privileges from a restricted account to full SYSTEM by replacing the Carousel.Service.exe file with a custom malicious executable. This service is independent of the associated IIS web site, which means that this service can be manipulated by an attacker without losing access to vulnerabilities in the web interface (which would potentially be used in conjunction with this attack, to control the service). Once the attacker has replaced Carousel.Service.exe, the server can be restarted using the command "shutdown -r -t 0" from a web shell, causing the system to reboot and launching the malicious Carousel.Service.exe as SYSTEM on startup. If this malicious Carousel.Service.exe is configured to launch a reverse shell back to the attacker, then upon reboot the attacker will have a fully privileged remote command-line environment to manipulate the system further.	2019- r/bt yet calculated 29	<a href="#">CVE-2018-18931</a> MISC
tightrope_media_systems -- carousel	The Tightrope Media Carousel digital signage product 7.0.4.104 contains an arbitrary file upload vulnerability in the Manage Bulletins/Upload feature, which can be leveraged to gain remote code execution. An authenticated attacker can upload a crafted ZIP file (based on an exported backup of existing "Bulletins") containing a malicious file. When uploaded, the system only checks for the presence of the needed files within the ZIP and, as long as the malicious file is named properly, will extract all contained files to a new directory on the system, named with a random GUID. The attacker can determine this GUID by previewing an image from the uploaded Bulletin within the web UI. Once the GUID is determined, the attacker can navigate to the malicious file and execute it. In testing, an ASPX web shell was uploaded, allowing for remote-code execution in the context of a restricted IIS user.	2019- r/bt yet calculated 29	<a href="#">CVE-2018-18930</a> MISC

trend_micro -- apex_one_and_officescan_and_worry-free_business_security	A directory traversal vulnerability in Trend Micro Apex One, OfficeScan (11.0, XG) and Worry-Free Business Security (9.5, 10.0) may allow an attacker to bypass authentication and log on to an affected product's management console as a root user. The vulnerability does not require authentication.	2019- rft yet calculated 28	<a href="#">CVE-2019-18189</a> N/A
turbovnc -- turbovnc	TurboVNC server code contains stack buffer overflow vulnerability in commit prior to cea98166008301e614e0d36776bf9435a536136e. This could possibly result into remote code execution, since stack frame is not protected with stack canary. This attack appear to be exploitable via network connectivity. To exploit this vulnerability authorization on server is required. These issues have been fixed in commit cea98166008301e614e0d36776bf9435a536136e.	2019- rft yet calculated 29	<a href="#">CVE-2019-15683</a> MISC
twiki -- twiki	TWiki allows arbitrary shell command execution via the Include function	2019- rft yet calculated 01	<a href="#">CVE-2005-3056</a> DEBIAN MISC CONFIRM
typo3 -- typo3	TYPO3 before 4.1.14, 4.2.x before 4.2.13, 4.3.x before 4.3.4 and 4.4.x before 4.4.1 allows Open Redirection on the backend.	2019- rft yet calculated 01	<a href="#">CVE-2010-3661</a> MISC MISC CONFIRM
typo3 -- typo3	TYPO3 before 4.1.14, 4.2.x before 4.2.13, 4.3.x before 4.3.4 and 4.4.x before 4.4.1 allows XSS on the backend.	2019- rft yet calculated 01	<a href="#">CVE-2010-3660</a> MISC MISC CONFIRM
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-201908101-SG and 6.5 before ESXi650-201910401-SG), Workstation (15.x before 15.5.0) and Fusion (11.x before 11.5.0) contain a denial-of-service vulnerability in the shader functionality. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion.	2019- rft yet calculated 28	<a href="#">CVE-2019-5536</a> MISC
vmware -- sd-wan	In VMware SD-WAN by VeloCloud versions 3.x prior to 3.3.0, the VeloCloud Orchestrator parameter authorization check mistakenly allows enterprise users to obtain information of Managed Service Provider accounts. Among the information is username, first and last name, phone numbers and e-mail address if present but no other personal data. VMware has evaluated the severity of this issue to be in the moderate severity range with a maximum CVSSv3 base score of 4.3.	2019- rft yet calculated 29	<a href="#">CVE-2019-5533</a> CONFIRM
vmware -- vcenter_server_appliance	Sensitive information disclosure vulnerability resulting from a lack of certificate validation during the File-Based Backup and Restore operations of VMware vCenter Server Appliance (6.7 before 6.7u3a and 6.5 before 6.5u3d) may allow a malicious actor to intercept sensitive data in transit over FTPS and HTTPS. A malicious actor with man-in-the-middle positioning between vCenter Server Appliance and a backup target may be able to intercept sensitive data in transit during File-Based Backup and Restore operations.	2019- rft yet calculated 28	<a href="#">CVE-2019-5537</a> MISC
vmware -- vcenter_server_appliance	Sensitive information disclosure vulnerability resulting from a lack of certificate validation during the File-Based Backup and Restore operations of VMware vCenter Server Appliance (6.7 before 6.7u3a and 6.5 before 6.5u3d) may allow a malicious actor to intercept sensitive data in transit over SCP. A malicious actor with man-in-the-middle positioning between vCenter Server Appliance and a backup target may be able to intercept sensitive data in transit during File-Based Backup and Restore operations.	2019- rft yet calculated 28	<a href="#">CVE-2019-5538</a> MISC
websieve -- websieve	Cross-site scripting (XSS) vulnerability in websieve v0.62 allows remote attackers to inject arbitrary web script or HTML code in the web user interface.	2019- rft yet calculated 01	<a href="#">CVE-2005-2350</a> MISC MISC
wordpress -- wordpress	plugin-fw/lib/yit-plugin-panel-wc.php in the YIT Plugin Framework through 3.3.8 for WordPress allows authenticated options changes.	2019- rft yet calculated 31	<a href="#">CVE-2019-16251</a> MISC MISC
wordpress -- wordpress	An issue was discovered in the Currency Switcher addon before 2.11.2 for WooCommerce if a user provides a currency that was not added by the administrator. In this case, even though the currency does not exist, it will be selected, but a price amount will fall back to the default currency. This means that if an attacker provides a currency that does not exist and is worth less than this default, the attacker can eventually purchase an item for a significantly cheaper price.	2019- rft yet calculated 02	<a href="#">CVE-2019-18668</a> MISC MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing 32-bit PV guest OS users to gain guest OS privileges by installing and using descriptors. There is missing descriptor table limit checking in x86 PV emulation. When emulating certain PV guest operations, descriptor table accesses are performed by the emulating code. Such accesses should respect the guest specified limits, unless otherwise guaranteed to fail in such a case. Without this, emulation of 32-bit guest user mode calls through call gates would allow guest user mode to install and then use descriptors of their choice, as long as the guest kernel did not itself install an LDT. (Most OSes don't install any LDT by default). 32-bit PV guest user mode can elevate its privileges to that of the guest kernel. Xen versions from at least 3.2 onwards are affected. Only 32-bit PV guest user mode can leverage this vulnerability. HVM, PVH, as well as 64-bit PV guests cannot leverage this vulnerability. Arm systems are unaffected.	2019- rft yet calculated 31	<a href="#">CVE-2019-18425</a> MLIST MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing ARM guest OS users to cause a denial of service via a XENMEM_add_to_physmap hypercall. p2m->max_mapped_gfn is used by the functions p2m_resolve_translation_fault() and p2m_get_entry() to sanity check guest physical frame. The rest of the code in the two functions will assume that there is a valid root table and check that with BUG_ON(). The function p2m_get_root_pointer() will ignore the unused top bits of a guest physical frame. This means that the function p2m_set_entry() will alias the frame. However, p2m->max_mapped_gfn will be updated using the original frame. It would be possible to set p2m->max_mapped_gfn high enough to cover a frame that would lead p2m_get_root_pointer() to return NULL in p2m_get_entry() and p2m_resolve_translation_fault(). Additionally, the sanity check on p2m->max_mapped_gfn is off-by-one allowing "highest mapped + 1" to be considered valid. However, p2m_get_root_pointer() will return NULL. The problem could be triggered with a specially crafted hypercall XENMEM_add_to_physmap{, _batch} followed by an access to an address (via hypercall or direct access) that passes the sanity check but cause p2m_get_root_pointer() to return NULL. A malicious guest administrator may cause a hypervisor crash, resulting in a Denial of Service (DoS). Xen version 4.8 and newer are vulnerable. Only Arm systems are vulnerable. x86 systems are not affected.	2019- rft yet calculated 31	<a href="#">CVE-2019-18423</a> MLIST MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing ARM guest OS users to cause a denial of service or gain privileges by leveraging the erroneous enabling of interrupts. Interrupts are unconditionally unmasked in exception handlers. When an exception occurs on an ARM system which is handled without changing processor level, some interrupts are unconditionally enabled during exception entry. So exceptions which occur when interrupts are masked will effectively unmask the interrupts. A malicious guest might contrive to arrange for critical Xen code to run with interrupts erroneously enabled. This could lead to data corruption, denial of service, or possibly even privilege escalation. However a precise attack technique has not been identified.	2019- rft yet calculated 31	<a href="#">CVE-2019-18422</a> MLIST MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing attackers to gain host OS privileges via DMA in a situation where an untrusted domain has access to a physical device. This occurs because passed through PCI devices may corrupt host memory after deassignment. When a PCI device is assigned to an untrusted domain, it is possible for that domain to program the device to DMA to an arbitrary address. The IOMMU is used to protect the host from malicious DMA by making sure that the device addresses can only target memory assigned to the guest. However, when the guest domain is torn down, or the device is deassigned, the device is assigned back to dom0, thus allowing any in-flight DMA to potentially target critical host data. An untrusted domain with access to a physical device can DMA into host memory, leading to privilege escalation. Only systems where guests are given direct access to physical devices capable of DMA (PCI pass-through) are vulnerable. Systems which do not use PCI pass-through are not vulnerable.	2019- rft yet calculated 31	<a href="#">CVE-2019-18424</a> MLIST MISC



xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing x86 PV guest OS users to cause a denial of service via a VCPUOP. Initialise hypercall, hypercall_create_continuation() is a variadic function which uses a printf-like format string to interpret its parameters. Error handling for a bad format character was done using BUG(), which crashes Xen. One path, via the VCPUOP_initialise hypercall, has a bad format character. The BUG() can be hit if VCPUOP_initialise executes for a sufficiently long period of time for a continuation to be created. Malicious guests may cause a hypervisor crash, resulting in a Denial of Service (DoS). Xen versions 4.6 and newer are vulnerable. Xen versions 4.5 and earlier are not vulnerable. Only x86 PV guests can exploit the vulnerability. HVM and PVH guests, and guests on ARM systems, cannot exploit the vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-18420</a> <a href="#">MLIST</a> <a href="#">MISC</a>
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing x86 PV guest OS users to gain host OS privileges by leveraging race conditions in pagetable promotion and demotion operations. There are issues with restartable PV type change operations. To avoid using shadow pagetables for PV guests, Xen exposes the actual hardware pagetables to the guest. In order to prevent the guest from modifying these page tables directly, Xen keeps track of how pages are used using a type system; pages must be "promoted" before being used as a pagetable, and "demoted" before being used for any other type. Xen also allows for "recursive" promotions: i.e., an operating system promoting a page to an L4 pagetable may end up causing pages to be promoted to L3s, which may in turn cause pages to be promoted to L2s, and so on. These operations may take an arbitrarily large amount of time, and so must be re-startable. Unfortunately, making recursive pagetable promotion and demotion operations restartable is incredibly complicated, and the code contains several races which, if triggered, can cause Xen to drop or retain extra type counts, potentially allowing guests to get write access to in-use pagetables. A malicious PV guest administrator may be able to escalate their privilege to that of the host. All x86 systems with untrusted PV guests are vulnerable. HVM and PVH guests cannot exercise this vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-18421</a> <a href="#">MLIST</a> <a href="#">MISC</a>
yandex -- clickhouse	ClickHouse before 19.13.5.44 allows HTTP header injection via the url table function.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-18657</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
youthtube -- youthtube	An issue was discovered in YouTube through 7.7. User input passed through the live_stream_code POST parameter to /plugin/LiveChat/getChat.json.php is not properly sanitized (in getFromChat in plugin/LiveChat/Objects/LiveChatObj.php) before being used to construct a SQL query. This can be exploited by malicious users to, e.g., read sensitive data from the database through in-band SQL Injection attacks. Successful exploitation of this vulnerability requires the Live Chat plugin to be enabled.	2019- r0bt yet calculated 02	<a href="#">CVE-2019-18662</a> <a href="#">MISC</a>
youthtube -- youthtube	An exploitable SQL injection vulnerability exist in YouTube 7.7. A specially crafted unauthenticated HTTP request can cause a SQL injection, possibly leading to denial of service, exfiltration of the database and local file inclusion, which could potentially further lead to code execution. An attacker can send an HTTP request to trigger this vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-5151</a> <a href="#">MISC</a>
youthtube -- youthtube	An exploitable SQL injection vulnerability exist in YouTube 7.7. When the "VideoTags" plugin is enabled, a specially crafted unauthenticated HTTP request can cause a SQL injection, possibly leading to denial of service, exfiltration of the database and local file inclusion, which could potentially further lead to code execution. An attacker can send an HTTP request to trigger this vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-5150</a> <a href="#">MISC</a>
yum -- yum	yum does not properly handle bad metadata, which allows an attacker to cause a denial of service and possibly have other unspecified impact via a Trojan horse file in the metadata of a remote repository.	2019- r0bt yet calculated 31	<a href="#">CVE-2013-1910</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zte -- zx297520v3	The 7520V3V1.0.0B09P27 version, and all earlier versions of ZTE product ZX297520V3 are impacted by a Command Injection vulnerability. Unauthorized users can exploit this vulnerability to control the user terminal system.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-3421</a> <a href="#">CONFIRM</a>
zte -- zxmp	A security vulnerability exists in a management port in the version of ZTE's ZXMP M721V3.10P01B10_M2NCP. An attacker could exploit this vulnerability to build a link to the device and send specific packets to cause a denial of service.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-3419</a> <a href="#">CONFIRM</a>
zuchetti -- infobusiness	In Zuchetti InfoBusiness before and including 4.4.1, an authenticated user can inject client-side code due to improper validation of the Title field in the InfoBusiness Web Component. The payload will be triggered every time a user browses the reports page.	2019- r0bt yet calculated 30	<a href="#">CVE-2019-18207</a> <a href="#">MISC</a>
zuchetti -- infobusiness	A cross-site request forgery (CSRF) vulnerability in Zuchetti InfoBusiness before and including 4.4.1 allows arbitrary file upload.	2019- r0bt yet calculated 30	<a href="#">CVE-2019-18206</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nasa.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)



From: [US-CERT](mailto:US-CERT@sunvalley.ca.us)  
To: [us-cert@sunvalley.ca.us](mailto:us-cert@sunvalley.ca.us)  
Subject: Vulnerability Summary for the Week of October 28, 2019  
Date: Monday, November 04, 2019 2:32:33 PM



National Cyber Awareness System:

## Vulnerability Summary for the Week of October 28, 2019

11/04/2019 02:07 AM EST

Original release date: November 4, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-10-25	7.5	<a href="#">CVE-2019-8088</a> CONFIRM
apache -- thrift	In Apache Thrift all versions up to and including 0.12.0, a server or client may run into an endless loop when feed with specific input data. Because the issue had already been partially fixed in version 0.11.0, depending on the installed version it affects only certain language bindings.	2019-10-29	7.8	<a href="#">CVE-2019-0205</a> MISC
bitlbee -- bitlbee	Bitlbee does not drop extra group privileges correctly in unix.c	2019-10-29	7.5	<a href="#">CVE-2012-1187</a> MISC MISC MISC MISC
cisco -- video_communications_server	Cisco Video Communications Server (VCS) before X7.0.3 contains a command injection vulnerability which allows remote, authenticated attackers to execute arbitrary commands.	2019-10-29	9	<a href="#">CVE-2011-2538</a> CONFIRM
codesys -- eni_server	CODESYS V2.3 ENI server up to V3.2.2.24 has a Buffer Overflow.	2019-10-25	7.5	<a href="#">CVE-2019-16265</a> CONFIRM MISC
d-link -- dir-865	D-Link DIR-865L has PHP File Inclusion in the router xml file.	2019-10-25	7.5	<a href="#">CVE-2013-4857</a> MISC MISC
d-link -- dir-865l_devices	D-Link DIR-865L has SMB Symlink Traversal due to misconfiguration in the SMB service allowing symbolic links to be created to locations outside of the Samba share.	2019-10-25	7.9	<a href="#">CVE-2013-4855</a> MISC MISC MISC
debian_project -- qtparted	qtparted has insecure library loading which may allow arbitrary code execution	2019-10-29	7.5	<a href="#">CVE-2010-3375</a> DEBIAN MISC MISC
google -- chrome	browser/extensions/api/dial_registry.cc in Google Chrome before 54.0.2840.98 on macOS, before 54.0.2840.99 on Windows, and before 54.0.2840.100 on Linux neglects to copy a device ID before an erase() call, which causes the erase operation to access data that that erase operation will destroy.	2019-10-25	7.5	<a href="#">CVE-2016-5202</a> MISC MISC MISC MISC MISC
hot-world -- repetier-server	A directory traversal vulnerability was discovered in RepetierServer.exe in Repetier-Server 0.8 through 0.91 that allows for the creation of a user controlled XML file at an unintended location. When this is combined with CVE-2019-14451, an attacker can upload an "external command" configuration as a printer configuration, and achieve remote code execution. After exploitation, loading of the external command configuration is dependent on a system reboot or service restart.	2019-10-28	10	<a href="#">CVE-2019-14450</a> CONFIRM MISC
hot-world -- repetier-server	RepetierServer.exe in Repetier-Server 0.8 through 0.91 does not properly validate the XML data structure provided when uploading a new printer configuration. When this is combined with CVE-2019-14450, an attacker can upload an "external command" configuration as a printer configuration, and achieve remote code execution. After exploitation, loading of the external command configuration is dependent on a system reboot or service restart.	2019-10-25	10	<a href="#">CVE-2019-14451</a> CONFIRM MISC
intrasrv -- intrasrv	A remote SEH buffer overflow has been discovered in IntraSrv 1.0 (2007-06-03). An attacker may send a crafted HTTP GET or HEAD request that can result in a compromise of the hosting system.	2019-10-28	10	<a href="#">CVE-2019-17181</a> MISC MISC
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.4, insecure Java Deserialization could potentially allow remote code execution.	2019-10-31	7.5	<a href="#">CVE-2019-18364</a> CONFIRM
k7_computing -- antivirus_premium_and_total_security	In K7 Antivirus Premium 16.0.xxx through 16.0.0120; K7 Total Security 16.0.xxx through 16.0.0120; and K7 Ultimate Security 16.0.xxx through 16.0.0120, the module K7TSHlp.dll improperly validates the administrative privileges of the user, allowing arbitrary registry writes in the K7AVOptn.dll module to facilitate escalation of privileges via inter-process communication with a service process.	2019-10-28	7.5	<a href="#">CVE-2019-16897</a> MISC
labf -- nfsaxe_ftp_client	Buffer overflow in LabF nfsAxe FTP client 3.7 allows an attacker to execute code remotely.	2019-10-25	7.5	<a href="#">CVE-2017-14742</a> EXPLOIT-DB
linksys -- ea6500_router	Linksys EA6500 has SMB Symlink Traversal allowing symbolic links to be created to locations outside of the Samba share.	2019-10-25	10	<a href="#">CVE-2013-4658</a> MISC MISC MISC
medoo -- medoo	columnQuote in medoo before 1.7.5 allows remote attackers to perform a SQL Injection due to improper escaping.	2019-10-30	7.5	<a href="#">CVE-2019-10762</a> MISC MISC
mikrotik -- routers	RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below insufficiently validate where upgrade packages are download from when using the autoupgrade feature. Therefore, a remote attacker can trick the router into "upgrading" to an older version of RouterOS and possibly resetting all the system's usernames and passwords.	2019-10-29	8.5	<a href="#">CVE-2019-3977</a> MISC
				<a href="#">CVE-2016-2356</a>

milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a buffer overflow in a web application via a long username or password.	2019-10-25	7.5	MISC MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 allow remote attackers to bypass authentication and access a protected resource by simultaneously making a request for the unprotected vb.htm resource.	2019-10-25	7.5	CVE-2016-2359 MISC MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Undocumented hard-coded user passwords for root, ineaadmin, mitsadmin, and maint could allow an attacker to gain unauthorised access to the RTU. (Also, the accounts ineaadmin and mitsadmin are able to escalate privileges to root without supplying a password due to insecure entries in /etc/sudoers on the RTU.)	2019-10-28	10	CVE-2019-14930 MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote OS Command Injection vulnerability allows an attacker to execute arbitrary commands on the RTU due to the passing of unsafe user supplied data to the RTU's system shell. Functionality in mobile.php provides users with the ability to ping sites or IP addresses via Mobile Connection Test. When the Mobile Connection Test is submitted, action.php is called to execute the test. An attacker can use a shell command separator (;) in the host variable to execute operating system commands upon submitting the test data.	2019-10-28	10	CVE-2019-14931 MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Hard-coded SSH keys allow an attacker to gain unauthorised access or disclose encrypted data on the RTU due to the keys not being regenerated on initial installation or with firmware updates. In other words, these devices use private-key values in /etc/ssh/ssh_host_rsa_key, /etc/ssh/ssh_host_ecdsa_key, and /etc/ssh/ssh_host_dsa_key files that are publicly available from the vendor web sites.	2019-10-28	7.5	CVE-2019-14926 MISC MISC
philips -- intellispace_perinatal	In IntelliSpace Perinatal, Versions K and prior, a vulnerability within the IntelliSpace Perinatal application environment could enable an unauthorized attacker with physical access to a locked application screen, or an authorized remote desktop session host application user to break-out from the containment of the application and access unauthorized resources from the Windows operating system as the limited-access Windows user. Due to potential Windows vulnerabilities, it may be possible for additional attack methods to be used to escalate privileges on the operating system.	2019-10-25	7.2	CVE-2019-13546 MISC
php -- php	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for FCGI protocol data, thus opening the possibility of remote code execution.	2019-10-28	7.5	CVE-2019-11043 REDHAT REDHAT REDHAT REDHAT CONFIRM MISC FEDORA FEDORA FEDORA CONFIRM CONFIRM UBUNTU UBUNTU DEBIAN DEBIAN
pixelpost -- pixelpost	pixelpost 1.7.1 has SQL injection	2019-10-28	7.5	CVE-2009-4899 MISC DEBIAN MISC
rconfig -- rconfig	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to search.crud.php because the catCommand parameter is passed to the exec function without filtering, which can lead to command execution.	2019-10-28	9	CVE-2019-16663 MISC MISC MISC MISC MISC
rconfig -- rconfig	An issue was discovered in rConfig 3.9.2. An attacker can directly execute system commands by sending a GET request to ajaxServerSettingsChk.php because the rootUname parameter is passed to the exec function without filtering, which can lead to command execution.	2019-10-28	10	CVE-2019-16662 MISC MISC MISC MISC MISC MISC
rittal -- rittal_chiller_sk_3232_series	Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems is configured using hard-coded credentials. These credentials could allow attackers to influence the primary operations of the affected systems, namely turning the cooling unit on and off and setting the temperature set point.	2019-10-25	10	CVE-2019-13553 FULLDISC MISC
sequelize -- sequelize	Sequelize all versions prior to 3.35.1, 4.44.3, and 5.8.11 are vulnerable to SQL Injection due to JSON path keys not being properly escaped for the MySQL/MariaDB dialects.	2019-10-29	7.5	CVE-2019-10748 MISC MISC MISC
sequelize -- sequelize	sequelize before version 3.35.1 allows attackers to perform a SQL Injection due to the JSON path keys not being properly sanitized in the Postgres dialect.	2019-10-29	7.5	CVE-2019-10749 MISC MISC
snoopy -- snoopy	Snoopy before 2.0.0 has a security hole in exec cURL	2019-10-28	7.5	CVE-2002-2444 MISC DEBIAN MISC
sugarcrm -- sugarcrm	SugarCRM CE <= 6.3.1 contains scripts that use "unserialize()" with user controlled input which allows remote attackers to execute arbitrary PHP code.	2019-10-29	7.5	CVE-2012-0694 MISC MISC EXPLOIT-DB
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains global buffer overflow in HandleCoRREBBP macro function, which can potentially result code execution. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	CVE-2019-8287 MLIST
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains heap buffer overflow in InitialiseRFBConnection function, which can potentially result code execution. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	CVE-2019-15679 MLIST
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains heap buffer overflow in rfbServerCutText handler, which can potentially result code execution.. This attack appear to be exploitable via network connectivity.	2019-10-29	7.5	CVE-2019-15678 MLIST

tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has Local File Inclusion	2019-10-28	7.5	<a href="#">CVE-2010-4239</a> MISC MISC MISC
tp-link -- tl-wdr4300_devices	TP-Link TL-WDR4300 version 3.13.31 has multiple CSRF vulnerabilities.	2019-10-25	9.3	<a href="#">CVE-2013-4848</a> MISC MISC MISC MISC
transmission -- transmission	Transmission before 1.92 allows an attacker to cause a denial of service (crash) or possibly have other unspecified impact via a large number of tr arguments in a magnet link.	2019-10-30	7.5	<a href="#">CVE-2010-0748</a> MISC CONFIRM MISC CONFIRM MLIST
youthtube -- youthtube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Uri in /objects/getImage.php is vulnerable to a command injection attack.	2019-10-25	7.5	<a href="#">CVE-2019-5127</a> MISC
youthtube -- youthtube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Uri in /objects/getImageMP4.php is vulnerable to a command injection attack.	2019-10-25	7.5	<a href="#">CVE-2019-5128</a> MISC
youthtube -- youthtube	A command injection have been found in YouPHPTube Encoder. A successful attack could allow an attacker to compromise the server. Exploitable unauthenticated command injections exist in YouPHPTube Encoder 2.3 a plugin for providing encoder functionality in YouPHPTube. The parameter base64Uri in /objects/getSpiritsFromVideo.php is vulnerable to a command injection attack.	2019-10-25	7.5	<a href="#">CVE-2019-5129</a> MISC
ytnef -- ytnef	ytnef has directory traversal	2019-10-29	7.5	<a href="#">CVE-2009-3887</a> MISC MISC MISC MISC
zend_framework -- zend_framework	Zend Framework before 2.2.10 and 2.3.x before 2.3.5 has Potential SQL injection in PostgreSQL ZendDb adapter.	2019-10-25	7.5	<a href="#">CVE-2015-0270</a> MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	<a href="#">CVE-2019-8087</a> CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4 and 6.3 have a cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	<a href="#">CVE-2019-8083</a> CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	<a href="#">CVE-2019-8084</a> CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a reflected cross site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	<a href="#">CVE-2019-8085</a> CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a cross-site request forgery vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	4.3	<a href="#">CVE-2019-8234</a> CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have an authentication bypass vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	<a href="#">CVE-2019-8081</a> CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	<a href="#">CVE-2019-8082</a> CONFIRM
adobe -- experience_manager	Adobe Experience Manager versions 6.5, 6.4, 6.3 and 6.2 have a xml external entity injection vulnerability. Successful exploitation could lead to sensitive information disclosure.	2019-10-25	5	<a href="#">CVE-2019-8086</a> CONFIRM
apache -- hadoop	Hadoop 1.0.3 contains a symlink vulnerability.	2019-10-29	5	<a href="#">CVE-2012-2945</a> MISC MISC
apache -- thrift	In Apache Thrift 0.9.3 to 0.12.0, a server implemented in Go using TJSPProtocol or TSimpleJSONProtocol may panic when feed with invalid input data.	2019-10-29	5	<a href="#">CVE-2019-0210</a> CONFIRM
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows directory traversal by issuing a special HTTP POST request with ../ characters. This could lead to create malicious HTML file, because they can inject a content with crafted template. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	<a href="#">CVE-2019-17324</a> MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows remote attacker to upload arbitrary local file via the ActiveX method in RexViewerCtrl30.ocx. That could lead to disclosure of sensitive information. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	<a href="#">CVE-2019-17325</a> MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows remote attacker to arbitrary file deletion by issuing a HTTP GET request with a specially crafted parameter. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	5.8	<a href="#">CVE-2019-17326</a> MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows arbitrary file creation via a POST request with the parameter set to the file path to be written. This can be an executable file that is written to in the arbitrary directory. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	4.3	<a href="#">CVE-2019-17322</a> MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version have an information disclosure issue. When requesting web page associated with session, could leak username via session file path of HTTP response data. No authentication is required.	2019-10-30	5	<a href="#">CVE-2019-17321</a> MISC
clipsoft -- rexpert	ClipSoft REXPERT 1.0.0.527 and earlier version allows arbitrary file creation and execution via report print function of rexpert viewer with modified XML document. User interaction is required to exploit this vulnerability in that the target must visit a malicious web page.	2019-10-30	6.8	<a href="#">CVE-2019-17323</a> MISC

corehr -- core_portal	CoreHR Core Portal before 27.0.7 allows stored XSS.	2019-10-25	4.3	<a href="#">CVE-2019-18221</a> MISC MISC
debian_project -- mercurial	Mercurial before 1.6.4 fails to verify the Common Name field of SSL certificates which allows remote attackers who acquire a certificate signed by a Certificate Authority to perform a man-in-the-middle attack.	2019-10-29	4.3	<a href="#">CVE-2010-4237</a> MISC CONFIRM CONFIRM MISC
debian_project -- poottle	poottle 2.0.5 has XSS via 'match_names' parameter	2019-10-28	4.3	<a href="#">CVE-2010-4245</a> MISC DEBIAN MISC MISC
debian_project -- xpdf	In xpdf, the xref table contains an infinite loop which allows remote attackers to cause a denial of service (application crash) in xpdf-based PDF viewers.	2019-10-30	4.3	<a href="#">CVE-2010-0207</a> MISC MISC
debian_project -- xpdf	xpdf allows remote attackers to cause a denial of service (NULL pointer dereference and crash) in the way it processes JBIG2 PDF stream objects.	2019-10-30	4.3	<a href="#">CVE-2010-0206</a> MISC MISC
debian_project -- zoo	Zoo 2.10 has Directory traversal	2019-10-28	5	<a href="#">CVE-2005-2349</a> MISC MISC
devada -- dzone_and_answerhub	An XML External Entity Injection vulnerability exists in Dzone AnswerHub.	2019-10-28	5	<a href="#">CVE-2017-15725</a> MISC
digium -- asterisk	asterisk allows calls on prohibited networks	2019-10-29	5	<a href="#">CVE-2009-3723</a> MISC MISC MISC
fabrik -- fabrik	Reflected Cross-Site Scripting (XSS) vulnerability in the fabrik_referrer hidden field in the Fabrikar Fabrik component through v3.8.1 for Joomla! allows remote attackers to inject arbitrary web script via the HTTP Referer header.	2019-10-29	4.3	<a href="#">CVE-2018-10727</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of Javascript in the HTML2PDF plugin. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8692.	2019-10-25	6.8	<a href="#">CVE-2019-17139</a> MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DXF files to PDF. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9276.	2019-10-25	6.8	<a href="#">CVE-2019-17145</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion of DWG files to PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9274.	2019-10-25	6.8	<a href="#">CVE-2019-17144</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of script within a Keystroke action of a listbox field. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9081.	2019-10-25	6.8	<a href="#">CVE-2019-17142</a> MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of script within a Calculate action of a text field. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9044.	2019-10-25	6.8	<a href="#">CVE-2019-17141</a> MISC MISC
foxit -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DWG files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-9273.	2019-10-25	4.3	<a href="#">CVE-2019-17143</a> MISC
foxit -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.6.0.25114. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the OnFocus event. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9091.	2019-10-25	6.8	<a href="#">CVE-2019-17140</a> MISC MISC
foxit -- studio_photo	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.909. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the conversion from JPEG to EPS. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8809.	2019-10-25	4.3	<a href="#">CVE-2019-17138</a> MISC MISC
gnuboard -- gnuboard5	GNUBOARD5 before 5.3.2.0 has XSS that allows remote attackers to inject arbitrary web script or HTML via the "board group extra contents" parameter, aka the adm/boardgroup_form_update.php gr_1~10 parameter.	2019-10-30	4.3	<a href="#">CVE-2018-18678</a> MISC MISC MISC
gpw -- gpw	gpw generates shorter passwords than required	2019-10-29	5	<a href="#">CVE-2011-4931</a> MISC MISC MISC MISC
honeywell -- ip-ak2	In IP-AK2 Access Control Panel Version 1.04.07 and prior, the integrated web server of the affected devices could allow remote attackers to obtain web configuration data, which can be accessed without authentication over the network.	2019-10-25	5	<a href="#">CVE-2019-13525</a> MISC
ibm -- api_connect	IBM API Connect version V5.0.0.0 through 5.0.8.7 could reveal sensitive information to an attacker using a specially crafted HTTP request. IBM X-Force ID: 167883.	2019-10-29	5	<a href="#">CVE-2019-4600</a> XF CONFIRM



ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 162260.	2019-10-25	5	<a href="#">CVE-2019-4399</a> XF CONFIRM
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 162261.	2019-10-25	4	<a href="#">CVE-2019-4400</a> XF CONFIRM
ibm -- maximo_asset_management	After installing the IBM Maximo Health- Safety and Environment Manager 7.6.1, a user is granted additional privileges that they are not normally allowed to access. IBM X-Force ID: 165948.	2019-10-29	6.5	<a href="#">CVE-2019-4546</a> XF CONFIRM
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance could allow unauthenticated attacker to cause a denial of service in the reverse proxy component. IBM X-Force ID: 156159.	2019-10-25	5	<a href="#">CVE-2019-4036</a> XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 161418.	2019-10-29	5	<a href="#">CVE-2019-4339</a> XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 specifies permissions for a security-critical resource which could lead to the exposure of sensitive information or the modification of that resource by unintended parties. IBM X-Force ID: 160986.	2019-10-29	6.4	<a href="#">CVE-2019-4306</a> XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores sensitive information in cleartext within a resource that might be accessible to another control sphere. IBM X-Force ID: 1610141.	2019-10-29	5	<a href="#">CVE-2019-4314</a> XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 does not set the secure attribute for cookies in HTTPS sessions, which could cause the user agent to send those cookies in plaintext over an HTTP session. IBM X-Force ID: 161210.	2019-10-29	4.3	<a href="#">CVE-2019-4330</a> XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 161209.	2019-10-29	4	<a href="#">CVE-2019-4329</a> XF CONFIRM
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161037.	2019-10-29	5	<a href="#">CVE-2019-4311</a> XF CONFIRM
ikiwiki -- ikiwiki	A cross-site scripting (XSS) vulnerability in ikiwiki before 3.20101112 allows remote attackers to inject arbitrary web script or HTML via a comment.	2019-10-30	4.3	<a href="#">CVE-2010-1673</a> CONFIRM MISC
ikiwiki -- ikiwiki	Cross Site Scripting (XSS) in ikiwiki before 3.20110122 could allow remote attackers to insert arbitrary JavaScript code to insufficient checking in comments.	2019-10-29	4.3	<a href="#">CVE-2011-0428</a> CONFIRM MISC
jetbrains -- teamcity	In JetBrains YouTrack before 2019.2.55152, removing tags from the issues list without the corresponding permission was possible.	2019-10-31	5	<a href="#">CVE-2019-18369</a> CONFIRM
jetbrains -- teamcity	In JetBrains TeamCity before 2019.1.2, access could be gained to the history of builds of a deleted build configuration under some circumstances.	2019-10-31	5	<a href="#">CVE-2019-18363</a> CONFIRM
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. It is possible to force a logged-in administrator to execute code through a /reports-viewScriptReport.view CSRF vulnerability.	2019-10-29	6.8	<a href="#">CVE-2019-9926</a> MISC MISC
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. Sending an SVG containing an XXE payload to the endpoint visualization-exportImage.view or visualization-exportPDF.view allows local files to be read.	2019-10-29	5	<a href="#">CVE-2019-9757</a> MISC MISC
libpod -- libpod	An issue was discovered in Podman in libpod before 1.6.0. It resolves a symlink in the host context during a copy operation from the container to the host, because an undesired glob operation occurs. An attacker could create a container image containing particular symlinks that, when copied by a victim user to the host filesystem, may overwrite existing files with others from the host.	2019-10-28	5.8	<a href="#">CVE-2019-18466</a> MISC MISC MISC MISC
mcafee -- mcafee_total_protection	A File Masquerade vulnerability in McAfee Total Protection (MTP) version 16.0.R21 and earlier in Windows client allowed an attacker to read the plaintext list of AV-Scan exclusion files from the Windows registry, and to possibly replace excluded files with potential malware without being detected.	2019-10-28	4.6	<a href="#">CVE-2019-3636</a> CONFIRM
mediawiki -- mediawiki	An issue was discovered in the AbuseFilter extension through 1.34 for MediaWiki. Previously hidden (restricted) AbuseFilter filters were viewable (or their differences were viewable) to unprivileged users, thus disclosing potentially sensitive information.	2019-10-29	5	<a href="#">CVE-2019-18612</a> MISC MISC
mediawiki -- mediawiki	A cross-site scripting (XSS) vulnerability in MediaWiki before 1.19.5 and 1.20.x before 1.20.4 and allows remote attackers to inject arbitrary web script or HTML via Lua function names.	2019-10-31	4.3	<a href="#">CVE-2013-1951</a> MISC MISC MISC MISC MISC MISC MISC CONFIRM MISC
mediawiki -- mediawiki	An issue was discovered in the CheckUser extension through 1.34 for MediaWiki. Certain sensitive information within oversights edit summaries made available via the MediaWiki API was potentially visible to users with various levels of access to this extension. Said users should not have been able to view these oversights edit summaries via the MediaWiki API.	2019-10-29	4	<a href="#">CVE-2019-18611</a> MISC MISC
mediawiki -- mediawiki	mediawiki allows deleted text to be exposed	2019-10-29	5	<a href="#">CVE-2012-0046</a> MISC MISC MISC
mikrotik -- routeros	RouterOS versions 6.45.6 Stable, 6.44.5 Long-term, and below are vulnerable to a DNS unrelated data attack. The router adds all A records to its DNS cache even when the records are unrelated to the domain that was queried. Therefore, a remote attacker controlled DNS server can poison the router's DNS cache via malicious responses with additional and untrue records.	2019-10-29	5	<a href="#">CVE-2019-3979</a> MISC
mikrotik -- routeros	RouterOS 6.45.6 Stable, RouterOS 6.44.5 Long-term, and below are vulnerable to an arbitrary directory creation vulnerability via the upgrade package's name field. If an authenticated user installs a malicious package then a directory could be created and the developer shell could be enabled.	2019-10-29	6.5	<a href="#">CVE-2019-3976</a> MISC
mikrotik -- routeros	RouterOS versions 6.45.6 Stable, 6.44.5 Long-term, and below allow remote unauthenticated attackers to trigger DNS queries via port 8291. The queries are sent from the router to a server of the attacker's choice. The DNS responses are cached by the router, potentially resulting in cache poisoning	2019-10-29	5	<a href="#">CVE-2019-3978</a> MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a default set of 10 privileged accounts with hardcoded credentials. They are accessible if the customer has not configured 10 actual user accounts.	2019-10-25	5	<a href="#">CVE-2016-2358</a> MISC MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a default root password in /etc/shadow that is the same across different customers' installations.	2019-10-25	5	<a href="#">CVE-2016-2360</a> MISC MISC MISC
milesight -- ip_security_cameras	Milesight IP security cameras through 2016-11-14 have a hardcoded SSL private key	2019-10-25	5	<a href="#">CVE-2016-2357</a> MISC

	under the /etc/config directory.			MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A world-readable /usr/smarttru/init/settings.xml configuration file on the file system allows an attacker to read sensitive configuration settings such as usernames, passwords, and other sensitive RTU data due to insecure permission assignment.	2019-10-28	4	<a href="#">CVE-2019-14925</a> MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. Stored cleartext passwords could allow an unauthenticated attacker to obtain configured username and password combinations on the RTU due to the weak credentials management on the RTU. An unauthenticated user can obtain the exposed password credentials to gain access to the following services: DDNS service, Mobile Network Provider, and OpenVPN service.	2019-10-28	5	<a href="#">CVE-2019-14929</a> MISC MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. An unauthenticated remote configuration download vulnerability allows an attacker to download the smartRTU's configuration file (which contains data such as usernames, passwords, and other sensitive RTU data).	2019-10-28	5	<a href="#">CVE-2019-14927</a> MISC MISC
netapp -- clustered_data_ontap	Clustered Data ONTAP versions 9.2 through 9.6 are susceptible to a vulnerability which allows an attacker to use IPping to cause a Denial of Service (DoS).	2019-10-25	5	<a href="#">CVE-2019-5508</a> MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to an information disclosure vulnerability because uninitialized scalars are sent over the network to a peer.	2019-10-29	5	<a href="#">CVE-2019-18602</a> MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to information leakage upon certain error conditions because uninitialized RPC output variables are sent over the network to a peer.	2019-10-29	4.3	<a href="#">CVE-2019-18603</a> MISC
openafs_foundation -- openafs	OpenAFS before 1.6.24 and 1.8.x before 1.8.5 is prone to denial of service from unserialized data access because remote attackers can make a series of VOTE_Debug RPC calls to crash a database server within the SVOTE_Debug RPC handler.	2019-10-29	5	<a href="#">CVE-2019-18601</a> MISC
pimcore -- pimcore	Pimcore 6.2.3 has XSS in the translations grid because bundles/AdminBundle/Resources/public/js/pimcore/settings/translations.js mishandles certain HTML elements.	2019-10-31	4.3	<a href="#">CVE-2019-18656</a> MISC
pixelpost -- pixelpost	pixelpost 1.7.1 has XSS	2019-10-28	4.3	<a href="#">CVE-2009-4900</a> MISC DEBIAN MISC
python_keyring_lib -- python_keyring_lib	Python keyring lib before 0.10 created keyring files with world-readable permissions.	2019-10-28	5	<a href="#">CVE-2012-5577</a> MISC CONFIRM MISC MISC MISC
rittal -- rittal_chiller_sk_3232_series	Rittal Chiller SK 3232-Series web interface as built upon Carel pCOWeb firmware A1.5.3 ? B1.2.4. The authentication mechanism on affected systems does not provide a sufficient level of protection against unauthorized configuration changes. Primary operations, namely turning the cooling unit on and off and setting the temperature set point, can be modified without authentication.	2019-10-25	5	<a href="#">CVE-2019-13549</a> FULLDISC MISC
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the firmware with no firmware image inside the package using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6841</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the firmware with a missing web server image inside the package using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6842</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the controller with an empty firmware package using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6843</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the PLC when upgrading the controller with a firmware package containing an invalid web server image using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6844</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause a Denial of Service attack on the FTP service when upgrading the firmware with a version incompatible with the application in the controller using FTP protocol.	2019-10-29	4	<a href="#">CVE-2019-6847</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-200: Information Exposure vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause the disclosure of sensitive information when using specific Modbus services provided by the REST API of the controller/communication module.	2019-10-29	5	<a href="#">CVE-2019-6849</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause a Denial of Service attack on the PLC when sending specific data on the REST API of the controller/communication module.	2019-10-29	5	<a href="#">CVE-2019-6848</a> CONFIRM
schneider_electric -- multiple_modicon_controllers	A CWE-200: Information Exposure vulnerability exists in Modicon M580, Modicon BMENOC 0311, and Modicon BMENOC 0321, which could cause the disclosure of sensitive information when reading specific registers with the REST API of the controller/communication module.	2019-10-29	5	<a href="#">CVE-2019-6850</a> CONFIRM
terramaster -- fs-210_devices	An issue was discovered on TerraMaster FS-210 4.0.19 devices. Normal users can use 1.user.php for privilege elevation.	2019-10-28	6.5	<a href="#">CVE-2019-18195</a> MISC
tightvnc_software -- tightvnc	TightVNC code version 1.3.10 contains null pointer dereference in HandleZlibBPP function, which results Denial of System (DoS). This attack appear to be exploitable via network connectivity.	2019-10-29	5	<a href="#">CVE-2019-15680</a> MLIST
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has XSS	2019-10-28	4.3	<a href="#">CVE-2010-4240</a> MISC MISC MISC MISC
tiki_wiki -- cms_groupware	Tiki Wiki CMS Groupware 5.2 has CSRF	2019-10-28	6.8	<a href="#">CVE-2010-4241</a> MISC MISC MISC MISC
total_defense -- anti-virus	The malware scan function in Total Defense Anti-virus 11.5.2.28 is vulnerable to a TOCTOU bug; consequently, symbolic link attacks allow privileged files to be deleted.	2019-10-31	5.8	<a href="#">CVE-2019-18644</a> MISC
transmission -- transmission	Transmission before 1.92 allows attackers to prevent download of a file by corrupted data during the endgame.	2019-10-30	5	<a href="#">CVE-2010-0749</a> MISC CONFIRM MISC CONFIRM MLIST
	Trend Micro Apex One could be exploited by an attacker utilizing a command injection			

trend_micro -- apex_one	vulnerability to extract files from an arbitrary zip file to a specific folder on the Apex One server, which could potentially lead to remote code execution (RCE). The remote process execution is bound to the IUSR account, which has restricted permission and is unable to make major system changes. An attempted attack requires user authentication.	2019-10-28	5	<a href="#">CVE-2019-18188</a> <a href="#">N/A</a>
trend_micro -- office_scan	Trend Micro OfficeScan versions 11.0 and XG (12.0) could be exploited by an attacker utilizing a directory traversal vulnerability to extract files from an arbitrary zip file to a specific folder on the OfficeScan server, which could potentially lead to remote code execution (RCE). The remote process execution is bound to a web service account, which depending on the web platform used may have restricted permissions. An attempted attack requires user authentication.	2019-10-28	5	<a href="#">CVE-2019-18187</a> <a href="#">N/A</a>
youshptube -- youshptube	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5120</a> <a href="#">MISC</a>
youshptube -- youshptube	SQL injection vulnerabilities exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter name in /objects/pluginSwitch.json.php.	2019-10-25	6.5	<a href="#">CVE-2019-5122</a> <a href="#">MISC</a>
youshptube -- youshptube	SQL injection vulnerabilities exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with Parameter uuid in /objects/pluginSwitch.json.php	2019-10-25	6.5	<a href="#">CVE-2019-5121</a> <a href="#">MISC</a>
youshptube -- youshptube	An exploitable SQL injection vulnerability exist in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configurations, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5119</a> <a href="#">MISC</a>
youshptube -- youshptube	Exploitable SQL injection vulnerabilities exists in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5117</a> <a href="#">MISC</a>
youshptube -- youshptube	An exploitable SQL injection vulnerability exists in the authenticated part of YouPHPTube 7.6. Specially crafted web requests can cause a SQL injection. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5116</a> <a href="#">MISC</a>
youshptube -- youshptube	An exploitable SQL injection vulnerability exists in the authenticated portion of YouPHPTube 7.6. Specially crafted web requests can cause SQL injections. An attacker can send a web request with parameters containing SQL injection attacks to trigger this vulnerability, potentially allowing exfiltration of the database, user credentials and in certain configuration, access the underlying operating system.	2019-10-25	6.5	<a href="#">CVE-2019-5114</a> <a href="#">MISC</a>
youshptube -- youshptube	Specially crafted web requests can cause SQL injections in YouPHPTube 7.6. An attacker can send a web request with Parameter dir in /objects/pluginSwitch.json.php.	2019-10-25	6.5	<a href="#">CVE-2019-5123</a> <a href="#">MISC</a>
zucchetti -- infobusiness	Multiple Reflected Cross-site Scripting (XSS) vulnerabilities exist in Zucchetti InfoBusiness before and including 4.4.1. The browsing component did not properly sanitize user input (encoded in base64). This also applies to the search functionality for the searchKey parameter.	2019-10-30	4.3	<a href="#">CVE-2019-18205</a> <a href="#">MISC</a>
zucchetti -- infobusiness	Zucchetti InfoBusiness before and including 4.4.1 allows any authenticated user to upload .php files in order to achieve code execution.	2019-10-30	6.5	<a href="#">CVE-2019-18204</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- airflow	A malicious admin user could edit the state of objects in the Airflow metadata database to execute arbitrary javascript on certain page views. This also presented a Local File Disclosure vulnerability to any file readable by the webserver process.	2019-10-30	3.5	<a href="#">CVE-2019-12417</a> <a href="#">MLIST</a>
d-link -- dir-865l_devices	D-Link DIR-865L has Information Disclosure.	2019-10-25	2.9	<a href="#">CVE-2013-4856</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
debian_project -- mailscanner	mailscanner can allow local users to prevent virus signatures from being updated	2019-10-28	2.1	<a href="#">CVE-2010-3293</a> <a href="#">MISC</a> <a href="#">DEBIAN</a> <a href="#">MISC</a> <a href="#">MISC</a>
debian_project -- paxtext	paxtext handles temporary files insecurely	2019-10-29	2.1	<a href="#">CVE-2010-3373</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gmer -- gmer	A stack based buffer overflow vulnerability exists in the method receiving data from SysTreeView32 control of the GMER 2.1.19357 application. A specially created long path can lead to a buffer overflow on the stack resulting in code execution. An attacker needs to create path longer than 99 characters to trigger this vulnerability.	2019-10-29	2.1	<a href="#">CVE-2016-4289</a> <a href="#">MISC</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 could allow a local user to obtain sensitive information from temporary script files. IBM X-Force ID: 162333.	2019-10-25	2.1	<a href="#">CVE-2019-4395</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 is vulnerable to HTTP response splitting attacks, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject arbitrary HTTP headers and cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning or cross-site scripting, and possibly obtain sensitive information. IBM X-Force ID: 162236.	2019-10-25	3.5	<a href="#">CVE-2019-4396</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 is vulnerable to HTTP Response Splitting caused by improper caching of content. This would allow the attacker to perform further attacks, such as Web Cache poisoning, cross-site scripting and possibly obtain sensitive information. IBM X-Force ID: 163682.	2019-10-25	3.5	<a href="#">CVE-2019-4461</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cloud_orchestrator	IBM Cloud Orchestrator 2.4 through 2.4.0.5 and 2.5 through 2.5.0.9 contain APIs that could be used by a local user to send email. IBM X-Force ID: 162232.	2019-10-25	2.1	<a href="#">CVE-2019-4394</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 160987.	2019-10-29	2.1	<a href="#">CVE-2019-4307</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium_big_data_intelligence	IBM Security Guardium Big Data Intelligence (SonarG) 4.0 uses hard coded credentials which could allow a local user to obtain highly sensitive information. IBM X-Force ID: 161035.	2019-10-29	2.1	<a href="#">CVE-2019-4309</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
labkey -- labkey_server	An issue was discovered in LabKey Server 19.1.0. The display name of a user is vulnerable to stored XSS that can execute on administrators from			<a href="#">CVE-2019-9758</a>

	security/permissions.view, security/addUsers.view, or wiki/Administration/page.view in the admin panel, leading to privilege escalation.	2019-10-29	3.5	MISC MISC
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the configuration report page (adm_config_report.php) in MantisBT 1.2.0rc1 before 1.2.14 allows remote authenticated users to inject arbitrary web script or HTML via a complex value.	2019-10-31	3.5	CVE-2013-1934 MISC MISC MISC CONFIRM MISC
mitsubishi_electric_and_inea -- me-rtu_devices	An issue was discovered on Mitsubishi Electric ME-RTU devices through 2.02 and INEA ME-RTU devices through 3.0. A number of stored cross-site script (XSS) vulnerabilities allow an attacker to inject malicious code directly into the application. An example input variable vulnerable to stored XSS is SerialInitialModemString in the index.php page.	2019-10-28	3.5	CVE-2019-14928 MISC MISC
postgresql -- postgresql	Postgresql, versions 11.x before 11.5, is vulnerable to a memory disclosure in cross-type comparison for hashed subplan.	2019-10-29	3.5	CVE-2019-10209 CONFIRM CONFIRM
postgresql -- postgresql_windows_installer	Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.	2019-10-29	1.9	CVE-2019-10210 CONFIRM CONFIRM
total_defense -- antivirus	The quarantine restoration function in Total Defense Anti-virus 11.5.2.28 is vulnerable to symbolic link attacks, allowing files to be written to privileged directories.	2019-10-31	2.1	CVE-2019-18645 MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published Score	Source & Patch Info
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. Lack of sanitization of user-supplied input cause SQL injection vulnerabilities. An attacker can leverage these vulnerabilities to disclose information.	2019- r/bt yet calculated 31	CVE-2019-18229 MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. There is an unsecured function that allows anyone who can access the IP address to use the function without authentication.	2019- r/bt yet calculated 31	CVE-2019-13547 MISC MISC
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. XXE vulnerabilities exist that may allow disclosure of sensitive data.	2019- r/bt yet calculated 31	CVE-2019-18227 MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
advantech -- wise-paas/rmm	Advantech WISE-PaaS/RMM, Versions 3.3.29 and prior. Path traversal vulnerabilities are caused by a lack of proper validation of a user-supplied path prior to use in file operations. An attacker can leverage these vulnerabilities to remotely execute code while posing as an administrator.	2019- r/bt yet calculated 31	CVE-2019-13551 MISC MISC MISC MISC MISC
amd -- atidxx64.dll_driver	An exploitable memory corruption vulnerability exists in AMD ATIDXX64.DLL driver, versions 25.20.15031.5004 and 25.20.15031.9002. A specially crafted pixel shader can cause an out-of-bounds memory write. An attacker can provide a specially crafted shader file to trigger this vulnerability. This vulnerability can be triggered from VMware guest, affecting VMware host.	2019- r/bt yet calculated 31	CVE-2019-5049 MISC
apache -- struts	Apache Struts before 2.3.1.2 allows remote attackers to bypass security protections in the ParameterInterceptor class and execute arbitrary commands.	2019- r/bt yet calculated 01	CVE-2011-3923 MISC EXPLOIT-DB BID MISC MISC XF MISC
apak -- wholesale_floorplanning_finance	Apak Wholesale Floorplanning Finance 6.31.8.3 and 6.31.8.5 allows XSS via the mainForm:loanNotesnotes:0:rich_text_editor_note_text parameter to WFS/agreementView.faces in the Notes section. Although versions 6.31.8.3 and 6.31.8.5 are confirmed to be affected, all versions with the vulnerable WYSIWYG ?Notes? section are likely affected.	2019- r/bt yet calculated 31	CVE-2019-17551 MISC
archiver -- archiver	All versions of archiver allow attacker to perform a Zip Slip attack via the "unarchive" functions. It is exploited using a specially crafted zip archive, that holds path traversal filenames. When exploited, a filename in a malicious archive is concatenated to the target extraction directory, which results in the final path ending up outside of the target folder. For instance, a zip may hold a file with a ".\\file.exe" location and thus break out of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.	2019- r/bt yet calculated 29	CVE-2019-10743 MISC MISC MISC
archos -- safe-t_devices	On Archos Safe-T devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. In other words, the side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data.	2019- r/bt yet calculated 02	CVE-2019-14358 MISC
aruba -- instant	Aruba Instant 4.x prior to 6.4.4.8-4.2.4.12, 6.5.x prior to 6.5.4.11, 8.3.x prior to 8.3.0.6, and 8.4.x prior to 8.4.0.1 allows Command injection.	2019- r/bt yet calculated 30	CVE-2018-16417 BID CONFIRM MISC CONFIRM MISC
	An exploitable uninitialized pointer vulnerability exists in the Word document parser of the the Atlantis Word Processor. A specially crafted document can cause an array fetch to return an	2019-	

atlantis_word_processor -- atlantis_word_processor	uninitialized pointer and then performs some arithmetic before writing a value to the result. Usage of this uninitialized pointer can allow an attacker to corrupt heap memory resulting in code execution under the context of the application. An attacker must convince a victim to open a document in order to trigger this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2018-3983</a> MISC
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app before 1.6.14_J8 for Jira. It is possible to obtain a list of all Jira projects without authentication/authorization via the plugins/servlet/nfj/ProjectFilter?searchQuery= URL.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-16908</a> MISC MISC
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app before 1.6.14_J8 for Jira. It is possible to obtain a list of all Jira projects (with authentication as a Jira user, but without authorization for specific projects) via the plugins/servlet/nfj/NotificationSettings URL.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-16909</a> MISC MISC
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app 1.6.13_J8 for Jira. It is possible to obtain a list of all valid Jira usernames without authentication/authorization via the plugins/servlet/nfj/UserFilter?searchQuery=@ URL.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16907</a> MISC BUGTRAQ
atlassian -- infostysa_for_jira	An issue was discovered in the Infostysa "In-App & Desktop Notifications" app 1.6.13_J8 for Jira. By using plugins/servlet/nfj/PushNotification?username= with a modified username, a different user's notifications can be read without authentication/authorization. These notifications are then no longer displayed to the normal user.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16906</a> MISC BUGTRAQ
atlassian -- jira	An issue summary information disclosure vulnerability exists in Atlassian Jira Tempo plugin, version 4.10.0. Authenticated users can obtain the summary for issues they do not have permission to view via the Tempo plugin.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5095</a> MISC
autojump -- autojump	autojump before 21.5.8 allows local users to gain privileges via a Trojan horse custom_install directory in the current working directory.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-2012</a> MISC MISC MISC CONFIRM CONFIRM MISC
avast -- antivirus	A Cross Site Scripting (XSS) issue exists in Avast AntiVirus (Free, Internet Security, and Premiere Edition) 19.3.2369 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-18653</a> MISC MISC
avg_technologies -- avg_antivirus	A Cross Site Scripting (XSS) issue exists in AVG AntiVirus (Internet Security Edition) 19.3.3084 build 19.3.4241.440 in the Network Notification Popup, allowing an attacker to execute JavaScript code via an SSID Name.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-18654</a> MISC MISC
axohelp -- axohelp	In axohelp.c before 1.3 in axohelp in axodraw2 before 2.1.1b, as distributed in TeXLive and other collections, sprintf is mishandled.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-18604</a> MISC
bitdefender -- box_firmware	An issue was discovered in Bitdefender BOX firmware versions before 2.1.37.37-34 that allows an attacker to pass arbitrary code to the BOX appliance via the web API. In order to exploit this vulnerability, an attacker needs presence in Bitdefender BOX setup network and Bitdefender BOX be in setup mode.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-12612</a> CONFIRM
centos-webpanel -- centos_web_panel	Stored XSS in filemanager2.php in CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.885 exists via the cmd_arg parameter. This can be exploited by a local attacker who supplies a crafted filename within a directory visited by the victim.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16295</a> MISC CONFIRM
cezerin -- cezerin	Cezerin v0.33.0 allows unauthorized order-information modification because certain internal attributes can be overwritten via a conflicting name when processing order requests. Hence, a malicious customer can manipulate an order (e.g., its payment status or shipping fee) by adding additional attributes to user-input during the PUT /ajax/cart operation for a checkout, because of getValidDocumentForUpdate in api/server/services/orders/orders.js.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-18608</a> MISC
chicken -- chicken	OS command injection vulnerability in the "qs" procedure from the "utils" module in Chicken before 4.9.0.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-2024</a> MISC MISC MISC MISC CONFIRM MISC MISC
chicken -- chicken	Multiple buffer overflows in the (1) R5RS char-ready, (2) tcp-accept-ready, and (3) file-select procedures in Chicken through 4.8.0.3 allows attackers to cause a denial of service (crash) by opening a file descriptor with a large integer value. NOTE: this issue exists because of an incomplete fix for CVE-2012-6122.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-2075</a> CONFIRM CONFIRM CONFIRM MISC MISC MISC CONFIRM MISC
chicken -- chicken	A casting error in Chicken before 4.8.0 on 64-bit platform caused the random number generator to return a constant value. NOTE: the vendor states "This function wasn't used for security purposes (and is advertised as being unsuitable)."	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6124</a> MISC MISC CONFIRM MISC
chicken -- chicken	Chicken before 4.8.0 does not properly handle NUL bytes in certain strings, which allows an attacker to conduct "poisoned NUL byte attack."	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6123</a> MISC MISC MISC
chicken -- chicken	Chicken before 4.8.0 is susceptible to algorithmic complexity attacks related to hash table collisions.	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6125</a> MISC MISC CONFIRM CONFIRM MISC
chicken -- chicken	Buffer overflow in the thread scheduler in Chicken before 4.8.0.1 allows attackers to cause a denial of service (crash) by opening a file descriptor with a large integer value.	2019- r/bt yet calculated 31	<a href="#">CVE-2012-6122</a> MISC MISC MISC MISC CONFIRM CONFIRM MISC
compal -- ch7465lg_modem	The web interface of the Compal Broadband CH7465LG modem (version CH7465LG-NCIP-6.12.18.25-2p6-NOSH) is vulnerable to a %2f path traversal attack, which can be exploited in order to test for the existence of a file pathname outside of the web root directory. If a file exists but is not part of the product, there is a 404 error. If a file does not exist, there is a 302 redirect to index.html.	2019- r/bt yet calculated 28	<a href="#">CVE-2019-17224</a> MISC MISC
cujo -- smart_firewall	An exploitable vulnerability exists in the safe browsing function of the CUJO Smart Firewall, version 7003. The flaw lies in the way the safe browsing function parses HTTP requests. The server hostname is extracted from captured HTTP/HTTPS requests and inserted as part of a Lua statement without prior sanitization, which results in arbitrary Lua script execution in the kernel. An attacker could send an HTTP request to exploit this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2018-4031</a> MISC
cujo -- smart_firewall	An exploitable denial-of-service vulnerability exists in the mDNScap binary of the CUJO Smart Firewall running firmware 7003. When parsing labels in mDNS packets, the firewall unsafely handles label compression pointers, leading to an uncontrolled recursion that eventually exhausts the stack, crashing the mDNScap process. An unauthenticated attacker can send an	2019- r/bt yet calculated 31	<a href="#">CVE-2018-4002</a> MISC



	mDNS message to trigger this vulnerability.		
debian_project -- autokey	The init script in autokey before 0.61.3-2 allows local attackers to write to arbitrary files via a symlink attack.	2019- r/bt yet calculated 30	<a href="#">CVE-2010-0398</a> MISC MISC
debian_project -- burn	burn allows file names to escape via mishandled quotation marks	2019- r/bt yet calculated 31	<a href="#">CVE-2009-5043</a> MISC
debian_project -- debian	The Debian backport of the fix for CVE-2017-3137 leads to assertion failure in validator.c:1858; Affects Debian versions 9.9.5.dfs-g-9+deb8u15; 9.9.5.dfs-g-9+deb8u18; 9.10.3.dfs-g.P4-12.3+deb9u5; 9.11.5.P4+dfs-g-5.1 No ISC releases are affected. Other packages from other distributions who did similar backports for the fix for 2017-3137 may also be affected.	2019- r/bt yet calculated 30	<a href="#">CVE-2018-5735</a> CONFIRM
debian_project -- mumble	Mumble: murmur-server has DoS due to malformed client query	2019- r/bt yet calculated 31	<a href="#">CVE-2010-2490</a> MISC MISC MISC
debian_project -- overkill	overkill has buffer overflow via long player names that can corrupt data on the server machine	2019- r/bt yet calculated 31	<a href="#">CVE-2009-5041</a> MISC
debian_project -- python-docutils	python-docutils allows insecure usage of temporary files	2019- r/bt yet calculated 31	<a href="#">CVE-2009-5042</a> MISC
debian_project -- drbd8	drbd8 allows local users to bypass intended restrictions for certain actions via netlink packets, similar to CVE-2009-3725.	2019- r/bt yet calculated 30	<a href="#">CVE-2010-0747</a> MISC CONFIRM
debian_project -- mutt	Mutt before 1.5.20 patch 7 allows an attacker to cause a denial of service via a series of requests to mutt temporary files.	2019- r/bt yet calculated 01	<a href="#">CVE-2005-2351</a> MISC MISC
elastic -- elasticsearch	Elasticsearch versions 7.0.0-7.3.2 and 6.7.0-6.8.3 contain a username disclosure flaw was found in the API Key service. An unauthenticated attacker could send a specially crafted request and determine if a username exists in the Elasticsearch native realm.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-7619</a> CONFIRM CONFIRM CONFIRM
elastic -- logstash	Logstash versions before 7.4.1 and 6.8.4 contain a denial of service flaw in the Logstash Beats input plugin. An unauthenticated user who is able to connect to the port the Logstash beats input could send a specially crafted network packet that would cause Logstash to stop responding.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-7620</a> CONFIRM CONFIRM CONFIRM
european_commission -- eidas_node_integration_package	European Commission eIDAS-Node Integration Package before 2.3.1 has Missing Certificate Validation because a certain ExplicitKeyTrustEvaluator return value is not checked. NOTE: only 2.1 is confirmed to be affected.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-18633</a> MISC
european_commission -- eidas_node_integration_package	European Commission eIDAS-Node Integration Package before 2.3.1 allows Certificate Faking because an attacker can sign a manipulated SAML response with a forged certificate.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-18632</a> MISC
f5 -- big-ip	On BIG-IP 13.1.0-13.1.3.1, 12.1.0-12.1.5, and 11.5.2-11.6.5.1, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the BIG-IP Configuration utility.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-6657</a> CONFIRM
f5 -- big-ip_afm	On BIG-IP AFM 15.0.0-15.0.1, 14.0.0-14.1.2, 13.1.0-13.1.3.1, and 12.1.0-12.1.5, a vulnerability in the AFM configuration utility may allow any authenticated BIG-IP user to run an SQL injection attack.	2019- r/bt yet calculated 01	<a href="#">CVE-2019-6658</a> CONFIRM
facebook -- whatsapp	The Wireless Emergency Alerts (WEA) protocol allows remote attackers to spoof a Presidential Alert because cryptographic authentication is not used, as demonstrated by MessageIdentifier 4370 in LTE System Information Block 12 (aka SIB12). NOTE: testing inside an RF-isolated shield box suggested that all LTE phones are affected by design (e.g., use of Android versus iOS does not matter); testing in an open RF environment is, of course, contraindicated.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18659</a> MISC
fastweb -- fastgate_devices	Fastweb FASTGate 1.0.1b devices allow partial authentication bypass by changing a certain check_pwd return value from 0 to 1. An attack does not achieve administrative control of a device; however, the attacker can view all of the web pages of the administration console.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18661</a> MISC MISC
fortinet -- fortitender	An OS command injection vulnerability in FortiExtender 4.1.1 and below under CLI admin console may allow unauthorized administrators to run arbitrary system level commands via specially crafted "execute date" commands.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-15710</a> CONFIRM
foswiki -- foswiki	Foswiki before 1.1.8 contains a code injection vulnerability in the MAKETEXT macro.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-1666</a> CONFIRM MISC MISC MISC
freebsd --freetsd	/usr/local/www/freeradius_view_config.php in the freeradius3 package before 0.15.7_3 for pSense on FreeBSD has XSS via a filename.	2019- r/bt yet calculated 02	<a href="#">CVE-2019-18667</a> MISC
freebsd -- freetsd	FreeBSD NSD before 3.2.13 allows remote attackers to crash a NSD child server process (SIGSEGV) and cause a denial of service in the NSD server.	2019- r/bt yet calculated 01	<a href="#">CVE-2012-2979</a> MISC CONFIRM MISC
freetds -- freetds	FreeTDS through 1.1.11 has a Buffer Overflow.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-13508</a> MISC
glpi_project -- glpi	GLPI 0.83.7 has Local File Inclusion in common.tabs.php.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2227</a> MISC MISC MISC MISC
gnome -- evince	evince is missing a check on number of pages which can lead to a segmentation fault	2019- r/bt yet calculated 01	<a href="#">CVE-2013-3718</a> MISC MISC MISC MISC
google -- nest_cam_iq_indoor	An exploitable denial-of-service vulnerability exists in the Weave daemon of the Nest Cam IQ Indoor, version 4620002. A set of TCP connections can cause unrestricted resource allocation, resulting in a denial of service. An attacker can connect multiple times to trigger this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5043</a> MISC
grsecurity -- pax	An exploitable vulnerability exists in the grsecurity PaX patch for the function read_kmem, in PaX from version pax-linux-4.9.8-test1 to 4.9.24-test7, grsecurity official from version grsecurity-3.1-4.9.8-201702060653 to grsecurity-3.1-4.9.24-201704252333, grsecurity unofficial from version v4.9.25-unofficialgrsec to v4.9.74-unofficialgrsec. PaX adds a temp buffer to the read_kmem function, which is never freed when an invalid address is supplied. This results in a memory leakage that can lead to a crash of the system. An attacker needs to induce a read to /dev/kmem using an invalid address to exploit this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5023</a> MISC
gs-gpl -- gs-gpl	I race condition in Temp files was found in gs-gpl before 8.56 addons scripts.	2019- r/bt yet calculated 01	<a href="#">CVE-2005-2352</a> MISC MISC
honeywell -- equip_and_performance_series_ip_cameras	Honeywell eQIP and Performance series IP cameras, multiple versions, A vulnerability exists where the affected product allows unauthenticated access to audio streaming over HTTP.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-18230</a> MISC



mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the configuration report page (adm_config_report.php) in MantisBT 1.2.13 allows remote authenticated users to inject arbitrary web script or HTML via a project name.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-1932</a> MISC MISC MISC CONFIRM MISC
mantisbt -- mantisbt	MantisBT 1.2.12 before 1.2.15 allows authenticated users to by the workflow restriction and close issues.	2019- r/bt yet calculated 31	<a href="#">CVE-2013-1930</a> MISC MISC MISC MISC MISC MISC MISC MISC
mapserver -- mapserver	Mapserver 5.2, 5.4 and 5.6 before 5.6.5-2 improperly validates symbol index values during Mapfile parsing.	2019- r/bt yet calculated 29	<a href="#">CVE-2010-1678</a> MISC MISC CONFIRM
maxthon -- maxthon_browser_for_windows	Unquoted Search Path in Maxthon 5.1.0 to 5.2.7 Browser for Windows.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-16647</a> MISC MISC
minidlna -- minidlna	MiniDLNA has heap-based buffer overflow	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2739</a> MISC MISC
minidlna -- minidlna	minidlna has SQL Injection that may allow retrieval of arbitrary files	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2738</a> MISC MISC MISC MISC
miniupnpd -- miniupnpd	MiniUPnPd has information disclosure use of snprintf()	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2600</a> MISC MISC MISC MISC MISC
mooltipass -- moolticute	An issue was discovered in Mooltipass Moolticute through v0.42.1 and v0.42.x-testing through v0.42.5-testing. There is a NULL pointer dereference in MPDevice_win.cpp.	2019- r/bt yet calculated 30	<a href="#">CVE-2019-18635</a> MISC MISC
opera -- opera_mini_for_android	Opera Mini for Android allows attackers to bypass intended restrictions on .apk file download/installation via an RTLO (aka Right to Left Override) approach, as demonstrated by misinterpretation of malicious%E2%80%AEtxt.apk as maliciouskpa.txt. This affects 44.1.2254.142553, 44.1.2254.142659, and 44.1.2254.143214.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-18624</a> MISC MISC
phoenix_contact -- pc_works_and_pc_worx_express_and_config+	An issue was discovered in PHOENIX CONTACT PC Worx through 1.86, PC Worx Express through 1.86, and Config+ through 1.86. A manipulated PC Worx or Config+ project file could lead to an Out-of-bounds Read and remote code execution. The attacker needs to get access to an original PC Worx or Config+ project to be able to manipulate data inside. After manipulation, the attacker needs to exchange the original files with the manipulated ones on the application programming workstation.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-16675</a> MISC MISC MISC
postgresql -- postgresql	A flaw was discovered in postgresql versions 9.4.x before 9.4.24, 9.5.x before 9.5.19, 9.6.x before 9.6.15, 10.x before 10.10 and 11.x before 11.5 where arbitrary SQL statements can be executed given a suitable SECURITY DEFINER function. An attacker, with EXECUTE permission on the function, can execute arbitrary SQL as the owner of the function.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-10208</a> CONFIRM CONFIRM
postgresql -- postgresql_windows_installer	Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable by bundled OpenSSL executing code from unprotected directory.	2019- r/bt yet calculated 29	<a href="#">CVE-2019-10211</a> CONFIRM CONFIRM
project_jupyter -- jupyter_notebook	Jupyter Notebook before 5.5.0 does not use a CSP header to treat served files as belonging to a separate origin. Thus, for example, an XSS payload can be placed in an SVG document.	2019- r/bt yet calculated 31	<a href="#">CVE-2018-21030</a> MISC MISC
python -- python	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 / 3.6.6. A specially crafted X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initiate or accept TLS connections using crafted certificates to trigger this vulnerability.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5010</a> MISC
qtum -- qtum	qtum through 0.16 (a chain-based proof-of-stake cryptocurrency) allows a remote denial of service. The attacker sends invalid headers/blocks. The attack requires no stake and can fill the victim's disk and RAM.	2019- r/bt yet calculated 29	<a href="#">CVE-2018-19151</a> MISC MISC
rainbow_pdf -- office_server_document_converter	A buffer overflow vulnerability exists in the PowerPoint document conversion function of Rainbow PDF Office Server Document Converter V7.0 Pro MR1 (7.0.2019.0220). While parsing a document text info container, the TxMasterStyleAtom::parse function is incorrectly checking the bounds corresponding to the number of style levels, causing a vtable pointer to be overwritten, which leads to code execution.	2019- r/bt yet calculated 31	<a href="#">CVE-2019-5030</a> MISC
rdesktop -- rdesktop	RDesktop version 1.8.4 contains multiple out-of-bound access read vulnerabilities in its code, which results in a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. These issues have been fixed in version 1.8.5	2019- r/bt yet calculated 30	<a href="#">CVE-2019-15682</a> MISC
red_hat -- jboss_operations_network	A missing permission check was found in The CLI in JBoss Operations Network before 2.3.1 does not properly check permissions, which allows JBoss ON users to perform management tasks and configuration changes with the privileges of the administrator user.	2019- r/bt yet calculated 30	<a href="#">CVE-2010-0737</a> MISC
red_hat -- openshift	cartridges/openshift-origin-cartridge-mongodb-2.2/info/bin/dump.sh in OpenShift does not properly create files in /tmp.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-0165</a> MISC
red_hat -- openstack	HTTPSConnections in OpenStack Keystone 2013, OpenStack Compute 2013.1, and possibly other OpenStack components, fail to validate server-side SSL certificates.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-2255</a> MISC MISC MISC MISC MISC MISC
red_hat -- red_hat_enterprise_linux	While backporting a feature for a newer branch of BIND9, RedHat introduced a path leading to an assertion failure in buffer.c:420. Affects RedHat versions bind-9.9.4-65.el7 -> bind-9.9.4-72.el7. No ISC releases are affected. Other packages from other distributions who made the same error may also be affected.	2019- r/bt yet calculated 30	<a href="#">CVE-2018-5742</a> CONFIRM
redis -- redis	Insecure temporary file vulnerability in Redis 2.6 related to /tmp/redis.ds.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-0180</a> MLIST MISC
redis -- redis	Insecure temporary file vulnerability in Redis before 2.6 related to /tmp/redis-%p.vm.	2019- r/bt yet calculated 01	<a href="#">CVE-2013-0178</a> MISC MISC MISC MISC MISC
			<a href="#">CVE-2010-2061</a>

rpcbind -- rpcbind	rpcbind 0.2.0 does not properly validate (1) /tmp/portmap.xdr and (2) /tmp/rpcbind.xdr, which can be created by an attacker before the daemon is started.	2019- r/bt yet calculated 29	MISC MISC MISC MLIST
rpcbind -- rpcbind	rpcbind 0.2.0 allows local users to write to arbitrary files or gain privileges via a symlink attack on (1) /tmp/portmap.xdr and (2) /tmp/rpcbind.xdr.	2019- r/bt yet calculated 29	CVE-2010-2064 MISC MISC MISC MLIST
ruby193 -- ruby193	ruby193 uses an insecure LD_LIBRARY_PATH setting.	2019- r/bt yet calculated 31	CVE-2013-1945 MISC
sahi_pro -- sahi_pro	Sahi Pro 8.0.0 has a script manager arena located at _s_/dyn/pro/DBReports with many different areas that are vulnerable to reflected XSS, by updating a script's Script Name, Suite Name, Base URL, Android, iOS, Scripts Run, Origin Machine, or Comment field. The sql parameter can be used to trigger reflected XSS.	2019- r/bt yet calculated 29	CVE-2019-13066 MISC MISC
schneider_electric -- multiple_modicon_products	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists in Modicon M580, Modicon M340, Modicon Premium , Modicon Quantum (all firmware versions), which could cause the disclosure of information when transferring applications to the controller using Modbus TCP protocol.	2019- r/bt yet calculated 29	CVE-2019-6845 CONFIRM
schneider_electric -- multiple_modicon_products	A CWE-538: File and Directory Information Exposure vulnerability exists in Modicon M580, Modicon M340, Modicon Premium , Modicon Quantum (all firmware versions), which could cause the disclosure of information from the controller when using TFTP protocol.	2019- r/bt yet calculated 29	CVE-2019-6851 CONFIRM
schneider_electric -- multiple_modicon_products	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists in Modicon M580, Modicon M340, Modicon BMxCRA and 140CRA modules (all firmware versions), which could cause information disclosure when using the FTP protocol.	2019- r/bt yet calculated 29	CVE-2019-6846 CONFIRM
secudos -- domos	The Log module in SECUDOS DOMOS before 5.6 allows XSS.	2019- r/bt yet calculated 02	CVE-2019-18664 MISC
secudos -- domos	The Log module in SECUDOS DOMOS before 5.6 allows local file inclusion.	2019- r/bt yet calculated 02	CVE-2019-18665 MISC
sensiolabs -- php-symphony2-validator	php-symphony2-Validator has loss of information during serialization	2019- r/bt yet calculated 01	CVE-2013-4751 MISC MISC MISC MISC MISC
shift_cryptosecurity -- bitbox02	On SHIFT BitBox02 devices, a side channel for the row-based OLED display was found. The power consumption of each row-based display cycle depends on the number of illuminated pixels, allowing a partial recovery of display contents. For example, a hardware implant in the USB cable might be able to leverage this behavior to recover confidential secrets such as the PIN and BIP39 mnemonic. Note: BIP39 secrets are not displayed by default on this device. The side channel is relevant only if the attacker has enough control over the device's USB connection to make power-consumption measurements at a time when secret data is displayed. The side channel is not relevant in other circumstances, such as a stolen device that is not currently displaying secret data.	2019- r/bt yet calculated 02	CVE-2019-18673 MISC
sierra_wireless -- airlink_es450_fw	An exploitable unverified password change vulnerability exists in the ACEManager upload.cgi functionality of Sierra Wireless AirLink ES450 FW 4.9.3. A specially crafted HTTP request can cause a unverified device configuration change, resulting in an unverified change of the user password on the device. An attacker can make an authenticated HTTP request to trigger this vulnerability.	2019- r/bt yet calculated 31	CVE-2018-4064 MISC
smokeping -- smokeping	Cross-site scripting (XSS) vulnerability in SmokePing 2.6.9 in the start and end time fields.	2019- r/bt yet calculated 01	CVE-2013-4168 MISC MISC MISC MISC MISC MISC
sonatype -- nexus_repository_manager	There is an OS Command Injection in Nexus Repository Manager <= 2.14.14 (bypass CVE-2019-5475) that could allow an attacker a Remote Code Execution (RCE). All instances using CommandLineExecutor.java with user-supplied data is vulnerable, such as the Yum Configuration Capability.	2019- r/bt yet calculated 01	CVE-2019-15588 MISC CONFIRM
symantec -- sonar	The Symantec SONAR component, prior to 12.0.2, may be susceptible to a tamper protection bypass vulnerability which could potentially allow an attacker to circumvent the existing tamper protection in use on the resident system.	2019- r/bt yet calculated 01	CVE-2019-12752 CONFIRM
systemd -- systemd	systemd 239 through 243 accepts any certificate signed by a trusted certificate authority for DNS Over TLS. Server Name Indication (SNI) is not sent, and there is no hostname validation with the GnuTLS backend.	2019- r/bt yet calculated 30	CVE-2018-21029 MISC MISC MISC
technicolor -- td5130v2_devices	An issue was discovered in certain Oi third-party firmware that may be installed on Technicolor TD5130v2 devices. A Command Injection in the Ping module in the Web Interface in Oi_Fw_V20 allows remote attackers to execute arbitrary OS commands in the pingAddr parameter to mnt_ping.cgi. NOTE: This may overlap CVE-2017714127.	2019- r/bt yet calculated 31	CVE-2019-18396 MISC MISC
tightrope_media_systems -- carousel	The Tightrope Media Carousel Seneca HDn Windows-based appliance 7.0.4.104 is shipped with a default local administrator username and password. This can be found by a limited user account in an "unattend.xml" file left over on the C: drive from the Sysprep process. An attacker with this username and password can leverage it to gain administrator-level access on the system.	2019- r/bt yet calculated 29	CVE-2018-18929 MISC
tightrope_media_systems -- carousel	An issue was discovered in the Tightrope Media Carousel digital signage product 7.0.4.104. Due to insecure default permissions on the C:\TRMS\Services directory, an attacker who has gained access to the system can elevate their privileges from a restricted account to full SYSTEM by replacing the Carousel.Service.exe file with a custom malicious executable. This service is independent of the associated IIS web site, which means that this service can be manipulated by an attacker without losing access to vulnerabilities in the web interface (which would potentially be used in conjunction with this attack, to control the service). Once the attacker has replaced Carousel.Service.exe, the server can be restarted using the command "shutdown -r -t 0" from a web shell, causing the system to reboot and launching the malicious Carousel.Service.exe as SYSTEM on startup. If this malicious Carousel.Service.exe is configured to launch a reverse shell back to the attacker, then upon reboot the attacker will have a fully privileged remote command-line environment to manipulate the system further.	2019- r/bt yet calculated 29	CVE-2018-18931 MISC
tightrope_media_systems -- carousel	The Tightrope Media Carousel Seneca HDn Windows-based appliance 7.0.4.104 contains an arbitrary file upload vulnerability in the Manage Bulletins/Upload feature, which can be leveraged to gain remote code execution. An authenticated attacker can upload a crafted ZIP file (based on an exported backup of existing "Bulletins") containing a malicious file. When uploaded, the system only checks for the presence of the needed files within the ZIP and, as long as the malicious file is named properly, will extract all contained files to a new directory on the system, named with a random GUID. The attacker can determine this GUID by previewing an image from the uploaded Bulletin within the web UI. Once the GUID is determined, the attacker can navigate to the malicious file and execute it. In testing, an ASPX web shell was uploaded, allowing for remote-code execution in the context of a restricted IIS user.	2019- r/bt yet calculated 29	CVE-2018-18930 MISC
	A directory traversal vulnerability in Trend Micro Apex One, OfficeScan (11.0, XG) and Worry-		

trend_micro -- apex_one_and_officescan_and_worry-free_business_security	Free Business Security (9.5, 10.0) may allow an attacker to bypass authentication and log on to an affected product's management console as a root user. The vulnerability does not require authentication.	2019- rft yet calculated 28	<a href="#">CVE-2019-18189</a> N/A
turbovnc -- turbovnc	TurboVNC server code contains stack buffer overflow vulnerability in commit prior to cea98166008301e614e0d36776bf9435a536136e. This could possibly result into remote code execution, since stack frame is not protected with stack canary. This attack appear to be exploitable via network connectivity. To exploit this vulnerability authorization on server is required. These issues have been fixed in commit cea98166008301e614e0d36776bf9435a536136e.	2019- rft yet calculated 29	<a href="#">CVE-2019-15683</a> MISC
twiki -- twiki	TWiki allows arbitrary shell command execution via the Include function	2019- rft yet calculated 01	<a href="#">CVE-2005-3056</a> DEBIAN MISC CONFIRM
typo3 -- typo3	TYPO3 before 4.1.14, 4.2.x before 4.2.13, 4.3.x before 4.3.4 and 4.4.x before 4.4.1 allows Open Redirection on the backend.	2019- rft yet calculated 01	<a href="#">CVE-2010-3661</a> MISC MISC CONFIRM
typo3 -- typo3	TYPO3 before 4.1.14, 4.2.x before 4.2.13, 4.3.x before 4.3.4 and 4.4.x before 4.4.1 allows XSS on the backend.	2019- rft yet calculated 01	<a href="#">CVE-2010-3660</a> MISC MISC CONFIRM
vmware -- esxi_and_workstation_and_fusion	VMware ESXi (6.7 before ESXi670-201908101-SG and 6.5 before ESXi650-201910401-SG), Workstation (15.x before 15.5.0) and Fusion (11.x before 11.5.0) contain a denial-of-service vulnerability in the shader functionality. Successful exploitation of this issue may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion.	2019- rft yet calculated 28	<a href="#">CVE-2019-5536</a> MISC
vmware -- sd-wan	In VMware SD-WAN by VeloCloud versions 3.x prior to 3.3.0, the VeloCloud Orchestrator parameter authorization check mistakenly allows enterprise users to obtain information of Managed Service Provider accounts. Among the information is username, first and last name, phone numbers and e-mail address if present but no other personal data. VMware has evaluated the severity of this issue to be in the moderate severity range with a maximum CVSSv3 base score of 4.3.	2019- rft yet calculated 29	<a href="#">CVE-2019-5533</a> CONFIRM
vmware -- vcenter_server_appliance	Sensitive information disclosure vulnerability resulting from a lack of certificate validation during the File-Based Backup and Restore operations of VMware vCenter Server Appliance (6.7 before 6.7u3a and 6.5 before 6.5u3d) may allow a malicious actor to intercept sensitive data in transit over FTPS and HTTPS. A malicious actor with man-in-the-middle positioning between vCenter Server Appliance and a backup target may be able to intercept sensitive data in transit during File-Based Backup and Restore operations.	2019- rft yet calculated 28	<a href="#">CVE-2019-5537</a> MISC
vmware -- vcenter_server_appliance	Sensitive information disclosure vulnerability resulting from a lack of certificate validation during the File-Based Backup and Restore operations of VMware vCenter Server Appliance (6.7 before 6.7u3a and 6.5 before 6.5u3d) may allow a malicious actor to intercept sensitive data in transit over SCP. A malicious actor with man-in-the-middle positioning between vCenter Server Appliance and a backup target may be able to intercept sensitive data in transit during File-Based Backup and Restore operations.	2019- rft yet calculated 28	<a href="#">CVE-2019-5538</a> MISC
websieve -- websieve	Cross-site scripting (XSS) vulnerability in websieve v0.62 allows remote attackers to inject arbitrary web script or HTML code in the web user interface.	2019- rft yet calculated 01	<a href="#">CVE-2005-2350</a> MISC MISC
wordpress -- wordpress	plugin-fw/lib/yit-plugin-panel-wc.php in the YIT Plugin Framework through 3.3.8 for WordPress allows authenticated options changes.	2019- rft yet calculated 31	<a href="#">CVE-2019-16251</a> MISC MISC
wordpress -- wordpress	An issue was discovered in the Currency Switcher addon before 2.11.2 for WooCommerce if a user provides a currency that was not added by the administrator. In this case, even though the currency does not exist, it will be selected, but a price amount will fall back to the default currency. This means that if an attacker provides a currency that does not exist and is worth less than this default, the attacker can eventually purchase an item for a significantly cheaper price.	2019- rft yet calculated 02	<a href="#">CVE-2019-18668</a> MISC MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing 32-bit PV guest OS users to gain guest OS privileges by installing and using descriptors. There is missing descriptor table limit checking in x86 PV emulation. When emulating certain PV guest operations, descriptor table accesses are performed by the emulating code. Such accesses should respect the guest specified limits, unless otherwise guaranteed to fail in such a case. Without this, emulation of 32-bit guest user mode calls through call gates would allow guest user mode to install and then use descriptors of their choice, as long as the guest kernel did not itself install an LDT. (Most OSes don't install any LDT by default). 32-bit PV guest user mode can elevate its privileges to that of the guest kernel. Xen versions from at least 3.2 onwards are affected. Only 32-bit PV guest user mode can leverage this vulnerability. HVM, PVH, as well as 64-bit PV guests cannot leverage this vulnerability. Arm systems are unaffected.	2019- rft yet calculated 31	<a href="#">CVE-2019-18425</a> MLIST MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing ARM guest OS users to cause a denial of service via a XENMEM_add_to_physmap hypercall. p2m->max_mapped_gfn is used by the functions p2m_resolve_translation_fault() and p2m_get_entry() to sanity check guest physical frame. The rest of the code in the two functions will assume that there is a valid root table and check that with BUG_ON(). The function p2m_get_root_pointer() will ignore the unused top bits of a guest physical frame. This means that the function p2m_set_entry() will alias the frame. However, p2m->max_mapped_gfn will be updated using the original frame. It would be possible to set p2m->max_mapped_gfn high enough to cover a frame that would lead p2m_get_root_pointer() to return NULL in p2m_get_entry() and p2m_resolve_translation_fault(). Additionally, the sanity check on p2m->max_mapped_gfn is off-by-one allowing "highest mapped + 1" to be considered valid. However, p2m_get_root_pointer() will return NULL. The problem could be triggered with a specially crafted hypercall XENMEM_add_to_physmap{,_batch} followed by an access to an address (via hypercall or direct access) that passes the sanity check but cause p2m_get_root_pointer() to return NULL. A malicious guest administrator may cause a hypervisor crash, resulting in a Denial of Service (DoS). Xen version 4.8 and newer are vulnerable. Only Arm systems are vulnerable. x86 systems are not affected.	2019- rft yet calculated 31	<a href="#">CVE-2019-18423</a> MLIST MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing ARM guest OS users to cause a denial of service or gain privileges by leveraging the erroneous enabling of interrupts. Interrupts are unconditionally unmasked in exception handlers. When an exception occurs on an ARM system which is handled without changing processor level, some interrupts are unconditionally enabled during exception entry. So exceptions which occur when interrupts are masked will effectively unmask the interrupts. A malicious guest might contrive to arrange for critical Xen code to run with interrupts erroneously enabled. This could lead to data corruption, denial of service, or possibly even privilege escalation. However a precise attack technique has not been identified.	2019- rft yet calculated 31	<a href="#">CVE-2019-18422</a> MLIST MISC
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing attackers to gain host OS privileges via DMA in a situation where an untrusted domain has access to a physical device. This occurs because passed through PCI devices may corrupt host memory after deassignment. When a PCI device is assigned to an untrusted domain, it is possible for that domain to program the device to DMA to an arbitrary address. The IOMMU is used to protect the host from malicious DMA by making sure that the device addresses can only target memory assigned to the guest. However, when the guest domain is torn down, or the device is deassigned, the device is assigned back to dom0, thus allowing any in-flight DMA to potentially target critical host data. An untrusted domain with access to a physical device can DMA into host memory, leading to privilege escalation. Only systems where guests are given direct access to physical devices capable of DMA (PCI pass-through) are vulnerable. Systems which do not use PCI pass-through are not vulnerable.	2019- rft yet calculated 31	<a href="#">CVE-2019-18424</a> MLIST MISC



xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing x86 PV guest OS users to cause a denial of service via a VCPUOP. Initialise hypercall, hypercall_create_continuation() is a variadic function which uses a printf-like format string to interpret its parameters. Error handling for a bad format character was done using BUG(), which crashes Xen. One path, via the VCPUOP_initialise hypercall, has a bad format character. The BUG() can be hit if VCPUOP_initialise executes for a sufficiently long period of time for a continuation to be created. Malicious guests may cause a hypervisor crash, resulting in a Denial of Service (DoS). Xen versions 4.6 and newer are vulnerable. Xen versions 4.5 and earlier are not vulnerable. Only x86 PV guests can exploit the vulnerability. HVM and PVH guests, and guests on ARM systems, cannot exploit the vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-18420</a> <a href="#">MLIST</a> <a href="#">MISC</a>
xen_project -- xen	An issue was discovered in Xen through 4.12.x allowing x86 PV guest OS users to gain host OS privileges by leveraging race conditions in pagetable promotion and demotion operations. There are issues with restartable PV type change operations. To avoid using shadow pagetables for PV guests, Xen exposes the actual hardware pagetables to the guest. In order to prevent the guest from modifying these page tables directly, Xen keeps track of how pages are used using a type system; pages must be "promoted" before being used as a pagetable, and "demoted" before being used for any other type. Xen also allows for "recursive" promotions: i.e., an operating system promoting a page to an L4 pagetable may end up causing pages to be promoted to L3s, which may in turn cause pages to be promoted to L2s, and so on. These operations may take an arbitrarily large amount of time, and so must be re-startable. Unfortunately, making recursive pagetable promotion and demotion operations restartable is incredibly complicated, and the code contains several races which, if triggered, can cause Xen to drop or retain extra type counts, potentially allowing guests to get write access to in-use pagetables. A malicious PV guest administrator may be able to escalate their privilege to that of the host. All x86 systems with untrusted PV guests are vulnerable. HVM and PVH guests cannot exercise this vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-18421</a> <a href="#">MLIST</a> <a href="#">MISC</a>
yandex -- clickhouse	ClickHouse before 19.13.5.44 allows HTTP header injection via the url table function.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-18657</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
youthtube -- youthtube	An issue was discovered in YouTube through 7.7. User input passed through the live_stream_code POST parameter to /plugin/LiveChat/getChat.json.php is not properly sanitized (in getFromChat in plugin/LiveChat/Objects/LiveChatObj.php) before being used to construct a SQL query. This can be exploited by malicious users to, e.g., read sensitive data from the database through in-band SQL Injection attacks. Successful exploitation of this vulnerability requires the Live Chat plugin to be enabled.	2019- r0bt yet calculated 02	<a href="#">CVE-2019-18662</a> <a href="#">MISC</a>
youthtube -- youthtube	An exploitable SQL injection vulnerability exist in YouTube 7.7. A specially crafted unauthenticated HTTP request can cause a SQL injection, possibly leading to denial of service, exfiltration of the database and local file inclusion, which could potentially further lead to code execution. An attacker can send an HTTP request to trigger this vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-5151</a> <a href="#">MISC</a>
youthtube -- youthtube	An exploitable SQL injection vulnerability exist in YouTube 7.7. When the "VideoTags" plugin is enabled, a specially crafted unauthenticated HTTP request can cause a SQL injection, possibly leading to denial of service, exfiltration of the database and local file inclusion, which could potentially further lead to code execution. An attacker can send an HTTP request to trigger this vulnerability.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-5150</a> <a href="#">MISC</a>
yum -- yum	yum does not properly handle bad metadata, which allows an attacker to cause a denial of service and possibly have other unspecified impact via a Trojan horse file in the metadata of a remote repository.	2019- r0bt yet calculated 31	<a href="#">CVE-2013-1910</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zte -- zx297520v3	The 7520V3V1.0.0B09P27 version, and all earlier versions of ZTE product ZX297520V3 are impacted by a Command Injection vulnerability. Unauthorized users can exploit this vulnerability to control the user terminal system.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-3421</a> <a href="#">CONFIRM</a>
zte -- zxmp	A security vulnerability exists in a management port in the version of ZTE's ZXMP M721V3.10P01B10. M2NCP. An attacker could exploit this vulnerability to build a link to the device and send specific packets to cause a denial of service.	2019- r0bt yet calculated 31	<a href="#">CVE-2019-3419</a> <a href="#">CONFIRM</a>
zuchetti -- infobusiness	In Zuchetti InfoBusiness before and including 4.4.1, an authenticated user can inject client-side code due to improper validation of the Title field in the InfoBusiness Web Component. The payload will be triggered every time a user browses the reports page.	2019- r0bt yet calculated 30	<a href="#">CVE-2019-18207</a> <a href="#">MISC</a>
zuchetti -- infobusiness	A cross-site request forgery (CSRF) vulnerability in Zuchetti InfoBusiness before and including 4.4.1 allows arbitrary file upload.	2019- r0bt yet calculated 30	<a href="#">CVE-2019-18206</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nasa.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)



**From:** [US-CERT](#)  
**To:** [tmcinnis@sunnyvale.ca.gov](mailto:tmcinnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of October 7, 2019  
**Date:** Tuesday, October 15, 2019 12:46:28 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of October 7, 2019](#)

10/14/2019 06:33 AM EDT

Original release date: October 14, 2019 | Last revised: October 15, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adhouma_cms_project -- adhouma_cms	Adhouma CMS through 2019-10-09 has SQL Injection via the post.php p_id parameter.	2019-10-10	<a href="#">7.5</a>	<a href="#">CVE-2019-17429</a> <a href="#">MISC</a>
awplife -- contact_form_widget	The new-contact-form-widget (aka Contact Form Widget - Contact Query, Form Maker) plugin 1.0.9 for WordPress has SQL Injection via all-query-page.php.	2019-10-10	<a href="#">7.5</a>	<a href="#">CVE-2019-17072</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_vm	In Centreon VM through 19.04.3, centreon-backup.pl allows attackers to become root via a crafted script, due to incorrect rights of sourced configuration files.	2019-10-08	<a href="#">10.0</a>	<a href="#">CVE-2018-21025</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML Jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.	2019-10-06	<a href="#">7.5</a>	<a href="#">CVE-2019-17267</a> <a href="#">MISC</a> <a href="#">MISC</a>
fon -- fon2601e-fsw-b_firmware	FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.	2019-10-04	<a href="#">7.8</a>	<a href="#">CVE-2019-6015</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- libsoup	libsoup from versions 2.65.1 until 2.68.1 have a heap-based buffer over-read because soup_ntlm_parse_challenge() in soup-auth-ntlm.c does not properly check an NTLM message's length before proceeding with a memcpy.	2019-10-06	<a href="#">7.5</a>	<a href="#">CVE-2019-17266</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a>
ibm -- mq	IBM MQ 8.0.0.4 - 8.0.0.12, 9.0.0.0 - 9.0.0.6, 9.1.0.0 - 9.1.0.2, and 9.1.0 - 9.1.2 AMQP Listeners could allow an unauthorized user to conduct a session fixation attack due to clients not being disconnected as they should. IBM X-Force ID: 159352.	2019-10-04	<a href="#">7.5</a>	<a href="#">CVE-2019-4227</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_scale	A security vulnerability has been identified in all levels of IBM Spectrum Scale V5.0.0.0 through V5.0.3.2 and IBM Spectrum Scale V4.2.0.0 through V4.2.3.17 that could allow a local attacker to obtain root privilege by injecting parameters into setuid files.	2019-10-09	<a href="#">7.2</a>	<a href="#">CVE-2019-4558</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intelliantech -- remote_access	Intellian Remote Access 3.18 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the Ping Test field.	2019-10-06	<a href="#">10.0</a>	<a href="#">CVE-2019-17269</a> <a href="#">MISC</a>
k-78 -- broken_link_manager	The broken-link-manager plugin before 0.5.0 for WordPress has wpslDelURL or wpslEditURL SQL injection via the url parameter.	2019-10-10	<a href="#">7.5</a>	<a href="#">CVE-2015-9467</a> <a href="#">MISC</a> <a href="#">MISC</a>

				MISC
linux -- linux_kernel	In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow.	2019-10-04	7.5	<a href="#">CVE-2019-17133</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.	2019-10-10	7.6	<a href="#">CVE-2019-1307</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366.	2019-10-10	7.6	<a href="#">CVE-2019-1308</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.	2019-10-10	7.6	<a href="#">CVE-2019-1335</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.	2019-10-10	7.6	<a href="#">CVE-2019-1366</a> MISC
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1331.	2019-10-10	9.3	<a href="#">CVE-2019-1327</a> MISC
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327.	2019-10-10	9.3	<a href="#">CVE-2019-1331</a> MISC
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.	2019-10-10	7.1	<a href="#">CVE-2019-1238</a> MISC
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1238.	2019-10-10	7.6	<a href="#">CVE-2019-1239</a> MISC
microsoft -- windows_10	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.	2019-10-10	9.3	<a href="#">CVE-2019-1060</a> MISC
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.	2019-10-10	9.3	<a href="#">CVE-2019-1311</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.	2019-10-10	7.2	<a href="#">CVE-2019-1315</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.	2019-10-10	7.2	<a href="#">CVE-2019-1316</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.	2019-10-10	7.2	<a href="#">CVE-2019-1319</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336.	2019-10-10	7.2	<a href="#">CVE-2019-1323</a> MISC
microsoft -- windows_10	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	2019-10-10	7.8	<a href="#">CVE-2019-1326</a> MISC
microsoft -- windows_10	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.	2019-10-10	9.3	<a href="#">CVE-2019-1333</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.	2019-10-10	7.2	<a href="#">CVE-2019-1336</a> MISC
nex-forms - _ultimate_form_builder_project -- nex-forms -_ultimate_form_builder	The nex-forms-express-wp-form-builder plugin before 4.6.1 for WordPress has SQL injection via the wp-admin/admin.php?page=nex-forms-main nex_forms_id parameter.	2019-10-07	7.5	<a href="#">CVE-2015-9452</a> MISC MISC MISC
	OpenEMR through 5.0.2 has SQL Injection in the Lifestyle			<a href="#">CVE-2019-17197</a>

open-emr -- openemr	demographic filter criteria in library/clinical_rules.php that affects library/patient.inc.	2019-10-05	7.5	MISC MISC
pcprotect -- antivirus	PC Protect Antivirus v4.14.31 installs by default to %PROGRAMFILES(X86)%\PCProtect with very weak folder permissions, granting any user full permission "Everyone: (F)" to the contents of the directory and its subfolders. In addition, the program installs a service called SecurityService that runs as LocalSystem. This allows any user to escalate privileges to "NT AUTHORITY\SYSTEM" by substituting the service's binary with a Trojan horse.	2019-10-07	7.2	CVE-2019-16913 MISC
signal -- signal_private_messenger	** DISPUTED ** The WebRTC component in the Signal Private Messenger application through 4.47.7 for Android processes videoconferencing RTP packets before a callee chooses to answer a call, which might make it easier for remote attackers to cause a denial of service or possibly have unspecified other impact via malformed packets. NOTE: the vendor plans to continue this behavior for performance reasons unless a WebRTC design change occurs.	2019-10-04	7.5	CVE-2019-17192 MISC MISC MISC
sitos -- sitos_six	SITOS six Build v6.2.1 allows an attacker to inject arbitrary PHP commands. As a result, an attacker can compromise the running server and execute system commands in the context of the web user.	2019-10-07	10.0	CVE-2019-15746 MISC
sitos -- sitos_six	SITOS six Build v6.2.1 permits unauthorised users to upload and import a SCORM 2004 package by browsing directly to affected pages. An unauthenticated attacker could use the upload and import functionality to import a malicious SCORM package that includes a PHP file, which could execute arbitrary PHP code.	2019-10-07	7.5	CVE-2019-15748 MISC
sitos -- sitos_six	An unrestricted file upload vulnerability in SITOS six Build v6.2.1 allows remote attackers to execute arbitrary code by uploading a SCORM file with an executable extension. This allows an unauthenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to the web root of the application.	2019-10-07	10.0	CVE-2019-15751 MISC
sizmic -- plugmatter_optin_feature_box	The plugmatter-optin-feature-box-lite plugin before 2.0.14 for WordPress has SQL injection via the wp-admin/admin-ajax.php? action=pmfb_cc pmfb_tid parameter.	2019-10-07	7.5	CVE-2015-9450 MISC MISC MISC
sizmic -- plugmatter_optin_feature_box	The plugmatter-optin-feature-box-lite plugin before 2.0.14 for WordPress has SQL injection via the wp-admin/admin-ajax.php? action=pmfb_mailchimp pmfb_tid parameter.	2019-10-07	7.5	CVE-2015-9451 MISC MISC MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because of an incompatibility between Process Context Identifiers (PCID) and TLB flushes.	2019-10-07	7.2	CVE-2019-17346 MISC
xerox -- atlatlink_firmware	Xerox AtlaLink B8045/B8055/B8065/B8075/B8090 C8030/C8035/C8045/C8055/C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.	2019-10-04	7.5	CVE-2019-17184 MISC
zingbox -- inspector	A command injection vulnerability exists in the Zingbox Inspector versions 1.286 and earlier, that allows for an authenticated user to execute arbitrary system commands in the CLI.	2019-10-09	9.0	CVE-2019-15014 MISC
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector.	2019-10-09	7.5	CVE-2019-15019 MISC
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.293 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector that could result in command injection.	2019-10-09	7.5	CVE-2019-15020 MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- hadoop	In Apache Hadoop 3.1.0 to 3.1.1, 3.0.0-alpha1 to 3.0.3, 2.9.0 to 2.9.1, and 2.0.0-alpha to 2.8.4, the user/group information can be corrupted across storing in fsimage and reading back from fsimage.	2019-10-04	5.0	CVE-2018-11768 MISC MLIST MLIST MLIST MLIST
axiosys -- bento4	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListInspector::Action in Core/AP4Descriptor.h.	2019-10-	4.3	CVE-2019-17452

	related to AP4_IodsAtom::InspectFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4dump.	10		<a href="#">MISC</a>
axiosys -- bento4	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListWriter::Action in Core/Ap4Descriptor.h, related to AP4_IodsAtom::WriteFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4encrypt or mp4compact.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-17453</a> <a href="#">MISC</a> <a href="#">MISC</a>
axiosys -- bento4	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_Descriptor::GetTag in Core/Ap4Descriptor.h, related to AP4_StsdAtom::GetSampleDescription in Core/Ap4StsdAtom.cpp, as demonstrated by mp4info.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-17454</a> <a href="#">MISC</a>
bludit -- bludit	bl-kernel/security.class.php in Bludit 3.9.2 allows attackers to bypass a brute-force protection mechanism by using many different forged X-Forwarded-For or Client-IP HTTP headers.	2019-10-06	<a href="#">4.3</a>	<a href="#">CVE-2019-17240</a> <a href="#">MISC</a> <a href="#">MISC</a>
brinidesigner -- awesome_filterable_portfolio	The awesome-filterable-portfolio plugin before 1.9 for WordPress has afp_get_new_portfolio_item_page SQL injection via the item_id parameter.	2019-10-10	<a href="#">6.5</a>	<a href="#">CVE-2019-9461</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_vm	In Centreon VM through 19.04.3, the cookie configuration within the Apache HTTP Server does not protect against theft because the HTTPOnly flag is not set.	2019-10-08	<a href="#">5.0</a>	<a href="#">CVE-2019-17104</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	In Centreon Web through 2.8.29, disclosure of external components' passwords allows authenticated attackers to move laterally to external components.	2019-10-08	<a href="#">4.0</a>	<a href="#">CVE-2019-17106</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows API token credentials to persist after an account has been renamed or terminated (SEC-517).	2019-10-09	<a href="#">6.5</a>	<a href="#">CVE-2019-17375</a> <a href="#">MISC</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in the SSL Certificate Upload interface (SEC-521).	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17376</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in LiveAPI example scripts (SEC-524).	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17377</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in the SSL Key Delete interface (SEC-526).	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17378</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self stored XSS in the WHM SSL Storage Manager interface (SEC-527).	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17379</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in the WHM Update Preferences interface (SEC-528).	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17380</a> <a href="#">MISC</a>
elementor -- elementor	The elementor-edit-template class in wp-admin/customize.php in the Elementor Pro plugin before 2.0.10 for WordPress has XSS.	2019-10-07	<a href="#">4.3</a>	<a href="#">CVE-2018-18379</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
eleopard -- animate_it!	The animate-it plugin before 2.3.4 for WordPress has XSS.	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17384</a> <a href="#">MISC</a> <a href="#">MISC</a>
eleopard -- animate_it!	The animate-it plugin before 2.3.5 for WordPress has XSS.	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17385</a> <a href="#">MISC</a> <a href="#">MISC</a>
etoilewebdesign -- ultimate_fa	Functions/EWD_UFAQ_Import.php in the ultimate-faqs plugin through 1.8.24 for WordPress allows unauthenticated options import.	2019-10-07	<a href="#">5.0</a>	<a href="#">CVE-2019-17232</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
etoilewebdesign -- ultimate_fa	Functions/EWD_UFAQ_Import.php in the ultimate-faqs plugin through 1.8.24 for WordPress allows HTML content injection.	2019-10-07	<a href="#">4.3</a>	<a href="#">CVE-2019-17233</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Exiv2 0.27.2 allows attackers to trigger a crash in Exiv2::getULong in types.cpp when called from	2019-10-		<a href="#">CVE-2019-</a>



exiv2 -- exiv2	Exiv2::Internal::CiffDirectory::readDirectory in crwimage_int.cpp, because there is no validation of the relationship of the total size to the offset and size.	09	4.3	<a href="#">17402 MISC</a>
eyoucms -- eyoucms	EyouCms through 2019-07-11 has XSS related to the login.php web_recordnum parameter.	2019-10-10	4.3	<a href="#">CVE-2019-17430 MISC MISC</a>
fastadmin -- fastadmin	An issue was discovered in fastadmin 1.0.0.20190705_beta. There is a public/index.php/admin/auth/admin/add CSRF vulnerability.	2019-10-10	6.8	<a href="#">CVE-2019-17431 MISC</a>
fecmall -- fecmall	An unrestricted file upload vulnerability was discovered in catalog/productinfo/imageupload in Fecshop FecMall 2.3.4. An attacker can bypass a front-end restriction and upload PHP code to the webserver, by providing image data and the image/jpeg content type, with a .php extension. This occurs because the code relies on the getimagesize function.	2019-10-04	6.5	<a href="#">CVE-2019-17188 MISC</a>
fiberhome -- hg2201t_firmware	/var/WEB-GUI/cgi-bin/downloadfile.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows pre-authentication Directory Traversal for reading arbitrary files.	2019-10-08	5.0	<a href="#">CVE-2019-17187 MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.	2019-10-04	6.8	<a href="#">CVE-2019-13315 MISC MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8757.	2019-10-04	6.8	<a href="#">CVE-2019-13316 MISC MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759.	2019-10-04	6.8	<a href="#">CVE-2019-13317 MISC MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of the util.printf Javascript method. The application processes the %p parameter in the format string, allowing heap addresses to be returned to the script. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8544.	2019-10-04	4.3	<a href="#">CVE-2019-13318 MISC MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.	2019-10-04	6.8	<a href="#">CVE-2019-13319 MISC MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8814.	2019-10-04	6.8	<a href="#">CVE-2019-13320 MISC MISC</a>

foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the deleteItemAt method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295.	2019-10-04	6.8	<a href="#">CVE-2019-6774</a> MISC MISC
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.	2019-10-04	6.8	<a href="#">CVE-2019-6775</a> MISC MISC
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing watermarks within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8801.	2019-10-04	6.8	<a href="#">CVE-2019-6776</a> MISC MISC
foxitsoftware -- reader	Foxit Reader before 9.7 allows an Access Violation and crash if insufficient memory exists.	2019-10-04	5.0	<a href="#">CVE-2019-17183</a> MISC
freerdp -- freerdp	libfreerdp/codec/region.c in FreeRDP through 1.1.x and 2.x through 2.0.0-rc4 has memory leaks because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.	2019-10-04	5.0	<a href="#">CVE-2019-17177</a> MISC MISC
freerdp -- freerdp	HuffmanTree_makeFromFrequencies in lodepng.c in LodePNG through 2019-09-28, as used in WinPR in FreeRDP and other products, has a memory leak because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.	2019-10-04	5.0	<a href="#">CVE-2019-17178</a> MISC MISC
gonitro -- nitropdf	A specifically crafted jpeg2000 file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5045</a> MISC
gonitro -- nitropdf	A specifically crafted jpeg2000 file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5046</a> MISC
gonitro -- nitropdf	An exploitable Use After Free vulnerability exists in the CharProcs parsing functionality of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a Use After Free. An attacker can craft a malicious PDF to trigger this vulnerability.	2019-10-09	6.8	<a href="#">CVE-2019-5047</a> MISC
gonitro -- nitropdf	A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5048</a> MISC
gonitro -- nitropdf	A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5050</a> MISC
gonitro -- nitropdf	An exploitable use-after-free vulnerability exists in the Length parsing function of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a use-after-free condition. An attacker can craft a malicious PDF to trigger this vulnerability.	2019-10-09	6.8	<a href="#">CVE-2019-5053</a> MISC
	Unrestricted file upload vulnerability in Micro Focus ArcSight	2019-10-		<a href="#">CVE-2019-</a>

hp -- arcsight_logger	Logger, version 6.7.0 and later. This vulnerability could allow Unrestricted Upload of File with Dangerous type.	04	<a href="#">6.5</a>	<a href="#">11655</a> <a href="#">MISC</a>
ibm -- control_desk	IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be used in further attacks against the system. IBM X-Force ID: 164554.	2019-10-09	<a href="#">4.0</a>	<a href="#">CVE-2019-4512</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_key_lifecycle_manager	IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 165136.	2019-10-04	<a href="#">5.0</a>	<a href="#">CVE-2019-4514</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_key_lifecycle_manager	IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2019-10-04	<a href="#">4.3</a>	<a href="#">CVE-2019-4564</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000d563.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17241</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000966f.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17242</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control Code Flow starting at JPEG_LS+0x0000000000003155.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17243</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control Code Flow starting at JPEG_LS+0x0000000000001d8a.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17244</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x0000000000004359.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17245</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000258c.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17246</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at JPEG_LS+0x00000000000007da8.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17247</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x00000000000025b6.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17248</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000d57b.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17249</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x00000000000042f5.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17250</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!GetPlugInInfo+0x0000000000007d43.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17251</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!Read_BadPNG+0x000000000000115.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17252</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at JPEG_LS+0x000000000000a6b8.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17253</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at FORMATS!Read_BadPNG+0x0000000000000101.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17254</a> <a href="#">MISC</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at EXR!ReadEXR+0x00000000000010836.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17255</a> <a href="#">MISC</a> <a href="#">MISC</a>

				MISC
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at DPX!ReadDPX_W+0x0000000000001203.	2019-10-08	6.8	<a href="#">CVE-2019-17256</a> MISC
irfanview -- irfanview	IrfanView 4.53 allows a Exception Handler Chain to be Corrupted starting at EXR!ReadEXR+0x000000000002af80.	2019-10-08	4.3	<a href="#">CVE-2019-17257</a> MISC
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at JPEG_LS+0x000000000000839c.	2019-10-08	6.8	<a href="#">CVE-2019-17258</a> MISC
jnoj -- jiangnan_online_judge	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[title] parameter to web/polygon/problem/create or web/polygon/problem/update or web/admin/problem/create.	2019-10-10	4.3	<a href="#">CVE-2019-17489</a> MISC
jnoj -- jiangnan_online_judge	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[description] parameter to web/admin/problem/create or web/polygon/problem/update.	2019-10-10	4.3	<a href="#">CVE-2019-17491</a> MISC
jnoj -- jiangnan_online_judge	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[sample_input] parameter to web/admin/problem/create or web/polygon/problem/update.	2019-10-10	4.3	<a href="#">CVE-2019-17493</a> MISC
joyplus-cms_project -- joyplus-cms	joyplus-cms 1.6.0 allows manager/admin_pic.php?rootpa h= absolute path traversal.	2019-10-04	5.0	<a href="#">CVE-2019-17175</a> MISC
k-78 -- broken_link_manager	The broken-link-manager plugin before 0.6.0 for WordPress has XSS via the HTTP Referer or User-Agent header to a URL hat does not exist.	2019-10-07	4.3	<a href="#">CVE-2015-9453</a> MISC
k-78 -- broken_link_manager	The broken-link-manager plugin 0.4.5 for WordPress has XSS via the page parameter in a delURL action.	2019-10-10	4.3	<a href="#">CVE-2015-9468</a> MISC
kmplayer -- kmplayer	KMPlayer 4.2.2.31 allows a User Mode Write AV starting at utils!src_new+0x000000000014d6ee.	2019-10-08	4.6	<a href="#">CVE-2019-17259</a> MISC
koji_project -- koji	Koji through 1.18.0 allows remote Directory Traversal, with resultant Privilege Escalation.	2019-10-09	4.0	<a href="#">CVE-2019-17109</a> MISC CONFIRM
liblnk_project -- liblnk	** DISPUTED ** In libyal liblnk before 20191006, liblnk_location_information_read_data in liblnk_location_information.c has a heap-based buffer over-read because an incorrect variable name is used for a certain offset. NOTE: the vendor has disputed this as described in the GitHub issue.	2019-10-06	6.8	<a href="#">CVE-2019-17264</a> MISC
libpng -- libpng	libpng 1.6.37 has memory leaks in png_malloc_warn and png_create_info_struct.	2019-10-09	4.3	<a href="#">CVE-2019-17371</a> MISC
liferay -- liferay_portal	Liferay Portal CE 6.2.5 allows remote command execution because of deserialization of a JSON payload.	2019-10-04	6.5	<a href="#">CVE-2019-16891</a> MISC
linux -- linux_kernel	An issue was discovered in drivers/xen/balloon.c in the Linux kernel before 5.2.3, as used in Xen through 4.12.x, allowing guest OS users to cause a denial of service because of unrestricted resource consumption during the mapping of guest memory, aka CID-6ef36ab967c7.	2019-10-07	4.9	<a href="#">CVE-2019-17351</a> MISC
lqd -- liquid_speech_balloon	The liquid-speech-balloon (aka LIQUID SPEECH BALLOON) plugin 1.0.5 for WordPress allows XSS with Internet Explorer.	2019-10-10	4.3	<a href="#">CVE-2019-17070</a> MISC
metinfo -- metinfo	An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=language&c=language_general&a=doSearchParameter appno parameter, a different issue than CVE-2019-16997.	2019-10-09	6.5	<a href="#">CVE-2019-17418</a> MISC
metinfo -- metinfo	An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=user&c=admin_user&a=doGetUserInfo id parameter.	2019-10-09	6.5	<a href="#">CVE-2019-17419</a> MISC
	A spoofing vulnerability exists when Microsoft Browsers does			<a href="#">CVE-2019-</a>

microsoft -- edge	not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.	2019-10-10	<a href="#">4.3</a>	<a href="#">0608 MISC</a>
microsoft -- edge	A spoofing vulnerability exists when Microsoft Browsers improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-1357 MISC</a>
microsoft -- open_enclave_software_development_kit	An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory, aka 'Open Enclave SDK Information Disclosure Vulnerability'.	2019-10-10	<a href="#">5.0</a>	<a href="#">CVE-2019-1369 MISC</a>
microsoft -- sharepoint_enterprise_server	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1329.	2019-10-10	<a href="#">4.0</a>	<a href="#">CVE-2019-1330 MISC</a>
microsoft -- sql_server_management_studio	An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1376.	2019-10-10	<a href="#">4.0</a>	<a href="#">CVE-2019-1313 MISC</a>
microsoft -- sql_server_management_studio	An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1313.	2019-10-10	<a href="#">4.0</a>	<a href="#">CVE-2019-1376 MISC</a>
microsoft -- windows_10	A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.	2019-10-10	<a href="#">5.6</a>	<a href="#">CVE-2019-1317 MISC</a>
microsoft -- windows_10	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-1318 MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340.	2019-10-10	<a href="#">4.6</a>	<a href="#">CVE-2019-1320 MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340.	2019-10-10	<a href="#">4.6</a>	<a href="#">CVE-2019-1322 MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.	2019-10-10	<a href="#">4.9</a>	<a href="#">CVE-2019-1325 MISC</a>
microsoft -- windows_7	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-1361 MISC MISC</a>
mpc-hc -- mpc-hc	MPC-HC through 1.7.13 allows a Read Access Violation on a Block Data Move starting at mpc_hc!memcpy+0x000000000000004e.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17260 MISC MISC</a>
netreo -- omniscanner	Netreo OmniCenter through 12.1.1 allows unauthenticated SQL Injection (Boolean Based Blind) in the redirect parameters and parameter name of the login page through a GET request. The injection allows an attacker to read sensitive information from the database used by the application.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-17128 MISC MISC</a>
nixos -- nix	Nix through 2.3 allows local users to gain access to an arbitrary user's account because the parent directory of the user-profile directories is world writable.	2019-10-09	<a href="#">4.6</a>	<a href="#">CVE-2019-17365 MISC MLIST</a>
open-emr -- openemr	XSS in library/custom_template/add_template.php in OpenEMR through 5.0.2 allows a malicious user to execute code in the context of a victim's browser via a crafted list_id query parameter.	2019-10-04	<a href="#">4.3</a>	<a href="#">CVE-2019-17179 MISC</a>
openproject -- openproject	An XSS vulnerability in project list in OpenProject before 9.0.4 and 10.x before 10.0.2 allows remote attackers to inject arbitrary web script or HTML via the sortBy parameter because error messages are mishandled.	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17092 MISC CONFIRM CONFIRM</a>
orbisius -- child_theme_creator	The orbisius-child-theme-creator plugin before 1.2.8 for WordPress has incorrect access control for file modification via the wp-admin/admin-ajax.php?	2019-10-	<a href="#">4.0</a>	<a href="#">CVE-2015-9456 MISC</a>



	action=orbisius_ctc_theme_editor_ajax&sub_cmd=save_file theme_1, theme_1_file, or theme_1_file_contents parameter.	07		<a href="#">MISC</a> <a href="#">CONFIRM</a>
otcms -- otcms	OTCMS v3.85 allows arbitrary PHP Code Execution because admin/sysCheckFile_deal.php blocks "into outfile" in a SELECT statement, but does not block the "into/**/outfile" manipulation. Therefore, the attacker can create a .php file.	2019-10-09	<a href="#">6.5</a>	<a href="#">CVE-2019-17370</a> <a href="#">MISC</a>
pi-hole -- pi-hole	Pi-Hole 4.3 allows Command Injection.	2019-10-09	<a href="#">6.8</a>	<a href="#">CVE-2019-13051</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
python -- pillow	An issue was discovered in Pillow before 6.2.0. When reading specially crafted invalid image files, the library can either allocate very large amounts of memory or take an extremely long period of time to process the image.	2019-10-04	<a href="#">4.3</a>	<a href="#">CVE-2019-16865</a> <a href="#">MISC</a>
realbigplugins -- client_dash	The client-dash (aka Client Dash) plugin 2.1.4 for WordPress allows XSS.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-17071</a> <a href="#">MISC</a> <a href="#">MISC</a>
redmine -- redmine	In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors.	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17427</a> <a href="#">MISC</a>
s-cms -- s-cms	S-CMS v1.5 has XSS in tpl.php via the member/member_login.php from parameter.	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17368</a> <a href="#">MISC</a>
sap -- financial_consolidation	Due to missing input validation, SAP Financial Consolidation, before versions 10.0 and 10.1, enables an attacker to use crafted input to interfere with the structure of the surrounding query leading to XPath Injection.	2019-10-08	<a href="#">6.4</a>	<a href="#">CVE-2019-0370</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- netweaver_process_integration	SAP NetWeaver Process Integration (B2B Toolkit), before versions 1.0 and 2.0, does not perform necessary authorization checks for an authenticated user, allowing the import of B2B table content that leads to Missing Authorization Check.	2019-10-08	<a href="#">4.0</a>	<a href="#">CVE-2019-0367</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
seo_searchterms_tagging_2_project -- seo_searchterms_tagging_2	The searchterms-tagging-2 plugin through 1.535 for WordPress has SQL injection via the pk_stt2_db_get_popular_terms count parameter exploitable via CSRF.	2019-10-10	<a href="#">6.5</a>	<a href="#">CVE-2015-9458</a> <a href="#">MISC</a> <a href="#">MISC</a>
seo_searchterms_tagging_2_project -- seo_searchterms_tagging_2	The searchterms-tagging-2 plugin through 1.535 for WordPress has XSS via the wp-admin/options-general.php count parameter.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2015-9459</a> <a href="#">MISC</a> <a href="#">MISC</a>
sitos -- sitos_six	SITOS six Build v6.2.1 allows a user with the user role of Seminar Coordinator to escalate their permission to the Systemadministrator role due to insufficient checks on the server side.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-15747</a> <a href="#">MISC</a>
sitos -- sitos_six	SITOS six Build v6.2.1 allows a user to change their password and recovery email address without requiring them to confirm the change with their old password. This would allow an attacker with access to the victim's account (e.g., via XSS or an unattended workstation) to change that password and address.	2019-10-07	<a href="#">4.3</a>	<a href="#">CVE-2019-15749</a> <a href="#">MISC</a>
sitos -- sitos_six	A Cross-Site Scripting (XSS) vulnerability in the blog function in SITOS six Build v6.2.1 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	2019-10-07	<a href="#">4.3</a>	<a href="#">CVE-2019-15750</a> <a href="#">MISC</a>
slidervilla -- smooth_slider	The smooth-slider plugin before 2.7 for WordPress has SQL Injection via the wp-admin/admin.php?page=smooth-slider-admin current_slider_id parameter.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2015-9454</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17292</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Project module by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17293</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the export function by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17294</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the history function by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17295</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-</a>

sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Contacts module by a Regular user.	2019-10-07	6.5	<a href="#">17296 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Quotes module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17297 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Administration module by a Developer user.	2019-10-07	6.5	<a href="#">CVE-2019-17298 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17299 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by a Developer user.	2019-10-07	6.5	<a href="#">CVE-2019-17300 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the ModuleBuilder module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17301 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the ModuleBuilder module by a Developer user.	2019-10-07	6.5	<a href="#">CVE-2019-17302 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by a Developer user.	2019-10-07	6.5	<a href="#">CVE-2019-17303 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17304 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17305 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Configurator module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17306 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Tracker module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17307 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Emails module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17308 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the EmailMan module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17309 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Campaigns module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17310 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the attachment function by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17311 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the file function by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17312 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the Studio module by a Developer user.	2019-10-07	6.5	<a href="#">CVE-2019-17313 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the Configurator module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17314 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Administration module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17315 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Import module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17316 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the UpgradeWizard module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17317 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17318 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Emails module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17319 MISC</a>
	The /usr/sbin/pinger binary packaged with squid in SUSE			

suse -- suse_linux_enterprise_server	Linux Enterprise Server 15 before and including version 4.8-5.8.1 and in SUSE Linux Enterprise Server 12 before and including 3.5.21-26.17.1 had squid:root, 0750 permissions. This allowed an attacker that compromised the squid user to gain persistence by changing the binary	2019-10-07	6.6	<a href="#">CVE-2019-3688</a> <a href="#">CONFIRM</a>
teampass -- teampass	TeamPass 2.1.27.36 allows Stored XSS by placing a payload in the username field during a login attempt. When an administrator looks at the log of failed logins, the XSS payload will be executed.	2019-10-05	4.3	<a href="#">CVE-2019-17205</a> <a href="#">MISC</a>
twitter -- twitter_kit	The Twitter Kit framework through 3.4.2 for iOS does not properly validate the api.twitter.com SSL certificate. Although the certificate chain must contain one of a set of pinned certificates, there are certain implementation errors such as a lack of hostname verification. NOTE: this is an end-of-life product.	2019-10-07	5.8	<a href="#">CVE-2019-16263</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
vbulletin -- vbulletin	vBulletin through 5.5.4 mishandles external URLs within the /core/vb/vurl.php file and the /core/vb/vurl directories.	2019-10-04	6.4	<a href="#">CVE-2019-17130</a> <a href="#">MISC</a>
vbulletin -- vbulletin	vBulletin before 5.5.4 allows clickjacking.	2019-10-04	4.3	<a href="#">CVE-2019-17131</a> <a href="#">MISC</a>
vbulletin -- vbulletin	vBulletin through 5.5.4 mishandles custom avatars.	2019-10-04	6.8	<a href="#">CVE-2019-17132</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
vbulletin -- vbulletin	vBulletin 5.5.4 allows SQL Injection via the ajax/api/hook/getHookList or ajax/api/widget/getWidgetList where parameter.	2019-10-08	4.0	<a href="#">CVE-2019-17271</a> <a href="#">MISC</a> <a href="#">MISC</a>
webbarxsecurity -- webbarx	The WebARX plugin 1.3.0 for WordPress has unauthenticated stored XSS via the URI or the X-Forwarded-For HTTP header.	2019-10-06	4.3	<a href="#">CVE-2019-17213</a> <a href="#">MISC</a> <a href="#">MISC</a>
webbarxsecurity -- webbarx	The WebARX plugin 1.3.0 for WordPress allows firewall bypass by appending &cc=1 to a URI.	2019-10-06	5.0	<a href="#">CVE-2019-17214</a> <a href="#">MISC</a>
webpagetest -- webpagetest	www/getfile.php in WPO WebPageTest 19.04 on Windows allows Directory Traversal (for reading arbitrary files) because of an unanchored regular expression, as demonstrated by the a.jpg\.. substring.	2019-10-05	5.0	<a href="#">CVE-2019-17199</a> <a href="#">MISC</a>
wpfactory -- download_plugins_and_themes_from_dashboard	includes/settings/class-alg-download-plugins-settings.php in the download-plugins-dashboard plugin through 1.5.0 for WordPress has multiple unauthenticated stored XSS issues.	2019-10-07	4.3	<a href="#">CVE-2019-17239</a> <a href="#">MISC</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 guest OS users to cause a denial of service or gain privileges because grant-table transfer requests are mishandled.	2019-10-07	6.1	<a href="#">CVE-2019-17340</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging a page-writability race condition during addition of a passed-through PCI device.	2019-10-07	6.9	<a href="#">CVE-2019-17341</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging a race condition that arose when XENMEM_exchange was introduced.	2019-10-07	4.4	<a href="#">CVE-2019-17342</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging incorrect use of the HVM physmap concept for PV domains.	2019-10-07	4.6	<a href="#">CVE-2019-17343</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service by leveraging a long-running operation that exists to support restartability of PTE updates.	2019-10-07	4.9	<a href="#">CVE-2019-17344</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen 4.8.x through 4.11.x allowing x86 PV guest OS users to cause a denial of service because mishandling of failed IOMMU operations causes a bug check during the cleanup of a crashed guest.	2019-10-07	4.9	<a href="#">CVE-2019-17345</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because a guest can manipulate its virtualised %cr4 in a way that is incompatible with Linux (and possibly other guest kernels).	2019-10-07	4.6	<a href="#">CVE-2019-17347</a> <a href="#">MISC</a>
	An issue was discovered in Xen through 4.11.x allowing x86			<a href="#">CVE-2019-</a>

xen -- xen	PV guest OS users to cause a denial of service because of an incompatibility between Process Context Identifiers (PCID) and shadow-pagetable switching.	2019-10-07	<a href="#">4.9</a>	<a href="#">17348 MISC</a>
xen -- xen	An issue was discovered in Xen through 4.12.x allowing Arm domU attackers to cause a denial of service (infinite loop) involving a LoadExcl or StoreExcl operation.	2019-10-07	<a href="#">4.9</a>	<a href="#">CVE-2019-17349 MISC</a>
xen -- xen	An issue was discovered in Xen through 4.12.x allowing Arm domU attackers to cause a denial of service (infinite loop) involving a compare-and-exchange operation.	2019-10-07	<a href="#">4.9</a>	<a href="#">CVE-2019-17350 MISC</a>
xnview -- xnview	XnView Classic 2.49.1 allows a User Mode Write AV starting at Xwsq+0x0000000000001e51.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17261 MISC</a>
xnview -- xnview	XnView Classic 2.49.1 allows a User Mode Write AV starting at Xwsq+0x0000000000001fc0.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17262 MISC</a>
zingbox -- inspector	An SQL injection vulnerability exists in the management interface of Zingbox Inspector versions 1.288 and earlier, that allows for unsanitized data provided by an authenticated user to be passed from the web UI into the database.	2019-10-09	<a href="#">6.5</a>	<a href="#">CVE-2019-15016 MISC</a>
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.280 and earlier, where authentication is not required when binding the Inspector instance to a different customer tenant.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15018 MISC</a>
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that can allow an attacker to easily identify instances of Zingbox Inspectors in a local area network.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15021 MISC</a>
zingbox -- inspector	A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that allows for the Inspector to be susceptible to ARP spoofing.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15022 MISC</a>
zingbox -- inspector	A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that results in passwords for 3rd party integrations being stored in cleartext in device configuration.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15023 MISC</a>
zingbox -- inspector	A security vulnerability exists in Zingbox Inspector version 1.293 and earlier, that allows for remote code execution if the Inspector were sent a malicious command from the Zingbox cloud, or if the Zingbox Inspector were tampered with to connect to an attacker's cloud endpoint.	2019-10-09	<a href="#">6.8</a>	<a href="#">CVE-2019-1584 MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cms_made_simple	CMS Made Simple (CMSMS) 2.2.11 allows XSS via the Site Admin > Module Manager > Search Term field.	2019-10-06	<a href="#">3.5</a>	<a href="#">CVE-2019-17226 MISC</a>
hp -- arcsight_logger	Stored XSS vulnerability in Micro Focus ArcSight Logger, affects versions prior to Logger 6.7.1 HotFix 6.7.1.8262.0. This vulnerability could allow Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').	2019-10-04	<a href="#">3.5</a>	<a href="#">CVE-2019-11656 MISC</a>
hrworks -- hrworks	HRworks 3.36.9 allows XSS via the purpose of a travel-expense report.	2019-10-08	<a href="#">3.5</a>	<a href="#">CVE-2019-16416 MISC</a>
hrworks -- hrworks	HRworks FLOW 3.36.9 allows XSS via the purpose of a travel-expense report.	2019-10-08	<a href="#">3.5</a>	<a href="#">CVE-2019-16417 MISC</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.0, 7.6.1, 7.6.2, and 7.6.3 does not have device root detection which could result in an attacker gaining sensitive information about the device. IBM X-Force ID: 160198.	2019-10-10	<a href="#">2.1</a>	<a href="#">CVE-2019-4265 XE CONFIRM</a>
intelliants -- subrion	Subrion 4.2.1 allows XSS via the panel/members/ Username, Full Name, or Email field, aka an "Admin Member JSON Update" issue.	2019-10-06	<a href="#">3.5</a>	<a href="#">CVE-2019-17225 MISC</a>
laravel-admin -- laravel-admin	z-song laravel-admin 1.7.3 has XSS via the Slug or Name on the Roles screen, because of mishandling on the "Operation log" screen.	2019-10-10	<a href="#">3.5</a>	<a href="#">CVE-2019-17433 MISC</a>

lavalite -- lavalite	LavaLite through 5.7 has XSS via a crafted account name that is mishandled on the Manage Clients screen.	2019-10-10	3.5	<a href="#">CVE-2019-17434</a> MISC
libfws_i_project -- libfws_i	In libyal libfws_i before 20191006, libfws_i_extension_block_copy_from_byte_stream in libfws_i_extension_block.c has a heap-based buffer over-read because rejection of an unsupported size only considers values less than 6, even though values of 6 and 7 are also unsupported.	2019-10-06	2.1	<a href="#">CVE-2019-17263</a> MISC MISC MISC
liblnk_project -- liblnk	** DISPUTED ** libyal liblnk 20191006 has a heap-based buffer over-read in the network_share_name_offset>20 code block of liblnk_location_information_read_data in liblnk_location_information.c, a different issue than CVE-2019-17264. NOTE: the vendor has disputed this as described in the GitHub issue.	2019-10-09	2.1	<a href="#">CVE-2019-17401</a> MISC
microsoft -- sharepoint_enterprise_server	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'.	2019-10-10	3.5	<a href="#">CVE-2019-1070</a> MISC
microsoft -- sharepoint_enterprise_server	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'.	2019-10-10	3.5	<a href="#">CVE-2019-1328</a> MISC
microsoft -- sharepoint_enterprise_server	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1330.	2019-10-10	3.5	<a href="#">CVE-2019-1329</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1334.	2019-10-10	2.1	<a href="#">CVE-2019-1345</a> MISC MISC
microsoft -- windows_7	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'.	2019-10-10	2.1	<a href="#">CVE-2019-1363</a> MISC
pbootcms -- pbootcms	PbootCMS 2.0.2 allows XSS via vectors involving the Pboot/admin.php?p=/Single/index/mcode/1 and Pboot/?contact/ URLs.	2019-10-09	3.5	<a href="#">CVE-2019-17417</a> MISC
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the chart title resulting in reflected Cross-Site Scripting	2019-10-08	3.5	<a href="#">CVE-2019-0374</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the export dialog box of the report name resulting in reflected Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0375</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows an attacker to save malicious scripts in the publication name, which can be executed later by the victim, resulting in Stored Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0376</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2, does not sufficiently encode user-controlled inputs and allows an attacker to store malicious scripts in the input controls, resulting in Stored Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0377</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before version 4.2, does not sufficiently encode user-controlled inputs and allows an attacker to store malicious scripts in the file name of the background image resulting in Stored Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0378</a> MISC CONFIRM
sap -- financial_consolidation	SAP Financial Consolidation, before versions 10.0 and 10.1, does not sufficiently encode user-controlled inputs, which allows an attacker to execute scripts by uploading files containing malicious scripts, leading to reflected cross site scripting vulnerability.	2019-10-08	3.5	<a href="#">CVE-2019-0369</a> MISC CONFIRM
teampass -- teampass	TeamPass 2.1.27.36 allows Stored XSS at the Search page by setting a crafted password for an item in any folder.	2019-10-05	3.5	<a href="#">CVE-2019-17203</a> MISC
	TeamPass 2.1.27.36 allows Stored XSS by setting a crafted	2019-10-		<a href="#">CVE-2019-</a>



teampass -- teampass	Knowledge Base label and adding any available item.	05	3.5	<a href="#">17204 MISC</a>
tibco -- master_data_management	The MDM server component of TIBCO Software Inc's TIBCO MDM contains multiple vulnerabilities that theoretically allow an authenticated user with specific roles to perform cross-site scripting (XSS) attacks. This issue affects TIBCO Software Inc.'s TIBCO MDM version 9 0.1 and prior versions; version 9.1.0.	2019-10-09	3.5	<a href="#">CVE-2019-11212 CONFIRM</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activesoft -- mybuilder	ActiveX Control in MyBuilder before 6.2.2019.814 allow an attacker to execute arbitrary command via the ShellOpen method. This can be leveraged for code execution	2019-10-07	not yet calculated	<a href="#">CVE-2019-12811 MISC</a>
activesoft -- mybuilder	MyBuilder viewer before 6.2.2019.814 allow an attacker to execute arbitrary command via specifically crafted configuration file. This can be leveraged for code execution.	2019-10-07	not yet calculated	<a href="#">CVE-2019-12812 MISC</a>
altair_engineering -- pbs_professional	Altair PBS Professional through 19.1.2 allows Privilege Escalation because an attacker can send a message directly to pbs_mom, which fails to properly authenticate the message. This results in code execution as an arbitrary user.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15719 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
amazon_web_services -- freertos	Amazon FreeRTOS up to and including v1.4.8 for AWS lacks length checking in prvProcessReceivedPublish, resulting in leakage of arbitrary memory contents on a device to an attacker. An attacker sends a malformed MQTT publish packet, and waits for an MQTTACK packet containing the leaked data.	2019-10-07	not yet calculated	<a href="#">CVE-2019-13120 CONFIRM</a>
arista_networks -- extensible_operating_system	A vulnerability has been found in the implementation of the Label Distribution Protocol (LDP) protocol in EOS. Under race conditions, the LDP agent can establish an LDP session with a malicious peer potentially allowing the possibility of a Denial of Service (DoS) attack on route updates and in turn potentially leading to an Out of Memory (OOM) condition that is disruptive to traffic forwarding. Affected EOS versions include: 4.22 release train: 4.22.1F and earlier releases 4.21 release train: 4.21.0F - 4.21.2.3F, 4.21.3F - 4.21.7.1M 4.20 release train: 4.20.14M and earlier releases 4.19 release train: 4.19.12M and earlier releases End of support release trains (4.18 and 4.17)	2019-10-10	not yet calculated	<a href="#">CVE-2019-14810 MISC</a> <a href="#">CONFIRM</a>
auth0 -- auth0	Auth0 auth0.net before 6.5.4 has Incorrect Access Control because IdentityTokenValidator can be accidentally used to validate untrusted ID tokens.	2019-10-08	not yet calculated	<a href="#">CVE-2019-16929 CONFIRM</a>
automatic -- mongoose	Automatic Mongoose through 5.7.4 allows attackers to bypass access control (in some applications) because any query object with a _bsontype attribute is ignored. For example, adding "_bsontype":"a" can sometimes interfere with a query filter. NOTE: this CVE is about Mongoose's failure to work around this _bsontype special case that exists in older versions of the bson parser (aka the mongodb/js-bson project).	2019-10-09	not yet calculated	<a href="#">CVE-2019-17426 MISC</a> <a href="#">MISC</a>
avira -- avira_software_updater	Avira Software Updater before 2.0.6.21094 allows a DLL side-loading attack.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17449 MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a SEGV in the function AP4_TfhdAtom::SetDefaultSampleSize at Core/AP4TfhdAtom.h when called from AP4_Processor::ProcessFragments in Core/AP4Processor.cpp.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17528 MISC</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a heap-based buffer over-read in AP4_CencSampleEncryption::DoInspectFields in Core/AP4CommonEncryption.cpp when called from AP4_Atom::Inspect in Core/AP4Atom.cpp.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17529 MISC</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a heap-based buffer over-read in AP4_PrintInspector::AddField in Core/AP4Atom.cpp when called from	2019-10-	not yet	<a href="#">CVE-2019-17530</a>

	AP4_CencSampleEncryption::DoInspectFields in Core/Ap4CommonEncryption.cpp, when called from AP4_Atom::Inspect in Core/Ap4Atom.cpp.	12	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
b3log -- symphony	b3log Symphony (aka Sym) before 3.6.0 has XSS via the HTTP User-Agent header.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17488</a> <a href="#">MISC</a>
belkin -- wemo_switch_28b_devices	An issue was discovered on Belkin Wemo Switch 28B WW_2.00.11057.PVT-OWRT-SNS devices. They allow remote attackers to cause a denial of service (persistent rules-processing outage) via a crafted ruleDbBody element in a StoreRules request to the upnp/control/rules1 URI, because database corruption occurs.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17532</a> <a href="#">MISC</a>
bootstrap-3-typeahead -- bootstrap-3-typeahead	Bootstrap-3-Typeahead after version 4.0.2 is vulnerable to a cross-site scripting flaw in the highlighter() function. An attacker could exploit this via user interaction to execute code in the user's browser.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10215</a> <a href="#">CONFIRM</a>
bouncy_castle -- bouncy_castle_crypto_package	The ASN.1 parser in Bouncy Castle Crypto (aka BC Java) 1.63 can trigger a large attempted memory allocation, and resultant OutOfMemoryError error, via crafted ASN.1 data. This is fixed in 1.64.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17359</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	getStats.php in Centreon Web before 2.8.28 allows authenticated attackers to execute arbitrary code via the ns_id parameter.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21023</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	licenseUpload.php in Centreon Web before 2.8.27 allows attackers to upload arbitrary files via a POST request.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21024</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
centreon -- centreon_web	img_gantt.php in Centreon Web before 2.8.27 allows attackers to perform SQL injections via the host_id parameter.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21021</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	makeXML_ListServices.php in Centreon Web before 2.8.28 allows attackers to perform SQL injections via the host_id parameter.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21022</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	The token generator in index.php in Centreon Web before 2.8.27 is predictable.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17105</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
centreon -- centreon_web	In very rare cases, a PHP type juggling vulnerability in centreonAuth.class.php in Centreon Web before 2.8.27 allows attackers to bypass authentication mechanisms in place.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21020</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	minPlayCommand.php in Centreon Web before 2.8.27 allows authenticated attackers to execute arbitrary code via the command_hostaddress parameter. NOTE: some sources have listed CVE-2019-17017 for this, but that is incorrect.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17107</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	Local file inclusion in brokerPerformance.php in Centreon Web before 2.8.28 allows attackers to disclose information or perform a stored XSS attack on a user.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17108</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- application_delivery_management	Citrix Application Delivery Management (ADM) 12.1 before build 54.13 has Incorrect Access Control.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17366</a> <a href="#">CONFIRM</a>
	The web application portal of the Cobham EXPLORER 710,			

cobham -- explorer_710	firmware version 1.07, has no authentication by default. This could allow an unauthenticated, local attacker connected to the device to access the portal and to make any change to the device.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9529</a> <a href="#">CERT-VN</a>
cobham -- explorer_710	The web application portal of the Cobham EXPLORER 710, firmware version 1.07, allows unauthenticated access to port 5454. This could allow an unauthenticated, remote attacker to connect to this port via Telnet and execute 86 Attention (AT) commands, including some that provide unauthenticated, shell-like access to the device.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9531</a> <a href="#">CERT-VN</a>
cobham -- explorer_710	The web root directory of the Cobham EXPLORER 710, firmware version 1.07, has no access restrictions on downloading and reading all files. This could allow an unauthenticated, local attacker connected to the device to access and download any file found in the web root directory.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9530</a> <a href="#">CERT-VN</a>
cobham -- explorer_710	The Cobham EXPLORER 710, firmware version 1.07, does not validate its firmware image. Development scripts left in the firmware can be used to upload a custom firmware image that the device runs. This could allow an unauthenticated, local attacker to upload their own firmware that could be used to intercept or modify traffic, spoof or intercept GPS traffic, exfiltrate private data, hide a backdoor, or cause a denial-of-service.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9534</a> <a href="#">CERT-VN</a>
cobham -- explorer_710	The root password of the Cobham EXPLORER 710 is the same for all versions of firmware up to and including v1.08. This could allow an attacker to reverse-engineer the password from available versions to gain authenticated access to the device.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9533</a> <a href="#">CERT-VN</a>
cobham -- explorer_710	The web application portal of the Cobham EXPLORER 710, firmware version 1.07, sends the login password in cleartext. This could allow an unauthenticated, local attacker to intercept the password and gain access to the portal.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9532</a> <a href="#">CERT-VN</a>
compal -- ch7465lg_devices	The setter.xml component of the Common Gateway Interface on Compal CH7465LG 6.12.18.25-2p4 devices does not properly validate ping command arguments, which allows remote authenticated users to execute OS commands as root via shell metacharacters in the Target_IP parameter.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17499</a> <a href="#">MISC</a>
craft_cms -- craft_cms	Craft CMS before 3.3.8 has stored XSS via a name field. This field is mishandled during site deletion.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17496</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dap-1320_routers	D-Link DAP-1320 A2-V1.21 routers have some web interfaces without authentication requirements, as demonstrated by uplink_info.xml. An attacker can remotely obtain a user's Wi-Fi SSID and password, which could be used to connect to Wi-Fi or perform a dictionary attack.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17505</a> <a href="#">MISC</a>
d-link -- dir-615_devices	An issue discovered on D-Link DIR-615 devices with firmware version 20.05 and 20.07. wan.htm can be accessed directly without authentication, which can lead to disclosure of information about the WAN, and can also be leveraged by an attacker to modify the data fields of the page.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17353</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-816l_devices	An issue was discovered on D-Link DIR-816 A1 1.06 devices. An attacker could access management pages of the router via a client that ignores the 'top.location.href = "/dir_login.asp"' line in a .asp file. This provides access to d_status.asp, version.asp, d_dhcptbl.asp, and d_acl.asp.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17507</a> <a href="#">MISC</a>
d-link -- dir-846_devices	D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending a /HNAP1/ request for SetMasterWlanSettings with shell metacharacters to /squashfs-root/www/HNAP1/control/SetMasterWlanSettings.php.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17509</a> <a href="#">MISC</a>
d-link -- dir-846_devices	D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending a /HNAP1/ request for SetWizardConfig with shell metacharacters to /squashfs-root/www/HNAP1/control/SetWizardConfig.php.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17510</a> <a href="#">MISC</a>
d-link -- dir-859_and_dir-8850_devices	On D-Link DIR-859 A3-1.06 and DIR-850 A1.13 devices, /etc/services/DEVICE.TIME.php allows command injection via the \$SERVER variable.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17508</a> <a href="#">MISC</a>
d-link -- dir-868l_and_dir-817lw_routers	There are some web interfaces without authentication requirements on D-Link DIR-868L B1-2.03 and DIR-817LW A1-1.04 routers. An attacker can get the router's username and password (and other information) via SERVICES=DEVICE.ACCOUNT&AUTHORIZED_GROUP=1%0a	2019-10-11	not yet calculated	<a href="#">CVE-2019-17506</a> <a href="#">MISC</a>

	to getcfg.php. This could be used to control the router remotely.			
dbell -- wi-fi_smart_video_doorbell	The dbell Wi-Fi Smart Video Doorbell DB01-S Gen 1 allows remote attackers to launch commands with no authentication verification via TCP port 81, because the loginuse and loginpass parameters to openlock.cgi can have arbitrary values. NOTE: the vendor's position is that this product reached end of life in 2016.	2019-10-08	not yet calculated	<a href="#">CVE-2019-13336</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- encryption_enterprise	The vulnerability is limited to the installers of Dell Encryption Enterprise versions prior to 10.4.0 and Dell Endpoint Security Suite Enterprise versions prior to 2.4.0. This issue is exploitable only during the installation of the product by an administrator. A local authenticated low privileged user potentially could exploit this vulnerability by staging a malicious DLL in the search path of the installer prior to its execution by a local administrator. This would cause loading of the malicious DLL, which would allow the attacker to execute arbitrary code in the context of an administrator.	2019-10-07	not yet calculated	<a href="#">CVE-2019-3745</a> <a href="#">MISC</a>
dell_emc -- avamar_server	Dell EMC Avamar Server versions 7.4.1, 7.5.0, 7.5.1, 18.2 and 19.1 and Dell EMC Integrated Data Protection Appliance (IDPA) versions 2.0, 2.1, 2.2, 2.3 and 2.4 contain an Incorrect Permission Assignment for Critical Resource vulnerability. A remote authenticated malicious user potentially could exploit this vulnerability to view or modify sensitive backup data. This could be used to make backups corrupt or potentially to trick a user into restoring a backup with malicious files in place.	2019-10-09	not yet calculated	<a href="#">CVE-2019-3765</a> <a href="#">CONFIRM</a>
envoy_proxy -- envoy	Upon receiving each incoming request header data, Envoy will iterate over existing request headers to verify that the total size of the headers stays below a maximum limit. The implementation in versions 1.10.0 through 1.11.1 for HTTP/1.x traffic and all versions of Envoy for HTTP/2 traffic had O(n^2) performance characteristics. A remote attacker may craft a request that stays below the maximum request header size but consists of many thousands of small headers to consume CPU and result in a denial-of-service attack.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15226</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
espressif -- esp-idf	An issue was discovered in Espressif ESP-IDF 2.x, 3.0.x through 3.0.9, 3.1.x through 3.1.6, 3.2.x through 3.2.3, and 3.3.x through 3.3.1. An attacker who uses fault injection to physically disrupt the ESP32 CPU can bypass the Secure Boot digest verification at startup, and boot unverified code from flash. The fault injection attack does not disable the Flash Encryption feature, so if the ESP32 is configured with the recommended combination of Secure Boot and Flash Encryption, then the impact is minimized. If the ESP32 is configured without Flash Encryption then successful fault injection allows arbitrary code execution. To protect devices with Flash Encryption and Secure Boot enabled against this attack, a firmware change must be made to permanently enable Flash Encryption in the field if it is not already permanently enabled.	2019-10-07	not yet calculated	<a href="#">CVE-2019-15894</a> <a href="#">CONFIRM</a>
fastadmin -- fastadmin	An issue was discovered in fastadmin 1.0.0.20190705_beta. There is a public/admin/general.config/edit CSRF vulnerability, as demonstrated by resultant XSS via the row&#91;name&#93; parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17432</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the apache-log4j-extra (version 1.2.x) jar in the classpath, and an attacker can provide a JNDI service to access, it is possible to make the service execute a malicious payload.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17531</a> <a href="#">MISC</a> <a href="#">MISC</a>
fiberhome -- hg2201t	/var/WEB-GUI/cgi-bin/telnet.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows pre-authentication remote code execution.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17186</a> <a href="#">MISC</a>
frost_ming -- redis_wrapper	Uncontrolled deserialization of a pickled object in models.py in Frost Ming rediswrapper (aka Redis Wrapper) before 0.3.0 allows attackers to execute arbitrary scripts.	2019-10-05	not yet calculated	<a href="#">CVE-2019-17206</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
genesys -- pureengage_digital	Genesys PureEngage Digital (eServices) 8.1.x allows XSS via HtmlChatPanel.jsp or HtmlChatFrameSet.jsp (ActionColor, ClientNickNameColor, Email, email, or email_address parameter).	2019-10-11	not yet calculated	<a href="#">CVE-2019-17176</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

gnu -- binutils	find_abstract_instance in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32, allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17450</a> <a href="#">MISC</a>
gnu -- binutils	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an integer overflow leading to a SEGV in _bfd_dwarf2_find_nearest_line in dwarf2.c, as demonstrated by nm.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17451</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnupg_project -- boa	Boa through 0.94.14rc21 allows remote attackers to trigger an out-of-memory (OOM) condition because malloc is mishandled.	2019-10-11	not yet calculated	<a href="#">CVE-2018-21027</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gnupg_project -- boa	Boa through 0.94.14rc21 allows remote attackers to trigger a memory leak because of missing calls to the free function.	2019-10-11	not yet calculated	<a href="#">CVE-2018-21028</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
google -- android	In generateServicesMap of RegisteredServicesCache.java, there is a possible account protection bypass due to a caching optimization. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-136261465	2019-10-11	not yet calculated	<a href="#">CVE-2019-2183</a> <a href="#">CONFIRM</a>
google -- android	In the default privileges of NFC, there is a possible local bypass of user interaction requirements on package installation due to a default permission. This could lead to local escalation of privilege by installing an application with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-123700348	2019-10-11	not yet calculated	<a href="#">CVE-2019-2114</a> <a href="#">CONFIRM</a>
google -- android	In GetMBheader of combined_decode.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-136175447	2019-10-11	not yet calculated	<a href="#">CVE-2019-2186</a> <a href="#">CONFIRM</a>
google -- android	In VlcDequantH263IntraBlock_SH of vlc_dequant.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-136173699	2019-10-11	not yet calculated	<a href="#">CVE-2019-2185</a> <a href="#">CONFIRM</a>
google -- android	In PV_DecodePredictedIntraDC of dec_pred_intra_dc.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-134578122	2019-10-11	not yet calculated	<a href="#">CVE-2019-2184</a> <a href="#">CONFIRM</a>
google -- android	In ScreenRotationAnimation of ScreenRotationAnimation.java, there is a possible capture of a secure screen due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-69703445	2019-10-11	not yet calculated	<a href="#">CVE-2019-2110</a> <a href="#">CONFIRM</a>
google -- android	In startActivityMayWait of ActivityStarter.java, there is a possible incorrect Activity launch due to an incorrect permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-123013720	2019-10-11	not yet calculated	<a href="#">CVE-2019-2173</a> <a href="#">CONFIRM</a>
google -- android	A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application.Product: AndroidAndroid ID: A-141720095	2019-10-11	not yet calculated	<a href="#">CVE-2019-2215</a> <a href="#">CONFIRM</a>
google -- android	In nfc_ncif_decode_rf_params of nfc_ncif.cc, there is a possible out of bounds read due to an integer underflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-124940143	2019-10-11	not yet calculated	<a href="#">CVE-2019-2187</a> <a href="#">CONFIRM</a>



graphite_project -- graphite	send_email in graphite-web/webapp/graphite/composer/views.py in Graphite through 1.1.5 is vulnerable to SSRF. The vulnerable SSRF endpoint can be used by an attacker to have the Graphite web server request any resource. The response to this SSRF request is encoded into an image file and then sent to an e-mail address that can be supplied by the attacker. Thus, an attacker can exfiltrate any information.	2019-10-11	not yet calculated	<a href="#">CVE-2017-18638</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gree -- gree+_application_for_andriod	The GREE+ (aka com.gree.greeplus) application 1.4.0.8 for Android suffers from Cross Site Request Forgery.	2019-10-11	not yet calculated	<a href="#">CVE-2018-20582</a> <a href="#">MISC</a> <a href="#">MISC</a>
hotaru_cms -- hotaru_cms	A stored XSS vulnerability was discovered in Hotaru CMS v1.7.2 via the admin_index.php?page=settings SITE_NAME field (aka SITE_NAME), a related issue to CVE-2011-4709.1.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17522</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- touchpoint_analytics	A potential security vulnerability has been identified with certain versions of HP Touchpoint Analytics prior to version 4.1.4.2827. This vulnerability may allow a local attacker with administrative privileges to execute arbitrary code via an HP Touchpoint Analytics system service.	2019-10-11	not yet calculated	<a href="#">CVE-2019-6333</a> <a href="#">CONFIRM</a>
hyrda -- hyrda	Hydra through 0.1.8 has a NULL pointer dereference and daemon crash when processing POST requests that lack a Content-Length header. read.c, request.c, and util.c contribute to this. The process_header_end() function calls boa_atoi(), which ultimately calls atoi() on a NULL pointer.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17502</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has a directory traversal vulnerability. This can result in loss of confidential data of IceWarp Mailserver and the operating system. Input passed via a certain parameter (script to basic/minimizer/index.php) is not properly sanitised and can therefore be exploited to browse the partition where IceWarp is installed (or the whole system) and read arbitrary files.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5335</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has a directory traversal vulnerability. This can result in loss of confidential data of IceWarp Mailserver and the operating system. Input passed via a certain parameter (_c to basic/index.html) is not properly sanitised and can therefore be exploited to browse the partition where IceWarp is installed (or the whole system) and read arbitrary files.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5334</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: admin/login.html with the parameter username is persistent in 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5336</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/basic/ with the parameter _dlg[capcha] [controller] is non-persistent in 10.1.3 and 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5337</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/basic/ with the parameter _dlg[capcha][action] is non-persistent in 10.1.3 and 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5338</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/basic/ with the parameter _dlg[capcha][uid] is non-persistent in 10.1.3 and 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5339</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/ with the parameter password is non-persistent in 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5340</a> <a href="#">MISC</a> <a href="#">MISC</a>
intel -- active_system_console	Insufficient path checking in the installer for Intel(R) Active System Console before version 8.0 Build 24 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-10-11	not yet calculated	<a href="#">CVE-2019-11120</a> <a href="#">CONFIRM</a>
intel -- nuc	Memory corruption in system firmware for Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-10-11	not yet calculated	<a href="#">CVE-2019-14570</a> <a href="#">CONFIRM</a>
intel -- nuc	Pointer corruption in system firmware for Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-10-11	not yet calculated	<a href="#">CVE-2019-14569</a> <a href="#">CONFIRM</a>
intel --	Improper file permission in software installer for Intel(R) Smart			<a href="#">CVE-</a>

smart_connect_technology_for_intel_nuc	Connect Technology for Intel(R) NUC may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-10-11	not yet calculated	<a href="#">2019-11167 CONFIRM</a>
internet_systems_consortium -- bind	An error in the EDNS Client Subnet (ECS) feature for recursive resolvers can cause BIND to exit with an assertion failure when processing a response that has malformed RRSIGs. Versions affected: BIND 9.10.5-S1 -> 9.11.6-S1 of BIND 9 Supported Preview Edition.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6469 CONFIRM</a>
internet_systems_consortium -- bind	A failure to free memory can occur when processing messages having a specific combination of EDNS options. Versions affected are: BIND 9.10.7 -> 9.10.8-P1, 9.11.3 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.10.7-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected.	2019-10-09	not yet calculated	<a href="#">CVE-2018-5744 CONFIRM</a>
internet_systems_consortium -- bind	A race condition which may occur when discarding malformed packets can result in BIND exiting due to a REQUIRE assertion failure in dispatch.c. Versions affected: BIND 9.11.0 -> 9.11.7, 9.12.0 -> 9.12.4-P1, 9.14.0 -> 9.14.2. Also all releases of the BIND 9.13 development branch and version 9.15.0 of the BIND 9.15 development branch and BIND Supported Preview Edition versions 9.11.3-S1 -> 9.11.7-S1.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6471 CONFIRM CONFIRM</a>
internet_systems_consortium -- bind	In BIND Supported Preview Edition, an error in the nxdomain-redirect feature can occur in versions which support EDNS Client Subnet (ECS) features. In those versions which have ECS support, enabling nxdomain-redirect is likely to lead to BIND exiting due to assertion failure. Versions affected: BIND Supported Preview Edition version 9.10.5-S1 -> 9.11.5-S5. ONLY BIND Supported Preview Edition releases are affected.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6468 CONFIRM</a>
internet_systems_consortium -- bind	A programming error in the nxdomain-redirect feature can cause an assertion failure in query.c if the alternate namespace used by nxdomain-redirect is a descendant of a zone that is served locally. The most likely scenario where this might occur is if the server, in addition to performing NXDOMAIN redirection for recursive clients, is also serving a local copy of the root zone or using mirroring to provide the root zone, although other configurations are also possible. Versions affected: BIND 9.12.0 -> 9.12.4, 9.14.0. Also affects all releases in the 9.13 development branch.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6467 CONFIRM</a>
internet_systems_consortium -- bind	Controls for zone transfers may not be properly applied to Dynamically Loadable Zones (DLZs) if the zones are writable. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P2, 9.12.0 -> 9.12.3-P2, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2019-6465.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6465 CONFIRM</a>
internet_systems_consortium -- bind	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contained an error which could be exploited to grow the number of simultaneous connections beyond this limit. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.6, 9.12.0 -> 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 -> 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 -> 9.13.7 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5743.	2019-10-09	not yet calculated	<a href="#">CVE-2018-5743 CONFIRM</a>
internet_systems_consortium -- bind	"managed-keys" is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which operators configure for use in DNSSEC validation. Due to an error in the managed-keys feature it is possible for a BIND server which uses managed-keys to exit due to an assertion failure if, during key rollover, a trust anchor's keys are replaced with keys which use an unsupported algorithm. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5745.	2019-10-09	not yet calculated	<a href="#">CVE-2018-5745 CONFIRM</a>
internet_systems_consortium -- isc_dhcp	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0	2019-10-09	not yet calculated	<a href="#">CVE-2018-5732 CONFIRM</a>

item2 -- item2	A vulnerability exists in the way that iTerm2 integrates with tmux's control mode, which may allow an attacker to execute arbitrary commands by providing malicious output to the terminal. This affects versions of iTerm2 up to and including 3.3.5. This vulnerability may allow an attacker to execute arbitrary commands on their victim's computer by providing malicious output to the terminal. It could be exploited using command-line utilities that print attacker-controlled content.	2019-10-09	not yet calculated	<a href="#">CVE-2019-9535</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CERT-VN</a>
jfinal -- jfinal	In JFinal cos before 2019-08-13, as used in JFinal 4.4, there is a vulnerability that can bypass the isSafeFile() function: one can upload any type of file. For example, a .jsp file may be stored and almost immediately deleted, but this deletion step does not occur for certain exceptions.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17352</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jiangnan_online_judge -- jiangnan_online_judge	app/modules/polygon/controllers/ProblemController in Jiangnan Online Judge (aka jnoj) 0.8.0 allows arbitrary file upload, as demonstrated by PHP code (with a .php filename but the image/png content type) to the web/polygon/problem/tests URI.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17490</a> <a href="#">MISC</a>
joicom_corporation -- renpho_application	An issue was discovered in the RENPHO application 3.0.0 for iOS. It transmits JSON data unencrypted to a server without an integrity check, if a user changes personal data in his profile tab (e.g., exposure of his birthday) or logs into his account (i.e., exposure of credentials).	2019-10-09	not yet calculated	<a href="#">CVE-2019-14808</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomlashack -- shack_forms_pro	The Shack Forms Pro extension before 4.0.32 for Joomla! allows path traversal via a file attachment.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17399</a> <a href="#">MISC</a>
juniper_networks -- junos_os	A session fixation vulnerability in J-Web on Junos OS may allow an attacker to use social engineering techniques to fix and hijack a J-Web administrators web session and potentially gain administrative access to the device. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D85 on SRX Series; 14.1X53 versions prior to 14.1X53-D51; 15.1 versions prior to 15.1F6-S13, 15.1R7-S5; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238; 16.1 versions prior to 16.1R4-S13, 16.1R7-S5; 16.2 versions prior to 16.2R2-S10; 17.1 versions prior to 17.1R3-S1; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R3-S5; 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2; 19.1 versions prior to 19.1R1-S2, 19.1R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0062</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os	The PKI keys exported using the command "run request security pki key-pair export" on Junos OS may have insecure file permissions. This may allow another user on the Junos OS device with shell access to read them. This issue affects: Juniper Networks Junos OS 15.1X49 versions prior to 15.1X49-D180; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0073</a> <a href="#">MISC</a>
juniper_networks -- junos_os	A memory leak vulnerability in the of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the device by sending specific commands from a peered BGP host and having those BGP states delivered to the vulnerable device. This issue affects: Juniper Networks Junos OS: 18.1 versions prior to 18.1R2-S4, 18.1R3-S1; 18.1X75 all versions. Versions before 18.1R1 are not affected.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0059</a> <a href="#">MISC</a>
juniper_networks -- junos_os	The management daemon (MGD) is responsible for all configuration and management operations in Junos OS. The Junos CLI communicates with MGD over an internal unix-domain socket and is granted special permission to open this protected mode socket. Due to a misconfiguration of the internal socket, a local, authenticated user may be able to exploit this vulnerability to gain administrative privileges. This issue only affects Linux-based platforms. FreeBSD-based platforms are unaffected by this vulnerability. Exploitation of this vulnerability requires Junos shell access. This issue cannot be exploited from the Junos CLI. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D171, 15.1X49-D180; 15.1X53 versions prior to 15.1X53-D496, 15.1X53-D69; 16.1 versions prior to 16.1R7-S4; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R2-S7, 17.2R3-S1; 17.3 versions prior to 17.3R3-S4; 17.4 versions prior to 17.4R1-S6, 17.4R1-S7, 17.4R2-S3, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S4; 18.2 versions prior to 18.2R1-S5, 18.2R2-S2,	2019-10-09	not yet calculated	<a href="#">CVE-2019-0061</a> <a href="#">MISC</a>

	18.2R3; 18.3 versions prior to 18.3R1-S3, 18.3R2; 18.4 versions prior to 18.4R1-S2, 18.4R2.			
juniper_networks -- junos_os	A path traversal vulnerability in NFX150 Series and QFX10K Series, EX9200 Series, MX Series and PTX Series devices with Next-Generation Routing Engine (NG-RE) allows a local authenticated user to read sensitive system files. This issue only affects NFX150 Series and QFX10K Series, EX9200 Series, MX Series and PTX Series with Next-Generation Routing Engine (NG-RE) which uses vmhost. This issue affects Juniper Networks Junos OS on NFX150 Series and QFX10K, EX9200 Series, MX Series and PTX Series with NG-RE and vmhost: 15.1F versions prior to 15.1F6-S12 16.1 versions starting from 16.1R6 and later releases, including the Service Releases, prior to 16.1R6-S6, 16.1R7-S3; 17.1 versions prior to 17.1R3; 17.2 versions starting from 17.2R1-S3, 17.2R3 and later releases, including the Service Releases, prior to 17.2R3-S1; 17.3 versions starting from 17.3R1-S1, 17.3R2 and later releases, including the Service Releases, prior to 17.3R3-S3; 17.4 versions starting from 17.4R1 and later releases, including the Service Releases, prior to 17.4R1-S6, 17.4R2-S2, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S3; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S2, 18.3R2; 18.4 versions prior to 18.4R1-S1, 18.4R2. This issue does not affect: Juniper Networks Junos OS 15.1 and 16.2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0074</a> <a href="#">MISC</a>
juniper_networks -- junos_os	Receipt of a specific link-local IPv6 packet destined to the RE may cause the system to crash and restart (vmcore). By continuously sending a specially crafted IPv6 packet, an attacker can repeatedly crash the system causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R6-S2, 16.1R7; 16.2 versions prior to 16.2R2-S10; 17.1 versions prior to 17.1R3. This issue does not affect Juniper Networks Junos OS version 15.1 and prior versions.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0067</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os	An unexpected status return value weakness in the Next-Generation Multicast VPN (NG-mVPN) service of Juniper Networks Junos OS allows attacker to cause a Denial of Service (DoS) condition and core the routing protocol daemon (rpd) process when a specific malformed IPv4 packet is received by the device running BGP. This malformed packet can be crafted and sent to a victim device including when forwarded directly through a device receiving such a malformed packet, but not if the malformed packet is first de-encapsulated from an encapsulated format by a receiving device. Continued receipt of the malformed packet will result in a sustained Denial of Service condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1F6-S12, 15.1R7-S2; 15.1X49 versions prior to 15.1X49-D150 on SRX Series; 15.1X53 versions prior to 15.1X53-D68, 15.1X53-D235, 15.1X53-D495, 15.1X53-D590; 16.1 versions prior to 16.1R3-S10, 16.1R4-S12, 16.1R6-S6, 16.1R7-S2; 16.2 versions prior to 16.2R2-S7; 17.1 versions prior to 17.1R2-S9, 17.1R3; 17.2 versions prior to 17.2R1-S7, 17.2R2-S6, 17.2R3; 17.3 versions prior to 17.3R2-S4, 17.3R3.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0066</a> <a href="#">MISC</a> <a href="#">MISC</a>
juniper_networks -- junos_os	A persistent Cross-Site Scripting (XSS) vulnerability in Junos OS J-Web interface may allow remote unauthenticated attackers to perform administrative actions on the Junos device. Successful exploitation requires a Junos administrator to first perform certain diagnostic actions on J-Web. This issue affects: Juniper Networks Junos OS 12.1X46 versions prior to 12.1X46-D86; 12.3 versions prior to 12.3R12-S13; 12.3X48 versions prior to 12.3X48-D80; 14.1X53 versions prior to 14.1X53-D51; 15.1 versions prior to 15.1F6-S13, 15.1R7-S4; 15.1X49 versions prior to 15.1X49-D171, 15.1X49-D180; 15.1X53 versions prior to 15.1X53-D497, 15.1X53-D69; 16.1 versions prior to 16.1R7-S5; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R2-S7, 17.2R3-S1; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R1-S7, 17.4R2-S4, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R1-S5, 18.2R2-S3, 18.2R3; 18.3 versions prior to 18.3R1-S3, 18.3R2, 18.3R3; 18.4 versions prior to 18.4R1-S2, 18.4R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0047</a> <a href="#">MISC</a>
juniper_networks -- junos_os_ex2300_and_ex3400_series	Veriexec is a kernel-based file integrity subsystem in Junos OS that ensures only authorized binaries are able to be executed. Due to a flaw in specific versions of Junos OS, affecting specific EX Series platforms, the Veriexec subsystem will fail to initialize, in essence disabling file integrity checking. This may allow a locally authenticated user with shell access to install untrusted executable images, and elevate privileges to gain full control of the system. During the installation of an affected version of Junos OS are installed, the following messages will be logged to the console: Initializing Verified Exec: /sbin/veriexec: Undefined	2019-10-	not yet	<a href="#">CVE-2019-0071</a>

	symbol "__aeabi_uidiv" /sbin/verixec: Undefined symbol symbol "__aeabi_uidiv" /sbin/verixec: Undefined symbol verixec: /.mount/packages/db/os-kernel-prd-arm-32-20190221.70c2600_builder_stable_11/boot/brcm-hr3.dtb: Authentication error verixec: /.mount/packages/db/os-kernel-prd-arm-32-20190221.70c2600_builder_stable_11/boot/contents.izo: Authentication error ... This issue affects Juniper Networks Junos OS: 18.1R3-S4 on EX2300, EX2300-C and EX3400; 18.3R1-S3 on EX2300, EX2300-C and EX3400.	09	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
juniper_networks -- junos_os_multiple_series	A vulnerability in the srpxfe process on Protocol Independent Multicast (PIM) enabled SRX series devices may lead to crash of the srpxfe process and an FPC reboot while processing (PIM) messages. Sustained receipt of these packets may lead to an extended denial of service condition. Affected releases are Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D80; 15.1X49 versions prior to 15.1X49-D160; 17.3 versions prior to 17.3R3-S7 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0075</a> <a href="#">MISC</a>
juniper_networks -- junos_os_multiple_series	On EX4600, QFX5100 Series, NFX Series, QFX10K Series, QFX5110, QFX5200 Series, QFX5110, QFX5200, QFX10K Series, vSRX, SRX1500, SRX4000 Series, vSRX, SRX1500, SRX4000, QFX5110, QFX5200, QFX10K Series, when the user uses console management port to authenticate, the credentials used during device authentication are written to a log file in clear text. This issue does not affect users that are logging-in using telnet, SSH or J-web to the management IP. This issue affects ACX, NFX, SRX, EX and QFX platforms with the Linux Host OS architecture, it does not affect other SRX and EX platforms that do not use the Linux Host OS architecture. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D110 on vSRX, SRX1500, SRX4000 Series; 15.1X53 versions prior to 15.1X53-D234 on QFX5110, QFX5200 Series; 15.1X53 versions prior to 15.1X53-D68 on QFX10K Series; 17.1 versions prior to 17.1R2-S8, 17.1R3, on QFX5110, QFX5200, QFX10K Series; 17.2 versions prior to 17.2R1-S7, 17.2R2-S6, 17.2R3 on QFX5110, QFX5200, QFX10K Series; 17.3 versions prior to 17.3R2 on vSRX, SRX1500, SRX4000, QFX5110, QFX5200, QFX10K Series; 14.1X53 versions prior to 14.1X53-D47 on ACX5000, EX4600, QFX5100 Series; 15.1 versions prior to 15.1R7 on ACX5000, EX4600, QFX5100 Series; 16.1R7 versions prior to 16.1R7 on ACX5000, EX4600, QFX5100 Series; 17.1 versions prior to 17.1R2-S10, 17.1R3 on ACX5000, EX4600, QFX5100 Series; 17.2 versions prior to 17.2R3 on ACX5000, EX4600, QFX5100 Series; 17.3 versions prior to 17.3R3 on ACX5000, EX4600, QFX5100 Series; 17.4 versions prior to 17.4R2 on ACX5000, EX4600, QFX5100 Series; 18.1 versions prior to 18.1R2 on ACX5000, EX4600, QFX5100 Series; 15.1X53 versions prior to 15.1X53-D496 on NFX Series, 17.2 versions prior to 17.2R3-S1 on NFX Series; 17.3 versions prior to 17.3R3-S4 on NFX Series; 17.4 versions prior to 17.4R2-S4, 17.4R3 on NFX Series, 18.1 versions prior to 18.1R3-S4 on NFX Series; 18.2 versions prior to 18.2R2-S3, 18.2R3 on NFX Series; 18.3 versions prior to 18.3R1-S3, 18.3R2 on NFX Series; 18.4 versions prior to 18.4R1-S1, 18.4R2 on NFX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0069</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os_mx_series	On MX Series, when the SIP ALG is enabled, receipt of a certain malformed SIP packet may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending a crafted SIP packet, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a sustained Denial of Service. This issue affects Juniper Networks Junos OS on MX Series: 16.1 versions prior to 16.1R7-S5; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R3-S6 ; 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S3; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0065</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os_mx_series	This issue only affects devices with three (3) or more MPC10's installed in a single chassis with OSPF enabled and configured on the device. An Insufficient Resource Pool weakness allows an attacker to cause the device's Open Shortest Path First (OSPF) states to transition to Down, resulting in a Denial of Service (DoS) attack. This attack requires a relatively large number of specific Internet Mixed (IMIXed) types of genuine and valid IPv6 packets to be transferred by the attacker in a relatively short period of time, across three or more PFE's on the device at the same time. Continued receipt of the traffic sent by the attacker will continue to cause OSPF to remain in the Down starting state, or flap between other states and then again to Down, causing a	2019-10-09	not yet calculated	<a href="#">CVE-2019-0056</a> <a href="#">MISC</a>



	<p>persistent Denial of Service. This attack will affect all IPv4, and IPv6 traffic served by the OSPF routes once the OSPF states transition to Down. This issue affects: Juniper Networks Junos OS on MX480, MX960, MX2008, MX2010, MX2020: 18.1 versions prior to 18.1R2-S4, 18.1R3-S5; 18.1X75 version 18.1X75-D10 and later versions; 18.2 versions prior to 18.2R1-S5, 18.2R2-S3, 18.2R3; 18.2X75 versions prior to 18.2X75-D50; 18.3 versions prior to 18.3R1-S4, 18.3R2, 18.3R3; 18.4 versions prior to 18.4R1-S2, 18.4R2.</p>			
juniper_networks -- junos_os_mx_series	<p>When an MX Series Broadband Remote Access Server (BRAS) is configured as a Broadband Network Gateway (BNG) with DHCPv6 enabled, jdhcpd might crash when receiving a specific crafted DHCP response message on a subscriber interface. The daemon automatically restarts without intervention, but continuous receipt of specific crafted DHCP messages will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue only affects systems configured with DHCPv6 enabled. DHCPv4 is unaffected by this issue. This issue affects Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S5 on MX Series; 16.1 versions prior to 16.1R7-S5 on MX Series; 16.2 versions prior to 16.2R2-S10 on MX Series; 17.1 versions prior to 17.1R3-S1 on MX Series; 17.2 versions prior to 17.2R3-S2 on MX Series; 17.3 versions prior to 17.3R3-S6 on MX Series; 17.4 versions prior to 17.4R2-S5, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S6 on MX Series; 18.2 versions prior to 18.2R2-S4, 18.2R3 on MX Series; 18.2X75 versions prior to 18.2X75-D50 on MX Series; 18.3 versions prior to 18.3R1-S5, 18.3R3 on MX Series; 18.4 versions prior to 18.4R2 on MX Series; 19.1 versions prior to 19.1R1-S2, 19.1R2 on MX Series.</p>	2019-10-09	not yet calculated	<a href="#">CVE-2019-0063</a> <a href="#">MISC</a>
juniper_networks -- junos_os_nfx_series	<p>An Improper Input Validation weakness allows a malicious local attacker to elevate their permissions to take control of other portions of the NFX platform they should not be able to access, and execute commands outside their authorized scope of control. This leads to the attacker being able to take control of the entire system. This issue affects: Juniper Networks Junos OS versions prior to 18.2R1 on NFX Series.</p>	2019-10-09	not yet calculated	<a href="#">CVE-2019-0070</a> <a href="#">MISC</a>
juniper_networks -- junos_os_nfx_series	<p>An improper authorization weakness in Juniper Networks Junos OS allows a local authenticated attacker to bypass regular security controls to access the Junos Device Manager (JDM) application and take control of the system. This issue affects: Juniper Networks Junos OS versions prior to 18.2R1, 18.2X75-D5.</p>	2019-10-09	not yet calculated	<a href="#">CVE-2019-0057</a> <a href="#">MISC</a>
juniper_networks -- junos_os_srx1500_series	<p>Under certain heavy traffic conditions srpxfe process can crash and result in a denial of service condition for the SRX1500 device. Repeated crashes of the srpxfe can result in an extended denial of service condition. The SRX device may fail to forward traffic when this condition occurs. Affected releases are Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D170 on SRX1500; 17.3 versions prior to 17.3R3-S7 on SRX1500; 17.4 versions prior to 17.4R2-S8, 17.4R3 on SRX1500; 18.1 versions prior to 18.1R3-S8 on SRX1500; 18.2 versions prior to 18.2R3 on SRX1500; 18.3 versions prior to 18.3R2 on SRX1500; 18.4 versions prior to 18.4R2 on SRX1500.</p>	2019-10-09	not yet calculated	<a href="#">CVE-2019-0050</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os_srx5000_series	<p>On SRX5000 Series devices, if 'set security zones security-zone &lt;zone&gt; tcp-rst' is configured, the flowd process may crash when a specific TCP packet is received by the device and triggers a new session. The process restarts automatically. However, receipt of a constant stream of these TCP packets may result in an extended Denial of Service (DoS) condition on the device. This issue affects Juniper Networks Junos OS: 18.2R3 on SRX 5000 Series; 18.4R2 on SRX 5000 Series; 19.2R1 on SRX 5000 Series.</p>	2019-10-09	not yet calculated	<a href="#">CVE-2019-0064</a> <a href="#">MISC</a>
juniper_networks -- junos_os_srx5000_series	<p>SSL-Proxy feature on SRX devices fails to handle a hardware resource limitation which can be exploited by remote SSL/TLS servers to crash the flowd daemon. Repeated crashes of the flowd daemon can result in an extended denial of service condition. For this issue to occur, clients protected by the SRX device must initiate a connection to the malicious server. This issue affects: Juniper Networks Junos OS on SRX5000 Series: 12.3X48 versions prior to 12.3X48-D85; 15.1X49 versions prior to 15.1X49-D180; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2; 19.1 versions prior to 19.1R2.</p>	2019-10-09	not yet calculated	<a href="#">CVE-2019-0051</a> <a href="#">MISC</a>
	<p>A vulnerability in the SIP ALG packet processing service of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the device by sending specific types of valid</p>			

juniper_networks -- junos_os_srx_series	SIP traffic to the device. In this case, the flowd process crashes and generates a core dump while processing SIP ALG traffic. Continued receipt of these valid SIP packets will result in a sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D61, 12.3X48-D65 on SRX Series; 15.1X49 versions prior to 15.1X49-D130 on SRX Series; 17.3 versions prior to 17.3R3 on SRX Series; 17.4 versions prior to 17.4R2 on SRX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0055</a> <a href="#">MISC</a> <a href="#">MLIST</a>
juniper_networks -- junos_os_srx_series	The SRX flowd process, responsible for packet forwarding, may crash and restart when processing specific multicast packets. By continuously sending the specific multicast packets, an attacker can repeatedly crash the flowd process causing a sustained Denial of Service. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D90; 15.1X49 versions prior to 15.1X49-D180; 17.3 versions; 17.4 versions prior to 17.4R2-S5, 17.4R3; 18.1 versions prior to 18.1R3-S6; 18.2 versions prior to 18.2R2-S4, 18.2R3; 18.3 versions prior to 18.3R2-S1, 18.3R3; 18.4 versions prior to 18.4R2; 19.1 versions prior to 19.1R1-S1, 19.1R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0068</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os_srx_series	The flowd process, responsible for forwarding traffic in SRX Series services gateways, may crash and restart when processing specific transit IP packets through an IPSec tunnel. Continued processing of these packets may result in an extended Denial of Service (DoS) condition. This issue only occurs when IPSec tunnels are configured. Systems without IPSec tunnel configurations are not vulnerable to this issue. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D171, 15.1X49-D180 on SRX Series; 18.2 versions 18.2R2-S1 and later, prior to 18.2R3 on SRX Series; 18.4 versions prior to 18.4R2 on SRX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0060</a> <a href="#">MISC</a> <a href="#">MISC</a>
juniper_networks -- junos_os_srx_series	A vulnerability in the Veriexec subsystem of Juniper Networks Junos OS allowing an attacker to fully compromise the host system. A local authenticated user can elevate privileges to gain full control of the system even if they are specifically denied access to perform certain actions. This issue affects: Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D80 on SRX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0058</a> <a href="#">MISC</a>
juniper_networks -- junos_os_srx_series	An Improper Certificate Validation weakness in the SRX Series Application Identification (app-id) signature update client of Juniper Networks Junos OS allows an attacker to perform Man-in-the-Middle (MitM) attacks which may compromise the integrity and confidentiality of the device. This issue affects: Juniper Networks Junos OS 15.1X49 versions prior to 15.1X49-D120 on SRX Series devices. No other versions of Junos OS are affected.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0054</a> <a href="#">MISC</a> <a href="#">MISC</a>
juniper_networks -- sbr_carrier	An Unprotected Storage of Credentials vulnerability in the identity and access management certificate generation procedure allows a local attacker to gain access to confidential information. This issue affects: Juniper Networks SBR Carrier: 8.4.1 versions prior to 8.4.1R13; 8.5.0 versions prior to 8.5.0R4.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0072</a> <a href="#">MISC</a>
kaseva -- vsa_rmm	An issue was discovered in Kaseya VSA RMM through 9.5.0.22. When using the default configuration, the LAN Cache feature creates a local account FSAdminxxxxxxxx (e.g., FSAdmin123456789) on the server that hosts the LAN Cache and all clients that are assigned to a LAN Cache. This account is placed into the local Administrators group of all clients assigned to the LAN Cache. When the assigned client is a Domain Controller, the FSAdminxxxxxxxx account is created as a domain account and automatically added as a member of the domain BUILTIN\Administrators group. Using the well known Pass-the-Hash techniques, an attacker can use the same FSAdminxxxxxxxx hash from any LAN Cache client and pass this to a Domain Controller, providing administrative rights to the attacker on any Domain Controller. (Local account Pass-the-Hash mitigations do not protect domain accounts.)	2019-10-11	not yet calculated	<a href="#">CVE-2019-14510</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
kirona -- dynamic_resource_scheduling	An issue was discovered in Kirona Dynamic Resource Scheduling (DRS) 5.5.3.5. An unauthenticated user can access /osm/REGISTER.cmd (aka /osm_tiles/REGISTER.cmd) directly: it contains sensitive information about the database through the SQL queries within this batch file. This file exposes SQL database information such as database version, table name, column name, etc.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17503</a> <a href="#">MISC</a>
kirona -- dynamic_resource_scheduling	An issue was discovered in Kirona Dynamic Resource Scheduling (DRS) 5.5.3.5. A reflected Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script via the /osm/report/ password parameter.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17504</a> <a href="#">MISC</a>
knex.js -- knex.js	knex.js versions before 0.19.5 are vulnerable to SQL Injection attack. Identifiers are escaped incorrectly as part of the MSSQL	2019-10-	not yet	<a href="#">CVE-2019-</a>

	dialect, allowing attackers to craft a malicious query to the host DB.	08	calculated	<a href="#">10757 CONFIRM</a>
kramer -- viaware	Kramer VIAware 2.5.0719.1034 has Incorrect Access Control.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17124 MISC</a>
landing-cms -- landing-cms	An issue was discovered in Landing-CMS 0.0.6. There is a CSRF vulnerability that can change the admin's password via the password/ URI,	2019-10-12	not yet calculated	<a href="#">CVE-2019-17521 MISC</a>
laravel-bjyblog -- laravel-bjyblog	laravel-bjyblog 6.1.1 has XSS via a crafted URL.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17494 MISC</a>
libntlm -- libntlm	Libntlm through 1.5 relies on a fixed buffer size for tSmbNtlmAuthRequest, tSmbNtlmAuthChallenge, and tSmbNtlmAuthResponse read and write operations, as demonstrated by a stack-based buffer over-read in buildSmbNtlmAuthRequest in smbutil.c for a crafted NTLM request.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17455 MISC</a>
libtom_project -- libtomcrypt	In LibTomCrypt through 1.18.2, the der_decode_utf8_string function (in der_decode_utf8_string.c) does not properly detect certain invalid UTF-8 sequences. This allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) or read information from other memory locations via carefully crafted DER-encoded data.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17362 MISC MISC MLIST MISC</a>
libvips -- libvips	vips_foreign_load_gif_scan_image in foreign/gifload.c in libvips before 8.8.2 tries to access a color map before a DGifGetImageDesc call, leading to a use-after-free.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17534 MISC MISC MISC</a>
mantisbt -- mantisbt	MantisBT before 1.3.20 and 2.22.1 allows Post Authentication Command Injection, leading to Remote Code Execution.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15715 CONFIRM CONFIRM CONFIRM MISC CONFIRM CONFIRM</a>
mcafee -- endpoint_security	Code Injection vulnerability in EPSetup.exe in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to get their malicious code installed by the ENS installer via code injection into EPSetup.exe by an attacker with access to the installer.	2019-10-09	not yet calculated	<a href="#">CVE-2019-3652 CONFIRM</a>
mcafee -- endpoint_security	Improper access control vulnerability in Configuration tool in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to gain access to security configuration via unauthorized use of the configuration tool.	2019-10-09	not yet calculated	<a href="#">CVE-2019-3653 CONFIRM</a>
microsoft -- azure_app_service_on_azure_stack	An remote code execution vulnerability exists when Azure App Service/ Antares on Azure Stack fails to check the length of a buffer prior to copying memory to it. An attacker who successfully exploited this vulnerability could allow an unprivileged function run by the user to execute code in the context of NT AUTHORITY\SYSTEM thereby escaping the Sandbox. The security update addresses the vulnerability by ensuring that Azure App Service sanitizes user inputs., aka 'Azure App Service Remote Code Execution Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1372 MISC</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1371 MISC</a>
microsoft -- microsoft_dynamics_365	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1375 MISC</a>
microsoft -- microsoft_edge	An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory, aka 'Microsoft Edge based on Edge HTML Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1356 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege	2019-10-	not yet	<a href="#">CVE-2019-1342</a>

	Vulnerability'. This CVE ID is unique from CVE-2019-1315, CVE-2019-1339.	10	calculated	<a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows Hyper-V Network Switch on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1230</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows CloudStore improperly handles file Discretionary Access Control List (DACL), aka 'Microsoft Windows CloudStore Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1321</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1166</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that the Windows Code Integrity Module handles objects in memory, aka 'Windows Code Integrity Module Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1344</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1345.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1334</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when Windows Update Client fails to properly handle objects in memory, aka 'Windows Update Client Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1337</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1315, CVE-2019-1342.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1339</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1343, CVE-2019-1347.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1346</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when umpo.dll of the Power Service, improperly handles a Registry Restore Key function, aka 'Windows Power Service Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1341</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1346, CVE-2019-1347.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1343</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality, aka 'Windows Secure Boot Security Feature Bypass Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1368</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Microsoft IIS Server fails to check the length of a buffer prior to copying memory to it. An attacker who successfully exploited this vulnerability can allow an unprivileged function ran by the user to execute code in the context of NT AUTHORITY\SYSTEM escaping the Sandbox. The security update addresses the vulnerability by correcting how Microsoft IIS Server sanitizes web requests., aka 'Microsoft IIS Server Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1365</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1358.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1359</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1359.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1358</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1343, CVE-2019-1346.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1347</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1322.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1340</a> <a href="#">MISC</a>
microsoft -- windows_10_mobile	A security feature bypass vulnerability exists in Windows 10 Mobile when Cortana allows a user to access files and folders through the locked screen, aka 'Windows 10 Mobile Security	2019-10-10	not yet calculated	<a href="#">CVE-2019-1314</a> <a href="#">MISC</a>

	Feature Bypass Vulnerability'.			
microsoft -- windows_7_and_windows_server_2008	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1364.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1362</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_7_and_windows_server_2008	A security feature bypass vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLMv2 protection if a client is also sending LMv2 responses, aka 'Windows NTLM Security Feature Bypass Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1338</a> <a href="#">MISC</a>
microsoft -- windows_7_and_windows_server_2008	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1362.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1364</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_update_assistant	An elevation of privilege vulnerability exists in Windows 10 Update Assistant in the way it handles permissions. A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows 10 Update Assistant Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1378</a> <a href="#">MISC</a>
moxa -- edr_810	Moxa EDR 810, all versions 5.1 and prior, allows an unauthenticated attacker to be able to retrieve some log files from the device, which may allow sensitive information disclosure. Log files must have previously been exported by a legitimate user.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10963</a> <a href="#">MISC</a>
moxa -- edr_810	Moxa EDR 810, all versions 5.1 and prior, allows an authenticated attacker to abuse the ping feature to execute unauthorized commands on the router, which may allow an attacker to perform remote code execution.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10969</a> <a href="#">MISC</a>
netaddr_gem_for_ruby_on_rails -- netaddr_gem_for_ruby_on_rails	The netaddr gem before 2.0.4 for Ruby has misconfigured file permissions, such that a gem install may result in 0777 permissions in the target filesystem.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17383</a> <a href="#">MISC</a> <a href="#">MISC</a>
netapp -- clustered_data_ontap	Clustered Data ONTAP versions 9.0 and higher do not enforce hostname verification under certain circumstances making them susceptible to impersonation via man-in-the-middle attacks.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5506</a> <a href="#">CONFIRM</a>
netapp -- snapmanager_for_oracle	SnapManager for Oracle prior to version 3.4.2P1 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5507</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices allow unauthenticated access to critical .cgi and .htm pages via a substring ending with .jpg, such as by appending ?x=1.jpg to a URL. This affects MBR1515, MBR1516, DGN2200, DGN2200M, DGN23700, WNR2000v2, WNR3300, WNR3400, WNR3500, and WNR834Bv2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17373</a> <a href="#">MISC</a>
netgear -- multiple_devices	Certain NETGEAR devices allow remote attackers to disable all authentication requirements by visiting genieDisableLanChanged.cgi. The attacker can then, for example, visit MNU_accessPassword_recovered.html to obtain a valid new admin password. This affects AC1450, D8500, DC112A, JNDR3000, LG2200D, R4500, R6200, R6200v2, R6250, R6300, R6300v2, R6400, R6700, R6900P, R6900, R7000P, R7000, R7100LG, R7300, R7900, R8000, R8300, R8500, WGR614v10, WN2500RPv2, WNR3400v2, WNR3700v3, WNR4000, WNR4500, WNR4500v2, WNR1000, WNR1000v3, WNR3500L, and WNR3500L.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17372</a> <a href="#">MISC</a>
netsarang -- xftp	NetSarang XFTP Client 6.0149 and earlier version contains a buffer overflow vulnerability caused by improper boundary checks when copying file name from an attacker controlled FTP server. That leads attacker to execute arbitrary code by sending a crafted filename.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17320</a> <a href="#">MISC</a>
node-red -- node-red-dashboard	It is possible to inject JavaScript within node-red-dashboard versions prior to version 2.17.0 due to the ui_notification node accepting raw HTML by default.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10756</a> <a href="#">CONFIRM</a>
nvidia -- shield_tv	NVIDIA Shield TV Experience prior to v8.0.1, NVIDIA Tegra software contains a vulnerability in the bootloader, where it does not validate the fields of the boot image, which may lead to code execution, denial of service, escalation of privileges, and information disclosure.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5700</a> <a href="#">CONFIRM</a>
nvidia -- shield_tv	NVIDIA Shield TV Experience prior to v8.0.1, NVIDIA Tegra bootloader contains a vulnerability where the software performs an incorrect bounds check, which may lead to buffer overflow resulting in escalation of privileges and code execution. escalation of privileges, and information disclosure, code execution, denial of service, or escalation of privileges.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5699</a> <a href="#">CONFIRM</a>



open_information_security_foundation -- libhttp	In OISF LibHTTP before 0.5.31, as used in Suricata 4.1.4 and other products, an HTTP protocol parsing error causes the http_header signature to not alert on a response with a single \r\n ending.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17420</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openbsd -- openssl	OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and remote code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.	2019-10-09	not yet calculated	<a href="#">CVE-2019-16905</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
openstack_project -- openstack_octavia	Amphora Images in OpenStack Octavia >=0.10.0 <2.1.2, >=3.0.0 <3.2.0, >=4.0.0 <4.1.0 allows anyone with access to the management network to bypass client-certificate based authentication and retrieve information or issue configuration commands via simple HTTP requests to the Agent on port https/9443, because the cmd/agent.py unicorn cert_reqs option is True but is supposed to be ssl.CERT_REQUIRED.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17134</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
otcms -- otcms	OTCMS v3.85 has CSRF in the admin/member_deal.php Admin Panel page, leading to creation of a new management group account, as demonstrated by superadmin.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17369</a> <a href="#">MISC</a>
palo_alto_networks -- zingbox_inspector	The SSH service is enabled on the Zingbox Inspector versions 1.294 and earlier, exposing SSH to the local network. When combined with PAN-SA-2019-0027, this can allow an attacker to authenticate to the service using hardcoded credentials.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15017</a> <a href="#">MISC</a>
palo_alto_networks -- zingbox_inspector	In the Zingbox Inspector, versions 1.294 and earlier, hardcoded credentials for root and inspector user accounts are present in the system software, which can result in unauthorized users gaining access to the system.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15015</a> <a href="#">MISC</a>
prettyphoto -- prettyphoto	prettyPhoto before 3.1.6 has jquery.prettyPhoto.js XSS.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9478</a> <a href="#">MISC</a> <a href="#">MISC</a>
python -- python	library/glob.html in the Python 2 and 3 documentation before 2016 has potentially misleading information about whether sorting occurs, as demonstrated by irreproducible cancer-research results. NOTE: the effects of this documentation cross application domains, and thus it is likely that security-relevant code elsewhere is affected. This issue is not a Python implementation bug, and there are no reports that NMR researchers were specifically relying on library/glob.html. In other words, because the older documentation stated "finds all the pa hnames matching a specified pattern according to the rules used by the Unix shell," one might have incorrectly inferred that the sorting that occurs in a Unix shell also occurred for glob.glob. There is a workaround in newer versions of Willoughby nmr-data_compilation-p2.py and nmr-data_compilation-p3.py, which call sort() directly.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17514</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
redhat -- ansible	Ansible, all ansible_engine-2.x versions and ansible_engine-3.x up to ansible_engine-3.5, was logging at the DEBUG level which lead to a disclosure of credentials if a plugin used a library that logged credentials at the DEBUG level. This flaw does not affect Ansible modules, as those are executed in a separate process.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14846</a> <a href="#">CONFIRM</a>
redhat -- openshift	A vulnerability was found in OpenShift builds, versions 4.1 up to 4.3. Builds that extract source from a container image, bypass the TLS hostname verification. An attacker can take advantage of this flaw by launching a man-in-the-middle attack and injecting malicious content.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14845</a> <a href="#">CONFIRM</a>
riot -- riot	In RIOT 2019.07, the MQTT-SN implementation (asymcute) mishandles errors occurring during a read operation on a UDP socket. The receive loop ends. This allows an attacker (via a large packet) to prevent a RIOT MQTT-SN client from working until the device is restarted.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17389</a> <a href="#">MISC</a>
	An issue was discovered in Rsyslog v8.1908.0. contrib/pmaixforwardedfrom/pmaixforwardedfrom.c has a heap overflow in the parser for AIX log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon)			

rsyslog -- rsyslog	but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.	2019-10-07	not yet calculated	<a href="#">CVE-2019-17041</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
samsung -- laser_printers	A potential security vulnerability has been identified with Samsung Laser Printers. This vulnerability could potentially be exploited to create a denial of service.	2019-10-11	not yet calculated	<a href="#">CVE-2019-6335</a> <a href="#">CONFIRM</a>
samsung -- multiple_p_phones	On certain Samsung P(9.0) phones, an attacker with physical access can start a TCP Dump capture without the user's knowledge. This feature of the Service Mode application is available after entering the *#9900# check code, but is protected by an OTP password. However, this password is created locally and (due to mishandling of cryptography) can be obtained easily by reversing the password creation logic.	2019-10-09	not yet calculated	<a href="#">CVE-2019-11341</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- customer_relationship_management	SAP Customer Relationship Management (Email Management), versions: S4CRM before 1.0 and 2.0, BBPCRM before 7.0, 7.01, 7.02, 7.12, 7.13 and 7.14, does not sufficiently encode user-controlled inputs within the mail client resulting in Cross-Site Scripting vulnerability.	2019-10-08	not yet calculated	<a href="#">CVE-2019-0368</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- landscape_management_enterprise_edition	Under certain conditions, SAP Landscape Management enterprise edition, before version 3.0, allows custom secure parameters? default values to be part of the application logs leading to Information Disclosure.	2019-10-08	not yet calculated	<a href="#">CVE-2019-0380</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- process_integration	SAP Process Integration, business-to-business add-on, versions 1.0, 2.0, does not perform authentication check properly when the default security provider is changed to BouncyCastle (BC), leading to Missing Authentication Check	2019-10-08	not yet calculated	<a href="#">CVE-2019-0379</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- sql_anywhere	A binary planing in SAP SQL Anywhere, before version 17.0, SAP IQ, before version 16.1, and SAP Dynamic Tier, before versions 1.0 and 2.0, can result in the inadvertent access of files located in directories outside of the paths specified by the user.	2019-10-08	not yet calculated	<a href="#">CVE-2019-0381</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
siemens -- multiple_products	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All versions), SIMATIC CFU PA (All versions < V1.2.0), SIMATIC ET 200AL (All versions), SIMATIC ET 200M (All versions), SIMATIC ET 200MP IM 155-5 PN BA (All versions < V4.2.3), SIMATIC ET 200MP IM 155-5 PN HF (All versions), SIMATIC ET 200MP IM 155-5 PN ST (All versions), SIMATIC ET 200S (All versions), S MATIC ET 200SP IM 155-6 PN BA (All versions), SIMATIC ET 200SP IM 155-6 PN HA (All versions), SIMATIC ET 200SP IM 155-6 PN HF (All versions < V4.2.2), SIMATIC ET 200SP IM 155-6 PN HS (All versions), SIMATIC ET 200SP IM 155-6 PN ST (All versions), SIMATIC ET 200SP IM 155-6 PN/2 HF (All versions < V4.2.2), SIMATIC ET 200SP IM 155-6 PN/3 HF (All versions < V4.2.1), SIMATIC ET 200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0) (All versions), SIMATIC ET 200pro (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI KTP Mobile Panels (All versions), SIMATIC PN/PN Coupler (All versions), SIMATIC PROFINET Driver (All versions < V2.1), SIMATIC S7-1200 CPU family (incl. F) (All versions), SIMATIC S7-1500 CPU family (incl. F) (All versions < V2.0), SIMATIC S7-300 CPU family (incl. F) (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-400 V6 (incl F) and below (All versions), SIMATIC S7-400H V6 (All versions < V6.0.9), S MATIC S7-410 V8 (All versions), SIMATIC WinAC RTX (F) 2010 (All versions < SIMATIC WinAC RTX 2010 SP3), SINAMICS DCM (All versions < V1.5 HF1), SINAMICS DCP (All versions), SINAMICS G110M V4.7 (PN Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G120 V4.7 (PN Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G130 V4.7 (Control Unit) (All versions), SINAMICS G150 (Control Unit) (All versions), SINAMICS GH150 V4.7 (Control Unit) (All versions), SINAMICS GL150 V4.7 (Control Unit) (All versions), SINAMICS GM150 V4.7 (Control Unit) (All versions), SINAMICS S110 (Control Unit) (All versions), SINAMICS S120 V4.7 (Control Unit) (All versions), SINAMICS S150 (Control Unit) (All versions), SINAMICS SL150 V4.7 (Control Unit) (All versions), SINAMICS SM120 V4.7 (Control	2019-10-10	not yet calculated	<a href="#">CVE-2019-10936</a> <a href="#">CONFIRM</a>

	Unit) (All versions), SINUMERIK 828D (All versions < V4.8 SP5), SINUMERIK 840D sl (All versions). Affected devices contain a vulnerability that allows an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large amount of specially crafted UDP packets are sent to device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- multiple_products	A vulnerability has been identified in CP1604 (All versions < V2.8), CP1616 (All versions < V2.8), Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions < V4.1.1 Patch 05), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All versions < V4.5.0 Patch 01), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All versions < V4.5.0), SCALANCE X-200IRT (All versions < V5.2.1), SIMATIC ET 200M (All versions), SIMATIC ET 200S (All versions), SIMATIC ET 200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0) (All versions), SIMATIC ET 200pro (All versions), SIMATIC PN/PN Coupler 6ES7158-3AD01-0XA0 (All versions), SIMATIC S7-300 CPU family (incl. F) (All versions), SIMATIC S7-400 (incl. F) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC WinAC RTX (F) 2010 (All versions < SIMATIC WinAC RTX 2010 SP3), SIMOTION (All versions), SINAMICS DCM (All versions < V1.5 HF1), SINAMICS DCP (All versions), SINAMICS G110M V4.7 (Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G120 V4.7 (Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G130 V4.7 (Control Unit) (All versions < V4.7 HF29), SINAMICS G150 (Control Unit) (All versions < V4.8), SINAMICS GH150 V4.7 (Control Unit) (All versions), SINAMICS GL150 V4.7 (Control Unit) (All versions), SINAMICS GM150 V4.7 (Control Unit) (All versions), SINAMICS S110 (Control Unit) (All versions), SINAMICS S120 V4.7 (Control Unit and CBE20) (All versions < V4.7 HF34), SINAMICS S150 (Control Unit) (All versions < V4.8), SINAMICS SL150 V4.7 (Control Unit) (All versions), SINAMICS SM120 V4.7 (Control Unit) (All versions), SINUMERIK 828D (All versions < V4.8 SP5), SINUMERIK 840D sl (All versions). An attacker with network access to an affected product may cause a Denial-of-Service condition by breaking the real-time synchronization (IRT) of the affected installation. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected installation. No user interaction is required to exploit this security vulnerability. The vulnerability impacts the availability of the affected installations.	2019-10-10	not yet calculated	<a href="#">CVE-2019-10923</a> <a href="#">CONFIRM</a>
siemens -- simatic_it_uadm	A vulnerability has been identified in SIMATIC IT UADM (All versions < V1.3). An authenticated remote attacker with network access to port 1434/tcp of SIMATIC IT UADM could potentially recover a password that can be used to gain read and write access to the related TeamCenter station. The security vulnerability could be exploited only if the attacker is authenticated. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises the confidentiality of the targeted system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2019-10-10	not yet calculated	<a href="#">CVE-2019-13929</a> <a href="#">CONFIRM</a>
siemens -- simatic_winac_rtx_(f)_2010	A vulnerability has been identified in SIMATIC WinAC RTX (F) 2010 (All versions). Affected versions of the software contain a vulnerability that could allow an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large HTTP request is sent to the executing service. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the service provided by the software. At the time of advisory publication no public exploitation of this security vulnerability was known.	2019-10-10	not yet calculated	<a href="#">CVE-2019-13921</a> <a href="#">CONFIRM</a>
signal -- private_messenger	The Signal Private Messenger application before 4.47.7 for Android allows a caller to force a call to be answered, without callee user interaction, via a connect message. The existence of the call is noticeable to the callee; however, the audio channel may be open before the callee can block eavesdropping.	2019-10-04	not yet calculated	<a href="#">CVE-2019-17191</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sma_solar_technology -- sunny_webbox	An attacker could send a malicious link to an authenticated operator, which may allow remote attackers to perform actions with the permissions of the user on the Sunny WebBox Firmware	2019-10-	not yet	<a href="#">CVE-2019-</a>

	Version 1.6 and prior. This device uses IP addresses to maintain communication after a successful login, which would increase the ease of exploitation.	09	calculated	<a href="#">13529 MISC MISC</a>
socomec -- diris_a-40_devices	Password disclosure in the web interface on socomec DIRIS A-40 devices before 48250501 allows a remote attacker to get full access to a device via the /password.jsn URL.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15859 MISC FULLDISC MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate (SI, MB, 840D) firmware through 1.71.00.1225. A CGI script is vulnerable to command injection via a maliciously crafted form parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2019-15051 MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate SI 1.60.01. A maintenance script, that is executable via sudo, is vulnerable to file path injection. This enables the Attacker to write files with superuser privileges in specific locations.	2019-10-10	not yet calculated	<a href="#">CVE-2019-11526 MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate SI 1.60.01. A CGI script is vulnerable to command injection with a maliciously crafted url parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2019-11527 MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate SI 1.60.01. A system default path for executables is user writable.	2019-10-10	not yet calculated	<a href="#">CVE-2019-11528 MISC</a>
softland -- file_sharing_wizard	A Structured Exception Handler (SEH) based buffer overflow in File Sharing Wizard 1.5.0 26-8-2008 allows remote unauthenticated attackers to execute arbitrary code via the HTTP DELETE method, a similar issue to CVE-2019-16724 and CVE-2010-2331.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17415 MISC</a>
solarwinds -- dameware_mini_remote_client	The Solarwinds Dameware Mini Remote Client agent v12.1.0.89 supports smart card authentication which can allow a user to upload an executable to be executed on the DWRC.exe host. An unauthenticated, remote attacker can request smart card login and upload and execute an arbitrary executable run under the Local System account.	2019-10-08	not yet calculated	<a href="#">CVE-2019-3980 MISC</a>
sophos -- cyberoamos	A shell injection vulnerability on the Sophos Cyberoam firewall appliance with CyberoamOS before 10.6.6 MR-6 allows remote attackers to execute arbitrary commands via the Web Admin and SSL VPN consoles.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17059 CONFIRM MISC MISC</a>
swagger -- swagger_ui	A Cascading Style Sheets (CSS) injection vulnerability in Swagger UI before 3.23.11 allows attackers to use the Relative Path Overwrite (RPO) technique to perform CSS-based input field value exfiltration, such as exfiltration of a CSRF token value. In other words, this product intentionally allows the embedding of untrusted JSON data from remote servers, but it was not previously known that <style>@import within the JSON data was a functional attack method.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17495 MISC MISC</a>
syslog -- rsyslog	An issue was discovered in Rsyslog v8.1908.0. contrib/pmcisconames/pmcisconames.c has a heap overflow in the parser for Cisco log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon), but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.	2019-10-07	not yet calculated	<a href="#">CVE-2019-17042 CONFIRM CONFIRM</a>
tbeu -- matio	Mat_VarReadNextInfo4 in mat4.c in MATIO 1.5.17 omits a certain ' ' character, leading to a heap-based buffer over-read in strdup_vprintf when uninitialized memory is accessed.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17533 MISC MISC</a>
tinytcl -- vino	tinytcl Vino through 2017-12-15 allows remote attackers to cause a denial of service ("vn_get_string error: Resource temporarily unavailable" error and daemon crash) via a long URL.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17414 MISC</a>
tracker_software -- pdf-xchange_editor	Tracker PDF-XChange Editor before 8.0.330.0 has an NTLM SSO hash theft vulnerability using crafted FDF or XFDF files (a	2019-10-	not yet	<a href="#">CVE-2019-</a>

	related issue to CVE-2018-4993). For example, an NTLM hash is sent for a link to \\192.168.0.2\C\$\file.pdf without user interaction.	10	calculated	<a href="#">17497 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the communication to the web service is unencrypted via http. An attacker is able to intercept and sniff communication to the web service.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17218 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. Password authentication uses MD5 to hash passwords. Cracking is possible with minimal effort.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17216 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no bruteforce protection (e.g., lockout) established. An attacker might be able to bruteforce the password to authenticate on the device.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17215 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no CSRF protection established on the web service.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17217 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the device does not enforce any authentication. An adjacent attacker is able to use the network interface without proper access control.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17219 MISC</a>
vmware -- multiple_products	ESXi, Workstation, Fusion, VMRC and Horizon Client contain a use-after-free vulnerability in the virtual sound device. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.5.	2019-10-10	not yet calculated	<a href="#">CVE-2019-5527 CONFIRM</a>
vmware -- workstation_and_fusion	VMware Workstation and Fusion contain a network denial-of-service vulnerability due to improper handling of certain IPv6 packets. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 4.7.	2019-10-10	not yet calculated	<a href="#">CVE-2019-5535 CONFIRM</a>
wordpress -- wordpress	The ThemeMakers Almera Responsive Portfolio theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9487 MISC</a>
wordpress -- wordpress	The ThemeMakers GamesTheme Premium theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9490 MISC</a>
wordpress -- wordpress	The ThemeMakers SmartIT Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9492 MISC</a>
wordpress -- wordpress	The buddypress-activity-plus plugin before 1.6.2 for WordPress has CSRF with resultant directory traversal via the wp-admin/admin-ajax.php bpfb_photos[] parameter in a bpfb_remove_temp_images action.	2019-10-07	not yet calculated	<a href="#">CVE-2015-9455 MISC</a>
wordpress -- wordpress	The history-collection plugin through 1.1.1 for WordPress has directory traversal via the download.php var parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9470 MISC</a>
wordpress -- wordpress	The pretty-link plugin before 1.6.8 for WordPress has PrliLinksController::list_links SQL injection via the group parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9457 MISC</a>
wordpress -- wordpress	The RobotCPA plugin 5 for WordPress has directory traversal via the f.php l parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9480 EXPLOIT-DB</a>
wordpress -- wordpress	The ACF-Frontend-Display plugin through 2015-07-03 for WordPress has arbitrary file upload via an action=upload request to js/blueimp-jQuery-File-Upload-d45deb1/server/php/index.php.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9479 MISC</a>
wordpress -- wordpress	The booking-system plugin before 2.1 for WordPress has DOPBSPBackEndTranslation: display SQL injection via the language parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9460 MISC</a>
				<a href="#">CVE-2015-9472</a>



wordpress -- wordpress	The incoming-links plugin before 0.9.10b for WordPress has referers.php XSS via the Referer HTTP header.	2019-10-10	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The wti-like-post plugin before 1.4.3 for WordPress has WtiLikePostProcessVote SQL injection via the HTTP_CLIENT_IP, HTTP_X_FORWARDED_FOR, HTTP_X_FORWARDED, HTTP_FORWARDED_FOR, or HTTP_FORWARDED variable.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9466</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The dzs-zoomsounds plugin through 2.0 for WordPress has admin/upload.php arbitrary file upload.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9471</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The s3bubble-amazon-s3-audio-streaming plugin 2.0 for WordPress has directory traversal via he adverts/assets/plugins/ultimate/content/downloader.php path parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9463</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The s3bubble-amazon-s3-html-5-video-with-adverts plugin 0.7 for WordPress has directory traversal via he adverts/assets/plugins/ultimate/content/downloader.php path parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9464</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
wordpress -- wordpress	The awesome-filterable-portfolio plugin before 1.9 for WordPress has afp_get_new_category_page SQL injection via the cat_id parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9462</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The content-grabber plugin 1.0 for WordPress has XSS via obj_field_name or obj_field_id.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9469</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The yet-another-stars-rating plugin before 0.9.1 for WordPress has yasr_get_multi_set_values_and_field SQL injection via the set_id parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Axioma Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9486</a> <a href="#">MISC</a>
wordpress -- wordpress	The estrutura-basica theme through 2015-09-13 for WordPress has directory traversal via the scripts/download.php arquivo parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9473</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Invento Responsive Gallery/Architecture Template component through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9483</a> <a href="#">MISC</a>
wordpress -- wordpress	The animate-it plugin before 2.3.6 for WordPress has CSRF in edsanimate.php.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17386</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Goodnex Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9489</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Almera Responsive Portfolio Site Template component through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9488</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Accio Responsive Parallax One Page Site Template component through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9485</a> <a href="#">MISC</a>
wordpress -- wordpress	The Simpolio theme 1.3.2 for WordPress has insufficient	2019-10-	not yet	<a href="#">CVE-2015-9474</a>

	restrictions on option updates.	10	calculated	<a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Accio One Page Parallax Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9484</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Car Dealer / Auto Dealer Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9482</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Diplomat   Political theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9481</a> <a href="#">MISC</a>
wordpress -- wordpress	The Vernissage theme 1.2.8 for WordPress has insufficient restrictions on option updates.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9477</a> <a href="#">MISC</a>
wordpress -- wordpress	The Teardrop theme 1.8.1 for WordPress has insufficient restrictions on option updates.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9476</a> <a href="#">MISC</a>
wordpress -- wordpress	The Pont theme 1.5 for WordPress has insufficient restrictions on option updates.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9475</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Blessing Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9491</a> <a href="#">MISC</a>
yealink -- multiple_phones	Yealink phones through 2019-08-04 do not properly check user roles in POST requests. Consequently, the default User account (with a password of user) can make admin requests via HTTP.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14656</a> <a href="#">MISC</a>
yealink -- multiple_phones	Yealink phones through 2019-08-04 have an issue with OpenVPN file upload. They execute tar as root to extract files, but do not validate the extraction directory. Creating a tar file with ../../../../ allows replacement of almost any file on a phone. This leads to password replacement and arbitrary code execution as root.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14657</a> <a href="#">MISC</a>
zabbix -- zabbix	An issue was discovered in zabbix.php? action=dashboard.view&dashboardid=1 in Zabbix through 4.4. An attacker can bypass the login page and access the dashboard page, and then create a Dashboard, Report, Screen, or Map without any Username/Password (i.e., anonymously). All created elements (Dashboard/Report/Screen/Map) are accessible by other users and by an admin.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17382</a> <a href="#">MISC</a>
zoho_manageengine -- datasecurity_plus	An issue was discovered in Zoho ManageEngine DataSecurity Plus before 5.0.1 5012. An exposed service allows a basic user ("Operator" access level) to access the configuration file of the mail server (except for the password).	2019-10-09	not yet calculated	<a href="#">CVE-2019-17112</a> <a href="#">MISC</a>
zyxel -- nbg-418n_router	wan.htm page on Zyxel NBG-418N v2 with firmware version V1.00(AARP.9)C0 can be accessed directly without authentication, which can lead to disclosure of information about the WAN, and can also be leveraged by an attacker to modify data fields of the page.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17354</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [lmoginnis@sunnyvale.ca.gov](mailto:lmoginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) - 245 Murray Lane SW Bldg 410  
Washington, DC 20508 - (888) 282-0870



**From:** US-CERT  
**To:** [wquitate@ci.sunnyvale.ca.us](mailto:wquitate@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of October 7, 2019  
**Date:** Tuesday, October 15, 2019 12:39:39 PM



National Cyber Awareness System:

## [Vulnerability Summary for the Week of October 7, 2019](#)

10/14/2019 06:33 AM EDT

Original release date: October 14, 2019 | Last revised: October 15, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adhouma_cms_project -- adhouma_cms	Adhouma CMS through 2019-10-09 has SQL Injection via the post.php p_id parameter.	2019-10-10	7.5	<a href="#">CVE-2019-17429</a> <a href="#">MISC</a>
awplife -- contact_form_widget	The new-contact-form-widget (aka Contact Form Widget - Contact Query, Form Maker) plugin 1.0.9 for WordPress has SQL Injection via all-query-page.php.	2019-10-10	7.5	<a href="#">CVE-2019-17072</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_vm	In Centreon VM through 19.04.3, centreon-backup.pl allows attackers to become root via a crafted script, due to incorrect rights of sourced configuration files.	2019-10-08	10.0	<a href="#">CVE-2018-21025</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML Jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.	2019-10-06	7.5	<a href="#">CVE-2019-17267</a> <a href="#">MISC</a> <a href="#">MISC</a>
fon -- fon2601e-fsw-b_firmware	FON2601E-SE, FON2601E-RE, FON2601E-FSW-S, and FON2601E-FSW-B with firmware versions 1.1.7 and earlier contain an issue where they may behave as open resolvers. If this vulnerability is exploited, FON routers may be leveraged for DNS amplification attacks to some other entities.	2019-10-04	7.8	<a href="#">CVE-2019-6015</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- libsoup	libsoup from versions 2.65.1 until 2.68.1 have a heap-based buffer over-read because soup_ntlm_parse_challenge() in soup-auth-ntlm.c does not properly check an NTLM message's length before proceeding with a memcpy.	2019-10-06	7.5	<a href="#">CVE-2019-17266</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a> <a href="#">MISC</a>
ibm -- mq	IBM MQ 8.0.0.4 - 8.0.0.12, 9.0.0.0 - 9.0.0.6, 9.1.0.0 - 9.1.0.2, and 9.1.0 - 9.1.2 AMQP Listeners could allow an unauthorized user to conduct a session fixation attack due to clients not being disconnected as they should. IBM X-Force ID: 159352.	2019-10-04	7.5	<a href="#">CVE-2019-4227</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_scale	A security vulnerability has been identified in all levels of IBM Spectrum Scale V5.0.0.0 through V5.0.3.2 and IBM Spectrum Scale V4.2.0.0 through V4.2.3.17 that could allow a local attacker to obtain root privilege by injecting parameters into setuid files.	2019-10-09	7.2	<a href="#">CVE-2019-4558</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
intelliantech -- remote_access	Intellian Remote Access 3.18 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the Ping Test field.	2019-10-06	10.0	<a href="#">CVE-2019-17269</a> <a href="#">MISC</a>
k-78 -- broken_link_manager	The broken-link-manager plugin before 0.5.0 for WordPress has wpstDelURL or wpstEditURL SQL injection via the url parameter.	2019-10-10	7.5	<a href="#">CVE-2015-9467</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/wireless/wext-sme.c does not reject a long SSID IE, leading to a	2019-10-04	7.5	<a href="#">CVE-2019-17133</a>

	Buffer Overflow.			<a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1308, CVE-2019-1335, CVE-2019-1366.	2019-10-10	<a href="#">7.6</a>	<a href="#">CVE-2019-1307</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1335, CVE-2019-1366.	2019-10-10	<a href="#">7.6</a>	<a href="#">CVE-2019-1308</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1366.	2019-10-10	<a href="#">7.6</a>	<a href="#">CVE-2019-1335</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1307, CVE-2019-1308, CVE-2019-1335.	2019-10-10	<a href="#">7.6</a>	<a href="#">CVE-2019-1366</a> <a href="#">MISC</a>
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1331.	2019-10-10	<a href="#">9.3</a>	<a href="#">CVE-2019-1327</a> <a href="#">MISC</a>
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1327.	2019-10-10	<a href="#">9.3</a>	<a href="#">CVE-2019-1331</a> <a href="#">MISC</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1239.	2019-10-10	<a href="#">7.1</a>	<a href="#">CVE-2019-1238</a> <a href="#">MISC</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'VBScript Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1238.	2019-10-10	<a href="#">7.6</a>	<a href="#">CVE-2019-1239</a> <a href="#">MISC</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.	2019-10-10	<a href="#">9.3</a>	<a href="#">CVE-2019-1060</a> <a href="#">MISC</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Imaging API improperly handles objects in memory, aka 'Windows Imaging API Remote Code Execution Vulnerability'.	2019-10-10	<a href="#">9.3</a>	<a href="#">CVE-2019-1311</a> <a href="#">MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1339, CVE-2019-1342.	2019-10-10	<a href="#">7.2</a>	<a href="#">CVE-2019-1315</a> <a href="#">MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in Microsoft Windows Setup when it does not properly handle privileges, aka 'Microsoft Windows Setup Elevation of Privilege Vulnerability'.	2019-10-10	<a href="#">7.2</a>	<a href="#">CVE-2019-1316</a> <a href="#">MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in Windows Error Reporting (WER) when WER handles and executes files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.	2019-10-10	<a href="#">7.2</a>	<a href="#">CVE-2019-1319</a> <a href="#">MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1336.	2019-10-10	<a href="#">7.2</a>	<a href="#">CVE-2019-1323</a> <a href="#">MISC</a>
microsoft -- windows_10	A denial of service vulnerability exists in Remote Desktop Protocol (RDP) when an attacker connects to the target system using RDP and sends specially crafted requests, aka 'Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability'.	2019-10-10	<a href="#">7.8</a>	<a href="#">CVE-2019-1326</a> <a href="#">MISC</a>
microsoft -- windows_10	A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server, aka 'Remote Desktop Client Remote Code Execution Vulnerability'.	2019-10-10	<a href="#">9.3</a>	<a href="#">CVE-2019-1333</a> <a href="#">MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in the Microsoft Windows Update Client when it does not properly handle privileges, aka 'Microsoft Windows Update Client Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1323.	2019-10-10	<a href="#">7.2</a>	<a href="#">CVE-2019-1336</a> <a href="#">MISC</a>
nex-forms - _ultimate_form_builder_project -- nex-forms - _ultimate_form_builder	The nex-forms-express-wp-form-builder plugin before 4.6.1 for WordPress has SQL injection via the wp-admin/admin.php?page=nex-forms-main nex_forms_id parameter.	2019-10-07	<a href="#">7.5</a>	<a href="#">CVE-2015-9452</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
open-emr -- openemr	OpenEMR through 5.0.2 has SQL Injection in the Lifestyle demographic filter criteria in library/clinical_rules.php that affects library/patient.inc.	2019-10-05	<a href="#">7.5</a>	<a href="#">CVE-2019-17197</a> <a href="#">MISC</a> <a href="#">MISC</a>
	PC Protect Antivirus v4.14.31 installs by default to			



pcprotect -- antivirus	%PROGRAMFILES(X86)%\PCProtect with very weak folder permissions, granting any user full permission "Everyone: (F)" to the contents of the directory and its subfolders. In addition, the program installs a service called SecurityService that runs as LocalSystem. This allows any user to escalate privileges to "NT AUTHORITY\SYSTEM" by substituting the service's binary with a Trojan horse.	2019-10-07	7.2	<a href="#">CVE-2019-16913</a> <a href="#">MISC</a>
signal -- signal_private_messenger	<b>** DISPUTED **</b> The WebRTC component in the Signal Private Messenger application through 4.47.7 for Android processes videoconferencing RTP packets before a callee chooses to answer a call, which might make it easier for remote attackers to cause a denial of service or possibly have unspecified other impact via malformed packets. NOTE: the vendor plans to continue this behavior for performance reasons unless a WebRTC design change occurs.	2019-10-04	7.5	<a href="#">CVE-2019-17192</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sitos -- sitos_six	SITOS six Build v6.2.1 allows an attacker to inject arbitrary PHP commands. As a result, an attacker can compromise the running server and execute system commands in the context of the web user.	2019-10-07	10.0	<a href="#">CVE-2019-15746</a> <a href="#">MISC</a>
sitos -- sitos_six	SITOS six Build v6.2.1 permits unauthorised users to upload and import a SCORM 2004 package by browsing directly to affected pages. An unauthenticated attacker could use the upload and import functionality to import a malicious SCORM package that includes a PHP file, which could execute arbitrary PHP code.	2019-10-07	7.5	<a href="#">CVE-2019-15748</a> <a href="#">MISC</a>
sitos -- sitos_six	An unrestricted file upload vulnerability in SITOS six Build v6.2.1 allows remote attackers to execute arbitrary code by uploading a SCORM file with an executable extension. This allows an unauthenticated attacker to upload a malicious file (containing PHP code to execute operating system commands) to the web root of the application.	2019-10-07	10.0	<a href="#">CVE-2019-15751</a> <a href="#">MISC</a>
sizmic -- plugmatter_optin_feature_box	The plugmatter-optin-feature-box-lite plugin before 2.0.14 for WordPress has SQL injection via the wp-admin/admin-ajax.php? action=pmfb_cc pmfb_tid parameter.	2019-10-07	7.5	<a href="#">CVE-2015-9450</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sizmic -- plugmatter_optin_feature_box	The plugmatter-optin-feature-box-lite plugin before 2.0.14 for WordPress has SQL injection via the wp-admin/admin-ajax.php? action=pmfb_mailchimp pmfb_tid parameter.	2019-10-07	7.5	<a href="#">CVE-2015-9451</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because of an incompatibility between Process Context Identifiers (PCID) and TLB flushes.	2019-10-07	7.2	<a href="#">CVE-2019-17346</a> <a href="#">MISC</a>
xerox -- atlalink_firmware	Xerox AtlaLink B8045/B8055/B8065/B8075/B8090 C8030/C8035/C8045/C8055/C8070 printers with software before 101.00x.089.22600 allow an attacker to gain privileges.	2019-10-04	7.5	<a href="#">CVE-2019-17184</a> <a href="#">MISC</a>
zingbox -- inspector	A command injection vulnerability exists in the Zingbox Inspector versions 1.286 and earlier, that allows for an authenticated user to execute arbitrary system commands in the CLI.	2019-10-09	9.0	<a href="#">CVE-2019-15014</a> <a href="#">MISC</a>
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector.	2019-10-09	7.5	<a href="#">CVE-2019-15019</a> <a href="#">MISC</a>
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.293 and earlier, that could allow an attacker to supply an invalid software update image to the Zingbox Inspector that could result in command injection.	2019-10-09	7.5	<a href="#">CVE-2019-15020</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- hadoop	In Apache Hadoop 3.1.0 to 3.1.1, 3.0.0-alpha1 to 3.0.3, 2.9.0 to 2.9.1, and 2.0.0-alpha to 2.8.4, the user/group information can be corrupted across storing in fsimage and reading back from fsimage.	2019-10-04	5.0	<a href="#">CVE-2018-11768</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
axiosys -- bento4	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListInspector::Action in Core/Ap4Descriptor.h, related to AP4_IodsAtom::InspectFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4dump.	2019-10-10	4.3	<a href="#">CVE-2019-17452</a> <a href="#">MISC</a>
	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListWriter::Action in Core/Ap4Descriptor.h,			<a href="#">CVE-2019-</a>

axiosys -- bento4	related to AP4_IodsAtom::WriteFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4encrypt or mp4compact.	2019-10-10	4.3	<a href="#">17453</a> <a href="#">MISC</a> <a href="#">MISC</a>
axiosys -- bento4	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_Descriptor::GetTag in Core/Ap4Descriptor.h, related to AP4_StsdAtom::GetSampleDescription in Core/Ap4StsdAtom.cpp, as demonstrated by mp4info.	2019-10-10	4.3	<a href="#">CVE-2019-17454</a> <a href="#">MISC</a>
bludit -- bludit	bl-kernel/security.class.php in Bludit 3.9.2 allows attackers to bypass a brute-force protection mechanism by using many different forged X-Forwarded-For or Client-IP HTTP headers.	2019-10-06	4.3	<a href="#">CVE-2019-17240</a> <a href="#">MISC</a> <a href="#">MISC</a>
brinidesigner -- awesome_filterable_portfolio	The awesome-filterable-portfolio plugin before 1.9 for WordPress has afp_get_new_portfolio_item_page SQL injection via the item_id parameter.	2019-10-10	6.5	<a href="#">CVE-2015-9461</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_vm	In Centreon VM through 19.04.3, the cookie configuration within the Apache HTTP Server does not protect against theft because the HTTPOnly flag is not set.	2019-10-08	5.0	<a href="#">CVE-2019-17104</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	In Centreon Web through 2.8.29, disclosure of external components' passwords allows authenticated attackers to move laterally to external components.	2019-10-08	4.0	<a href="#">CVE-2019-17106</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows API token credentials to persist after an account has been renamed or terminated (SEC-517).	2019-10-09	6.5	<a href="#">CVE-2019-17375</a> <a href="#">MISC</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in the SSL Certificate Upload interface (SEC-521).	2019-10-09	4.3	<a href="#">CVE-2019-17376</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in LiveAPI example scripts (SEC-524).	2019-10-09	4.3	<a href="#">CVE-2019-17377</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in the SSL Key Delete interface (SEC-526).	2019-10-09	4.3	<a href="#">CVE-2019-17378</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self stored XSS in the WHM SSL Storage Manager interface (SEC-527).	2019-10-09	4.3	<a href="#">CVE-2019-17379</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.15 allows self XSS in the WHM Update Preferences interface (SEC-528).	2019-10-09	4.3	<a href="#">CVE-2019-17380</a> <a href="#">MISC</a>
elementor -- elementor	The elementor-edit-template class in wp-admin/customize.php in the Elementor Pro plugin before 2.0.10 for WordPress has XSS.	2019-10-07	4.3	<a href="#">CVE-2018-18379</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
eleopard -- animate_it!	The animate-it plugin before 2.3.4 for WordPress has XSS.	2019-10-09	4.3	<a href="#">CVE-2019-17384</a> <a href="#">MISC</a> <a href="#">MISC</a>
eleopard -- animate_it!	The animate-it plugin before 2.3.5 for WordPress has XSS.	2019-10-09	4.3	<a href="#">CVE-2019-17385</a> <a href="#">MISC</a> <a href="#">MISC</a>
etoilewebdesign -- ultimate_faq	Functions/EWD_UFAQ_Import.php in the ultimate-faqs plugin through 1.8.24 for WordPress allows unauthenticated options import.	2019-10-07	5.0	<a href="#">CVE-2019-17232</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
etoilewebdesign -- ultimate_faq	Functions/EWD_UFAQ_Import.php in the ultimate-faqs plugin through 1.8.24 for WordPress allows HTML content injection.	2019-10-07	4.3	<a href="#">CVE-2019-17233</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	Exiv2 0.27.2 allows attackers to trigger a crash in Exiv2::getULong in types.cpp when called from Exiv2::Internal::CiffDirectory::readDirectory in crwimage_int.cpp, because there is no validation of the relationship of the total size to the offset and size.	2019-10-09	4.3	<a href="#">CVE-2019-17402</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-</a>

eyoucms -- eyoucms	EyouCms through 2019-07-11 has XSS related to the login.php web_recordnum parameter.	2019-10-10	<a href="#">4.3</a>	<a href="#">17430</a> <a href="#">MISC</a> <a href="#">MISC</a>
fastadmin -- fastadmin	An issue was discovered in fastadmin 1.0.0.20190705_beta. There is a public/index.php/admin/auth/admin/add CSRF vulnerability.	2019-10-10	<a href="#">6.8</a>	<a href="#">CVE-2019-17431</a> <a href="#">MISC</a>
fecmall -- fecmall	An unrestricted file upload vulnerability was discovered in catalog/productinfo/imageupload in Fecshop FecMall 2.3.4. An attacker can bypass a front-end restriction and upload PHP code to the webserver, by providing image data and the image/jpeg content type, with a .php extension. This occurs because the code relies on the getimagesize function.	2019-10-04	<a href="#">6.5</a>	<a href="#">CVE-2019-17188</a> <a href="#">MISC</a>
fiberhome -- hg2201t_firmware	/var/WEB-GUI/cgi-bin/downloadfile.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows pre-authentication Directory Traversal for reading arbitrary files.	2019-10-08	<a href="#">5.0</a>	<a href="#">CVE-2019-17187</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8656.	2019-10-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13315</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8757.	2019-10-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13316</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of Calculate actions. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8759.	2019-10-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13317</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of the util.printf Javascript method. The application processes the %p parameter in the format string, allowing heap addresses to be returned to the script. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8544.	2019-10-04	<a href="#">4.3</a>	<a href="#">CVE-2019-13318</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA forms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8669.	2019-10-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13319</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8814.	2019-10-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13320</a> <a href="#">MISC</a> <a href="#">MISC</a>
	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.4.1.16828. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.			<a href="#">CVE-2019-</a>

foxitsoftware -- phantompdf	The specific flaw exists within the deleteItemAt method when processing AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8295.	2019-10-04	6.8	<a href="#">CVE-2019-6774</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the exportValues method within a AcroForm. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-8491.	2019-10-04	6.8	<a href="#">CVE-2019-6775</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- phantompdf	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.5.0.20723. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the removeField method when processing watermarks within AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-8801.	2019-10-04	6.8	<a href="#">CVE-2019-6776</a> <a href="#">MISC</a> <a href="#">MISC</a>
foxitsoftware -- reader	Foxit Reader before 9.7 allows an Access Violation and crash if insufficient memory exists.	2019-10-04	5.0	<a href="#">CVE-2019-17183</a> <a href="#">MISC</a>
freerdp -- freerdp	libfreerdp/codecs/region.c in FreeRDP through 1.1.x and 2.x through 2.0.0-rc4 has memory leaks because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.	2019-10-04	5.0	<a href="#">CVE-2019-17177</a> <a href="#">MISC</a> <a href="#">MISC</a>
freerdp -- freerdp	HuffmanTree_makeFromFrequencies in lodepng.c in LodePNG through 2019-09-28, as used in WinPR in FreeRDP and other products, has a memory leak because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.	2019-10-04	5.0	<a href="#">CVE-2019-17178</a> <a href="#">MISC</a> <a href="#">MISC</a>
gonitro -- nitropdf	A specifically crafted jpeg2000 file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5045</a> <a href="#">MISC</a>
gonitro -- nitropdf	A specifically crafted jpeg2000 file embedded in a PDF file can lead to a heap corruption when opening a PDF document in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5046</a> <a href="#">MISC</a>
gonitro -- nitropdf	An exploitable Use After Free vulnerability exists in the CharProcs parsing functionality of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a Use After Free. An attacker can craft a malicious PDF to trigger this vulnerability.	2019-10-09	6.8	<a href="#">CVE-2019-5047</a> <a href="#">MISC</a>
gonitro -- nitropdf	A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5048</a> <a href="#">MISC</a>
gonitro -- nitropdf	A specifically crafted PDF file can lead to a heap corruption when opened in NitroPDF 12.12.1.522. With careful memory manipulation, this can lead to arbitrary code execution. In order to trigger this vulnerability, the victim would need to open the malicious file.	2019-10-09	6.8	<a href="#">CVE-2019-5050</a> <a href="#">MISC</a>
gonitro -- nitropdf	An exploitable use-after-free vulnerability exists in the Length parsing function of NitroPDF. A specially crafted PDF can cause a type confusion, resulting in a use-after-free condition. An attacker can craft a malicious PDF to trigger this vulnerability.	2019-10-09	6.8	<a href="#">CVE-2019-5053</a> <a href="#">MISC</a>
hp -- arcsight_logger	Unrestricted file upload vulnerability in Micro Focus ArcSight Logger, version 6.7.0 and later. This vulnerability could allow Unrestricted Upload of File with Dangerous type.	2019-10-04	6.5	<a href="#">CVE-2019-11655</a> <a href="#">MISC</a>
ibm -- control_desk	IBM Maximo Asset Management 7.6.1.1 generates an error message that includes sensitive information that could be	2019-10-	4.0	<a href="#">CVE-2019-4512</a>

	used in further attacks against the system. IBM X-Force ID: 164554.	09		<a href="#">XE CONFIRM</a>
ibm -- security_key_lifecycle_manager	IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 165136.	2019-10-04	<a href="#">5.0</a>	<a href="#">CVE-2019-4514</a> <a href="#">XE CONFIRM</a>
ibm -- security_key_lifecycle_manager	IBM Security Key Lifecycle Manager 2.6, 2.7, 3.0, and 3.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2019-10-04	<a href="#">4.3</a>	<a href="#">CVE-2019-4564</a> <a href="#">XE CONFIRM</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000d563.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17241</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000966f.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17242</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control Code Flow starting at JPEG_LS+0x0000000000003155.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17243</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control Code Flow starting at JPEG_LS+0x0000000000001d8a.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17244</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x0000000000004359.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17245</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000258c.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17246</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at JPEG_LS+0x00000000000007da8.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17247</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x00000000000025b6.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17248</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000d57b.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17249</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at WSQ!ReadWSQ+0x000000000000042f5.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17250</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!GetPlugInInfo+0x00000000000007d43.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17251</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at FORMATS!Read_BadPNG+0x0000000000000115.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17252</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at JPEG_LS+0x000000000000a6b8.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17253</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at FORMATS!Read_BadPNG+0x00000000000000101.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17254</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at EXR!ReadEXR+0x00000000000010836.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17255</a> <a href="#">MISC MISC</a>
irfanview -- irfanview	IrfanView 4.53 allows a User Mode Write AV starting at DPX!ReadDPX_W+0x0000000000001203.	2019-10-08	<a href="#">6.8</a>	<a href="#">CVE-2019-17256</a> <a href="#">MISC</a>



				MISC
irfanview -- irfanview	IrfanView 4.53 allows a Exception Handler Chain to be Corrupted starting at EXR!ReadEXR+0x000000000002af80.	2019-10-08	4.3	<a href="#">CVE-2019-17257</a> MISC
irfanview -- irfanview	IrfanView 4.53 allows Data from a Faulting Address to control a subsequent Write Address starting at JPEG_LS+0x000000000000839c.	2019-10-08	6.8	<a href="#">CVE-2019-17258</a> MISC
jnoj -- jiangnan_online_judge	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[title] parameter to web/polygon/problem/create or web/polygon/problem/update or web/admin/problem/create.	2019-10-10	4.3	<a href="#">CVE-2019-17489</a> MISC
jnoj -- jiangnan_online_judge	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[description] parameter to web/admin/problem/create or web/polygon/problem/update.	2019-10-10	4.3	<a href="#">CVE-2019-17491</a> MISC
jnoj -- jiangnan_online_judge	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[sample_input] parameter to web/admin/problem/create or web/polygon/problem/update.	2019-10-10	4.3	<a href="#">CVE-2019-17493</a> MISC
joyplus-cms_project -- joyplus-cms	joyplus-cms 1.6.0 allows manager/admin_pic.php?rootpa h= absolute path traversal.	2019-10-04	5.0	<a href="#">CVE-2019-17175</a> MISC
k-78 -- broken_link_manager	The broken-link-manager plugin before 0.6.0 for WordPress has XSS via the HTTP Referer or User-Agent header to a URL hat does not exist.	2019-10-07	4.3	<a href="#">CVE-2015-9453</a> MISC
k-78 -- broken_link_manager	The broken-link-manager plugin 0.4.5 for WordPress has XSS via the page parameter in a delURL action.	2019-10-10	4.3	<a href="#">CVE-2015-9468</a> MISC
kmplayer -- kmplayer	KMPlayer 4.2.2.31 allows a User Mode Write AV starting at utils!src_new+0x000000000014d6ee.	2019-10-08	4.6	<a href="#">CVE-2019-17259</a> MISC
koji_project -- koji	Koji through 1.18.0 allows remote Directory Traversal, with resultant Privilege Escalation.	2019-10-09	4.0	<a href="#">CVE-2019-17109</a> MISC CONFIRM
liblnk_project -- liblnk	** DISPUTED ** In libyal liblnk before 20191006, liblnk_location_information_read_data in liblnk_location_information.c has a heap-based buffer over-read because an incorrect variable name is used for a certain offset. NOTE: the vendor has disputed this as described in the GitHub issue.	2019-10-06	6.8	<a href="#">CVE-2019-17264</a> MISC
libpng -- libpng	libpng 1.6.37 has memory leaks in png_malloc_warn and png_create_info_struct.	2019-10-09	4.3	<a href="#">CVE-2019-17371</a> MISC
liferay -- liferay_portal	Liferay Portal CE 6.2.5 allows remote command execution because of deserialization of a JSON payload.	2019-10-04	6.5	<a href="#">CVE-2019-16891</a> MISC
linux -- linux_kernel	An issue was discovered in drivers/xen/balloon.c in the Linux kernel before 5.2.3, as used in Xen through 4.12.x, allowing guest OS users to cause a denial of service because of unrestricted resource consumption during the mapping of guest memory, aka CID-6ef36ab967c7.	2019-10-07	4.9	<a href="#">CVE-2019-17351</a> MISC
lqd -- liquid_speech_balloon	The liquid-speech-balloon (aka LIQUID SPEECH BALLOON) plugin 1.0.5 for WordPress allows XSS with Internet Explorer.	2019-10-10	4.3	<a href="#">CVE-2019-17070</a> MISC
metinfo -- metinfo	An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/? n=language&c=language_general&a=doSearchParameter appno parameter, a different issue than CVE-2019-16997.	2019-10-09	6.5	<a href="#">CVE-2019-17418</a> MISC
metinfo -- metinfo	An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/? n=user&c=admin_user&a=doGetUserInfo id parameter.	2019-10-09	6.5	<a href="#">CVE-2019-17419</a> MISC
microsoft -- edge	A spoofing vulnerability exists when Microsoft Browsers does not properly parse HTTP content, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-1357.	2019-10-10	4.3	<a href="#">CVE-2019-0608</a> MISC
	A spoofing vulnerability exists when Microsoft Browsers			<a href="#">CVE-2019-</a>

microsoft -- edge	improperly handle browser cookies, aka 'Microsoft Browser Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0608.	2019-10-10	<a href="#">4.3</a>	<a href="#">1357 MISC</a>
microsoft -- open_enclave_software_development_kit	An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory, aka 'Open Enclave SDK Information Disclosure Vulnerability'.	2019-10-10	<a href="#">5.0</a>	<a href="#">CVE-2019-1369 MISC</a>
microsoft -- sharepoint_enterprise_server	An elevation of privilege vulnerability exists in Microsoft SharePoint, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1329.	2019-10-10	<a href="#">4.0</a>	<a href="#">CVE-2019-1330 MISC</a>
microsoft -- sql_server_management_studio	An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1376.	2019-10-10	<a href="#">4.0</a>	<a href="#">CVE-2019-1313 MISC</a>
microsoft -- sql_server_management_studio	An information disclosure vulnerability exists in Microsoft SQL Server Management Studio (SSMS) when it improperly enforces permissions, aka 'SQL Server Management Studio Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1313.	2019-10-10	<a href="#">4.0</a>	<a href="#">CVE-2019-1376 MISC</a>
microsoft -- windows_10	A denial of service vulnerability exists when Windows improperly handles hard links, aka 'Microsoft Windows Denial of Service Vulnerability'.	2019-10-10	<a href="#">5.6</a>	<a href="#">CVE-2019-1317 MISC</a>
microsoft -- windows_10	A spoofing vulnerability exists when Transport Layer Security (TLS) accesses non- Extended Master Secret (EMS) sessions, aka 'Microsoft Windows Transport Layer Security Spoofing Vulnerability'.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-1318 MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1322, CVE-2019-1340.	2019-10-10	<a href="#">4.6</a>	<a href="#">CVE-2019-1320 MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1340.	2019-10-10	<a href="#">4.6</a>	<a href="#">CVE-2019-1322 MISC</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in the Windows redirected drive buffering system (rdbss.sys) when the operating system improperly handles specific local calls within Windows 7 for 32-bit systems, aka 'Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability'.	2019-10-10	<a href="#">4.9</a>	<a href="#">CVE-2019-1325 MISC</a>
microsoft -- windows_7	An information disclosure vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Information Disclosure Vulnerability'.	2019-10-10	<a href="#">4.3</a>	<a href="#">CVE-2019-1361 MISC</a>
mpc-hc -- mpc-hc	MPC-HC through 1.7.13 allows a Read Access Violation on a Block Data Move starting at mpc_hc!memcpy+0x000000000000004e.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17260 MISC</a>
netreo -- omniscener	Netreo OmniCenter through 12.1.1 allows unauthenticated SQL Injection (Boolean Based Blind) in the redirect parameters and parameter name of the login page through a GET request. The injection allows an attacker to read sensitive information from the database used by the application.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-17128 MISC</a>
nixos -- nix	Nix through 2.3 allows local users to gain access to an arbitrary user's account because the parent directory of the user-profile directories is world writable.	2019-10-09	<a href="#">4.6</a>	<a href="#">CVE-2019-17365 MISC</a>
open-emr -- openemr	XSS in library/custom_template/add_template.php in OpenEMR through 5.0.2 allows a malicious user to execute code in the context of a victim's browser via a crafted list_id query parameter.	2019-10-04	<a href="#">4.3</a>	<a href="#">CVE-2019-17179 MISC</a>
openproject -- openproject	An XSS vulnerability in project list in OpenProject before 9.0.4 and 10.x before 10.0.2 allows remote attackers to inject arbitrary web script or HTML via the sortBy parameter because error messages are mishandled.	2019-10-09	<a href="#">4.3</a>	<a href="#">CVE-2019-17092 MISC</a>
orbisius -- child_theme_creator	The orbisius-child-theme-creator plugin before 1.2.8 for WordPress has incorrect access control for file modification via the wp-admin/admin-ajax.php? action=orbisius_ctc_theme_editor_ajax&sub_cmd=save_file theme_1, theme_1_file, or theme_1_file_contents parameter.	2019-10-07	<a href="#">4.0</a>	<a href="#">CVE-2015-9456 MISC</a>
	OTCMS v3.85 allows arbitrary PHP Code Execution because admin/sysCheckFile_deal.php blocks "into outfile" in a	2019-10-		<a href="#">CVE-2019-</a>

otcms -- otcms	SELECT statement, but does not block the "into/**/outfile" manipulation. Therefore, the attacker can create a .php file.	09	6.5	<a href="#">17370 MISC</a>
pi-hole -- pi-hole	Pi-Hole 4.3 allows Command Injection.	2019-10-09	6.8	<a href="#">CVE-2019-13051 MISC MISC MISC MISC</a>
python -- pillow	An issue was discovered in Pillow before 6.2.0. When reading specially crafted invalid image files, the library can either allocate very large amounts of memory or take an extremely long period of time to process the image.	2019-10-04	4.3	<a href="#">CVE-2019-16865 MISC</a>
realbigplugins -- client_dash	The client-dash (aka Client Dash) plugin 2.1.4 for WordPress allows XSS.	2019-10-10	4.3	<a href="#">CVE-2019-17071 MISC MISC</a>
redmine -- redmine	In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors.	2019-10-09	4.3	<a href="#">CVE-2019-17427 MISC</a>
s-cms -- s-cms	S-CMS v1.5 has XSS in tpl.php via the member/member_login.php from parameter.	2019-10-09	4.3	<a href="#">CVE-2019-17368 MISC</a>
sap -- financial_consolidation	Due to missing input validation, SAP Financial Consolidation, before versions 10.0 and 10.1, enables an attacker to use crafted input to interfere with the structure of the surrounding query leading to XPath Injection.	2019-10-08	6.4	<a href="#">CVE-2019-0370 MISC CONFIRM</a>
sap -- netweaver_process_integration	SAP NetWeaver Process Integration (B2B Toolkit), before versions 1.0 and 2.0, does not perform necessary authorization checks for an authenticated user, allowing the import of B2B table content that leads to Missing Authorization Check.	2019-10-08	4.0	<a href="#">CVE-2019-0367 MISC CONFIRM</a>
seo_searchterms_tagging_2_project -- seo_searchterms_tagging_2	The searchterms-tagging-2 plugin through 1.535 for WordPress has SQL injection via the pk_stt2_db_get_popular_terms count parameter exploitable via CSRF.	2019-10-10	6.5	<a href="#">CVE-2015-9458 MISC MISC</a>
seo_searchterms_tagging_2_project -- seo_searchterms_tagging_2	The searchterms-tagging-2 plugin through 1.535 for WordPress has XSS via the wp-admin/options-general.php count parameter.	2019-10-10	4.3	<a href="#">CVE-2015-9459 MISC MISC</a>
sitos -- sitos_six	SITOS six Build v6.2.1 allows a user with the user role of Seminar Coordinator to escalate their permission to the Systemadministrator role due to insufficient checks on the server side.	2019-10-07	6.5	<a href="#">CVE-2019-15747 MISC</a>
sitos -- sitos_six	SITOS six Build v6.2.1 allows a user to change their password and recovery email address without requiring them to confirm the change with their old password. This would allow an attacker with access to the victim's account (e.g., via XSS or an unattended workstation) to change that password and address.	2019-10-07	4.3	<a href="#">CVE-2019-15749 MISC</a>
sitos -- sitos_six	A Cross-Site Scripting (XSS) vulnerability in the blog function in SITOS six Build v6.2.1 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	2019-10-07	4.3	<a href="#">CVE-2019-15750 MISC</a>
slidervilla -- smooth_slider	The smooth-slider plugin before 2.7 for WordPress has SQL Injection via the wp-admin/admin.php?page=smooth-slider-admin current_slider_id parameter.	2019-10-07	6.5	<a href="#">CVE-2015-9454 MISC MISC MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by an Admin user.	2019-10-07	6.5	<a href="#">CVE-2019-17292 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Project module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17293 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the export function by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17294 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the history function by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17295 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Contacts module by a Regular user.	2019-10-07	6.5	<a href="#">CVE-2019-17296 MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL	2019-10-	6.5	<a href="#">CVE-2019-17297</a>

	injection in the Quotes module by a Regular user.	07		<a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Administration module by a Developer user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17298</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17299</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Administration module by a Developer user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17300</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the ModuleBuilder module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17301</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the ModuleBuilder module by a Developer user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17302</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by a Developer user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17303</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17304</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the MergeRecords module by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17305</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Configurator module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17306</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Tracker module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17307</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Emails module by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17308</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the EmailMan module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17309</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP code injection in the Campaigns module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17310</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the attachment function by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17311</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the file function by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17312</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the Studio module by a Developer user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17313</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows directory traversal in the Configurator module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17314</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Administration module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17315</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the Import module by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17316</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows PHP object injection in the UpgradeWizard module by an Admin user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17317</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the pmse_Inbox module by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17318</a> <a href="#">MISC</a>
sugarcrm -- sugarcrm	SugarCRM before 8.0.4 and 9.x before 9.0.2 allows SQL injection in the Emails module by a Regular user.	2019-10-07	<a href="#">6.5</a>	<a href="#">CVE-2019-17319</a> <a href="#">MISC</a>
suse -- suse_linux_enterprise_server	The /usr/sbin/pinger binary packaged with squid in SUSE Linux Enterprise Server 15 before and including version 4.8-5.8.1 and in SUSE Linux Enterprise Server 12 before and including 3.5.21-26.17.1 had squid:root, 0750 permissions. This allowed an attacker that compromised the squid user to	2019-10-07	<a href="#">6.6</a>	<a href="#">CVE-2019-3688</a> <a href="#">CONFIRM</a>

	gain persistence by changing the binary			
teampass -- teampass	TeamPass 2.1.27.36 allows Stored XSS by placing a payload in the username field during a login attempt. When an administrator looks at the log of failed logins, the XSS payload will be executed.	2019-10-05	<a href="#">4.3</a>	<a href="#">CVE-2019-17205</a> MISC
twitter -- twitter_kit	The Twitter Kit framework through 3.4.2 for iOS does not properly validate the api.twitter.com SSL certificate. Although the certificate chain must contain one of a set of pinned certificates, there are certain implementation errors such as a lack of hostname verification. NOTE: this is an end-of-life product.	2019-10-07	<a href="#">5.8</a>	<a href="#">CVE-2019-16263</a> MISC MISC MISC
vbulletin -- vbulletin	vBulletin through 5.5.4 mishandles external URLs within the /core/vb/vurl.php file and the /core/vb/vurl directories.	2019-10-04	<a href="#">6.4</a>	<a href="#">CVE-2019-17130</a> MISC
vbulletin -- vbulletin	vBulletin before 5.5.4 allows clickjacking.	2019-10-04	<a href="#">4.3</a>	<a href="#">CVE-2019-17131</a> MISC
vbulletin -- vbulletin	vBulletin through 5.5.4 mishandles custom avatars.	2019-10-04	<a href="#">6.8</a>	<a href="#">CVE-2019-17132</a> MISC FULL DISC MISC
vbulletin -- vbulletin	vBulletin 5.5.4 allows SQL Injection via the ajax/api/hook/getHookList or ajax/api/widget/getWidgetList where parameter.	2019-10-08	<a href="#">4.0</a>	<a href="#">CVE-2019-17271</a> MISC MISC
webarxsecurity -- webarx	The WebARX plugin 1.3.0 for WordPress has unauthenticated stored XSS via the URI or the X-Forwarded-For HTTP header.	2019-10-06	<a href="#">4.3</a>	<a href="#">CVE-2019-17213</a> MISC MISC
webarxsecurity -- webarx	The WebARX plugin 1.3.0 for WordPress allows firewall bypass by appending &cc=1 to a URI.	2019-10-06	<a href="#">5.0</a>	<a href="#">CVE-2019-17214</a> MISC
webpagetest -- webpagetest	www/getfile.php in WPO WebPageTest 19.04 on Windows allows Directory Traversal (for reading arbitrary files) because of an unanchored regular expression, as demonstrated by the a.jpg\.. substring.	2019-10-05	<a href="#">5.0</a>	<a href="#">CVE-2019-17199</a> MISC
wpfactory -- download_plugins_and_themes_from_dashboard	includes/settings/class-alg-download-plugins-settings.php in the download-plugins-dashboard plugin through 1.5.0 for WordPress has multiple unauthenticated stored XSS issues.	2019-10-07	<a href="#">4.3</a>	<a href="#">CVE-2019-17239</a> MISC MISC MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 guest OS users to cause a denial of service or gain privileges because grant-table transfer requests are mishandled.	2019-10-07	<a href="#">6.1</a>	<a href="#">CVE-2019-17340</a> MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging a page-writability race condition during addition of a passed-through PCI device.	2019-10-07	<a href="#">6.9</a>	<a href="#">CVE-2019-17341</a> MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging a race condition that arose when XENMEM_exchange was introduced.	2019-10-07	<a href="#">4.4</a>	<a href="#">CVE-2019-17342</a> MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges by leveraging incorrect use of the HVM physmap concept for PV domains.	2019-10-07	<a href="#">4.6</a>	<a href="#">CVE-2019-17343</a> MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service by leveraging a long-running operation that exists to support restartability of PTE updates.	2019-10-07	<a href="#">4.9</a>	<a href="#">CVE-2019-17344</a> MISC
xen -- xen	An issue was discovered in Xen 4.8.x through 4.11.x allowing x86 PV guest OS users to cause a denial of service because mishandling of failed IOMMU operations causes a bug check during the cleanup of a crashed guest.	2019-10-07	<a href="#">4.9</a>	<a href="#">CVE-2019-17345</a> MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service or gain privileges because a guest can manipulate its virtualised %cr4 in a way that is incompatible with Linux (and possibly other guest kernels).	2019-10-07	<a href="#">4.6</a>	<a href="#">CVE-2019-17347</a> MISC
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service because of an incompatibility between Process Context Identifiers (PCID) and shadow-pagetable switching.	2019-10-07	<a href="#">4.9</a>	<a href="#">CVE-2019-17348</a> MISC
	An issue was discovered in Xen through 4.12.x allowing Arm	2019-10-		<a href="#">CVE-2019-</a>



xen -- xen	domU attackers to cause a denial of service (infinite loop) involving a LoadExcl or StoreExcl operation.	07	<a href="#">4.9</a>	<a href="#">17349 MISC</a>
xen -- xen	An issue was discovered in Xen through 4.12.x allowing Arm domU attackers to cause a denial of service (infinite loop) involving a compare-and-exchange operation.	2019-10-07	<a href="#">4.9</a>	<a href="#">CVE-2019-17350 MISC</a>
xnview -- xnview	XnView Classic 2.49.1 allows a User Mode Write AV starting at Xwsq+0x0000000000001e51.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17261 MISC</a>
xnview -- xnview	XnView Classic 2.49.1 allows a User Mode Write AV starting at Xwsq+0x0000000000001fc0.	2019-10-08	<a href="#">4.6</a>	<a href="#">CVE-2019-17262 MISC</a>
zingbox -- inspector	An SQL injection vulnerability exists in the management interface of Zingbox Inspector versions 1.288 and earlier, that allows for unsanitized data provided by an authenticated user to be passed from the web UI into the database.	2019-10-09	<a href="#">6.5</a>	<a href="#">CVE-2019-15016 MISC</a>
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.280 and earlier, where authentication is not required when binding the Inspector instance to a different customer tenant.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15018 MISC</a>
zingbox -- inspector	A security vulnerability exists in the Zingbox Inspector versions 1.294 and earlier, that can allow an attacker to easily identify instances of Zingbox Inspectors in a local area network.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15021 MISC</a>
zingbox -- inspector	A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that allows for the Inspector to be susceptible to ARP spoofing.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15022 MISC</a>
zingbox -- inspector	A security vulnerability exists in Zingbox Inspector versions 1.294 and earlier, that results in passwords for 3rd party integrations being stored in cleartext in device configuration.	2019-10-09	<a href="#">5.0</a>	<a href="#">CVE-2019-15023 MISC</a>
zingbox -- inspector	A security vulnerability exists in Zingbox Inspector version 1.293 and earlier, that allows for remote code execution if the Inspector were sent a malicious command from the Zingbox cloud, or if the Zingbox Inspector were tampered with to connect to an attacker's cloud endpoint.	2019-10-09	<a href="#">6.8</a>	<a href="#">CVE-2019-1584 MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cmsmadesimple -- cms_made_simple	CMS Made Simple (CMSMS) 2.2.11 allows XSS via the Site Admin > Module Manager > Search Term field.	2019-10-06	<a href="#">3.5</a>	<a href="#">CVE-2019-17226 MISC</a>
hp -- arcsight_logger	Stored XSS vulnerability in Micro Focus ArcSight Logger, affects versions prior to Logger 6.7.1 HotFix 6.7.1.8262.0. This vulnerability could allow Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').	2019-10-04	<a href="#">3.5</a>	<a href="#">CVE-2019-11656 MISC</a>
hrworks -- hrworks	HRworks 3.36.9 allows XSS via the purpose of a travel-expense report.	2019-10-08	<a href="#">3.5</a>	<a href="#">CVE-2019-16416 MISC</a>
hrworks -- hrworks	HRworks FLOW 3.36.9 allows XSS via the purpose of a travel-expense report.	2019-10-08	<a href="#">3.5</a>	<a href="#">CVE-2019-16417 MISC</a>
ibm -- maximo_anywhere	IBM Maximo Anywhere 7.6.0, 7.6.1, 7.6.2, and 7.6.3 does not have device root detection which could result in an attacker gaining sensitive information about the device. IBM X-Force ID: 160198.	2019-10-10	<a href="#">2.1</a>	<a href="#">CVE-2019-4265 XE CONFIRM</a>
intelliants -- subrion	Subrion 4.2.1 allows XSS via the panel/members/ Username, Full Name, or Email field, aka an "Admin Member JSON Update" issue.	2019-10-06	<a href="#">3.5</a>	<a href="#">CVE-2019-17225 MISC</a>
laravel-admin -- laravel-admin	z-song laravel-admin 1.7.3 has XSS via the Slug or Name on the Roles screen, because of mishandling on the "Operation log" screen.	2019-10-10	<a href="#">3.5</a>	<a href="#">CVE-2019-17433 MISC</a>
lavalite -- lavalite	LavaLite through 5.7 has XSS via a crafted account name that is mishandled on the Manage Clients screen.	2019-10-10	<a href="#">3.5</a>	<a href="#">CVE-2019-17434 MISC</a>

libfws_i_project -- libfws_i	In libyal libfws_i before 20191006, libfws_i_extension_block_copy_from_byte_stream in libfws_i_extension_block.c has a heap-based buffer over-read because rejection of an unsupported size only considers values less than 6, even though values of 6 and 7 are also unsupported.	2019-10-06	2.1	<a href="#">CVE-2019-17263</a> MISC MISC MISC
liblnk_project -- liblnk	** DISPUTED ** libyal liblnk 20191006 has a heap-based buffer over-read in the network_share_name_offset>20 code block of liblnk_location_information_read_data in liblnk_location_information.c, a different issue than CVE-2019-17264. NOTE: the vendor has disputed this as described in the GitHub issue.	2019-10-09	2.1	<a href="#">CVE-2019-17401</a> MISC
microsoft -- sharepoint_enterprise_server	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'.	2019-10-10	3.5	<a href="#">CVE-2019-1070</a> MISC
microsoft -- sharepoint_enterprise_server	A spoofing vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Spoofing Vulnerability'.	2019-10-10	3.5	<a href="#">CVE-2019-1328</a> MISC
microsoft -- sharepoint_enterprise_server	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1330.	2019-10-10	3.5	<a href="#">CVE-2019-1329</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1334.	2019-10-10	2.1	<a href="#">CVE-2019-1345</a> MISC MISC
microsoft -- windows_7	An information disclosure vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in memory, allowing an attacker to retrieve information from a targeted system, aka 'Windows GDI Information Disclosure Vulnerability'.	2019-10-10	2.1	<a href="#">CVE-2019-1363</a> MISC
pbootcms -- pbootcms	PbootCMS 2.0.2 allows XSS via vectors involving the Pboot/admin.php?p=/Single/index/mcode/1 and Pboot/?contact/ URLs.	2019-10-09	3.5	<a href="#">CVE-2019-17417</a> MISC
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the chart title resulting in reflected Cross-Site Scripting	2019-10-08	3.5	<a href="#">CVE-2019-0374</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows execution of scripts in the export dialog box of the report name resulting in reflected Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0375</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2 and 4.3, does not sufficiently encode user-controlled inputs and allows an attacker to save malicious scripts in the publication name, which can be executed later by the victim, resulting in Stored Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0376</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before versions 4.2, does not sufficiently encode user-controlled inputs and allows an attacker to store malicious scripts in the input controls, resulting in Stored Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0377</a> MISC CONFIRM
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), before version 4.2, does not sufficiently encode user-controlled inputs and allows an attacker to store malicious scripts in the file name of the background image resulting in Stored Cross-Site Scripting.	2019-10-08	3.5	<a href="#">CVE-2019-0378</a> MISC CONFIRM
sap -- financial_consolidation	SAP Financial Consolidation, before versions 10.0 and 10.1, does not sufficiently encode user-controlled inputs, which allows an attacker to execute scripts by uploading files containing malicious scripts, leading to reflected cross site scripting vulnerability.	2019-10-08	3.5	<a href="#">CVE-2019-0369</a> MISC CONFIRM
teampass -- teampass	TeamPass 2.1.27.36 allows Stored XSS at the Search page by setting a crafted password for an item in any folder.	2019-10-05	3.5	<a href="#">CVE-2019-17203</a> MISC
teampass -- teampass	TeamPass 2.1.27.36 allows Stored XSS by setting a crafted Knowledge Base label and adding any available item.	2019-10-05	3.5	<a href="#">CVE-2019-17204</a> MISC
	The MDM server component of TIBCO Software Inc's TIBCO			

tibco -- master_data_management	MDM contains multiple vulnerabilities that theoretically allow an authenticated user with specific roles to perform cross-site scripting (XSS) attacks. This issue affects TIBCO Software Inc.'s TIBCO MDM version 9.0.1 and prior versions; version 9.1.0.	2019-10-09	3.5	<a href="#">CVE-2019-11212</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
---------------------------------	---	------------	-----	--

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activesoft -- mybuilder	ActiveX Control in MyBuilder before 6.2.2019.814 allow an attacker to execute arbitrary command via the ShellOpen method. This can be leveraged for code execution	2019-10-07	not yet calculated	<a href="#">CVE-2019-12811</a> <a href="#">MISC</a>
activesoft -- mybuilder	MyBuilder viewer before 6.2.2019.814 allow an attacker to execute arbitrary command via specifically crafted configuration file. This can be leveraged for code execution.	2019-10-07	not yet calculated	<a href="#">CVE-2019-12812</a> <a href="#">MISC</a>
altair_engineering -- pbs_professional	Altair PBS Professional through 19.1.2 allows Privilege Escalation because an attacker can send a message directly to pbs_mom, which fails to properly authenticate the message. This results in code execution as an arbitrary user.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15719</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
amazon_web_services -- freertos	Amazon FreeRTOS up to and including v1.4.8 for AWS lacks length checking in prvProcessReceivedPublish, resulting in leakage of arbitrary memory contents on a device to an attacker. An attacker sends a malformed MQTT publish packet, and waits for an MQTTPACK packet containing the leaked data.	2019-10-07	not yet calculated	<a href="#">CVE-2019-13120</a> <a href="#">CONFIRM</a>
arista_networks -- extensible_operating_system	A vulnerability has been found in the implementation of the Label Distribution Protocol (LDP) protocol in EOS. Under race conditions, the LDP agent can establish an LDP session with a malicious peer potentially allowing the possibility of a Denial of Service (DoS) attack on route updates and in turn potentially leading to an Out of Memory (OOM) condition that is disruptive to traffic forwarding. Affected EOS versions include: 4.22 release train: 4.22.1F and earlier releases 4.21 release train: 4.21.0F - 4.21.2.3F, 4.21.3F - 4.21.7.1M 4.20 release train: 4.20.14M and earlier releases 4.19 release train: 4.19.12M and earlier releases End of support release trains (4.18 and 4.17)	2019-10-10	not yet calculated	<a href="#">CVE-2019-14810</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
auth0 -- auth0	Auth0 auth0.net before 6.5.4 has Incorrect Access Control because IdentityTokenValidator can be accidentally used to validate untrusted ID tokens.	2019-10-08	not yet calculated	<a href="#">CVE-2019-16929</a> <a href="#">CONFIRM</a>
automattic -- mongoose	Automattic Mongoose through 5.7.4 allows attackers to bypass access control (in some applications) because any query object with a _bsontype attribute is ignored. For example, adding "_bsontype":"a" can sometimes interfere with a query filter. NOTE: this CVE is about Mongoose's failure to work around this _bsontype special case that exists in older versions of the bson parser (aka the mongodb/js-bson project).	2019-10-09	not yet calculated	<a href="#">CVE-2019-17426</a> <a href="#">MISC</a> <a href="#">MISC</a>
avira -- avira_software_updater	Avira Software Updater before 2.0.6.21094 allows a DLL side-loading attack.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17449</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a SEGV in the function AP4_TfhdAtom::SetDefaultSampleSize at Core/AP4TfhdAtom.h when called from AP4_Processor::ProcessFragments in Core/AP4Processor.cpp.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17528</a> <a href="#">MISC</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a heap-based buffer over-read in AP4_CencSampleEncryption::DoInspectFields in Core/AP4CommonEncryption.cpp when called from AP4_Atom::Inspect in Core/AP4Atom.cpp.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17529</a> <a href="#">MISC</a> <a href="#">MISC</a>
axiomatic_systems -- bento4	An issue was discovered in Bento4 1.5.1.0. There is a heap-based buffer over-read in AP4_PrintInspector::AddField in Core/AP4Atom.cpp when called from AP4_CencSampleEncryption::DoInspectFields in Core/AP4CommonEncryption.cpp, when called from AP4_Atom::Inspect in Core/AP4Atom.cpp.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17530</a> <a href="#">MISC</a> <a href="#">MISC</a>

b3log -- symphony	b3log Symphony (aka Sym) before 3.6.0 has XSS via the HTTP User-Agent header.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17488</a> <a href="#">MISC</a>
belkin -- wemo_switch_28b_devices	An issue was discovered on Belkin Wemo Switch 28B WW_2.00.11057.PVT-OWRT-SNS devices. They allow remote attackers to cause a denial of service (persistent rules-processing outage) via a crafted ruleDbBody element in a StoreRules request to the upnp/control/rules1 URI, because database corruption occurs.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17532</a> <a href="#">MISC</a>
bootstrap-3-typeahead -- bootstrap-3-typeahead	Bootstrap-3-Typeahead after version 4.0.2 is vulnerable to a cross-site scripting flaw in the highlighter() function. An attacker could exploit this via user interaction to execute code in the user's browser.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10215</a> <a href="#">CONFIRM</a>
bouncy_castle -- bouncy_castle_crypto_package	The ASN.1 parser in Bouncy Castle Crypto (aka BC Java) 1.63 can trigger a large attempted memory allocation, and resultant OutOfMemoryError error, via crafted ASN.1 data. This is fixed in 1.64.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17359</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	getStats.php in Centreon Web before 2.8.28 allows authenticated attackers to execute arbitrary code via the ns_id parameter.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21023</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	licenseUpload.php in Centreon Web before 2.8.27 allows attackers to upload arbitrary files via a POST request.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21024</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
centreon -- centreon_web	img_gantt.php in Centreon Web before 2.8.27 allows attackers to perform SQL injections via the host_id parameter.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21021</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	makeXML_ListServices.php in Centreon Web before 2.8.28 allows attackers to perform SQL injections via the host_id parameter.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21022</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	The token generator in index.php in Centreon Web before 2.8.27 is predictable.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17105</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
centreon -- centreon_web	In very rare cases, a PHP type juggling vulnerability in centreonAuth.class.php in Centreon Web before 2.8.27 allows attackers to bypass authentication mechanisms in place.	2019-10-08	not yet calculated	<a href="#">CVE-2018-21020</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	minPlayCommand.php in Centreon Web before 2.8.27 allows authenticated attackers to execute arbitrary code via the command_hostaddress parameter. NOTE: some sources have listed CVE-2019-17017 for this, but that is incorrect.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17107</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon_web	Local file inclusion in brokerPerformance.php in Centreon Web before 2.8.28 allows attackers to disclose information or perform a stored XSS attack on a user.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17108</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- application_delivery_management	Citrix Application Delivery Management (ADM) 12.1 before build 54.13 has Incorrect Access Control.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17366</a> <a href="#">CONFIRM</a>
cobham -- explorer_710	The web application portal of the Cobham EXPLORER 710, firmware version 1.07, has no authentication by default. This could allow an unauthenticated, local attacker connected to the device to access the portal and to make any change to the	2019-10-10	not yet calculated	<a href="#">CVE-2019-9529</a> <a href="#">CERT-VN</a>

	device.			
cobham -- explorer_710	The web application portal of the Cobham EXPLORER 710, firmware version 1.07, allows unauthenticated access to port 5454. This could allow an unauthenticated, remote attacker to connect to this port via Telnet and execute 86 Attention (AT) commands, including some that provide unauthenticated, shell-like access to the device.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9531 CERT-VN</a>
cobham -- explorer_710	The web root directory of the Cobham EXPLORER 710, firmware version 1.07, has no access restrictions on downloading and reading all files. This could allow an unauthenticated, local attacker connected to the device to access and download any file found in the web root directory.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9530 CERT-VN</a>
cobham -- explorer_710	The Cobham EXPLORER 710, firmware version 1.07, does not validate its firmware image. Development scripts left in the firmware can be used to upload a custom firmware image that the device runs. This could allow an unauthenticated, local attacker to upload their own firmware that could be used to intercept or modify traffic, spoof or intercept GPS traffic, exfiltrate private data, hide a backdoor, or cause a denial-of-service.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9534 CERT-VN</a>
cobham -- explorer_710	The root password of the Cobham EXPLORER 710 is the same for all versions of firmware up to and including v1.08. This could allow an attacker to reverse-engineer the password from available versions to gain authenticated access to the device.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9533 CERT-VN</a>
cobham -- explorer_710	The web application portal of the Cobham EXPLORER 710, firmware version 1.07, sends the login password in cleartext. This could allow an unauthenticated, local attacker to intercept the password and gain access to the portal.	2019-10-10	not yet calculated	<a href="#">CVE-2019-9532 CERT-VN</a>
compal -- ch7465lg_devices	The setter.xml component of the Common Gateway Interface on Compal CH7465LG 6.12.18.25-2p4 devices does not properly validate ping command arguments, which allows remote authenticated users to execute OS commands as root via shell metacharacters in the Target_IP parameter.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17499 MISC</a>
craft_cms -- craft_cms	Craft CMS before 3.3.8 has stored XSS via a name field. This field is mishandled during site deletion.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17496 MISC MISC</a>
d-link -- dap-1320_routers	D-Link DAP-1320 A2-V1.21 routers have some web interfaces without authentication requirements, as demonstrated by uplink_info.xml. An attacker can remotely obtain a user's Wi-Fi SSID and password, which could be used to connect to Wi-Fi or perform a dictionary attack.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17505 MISC</a>
d-link -- dir-615_devices	An issue discovered on D-Link DIR-615 devices with firmware version 20.05 and 20.07. wan.htm can be accessed directly without authentication, which can lead to disclosure of information about the WAN, and can also be leveraged by an attacker to modify the data fields of the page.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17353 MISC MISC MISC</a>
d-link -- dir-816l_devices	An issue was discovered on D-Link DIR-816 A1 1.06 devices. An attacker could access management pages of the router via a client that ignores the "top.location.href = "/dir_login.asp" line in a .asp file. This provides access to d_status.asp, version.asp, d_dhcptbl.asp, and d_acl.asp.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17507 MISC</a>
d-link -- dir-846_devices	D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending a /HNAP1/ request for SetMasterWlanSettings with shell metacharacters to /squashfs-root/www/HNAP1/control/SetMasterWlanSettings.php.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17509 MISC</a>
d-link -- dir-846_devices	D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending a /HNAP1/ request for SetWizardConfig with shell metacharacters to /squashfs-root/www/HNAP1/control/SetWizardConfig.php.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17510 MISC</a>
d-link -- dir-859_and_dir-8850_devices	On D-Link DIR-859 A3-1.06 and DIR-850 A1.13 devices, /etc/services/DEVICE.TIME.php allows command injection via the \$SERVER variable.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17508 MISC</a>
d-link -- dir-868l_and_dir-817lw_routers	There are some web interfaces without authentication requirements on D-Link DIR-868L B1-2.03 and DIR-817LW A1-1.04 routers. An attacker can get the router's username and password (and other information) via SERVICES=DEVICE.ACCOUNT&AUTHORIZED_GROUP=1%0a to getcfg.php. This could be used to control the router remotely.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17506 MISC</a>
	The dbell Wi-Fi Smart Video Doorbell DB01-S Gen 1 allows			<a href="#">CVE-</a>



dbell -- wi-fi_smart_video_doorbell	remote attackers to launch commands with no authentication verification via TCP port 81, because the loginuse and loginpass parameters to openlock.cgi can have arbitrary values. NOTE: the vendor's position is that this product reached end of life in 2016.	2019-10-08	not yet calculated	<a href="#">2019-13336</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- encryption_enterprise	The vulnerability is limited to the installers of Dell Encryption Enterprise versions prior to 10.4.0 and Dell Endpoint Security Suite Enterprise versions prior to 2.4.0. This issue is exploitable only during the installation of the product by an administrator. A local authenticated low privileged user potentially could exploit this vulnerability by staging a malicious DLL in the search path of the installer prior to its execution by a local administrator. This would cause loading of the malicious DLL, which would allow the attacker to execute arbitrary code in the context of an administrator.	2019-10-07	not yet calculated	<a href="#">CVE-2019-3745</a> <a href="#">MISC</a>
dell_emc -- avamar_server	Dell EMC Avamar Server versions 7.4.1, 7.5.0, 7.5.1, 18.2 and 19.1 and Dell EMC Integrated Data Protection Appliance (IDPA) versions 2.0, 2.1, 2.2, 2.3 and 2.4 contain an Incorrect Permission Assignment for Critical Resource vulnerability. A remote authenticated malicious user potentially could exploit this vulnerability to view or modify sensitive backup data. This could be used to make backups corrupt or potentially to trick a user into restoring a backup with malicious files in place.	2019-10-09	not yet calculated	<a href="#">CVE-2019-3765</a> <a href="#">CONFIRM</a>
envoy_proxy -- envoy	Upon receiving each incoming request header data, Envoy will iterate over existing request headers to verify that the total size of the headers stays below a maximum limit. The implementation in versions 1.10.0 through 1.11.1 for HTTP/1.x traffic and all versions of Envoy for HTTP/2 traffic had O(n^2) performance characteristics. A remote attacker may craft a request that stays below the maximum request header size but consists of many thousands of small headers to consume CPU and result in a denial-of-service attack.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15226</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
espressif -- esp-idf	An issue was discovered in Espressif ESP-IDF 2.x, 3.0.x through 3.0.9, 3.1.x through 3.1.6, 3.2.x through 3.2.3, and 3.3.x through 3.3.1. An attacker who uses fault injection to physically disrupt the ESP32 CPU can bypass the Secure Boot digest verification at startup, and boot unverified code from flash. The fault injection attack does not disable the Flash Encryption feature, so if the ESP32 is configured with the recommended combination of Secure Boot and Flash Encryption, then the impact is minimized. If the ESP32 is configured without Flash Encryption then successful fault injection allows arbitrary code execution. To protect devices with Flash Encryption and Secure Boot enabled against this attack, a firmware change must be made to permanently enable Flash Encryption in the field if it is not already permanently enabled.	2019-10-07	not yet calculated	<a href="#">CVE-2019-15894</a> <a href="#">CONFIRM</a>
fastadmin -- fastadmin	An issue was discovered in fastadmin 1.0.0.20190705_beta. There is a public/admin/general.config/edit CSRF vulnerability, as demonstrated by resultant XSS via the row&#91;name&#93; parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17432</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the apache-log4j-extra (version 1.2.x) jar in the classpath, and an attacker can provide a JNDI service to access, it is possible to make the service execute a malicious payload.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17531</a> <a href="#">MISC</a> <a href="#">MISC</a>
fiberhome -- hg2201t	/var/WEB-GUI/cgi-bin/telnet.cgi on FiberHome HG2201T 1.00.M5007_JS_201804 devices allows pre-authentication remote code execution.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17186</a> <a href="#">MISC</a>
frost_ming -- redis_wrapper	Uncontrolled deserialization of a pickled object in models.py in Frost Ming rediswrapper (aka Redis Wrapper) before 0.3.0 allows attackers to execute arbitrary scripts.	2019-10-05	not yet calculated	<a href="#">CVE-2019-17206</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
genesys -- pureengage_digital	Genesys PureEngage Digital (eServices) 8.1.x allows XSS via HtmlChatPanel.jsp or HtmlChatFrameSet.jsp (ActionColor, ClientNickNameColor, Email, email, or email_address parameter).	2019-10-11	not yet calculated	<a href="#">CVE-2019-17176</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- binutils	find_abstract_instance in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32,	2019-10-	not yet	<a href="#">CVE-2019-</a>

	allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.	10	calculated	<a href="#">CVE-2017-17450</a> <a href="#">MISC</a>
gnu -- binutils	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an integer overflow leading to a SEGV in _bfd_dwarf2_find_nearest_line in dwarf2.c, as demonstrated by nm.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17451</a> <a href="#">MISC</a>
gnupg_project -- boa	Boa through 0.94.14rc21 allows remote attackers to trigger an out-of-memory (OOM) condition because malloc is mishandled.	2019-10-11	not yet calculated	<a href="#">CVE-2018-21027</a> <a href="#">CONFIRM</a>
gnupg_project -- boa	Boa through 0.94.14rc21 allows remote attackers to trigger a memory leak because of missing calls to the free function.	2019-10-11	not yet calculated	<a href="#">CVE-2018-21028</a> <a href="#">CONFIRM</a>
google -- android	In generateServicesMap of RegisteredServicesCache.java, there is a possible account protection bypass due to a caching optimization. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-136261465	2019-10-11	not yet calculated	<a href="#">CVE-2019-2183</a> <a href="#">CONFIRM</a>
google -- android	In the default privileges of NFC, there is a possible local bypass of user interaction requirements on package installation due to a default permission. This could lead to local escalation of privilege by installing an application with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-123700348	2019-10-11	not yet calculated	<a href="#">CVE-2019-2114</a> <a href="#">CONFIRM</a>
google -- android	In GetMBheader of combined_decode.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-136175447	2019-10-11	not yet calculated	<a href="#">CVE-2019-2186</a> <a href="#">CONFIRM</a>
google -- android	In VlcDequantH263IntraBlock_SH of vlc_dequant.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-136173699	2019-10-11	not yet calculated	<a href="#">CVE-2019-2185</a> <a href="#">CONFIRM</a>
google -- android	In PV_DecodePredictedIntraDC of dec_pred_intra_dc.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-134578122	2019-10-11	not yet calculated	<a href="#">CVE-2019-2184</a> <a href="#">CONFIRM</a>
google -- android	In ScreenRotationAnimation of ScreenRotationAnimation.java, there is a possible capture of a secure screen due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-69703445	2019-10-11	not yet calculated	<a href="#">CVE-2019-2110</a> <a href="#">CONFIRM</a>
google -- android	In startActivityMayWait of ActivityStarter.java, there is a possible incorrect Activity launch due to an incorrect permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-123013720	2019-10-11	not yet calculated	<a href="#">CVE-2019-2173</a> <a href="#">CONFIRM</a>
google -- android	A use-after-free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application.Product: AndroidAndroid ID: A-141720095	2019-10-11	not yet calculated	<a href="#">CVE-2019-2215</a> <a href="#">CONFIRM</a>
google -- android	In nfc_ncif_decode_rf_params of nfc_ncif.cc, there is a possible out of bounds read due to an integer underflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-124940143	2019-10-11	not yet calculated	<a href="#">CVE-2019-2187</a> <a href="#">CONFIRM</a>
	send_email in graphite-web/webapp/graphite/composer/views.py in Graphite through 1.1.5 is vulnerable to SSRF. The vulnerable			<a href="#">CVE-2017-</a>

graphite_project -- graphite	SSRF endpoint can be used by an attacker to have the Graphite web server request any resource. The response to this SSRF request is encoded into an image file and then sent to an e-mail address that can be supplied by the attacker. Thus, an attacker can exfiltrate any information.	2019-10-11	not yet calculated	<a href="#">18638</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gree -- gree+_application_for_andriod	The GREE+ (aka com.gree.greeplus) application 1.4.0.8 for Android suffers from Cross Site Request Forgery.	2019-10-11	not yet calculated	<a href="#">CVE-2018-20582</a> <a href="#">MISC</a> <a href="#">MISC</a>
hotaru_cms -- hotaru_cms	A stored XSS vulnerability was discovered in Hotaru CMS v1.7.2 via the admin_index.php?page=settings SITE NAME field (aka SITE_NAME), a related issue to CVE-2011-4709.1.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17522</a> <a href="#">MISC</a> <a href="#">MISC</a>
hp -- touchpoint_analytics	A potential security vulnerability has been identified with certain versions of HP Touchpoint Analytics prior to version 4.1.4.2827. This vulnerability may allow a local attacker with administrative privileges to execute arbitrary code via an HP Touchpoint Analytics system service.	2019-10-11	not yet calculated	<a href="#">CVE-2019-6333</a> <a href="#">CONFIRM</a>
hyrda -- hyrda	Hydra through 0.1.8 has a NULL pointer dereference and daemon crash when processing POST requests that lack a Content-Length header. read.c, request.c, and util.c contribute to this. The process_header_end() function calls boa_atoi(), which ultimately calls atoi() on a NULL pointer.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17502</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has a directory traversal vulnerability. This can result in loss of confidential data of IceWarp Mailserver and the operating system. Input passed via a certain parameter (script to basic/minimizer/index.php) is not properly sanitised and can therefore be exploited to browse the partition where IceWarp is installed (or the whole system) and read arbitrary files.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5335</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has a directory traversal vulnerability. This can result in loss of confidential data of IceWarp Mailserver and the operating system. Input passed via a certain parameter (_c to basic/index.html) is not properly sanitised and can therefore be exploited to browse the partition where IceWarp is installed (or the whole system) and read arbitrary files.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5334</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: admin/login.html with the parameter username is persistent in 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5336</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/basic/ with the parameter _dlg[capcha] [controller] is non-persistent in 10.1.3 and 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5337</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/basic/ with the parameter _dlg[capcha][action] is non-persistent in 10.1.3 and 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5338</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/basic/ with the parameter _dlg[capcha][uid] is non-persistent in 10.1.3 and 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5339</a> <a href="#">MISC</a> <a href="#">MISC</a>
icewrap -- webclient	IceWarp Webclient before 10.2.1 has XSS via an HTTP POST request: webmail/ with the parameter password is non-persistent in 10.2.0.	2019-10-11	not yet calculated	<a href="#">CVE-2010-5340</a> <a href="#">MISC</a> <a href="#">MISC</a>
intel -- active_system_console	Insufficient path checking in the installer for Intel(R) Active System Console before version 8.0 Build 24 may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-10-11	not yet calculated	<a href="#">CVE-2019-11120</a> <a href="#">CONFIRM</a>
intel -- nuc	Memory corruption in system firmware for Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-10-11	not yet calculated	<a href="#">CVE-2019-14570</a> <a href="#">CONFIRM</a>
intel -- nuc	Pointer corruption in system firmware for Intel(R) NUC may allow a privileged user to potentially enable escalation of privilege, denial of service and/or information disclosure via local access.	2019-10-11	not yet calculated	<a href="#">CVE-2019-14569</a> <a href="#">CONFIRM</a>
intel -- smart_connect_technology_for_intel_nuc	Improper file permission in software installer for Intel(R) Smart Connect Technology for Intel(R) NUC may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-10-11	not yet calculated	<a href="#">CVE-2019-11167</a>

				<a href="#">CONFIRM</a>
internet_systems_consortium -- bind	An error in the EDNS Client Subnet (ECS) feature for recursive resolvers can cause BIND to exit with an assertion failure when processing a response that has malformed RRSIGs. Versions affected: BIND 9.10.5-S1 -> 9.11.6-S1 of BIND 9 Supported Preview Edition.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6469</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- bind	A failure to free memory can occur when processing messages having a specific combination of EDNS options. Versions affected are: BIND 9.10.7 -> 9.10.8-P1, 9.11.3 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.10.7-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected.	2019-10-09	not yet calculated	<a href="#">CVE-2018-5744</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- bind	A race condition which may occur when discarding malformed packets can result in BIND exiting due to a REQUIRE assertion failure in dispatch.c. Versions affected: BIND 9.11.0 -> 9.11.7, 9.12.0 -> 9.12.4-P1, 9.14.0 -> 9.14.2. Also all releases of the BIND 9.13 development branch and version 9.15.0 of the BIND 9.15 development branch and BIND Supported Preview Edition versions 9.11.3-S1 -> 9.11.7-S1.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6471</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- bind	In BIND Supported Preview Edition, an error in the nxdomain-redirect feature can occur in versions which support EDNS Client Subnet (ECS) features. In those versions which have ECS support, enabling nxdomain-redirect is likely to lead to BIND exiting due to assertion failure. Versions affected: BIND Supported Preview Edition version 9.10.5-S1 -> 9.11.5-S5. ONLY BIND Supported Preview Edition releases are affected.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6468</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- bind	A programming error in the nxdomain-redirect feature can cause an assertion failure in query.c if the alternate namespace used by nxdomain-redirect is a descendant of a zone that is served locally. The most likely scenario where this might occur is if the server, in addition to performing NXDOMAIN redirection for recursive clients, is also serving a local copy of the root zone or using mirroring to provide the root zone, although other configurations are also possible. Versions affected: BIND 9.12.0 -> 9.12.4, 9.14.0. Also affects all releases in the 9.13 development branch.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6467</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- bind	Controls for zone transfers may not be properly applied to Dynamically Loadable Zones (DLZs) if the zones are writable. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P2, 9.12.0 -> 9.12.3-P2, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2019-6465.	2019-10-09	not yet calculated	<a href="#">CVE-2019-6465</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- bind	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contained an error which could be exploited to grow the number of simultaneous connections beyond this limit. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.6, 9.12.0 -> 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 -> 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 -> 9.13.7 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5743.	2019-10-09	not yet calculated	<a href="#">CVE-2018-5743</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- bind	"managed-keys" is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which operators configure for use in DNSSEC validation. Due to an error in the managed-keys feature it is possible for a BIND server which uses managed-keys to exit due to an assertion failure if, during key rollover, a trust anchor's keys are replaced with keys which use an unsupported algorithm. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5745.	2019-10-09	not yet calculated	<a href="#">CVE-2018-5745</a> <a href="#">CONFIRM</a>
internet_systems_consortium -- isc_dhcp	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0	2019-10-09	not yet calculated	<a href="#">CVE-2018-5732</a> <a href="#">CONFIRM</a>
	A vulnerability exists in the way that iTerm2 integrates with tmux's control mode, which may allow an attacker to execute arbitrary			<a href="#">CVE-</a>

item2 -- item2	commands by providing malicious output to the terminal. This affects versions of iTerm2 up to and including 3.3.5. This vulnerability may allow an attacker to execute arbitrary commands on their victim's computer by providing malicious output to the terminal. It could be exploited using command-line utilities that print attacker-controlled content.	2019-10-09	not yet calculated	<a href="#">2019-9535</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CERT-VN</a>
jfinal -- jfinal	In JFinal cos before 2019-08-13, as used in JFinal 4.4, there is a vulnerability that can bypass the isSafeFile() function: one can upload any type of file. For example, a .jsp file may be stored and almost immediately deleted, but this deletion step does not occur for certain exceptions.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17352</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jiangnan_online_judge -- jiangnan_online_judge	app\modules\polygon\controllers\ProblemController in Jiangnan Online Judge (aka jnoj) 0.8.0 allows arbitrary file upload, as demonstrated by PHP code (with a .php filename but the image/png content type) to the web/polygon/problem/tests URI.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17490</a> <a href="#">MISC</a>
joicom_corporation -- renpho_application	An issue was discovered in the RENPHO application 3.0.0 for iOS. It transmits JSON data unencrypted to a server without an integrity check, if a user changes personal data in his profile tab (e.g., exposure of his birthday) or logs into his account (i.e., exposure of credentials).	2019-10-09	not yet calculated	<a href="#">CVE-2019-14808</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
joomlashack -- shack_forms_pro	The Shack Forms Pro extension before 4.0.32 for Joomla! allows path traversal via a file attachment.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17399</a> <a href="#">MISC</a>
juniper_networks -- junos_os	A session fixation vulnerability in J-Web on Junos OS may allow an attacker to use social engineering techniques to fix and hijack a J-Web administrators web session and potentially gain administrative access to the device. This issue affects: Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S15 on EX Series; 12.3X48 versions prior to 12.3X48-D85 on SRX Series; 14.1X53 versions prior to 14.1X53-D51; 15.1 versions prior to 15.1F6-S13, 15.1R7-S5; 15.1X49 versions prior to 15.1X49-D180 on SRX Series; 15.1X53 versions prior to 15.1X53-D238; 16.1 versions prior to 16.1R4-S13, 16.1R7-S5; 16.2 versions prior to 16.2R2-S10; 17.1 versions prior to 17.1R3-S1; 17.2 versions prior to 17.2R2-S8, 17.2R3-S3; 17.3 versions prior to 17.3R3-S5; 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R3; 18.4 versions prior to 18.4R2; 19.1 versions prior to 19.1R1-S2, 19.1R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0062</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os	The PKI keys exported using the command "run request security pki key-pair export" on Junos OS may have insecure file permissions. This may allow another user on the Junos OS device with shell access to read them. This issue affects: Juniper Networks Junos OS 15.1X49 versions prior to 15.1X49-D180; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0073</a> <a href="#">MISC</a>
juniper_networks -- junos_os	A memory leak vulnerability in the of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the device by sending specific commands from a peered BGP host and having those BGP states delivered to the vulnerable device. This issue affects: Juniper Networks Junos OS: 18.1 versions prior to 18.1R2-S4, 18.1R3-S1; 18.1X75 all versions. Versions before 18.1R1 are not affected.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0059</a> <a href="#">MISC</a>
juniper_networks -- junos_os	The management daemon (MGD) is responsible for all configuration and management operations in Junos OS. The Junos CLI communicates with MGD over an internal unix-domain socket and is granted special permission to open this protected mode socket. Due to a misconfiguration of the internal socket, a local, authenticated user may be able to exploit this vulnerability to gain administrative privileges. This issue only affects Linux-based platforms. FreeBSD-based platforms are unaffected by this vulnerability. Exploitation of this vulnerability requires Junos shell access. This issue cannot be exploited from the Junos CLI. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D171, 15.1X49-D180; 15.1X53 versions prior to 15.1X53-D496, 15.1X53-D69; 16.1 versions prior to 16.1R7-S4; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R2-S7, 17.2R3-S1; 17.3 versions prior to 17.3R3-S4; 17.4 versions prior to 17.4R1-S6, 17.4R1-S7, 17.4R2-S3, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S4; 18.2 versions prior to 18.2R1-S5, 18.2R2-S2, 18.2R3; 18.3 versions prior to 18.3R1-S3, 18.3R2; 18.4 versions prior to 18.4R1-S2, 18.4R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0061</a> <a href="#">MISC</a>



juniper_networks -- junos_os	A path traversal vulnerability in NFX150 Series and QFX10K Series, EX9200 Series, MX Series and PTX Series devices with Next-Generation Routing Engine (NG-RE) allows a local authenticated user to read sensitive system files. This issue only affects NFX150 Series and QFX10K Series, EX9200 Series, MX Series and PTX Series with Next-Generation Routing Engine (NG-RE) which uses vmhost. This issue affects Juniper Networks Junos OS on NFX150 Series and QFX10K, EX9200 Series, MX Series and PTX Series with NG-RE and vmhost: 15.1F versions prior to 15.1F6-S12 16.1 versions starting from 16.1R6 and later releases, including the Service Releases, prior to 16.1R6-S6, 16.1R7-S3; 17.1 versions prior to 17.1R3; 17.2 versions starting from 17.2R1-S3, 17.2R3 and later releases, including the Service Releases, prior to 17.2R3-S1; 17.3 versions starting from 17.3R1-S1, 17.3R2 and later releases, including the Service Releases, prior to 17.3R3-S3; 17.4 versions starting from 17.4R1 and later releases, including the Service Releases, prior to 17.4R1-S6, 17.4R2-S2, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S3; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S2, 18.3R2; 18.4 versions prior to 18.4R1-S1, 18.4R2. This issue does not affect: Juniper Networks Junos OS 15.1 and 16.2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0074</a> <a href="#">MISC</a>
juniper_networks -- junos_os	Receipt of a specific link-local IPv6 packet destined to the RE may cause the system to crash and restart (vmcore). By continuously sending a specially crafted IPv6 packet, an attacker can repeatedly crash the system causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 16.1 versions prior to 16.1R6-S2, 16.1R7; 16.2 versions prior to 16.2R2-S10; 17.1 versions prior to 17.1R3. This issue does not affect Juniper Networks Junos OS version 15.1 and prior versions.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0067</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os	An unexpected status return value weakness in the Next-Generation Multicast VPN (NG-mVPN) service of Juniper Networks Junos OS allows attacker to cause a Denial of Service (DoS) condition and core the routing protocol daemon (rpd) process when a specific malformed IPv4 packet is received by the device running BGP. This malformed packet can be crafted and sent to a victim device including when forwarded directly through a device receiving such a malformed packet, but not if the malformed packet is first de-encapsulated from an encapsulated format by a receiving device. Continued receipt of the malformed packet will result in a sustained Denial of Service condition. This issue affects: Juniper Networks Junos OS 15.1 versions prior to 15.1F6-S12, 15.1R7-S2; 15.1X49 versions prior to 15.1X49-D150 on SRX Series; 15.1X53 versions prior to 15.1X53-D68, 15.1X53-D235, 15.1X53-D495, 15.1X53-D590; 16.1 versions prior to 16.1R3-S10, 16.1R4-S12, 16.1R6-S6, 16.1R7-S2; 16.2 versions prior to 16.2R2-S7; 17.1 versions prior to 17.1R2-S9, 17.1R3; 17.2 versions prior to 17.2R1-S7, 17.2R2-S6, 17.2R3; 17.3 versions prior to 17.3R2-S4, 17.3R3.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0066</a> <a href="#">MISC</a>
juniper_networks -- junos_os	A persistent Cross-Site Scripting (XSS) vulnerability in Junos OS J-Web interface may allow remote unauthenticated attackers to perform administrative actions on the Junos device. Successful exploitation requires a Junos administrator to first perform certain diagnostic actions on J-Web. This issue affects: Juniper Networks Junos OS 12.1X46 versions prior to 12.1X46-D86; 12.3 versions prior to 12.3R12-S13; 12.3X48 versions prior to 12.3X48-D80; 14.1X53 versions prior to 14.1X53-D51; 15.1 versions prior to 15.1F6-S13, 15.1R7-S4; 15.1X49 versions prior to 15.1X49-D171, 15.1X49-D180; 15.1X53 versions prior to 15.1X53-D497, 15.1X53-D69; 16.1 versions prior to 16.1R7-S5; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R2-S7, 17.2R3-S1; 17.3 versions prior to 17.3R3-S6; 17.4 versions prior to 17.4R1-S7, 17.4R2-S4, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R1-S5, 18.2R2-S3, 18.2R3; 18.3 versions prior to 18.3R1-S3, 18.3R2, 18.3R3; 18.4 versions prior to 18.4R1-S2, 18.4R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0047</a> <a href="#">MISC</a>
juniper_networks -- junos_os_ex2300_and_ex3400_series	Veriexec is a kernel-based file integrity subsystem in Junos OS that ensures only authorized binaries are able to be executed. Due to a flaw in specific versions of Junos OS, affecting specific EX Series platforms, the Veriexec subsystem will fail to initialize, in essence disabling file integrity checking. This may allow a locally authenticated user with shell access to install untrusted executable images, and elevate privileges to gain full control of the system. During the installation of an affected version of Junos OS are installed, the following messages will be logged to the console: Initializing Verified Exec: /sbin/veriexec: Undefined symbol "__aeabi_uidv" /sbin/veriexec: Undefined symbol "__aeabi_uidv" /sbin/veriexec: Undefined symbol "__aeabi_uidv"	2019-10-09	not yet calculated	<a href="#">CVE-2019-0071</a> <a href="#">MISC</a>

	verixec: /.mount/packages/db/os-kernel-prd-arm-32-20190221.70c2600_builder_stable_11/boot/brcm-hr3.dtb: Authentication error verixec: /.mount/packages/db/os-kernel-prd-arm-32-20190221.70c2600_builder_stable_11/boot/contents.izo: Authentication error ... This issue affects Juniper Networks Junos OS: 18.1R3-S4 on EX2300, EX2300-C and EX3400; 18.3R1-S3 on EX2300, EX2300-C and EX3400.			
juniper_networks -- junos_os_multiple_series	A vulnerability in the srxpfe process on Protocol Independent Multicast (PIM) enabled SRX series devices may lead to crash of the srxpfe process and an FPC reboot while processing (PIM) messages. Sustained receipt of these packets may lead to an extended denial of service condition. Affected releases are Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D80; 15.1X49 versions prior to 15.1X49-D160; 17.3 versions prior to 17.3R3-S7 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R2; 18.3 versions prior to 18.3R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0075 MISC</a>
juniper_networks -- junos_os_multiple_series	On EX4600, QFX5100 Series, NFX Series, QFX10K Series, QFX5110, QFX5200 Series, QFX5110, QFX5200, QFX10K Series, vSRX, SRX1500, SRX4000 Series, vSRX, SRX1500, SRX4000, QFX5110, QFX5200, QFX10K Series, when the user uses console management port to authenticate, the credentials used during device authentication are written to a log file in clear text. This issue does not affect users that are logging-in using telnet, SSH or J-web to the management IP. This issue affects ACX, NFX, SRX, EX and QFX platforms with the Linux Host OS architecture, it does not affect other SRX and EX platforms that do not use the Linux Host OS architecture. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D110 on vSRX, SRX1500, SRX4000 Series; 15.1X53 versions prior to 15.1X53-D234 on QFX5110, QFX5200 Series; 15.1X53 versions prior to 15.1X53-D68 on QFX10K Series; 17.1 versions prior to 17.1R2-S8, 17.1R3, on QFX5110, QFX5200, QFX10K Series; 17.2 versions prior to 17.2R1-S7, 17.2R2-S6, 17.2R3 on QFX5110, QFX5200, QFX10K Series; 17.3 versions prior to 17.3R2 on vSRX, SRX1500, SRX4000, QFX5110, QFX5200, QFX10K Series; 14.1X53 versions prior to 14.1X53-D47 on ACX5000, EX4600, QFX5100 Series; 15.1 versions prior to 15.1R7 on ACX5000, EX4600, QFX5100 Series; 16.1R7 versions prior to 16.1R7 on ACX5000, EX4600, QFX5100 Series; 17.1 versions prior to 17.1R2-S10, 17.1R3 on ACX5000, EX4600, QFX5100 Series; 17.2 versions prior to 17.2R3 on ACX5000, EX4600, QFX5100 Series; 17.3 versions prior to 17.3R3 on ACX5000, EX4600, QFX5100 Series; 17.4 versions prior to 17.4R2 on ACX5000, EX4600, QFX5100 Series; 18.1 versions prior to 18.1R2 on ACX5000, EX4600, QFX5100 Series; 15.1X53 versions prior to 15.1X53-D496 on NFX Series; 17.2 versions prior to 17.2R3-S1 on NFX Series; 17.3 versions prior to 17.3R3-S4 on NFX Series; 17.4 versions prior to 17.4R2-S4, 17.4R3 on NFX Series; 18.1 versions prior to 18.1R3-S4 on NFX Series; 18.2 versions prior to 18.2R2-S3, 18.2R3 on NFX Series; 18.3 versions prior to 18.3R1-S3, 18.3R2 on NFX Series; 18.4 versions prior to 18.4R1-S1, 18.4R2 on NFX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0069 CONFIRM</a>
juniper_networks -- junos_os_mx_series	On MX Series, when the SIP ALG is enabled, receipt of a certain malformed SIP packet may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending a crafted SIP packet, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a sustained Denial of Service. This issue affects Juniper Networks Junos OS on MX Series: 16.1 versions prior to 16.1R7-S5; 16.2 versions prior to 16.2R2-S11; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3-S3; 17.3 versions prior to 17.3R3-S6 ; 17.4 versions prior to 17.4R2-S8, 17.4R3; 18.1 versions prior to 18.1R3-S3; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0065 CONFIRM</a>
juniper_networks -- junos_os_mx_series	This issue only affects devices with three (3) or more MPC10's installed in a single chassis with OSPF enabled and configured on the device. An Insufficient Resource Pool weakness allows an attacker to cause the device's Open Shortest Path First (OSPF) states to transition to Down, resulting in a Denial of Service (DoS) attack. This attack requires a relatively large number of specific Internet Mixed (IMIXed) types of genuine and valid IPv6 packets to be transferred by the attacker in a relatively short period of time, across three or more PFE's on the device at the same time. Continued receipt of the traffic sent by the attacker will continue to cause OSPF to remain in the Down starting state, or flap between other states and then again to Down, causing a persistent Denial of Service. This attack will affect all IPv4, and IPv6 traffic served by the OSPF routes once the OSPF states transition to Down. This issue affects: Juniper Networks Junos	2019-10-09	not yet calculated	<a href="#">CVE-2019-0056 MISC</a>

	OS on MX480, MX960, MX2008, MX2010, MX2020: 18.1 versions prior to 18.1R2-S4, 18.1R3-S5; 18.1X75 version 18.1X75-D10 and later versions; 18.2 versions prior to 18.2R1-S5, 18.2R2-S3, 18.2R3; 18.2X75 versions prior to 18.2X75-D50; 18.3 versions prior to 18.3R1-S4, 18.3R2, 18.3R3; 18.4 versions prior to 18.4R1-S2, 18.4R2.			
juniper_networks -- junos_os_mx_series	When an MX Series Broadband Remote Access Server (BRAS) is configured as a Broadband Network Gateway (BNG) with DHCPv6 enabled, jdhcpd might crash when receiving a specific crafted DHCP response message on a subscriber interface. The daemon automatically restarts without intervention, but continuous receipt of specific crafted DHCP messages will repeatedly crash jdhcpd, leading to an extended Denial of Service (DoS) condition. This issue only affects systems configured with DHCPv6 enabled. DHCPv4 is unaffected by this issue. This issue affects Juniper Networks Junos OS: 15.1 versions prior to 15.1R7-S5 on MX Series; 16.1 versions prior to 16.1R7-S5 on MX Series; 16.2 versions prior to 16.2R2-S10 on MX Series; 17.1 versions prior to 17.1R3-S1 on MX Series; 17.2 versions prior to 17.2R3-S2 on MX Series; 17.3 versions prior to 17.3R3-S6 on MX Series; 17.4 versions prior to 17.4R2-S5, 17.4R3 on MX Series; 18.1 versions prior to 18.1R3-S6 on MX Series; 18.2 versions prior to 18.2R2-S4, 18.2R3 on MX Series; 18.2X75 versions prior to 18.2X75-D50 on MX Series; 18.3 versions prior to 18.3R1-S5, 18.3R3 on MX Series; 18.4 versions prior to 18.4R2 on MX Series; 19.1 versions prior to 19.1R1-S2, 19.1R2 on MX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0063</a> <a href="#">MISC</a>
juniper_networks -- junos_os_nfx_series	An Improper Input Validation weakness allows a malicious local attacker to elevate their permissions to take control of other portions of the NFX platform they should not be able to access, and execute commands outside their authorized scope of control. This leads to the attacker being able to take control of the entire system. This issue affects: Juniper Networks Junos OS versions prior to 18.2R1 on NFX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0070</a> <a href="#">MISC</a>
juniper_networks -- junos_os_nfx_series	An improper authorization weakness in Juniper Networks Junos OS allows a local authenticated attacker to bypass regular security controls to access the Junos Device Manager (JDM) application and take control of the system. This issue affects: Juniper Networks Junos OS versions prior to 18.2R1, 18.2X75-D5.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0057</a> <a href="#">MISC</a>
juniper_networks -- junos_os_srx1500_series	Under certain heavy traffic conditions srxpfe process can crash and result in a denial of service condition for the SRX1500 device. Repeated crashes of the srxpfe can result in an extended denial of service condition. The SRX device may fail to forward traffic when this condition occurs. Affected releases are Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D170 on SRX1500; 17.3 versions prior to 17.3R3-S7 on SRX1500; 17.4 versions prior to 17.4R2-S8, 17.4R3 on SRX1500; 18.1 versions prior to 18.1R3-S8 on SRX1500; 18.2 versions prior to 18.2R3 on SRX1500; 18.3 versions prior to 18.3R2 on SRX1500; 18.4 versions prior to 18.4R2 on SRX1500.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0050</a> <a href="#">CONFIRM</a>
juniper_networks -- junos_os_srx5000_series	On SRX5000 Series devices, if 'set security zones security-zone <zone> tcp-rst' is configured, the flowd process may crash when a specific TCP packet is received by the device and triggers a new session. The process restarts automatically. However, receipt of a constant stream of these TCP packets may result in an extended Denial of Service (DoS) condition on the device. This issue affects Juniper Networks Junos OS: 18.2R3 on SRX 5000 Series; 18.4R2 on SRX 5000 Series; 19.2R1 on SRX 5000 Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0064</a> <a href="#">MISC</a>
juniper_networks -- junos_os_srx5000_series	SSL-Proxy feature on SRX devices fails to handle a hardware resource limitation which can be exploited by remote SSL/TLS servers to crash the flowd daemon. Repeated crashes of the flowd daemon can result in an extended denial of service condition. For this issue to occur, clients protected by the SRX device must initiate a connection to the malicious server. This issue affects: Juniper Networks Junos OS on SRX5000 Series: 12.3X48 versions prior to 12.3X48-D85; 15.1X49 versions prior to 15.1X49-D180; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R2-S6, 17.4R3; 18.1 versions prior to 18.1R3-S8; 18.2 versions prior to 18.2R3; 18.3 versions prior to 18.3R2; 18.4 versions prior to 18.4R2; 19.1 versions prior to 19.1R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0051</a> <a href="#">MISC</a>
juniper_networks -- junos_os_srx_series	A vulnerability in the SIP ALG packet processing service of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the device by sending specific types of valid SIP traffic to the device. In this case, the flowd process crashes and generates a core dump while processing SIP ALG traffic. Continued receipt of these valid SIP packets will result in a	2019-10-	not yet	<a href="#">CVE-2019-0055</a>

	sustained Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D61, 12.3X48-D65 on SRX Series; 15.1X49 versions prior to 15.1X49-D130 on SRX Series; 17.3 versions prior to 17.3R3 on SRX Series; 17.4 versions prior to 17.4R2 on SRX Series.	09	calculated	<a href="#">MISC MLIST</a>
juniper_networks -- junos_os_srx_series	The SRX flowd process, responsible for packet forwarding, may crash and restart when processing specific multicast packets. By continuously sending the specific multicast packets, an attacker can repeatedly crash the flowd process causing a sustained Denial of Service. This issue affects Juniper Networks Junos OS on SRX Series: 12.3X48 versions prior to 12.3X48-D90; 15.1X49 versions prior to 15.1X49-D180; 17.3 versions; 17.4 versions prior to 17.4R2-S5, 17.4R3; 18.1 versions prior to 18.1R3-S6; 18.2 versions prior to 18.2R2-S4, 18.2R3; 18.3 versions prior to 18.3R2-S1, 18.3R3; 18.4 versions prior to 18.4R2; 19.1 versions prior to 19.1R1-S1, 19.1R2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0068 CONFIRM</a>
juniper_networks -- junos_os_srx_series	The flowd process, responsible for forwarding traffic in SRX Series services gateways, may crash and restart when processing specific transit IP packets through an IPSec tunnel. Continued processing of these packets may result in an extended Denial of Service (DoS) condition. This issue only occurs when IPSec tunnels are configured. Systems without IPSec tunnel configurations are not vulnerable to this issue. This issue affects Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D171, 15.1X49-D180 on SRX Series; 18.2 versions 18.2R2-S1 and later, prior to 18.2R3 on SRX Series; 18.4 versions prior to 18.4R2 on SRX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0060 MISC MISC</a>
juniper_networks -- junos_os_srx_series	A vulnerability in the Veriexec subsystem of Juniper Networks Junos OS allowing an attacker to fully compromise the host system. A local authenticated user can elevate privileges to gain full control of the system even if they are specifically denied access to perform certain actions. This issue affects: Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D80 on SRX Series.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0058 MISC</a>
juniper_networks -- junos_os_srx_series	An Improper Certificate Validation weakness in the SRX Series Application Identification (app-id) signature update client of Juniper Networks Junos OS allows an attacker to perform Man-in-the-Middle (MitM) attacks which may compromise the integrity and confidentiality of the device. This issue affects: Juniper Networks Junos OS 15.1X49 versions prior to 15.1X49-D120 on SRX Series devices. No other versions of Junos OS are affected.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0054 MISC MISC</a>
juniper_networks -- sbr_carrier	An Unprotected Storage of Credentials vulnerability in the identity and access management certificate generation procedure allows a local attacker to gain access to confidential information. This issue affects: Juniper Networks SBR Carrier: 8.4.1 versions prior to 8.4.1R13; 8.5.0 versions prior to 8.5.0R4.	2019-10-09	not yet calculated	<a href="#">CVE-2019-0072 MISC</a>
kaseva -- vsa_rmm	An issue was discovered in Kaseya VSA RMM through 9.5.0.22. When using the default configuration, the LAN Cache feature creates a local account FSAdminxxxxxxxx (e.g., FSAdmin123456789) on the server that hosts the LAN Cache and all clients that are assigned to a LAN Cache. This account is placed into the local Administrators group of all clients assigned to the LAN Cache. When the assigned client is a Domain Controller, the FSAdminxxxxxxxx account is created as a domain account and automatically added as a member of the domain BUILTINAdministrators group. Using the well known Pass-the-Hash techniques, an attacker can use the same FSAdminxxxxxxxx hash from any LAN Cache client and pass this to a Domain Controller, providing administrative rights to the attacker on any Domain Controller. (Local account Pass-the-Hash mitigations do not protect domain accounts.)	2019-10-11	not yet calculated	<a href="#">CVE-2019-14510 MISC MISC MISC MISC</a>
kirona -- dynamic_resource_scheduling	An issue was discovered in Kirona Dynamic Resource Scheduling (DRS) 5.5.3.5. An unauthenticated user can access /osm/REGISTER.cmd (aka /osm_tiles/REGISTER.cmd) directly: it contains sensitive information about the database through the SQL queries within this batch file. This file exposes SQL database information such as database version, table name, column name, etc.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17503 MISC</a>
kirona -- dynamic_resource_scheduling	An issue was discovered in Kirona Dynamic Resource Scheduling (DRS) 5.5.3.5. A reflected Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script via the /osm/report/ password parameter.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17504 MISC</a>
knex.js -- knex.js	knex.js versions before 0.19.5 are vulnerable to SQL Injection attack. Identifiers are escaped incorrectly as part of the MSSQL dialect, allowing attackers to craft a malicious query to the host DB.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10757 CONFIRM</a>

kramer -- viaware	Kramer VIAware 2.5.0719.1034 has Incorrect Access Control.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17124 MISC</a>
landing-cms -- landing-cms	An issue was discovered in Landing-CMS 0.0.6. There is a CSRF vulnerability that can change the admin's password via the password/ URL,	2019-10-12	not yet calculated	<a href="#">CVE-2019-17521 MISC</a>
laravel-bjyblog -- laravel-bjyblog	laravel-bjyblog 6.1.1 has XSS via a crafted URL.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17494 MISC</a>
libntlm -- libntlm	Libntlm through 1.5 relies on a fixed buffer size for tSmbNtlmAuthRequest, tSmbNtlmAuthChallenge, and tSmbNtlmAuthResponse read and write operations, as demonstrated by a stack-based buffer over-read in buildSmbNtlmAuthRequest in smbutil.c for a crafted NTLM request.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17455 MISC</a>
libtom_project -- libtomcrypt	In LibTomCrypt through 1.18.2, the der_decode_utf8_string function (in der_decode_utf8_string.c) does not properly detect certain invalid UTF-8 sequences. This allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) or read information from other memory locations via carefully crafted DER-encoded data.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17362 MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MISC</a>
libvips -- libvips	vips_foreign_load_gif_scan_image in foreign/gifload.c in libvips before 8.8.2 tries to access a color map before a DGifGetImageDesc call, leading to a use-after-free.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17534 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mantisbt -- mantisbt	MantisBT before 1.3.20 and 2.22.1 allows Post Authentication Command Injection, leading to Remote Code Execution.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15715 CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
mcafee -- endpoint_security	Code Injection vulnerability in EPSetup.exe in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to get their malicious code installed by the ENS installer via code injection into EPSetup.exe by an attacker with access to the installer.	2019-10-09	not yet calculated	<a href="#">CVE-2019-3652 CONFIRM</a>
mcafee -- endpoint_security	Improper access control vulnerability in Configuration tool in McAfee Endpoint Security (ENS) Prior to 10.6.1 October 2019 Update allows local user to gain access to security configuration via unauthorized use of the configuration tool.	2019-10-09	not yet calculated	<a href="#">CVE-2019-3653 CONFIRM</a>
microsoft -- azure_app_service_on_azure_stack	An remote code execution vulnerability exists when Azure App Service/ Antares on Azure Stack fails to check the length of a buffer prior to copying memory to it. An attacker who successfully exploited this vulnerability could allow an unprivileged function run by the user to execute code in the context of NT AUTHORITY\SYSTEM thereby escaping the Sandbox. The security update addresses the vulnerability by ensuring that Azure App Service sanitizes user inputs., aka 'Azure App Service Remote Code Execution Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1372 MISC</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1371 MISC</a>
microsoft -- microsoft_dynamics_365	A cross site scripting vulnerability exists when Microsoft Dynamics 365 (on-premises) does not properly sanitize a specially crafted web request to an affected Dynamics server, aka 'Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1375 MISC</a>
microsoft -- microsoft_edge	An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory, aka 'Microsoft Edge based on Edge HTML Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1356 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles a process crash, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1315, CVE-2019-1339.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1342 MISC</a>



microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows Hyper-V Network Switch on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Hyper-V Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1230 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows CloudStore improperly handles file Discretionary Access Control List (DACL), aka 'Microsoft Windows CloudStore Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1321 MISC</a>
microsoft -- multiple_windows_products	A tampering vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection, aka 'Windows NTLM Tampering Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1166 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists in the way that the Windows Code Integrity Module handles objects in memory, aka 'Windows Code Integrity Module Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1344 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1345.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1334 MISC</a>
microsoft -- multiple_windows_products	An information disclosure vulnerability exists when Windows Update Client fails to properly handle objects in memory, aka 'Windows Update Client Information Disclosure Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1337 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Windows Error Reporting manager improperly handles hard links, aka 'Windows Error Reporting Manager Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1315, CVE-2019-1342.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1339 MISC</a>
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1343, CVE-2019-1347.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1346 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when umpo.dll of the Power Service, improperly handles a Registry Restore Key function, aka 'Windows Power Service Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1341 MISC</a>
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1346, CVE-2019-1347.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1343 MISC</a>
microsoft -- multiple_windows_products	A security feature bypass exists when Windows Secure Boot improperly restricts access to debugging functionality, aka 'Windows Secure Boot Security Feature Bypass Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1368 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists when Microsoft IIS Server fails to check the length of a buffer prior to copying memory to it. An attacker who successfully exploited this vulnerability can allow an unprivileged function ran by the user to execute code in the context of NT AUTHORITY\SYSTEM escaping the Sandbox. The security update addresses the vulnerability by correcting how Microsoft IIS Server sanitizes web requests., aka 'Microsoft IIS Server Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1365 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1358.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1359 MISC</a>
microsoft -- multiple_windows_products	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1359.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1358 MISC</a>
microsoft -- multiple_windows_products	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-1343, CVE-2019-1346.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1347 MISC</a>
microsoft -- multiple_windows_products	An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1320, CVE-2019-1322.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1340 MISC</a>
microsoft -- windows_10_mobile	A security feature bypass vulnerability exists in Windows 10 Mobile when Cortana allows a user to access files and folders through the locked screen, aka 'Windows 10 Mobile Security Feature Bypass Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1314 MISC</a>
	An elevation of privilege vulnerability exists in Windows when the			<a href="#">CVE-2019-1362</a>

microsoft -- windows_7_and_windows_server_2008	Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1364.	2019-10-10	not yet calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_7_and_windows_server_2008	A security feature bypass vulnerability exists in Microsoft Windows when a man-in-the-middle attacker is able to successfully bypass the NTLMv2 protection if a client is also sending LMv2 responses, aka 'Windows NTLM Security Feature Bypass Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1338</a> <a href="#">MISC</a>
microsoft -- windows_7_and_windows_server_2008	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1362.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1364</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- windows_update_assistant	An elevation of privilege vulnerability exists in Windows 10 Update Assistant in the way it handles permissions. A locally authenticated attacker could run arbitrary code with elevated system privileges, aka 'Windows 10 Update Assistant Elevation of Privilege Vulnerability'.	2019-10-10	not yet calculated	<a href="#">CVE-2019-1378</a> <a href="#">MISC</a>
moxa -- edr_810	Moxa EDR 810, all versions 5.1 and prior, allows an unauthenticated attacker to be able to retrieve some log files from the device, which may allow sensitive information disclosure. Log files must have previously been exported by a legitimate user.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10963</a> <a href="#">MISC</a>
moxa -- edr_810	Moxa EDR 810, all versions 5.1 and prior, allows an authenticated attacker to abuse the ping feature to execute unauthorized commands on the router, which may allow an attacker to perform remote code execution.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10969</a> <a href="#">MISC</a>
netaddr_gem_for_ruby_on_rails -- netaddr_gem_for_ruby_on_rails	The netaddr gem before 2.0.4 for Ruby has misconfigured file permissions, such that a gem install may result in 0777 permissions in the target filesystem.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17383</a> <a href="#">MISC</a> <a href="#">MISC</a>
netapp -- clustered_data_ontap	Clustered Data ONTAP versions 9.0 and higher do not enforce hostname verification under certain circumstances making them susceptible to impersonation via man-in-the-middle attacks.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5506</a> <a href="#">CONFIRM</a>
netapp -- snapmanager_for_oracle	SnapManager for Oracle prior to version 3.4.2P1 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5507</a> <a href="#">CONFIRM</a>
netgear -- multiple_devices	Certain NETGEAR devices allow unauthenticated access to critical .cgi and .htm pages via a substring ending with .jpg, such as by appending ?x=1.jpg to a URL. This affects MBR1515, MBR1516, DGN2200, DGN2200M, DGN23700, WNR2000v2, WNR3300, WNR3400, WNR3500, and WNR834Bv2.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17373</a> <a href="#">MISC</a>
netgear -- multiple_devices	Certain NETGEAR devices allow remote attackers to disable all authentication requirements by visiting genieDisableLanChanged.cgi. The attacker can then, for example, visit MNU_accessPassword_recovered.html to obtain a valid new admin password. This affects AC1450, D8500, DC112A, JNDR3000, LG2200D, R4500, R6200, R6200v2, R6250, R6300, R6300v2, R6400, R6700, R6900P, R6900, R7000P, R7000, R7100LG, R7300, R7900, R8000, R8300, R8500, WGR614v10, WN2500RPv2, WNR3400v2, WNR3700v3, WNR4000, WNR4500, WNR4500v2, WNR1000, WNR1000v3, WNR3500L, and WNR3500L.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17372</a> <a href="#">MISC</a>
netsarang -- xftp	NetSarang XFTP Client 6.0149 and earlier version contains a buffer overflow vulnerability caused by improper boundary checks when copying file name from an attacker controlled FTP server. That leads attacker to execute arbitrary code by sending a crafted filename.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17320</a> <a href="#">MISC</a>
node-red -- node-red-dashboard	It is possible to inject JavaScript within node-red-dashboard versions prior to version 2.17.0 due to the ui_notification node accepting raw HTML by default.	2019-10-08	not yet calculated	<a href="#">CVE-2019-10756</a> <a href="#">CONFIRM</a>
nvidia -- shield_tv	NVIDIA Shield TV Experience prior to v8.0.1, NVIDIA Tegra software contains a vulnerability in the bootloader, where it does not validate the fields of the boot image, which may lead to code execution, denial of service, escalation of privileges, and information disclosure.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5700</a> <a href="#">CONFIRM</a>
nvidia -- shield_tv	NVIDIA Shield TV Experience prior to v8.0.1, NVIDIA Tegra bootloader contains a vulnerability where the software performs an incorrect bounds check, which may lead to buffer overflow resulting in escalation of privileges and code execution. escalation of privileges, and information disclosure, code execution, denial of service, or escalation of privileges.	2019-10-09	not yet calculated	<a href="#">CVE-2019-5699</a> <a href="#">CONFIRM</a>
open_information_security_foundation --	In OISF LibHTTP before 0.5.31, as used in Suricata 4.1.4 and other products, an HTTP protocol parsing error causes the	2019-10-	not yet	<a href="#">CVE-2019-17420</a>

libhttp	http_header signature to not alert on a response with a single \r\n ending.	09	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openbsd -- openssl	OpenSSH 7.7 through 7.9 and 8.x before 8.1, when compiled with an experimental key type, has a pre-authentication integer overflow if a client or server is configured to use a crafted XMSS key. This leads to memory corruption and remote code execution because of an error in the XMSS key parsing algorithm. NOTE: the XMSS implementation is considered experimental in all released OpenSSH versions, and there is no supported way to enable it when building portable OpenSSH.	2019-10-09	not yet calculated	<a href="#">CVE-2019-16905</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
openstack_project -- openstack_octavia	Amphora Images in OpenStack Octavia >=0.10.0 <2.1.2, >=3.0.0 <3.2.0, >=4.0.0 <4.1.0 allows anyone with access to the management network to bypass client-certificate based authentication and retrieve information or issue configuration commands via simple HTTP requests to the Agent on port https/9443, because the cmd/agent.py unicorn cert_reqs option is True but is supposed to be ssl.CERT_REQUIRED.	2019-10-08	not yet calculated	<a href="#">CVE-2019-17134</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
otcms -- otcms	OTCMS v3.85 has CSRF in the admin/member_deal.php Admin Panel page, leading to creation of a new management group account, as demonstrated by superadmin.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17369</a> <a href="#">MISC</a>
palo_alto_networks -- zingbox_inspector	The SSH service is enabled on the Zingbox Inspector versions 1.294 and earlier, exposing SSH to the local network. When combined with PAN-SA-2019-0027, this can allow an attacker to authenticate to the service using hardcoded credentials.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15017</a> <a href="#">MISC</a>
palo_alto_networks -- zingbox_inspector	In the Zingbox Inspector, versions 1.294 and earlier, hardcoded credentials for root and inspector user accounts are present in the system software, which can result in unauthorized users gaining access to the system.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15015</a> <a href="#">MISC</a>
prettyphoto -- prettyphoto	prettyPhoto before 3.1.6 has js/jquery.prettyPhoto.js XSS.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9478</a> <a href="#">MISC</a> <a href="#">MISC</a>
python -- python	library/glob.html in the Python 2 and 3 documentation before 2016 has potentially misleading information about whether sorting occurs, as demonstrated by irreproducible cancer-research results. NOTE: the effects of this documentation cross application domains, and thus it is likely that security-relevant code elsewhere is affected. This issue is not a Python implementation bug, and there are no reports that NMR researchers were specifically relying on library/glob.html. In other words, because the older documentation stated "finds all the pa hnames matching a specified pattern according to the rules used by the Unix shell," one might have incorrectly inferred that the sorting that occurs in a Unix shell also occurred for glob.glob. There is a workaround in newer versions of Willoughby nmr-data_compilation-p2.py and nmr-data_compilation-p3.py, which call sort() directly.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17514</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
redhat -- ansible	Ansible, all ansible_engine-2.x versions and ansible_engine-3.x up to ansible_engine-3.5, was logging at the DEBUG level which lead to a disclosure of credentials if a plugin used a library that logged credentials at the DEBUG level. This flaw does not affect Ansible modules, as those are executed in a separate process.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14846</a> <a href="#">CONFIRM</a>
redhat -- openshift	A vulnerability was found in OpenShift builds, versions 4.1 up to 4.3. Builds that extract source from a container image, bypass the TLS hostname verification. An attacker can take advantage of this flaw by launching a man-in-the-middle attack and injecting malicious content.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14845</a> <a href="#">CONFIRM</a>
riot -- riot	In RIOT 2019.07, the MQTT-SN implementation (asymcute) mishandles errors occurring during a read operation on a UDP socket. The receive loop ends. This allows an attacker (via a large packet) to prevent a RIOT MQTT-SN client from working until the device is restarted.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17389</a> <a href="#">MISC</a>
	An issue was discovered in Rsyslog v8.1908.0. contrib/pmaixforwardedfrom/pmaixforwardedfrom.c has a heap overflow in the parser for AIX log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon) but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the			<a href="#">CVE-</a>

rsyslog -- rsyslog	value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.	2019-10-07	not yet calculated	<a href="#">2019-17041</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
samsung -- laser_printers	A potential security vulnerability has been identified with Samsung Laser Printers. This vulnerability could potentially be exploited to create a denial of service.	2019-10-11	not yet calculated	<a href="#">CVE-2019-6335</a> <a href="#">CONFIRM</a>
samsung -- multiple_p_phones	On certain Samsung P(9.0) phones, an attacker with physical access can start a TCP Dump capture without the user's knowledge. This feature of the Service Mode application is available after entering the *#9900# check code, but is protected by an OTP password. However, this password is created locally and (due to mishandling of cryptography) can be obtained easily by reversing the password creation logic.	2019-10-09	not yet calculated	<a href="#">CVE-2019-11341</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- customer_relationship_management	SAP Customer Relationship Management (Email Management), versions: S4CRM before 1.0 and 2.0, BBPCRM before 7.0, 7.01, 7.02, 7.12, 7.13 and 7.14, does not sufficiently encode user-controlled inputs within the mail client resulting in Cross-Site Scripting vulnerability.	2019-10-08	not yet calculated	<a href="#">CVE-2019-0368</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- landscape_management_enterprise_edition	Under certain conditions, SAP Landscape Management enterprise edition, before version 3.0, allows custom secure parameters? default values to be part of the application logs leading to Information Disclosure.	2019-10-08	not yet calculated	<a href="#">CVE-2019-0380</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- process_integration	SAP Process Integration, business-to-business add-on, versions 1.0, 2.0, does not perform authentication check properly when the default security provider is changed to BouncyCastle (BC), leading to Missing Authentication Check	2019-10-08	not yet calculated	<a href="#">CVE-2019-0379</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- sql_anywhere	A binary plan in SAP SQL Anywhere, before version 17.0, SAP IQ, before version 16.1, and SAP Dynamic Tier, before versions 1.0 and 2.0, can result in the inadvertent access of files located in directories outside of the paths specified by the user.	2019-10-08	not yet calculated	<a href="#">CVE-2019-0381</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
siemens -- multiple_products	A vulnerability has been identified in Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All versions), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All versions), SIMATIC CFU PA (All versions < V1.2.0), SIMATIC ET 200AL (All versions), SIMATIC ET 200M (All versions), SIMATIC ET 200MP IM 155-5 PN BA (All versions < V4.2.3), SIMATIC ET 200MP IM 155-5 PN HF (All versions), SIMATIC ET 200MP IM 155-5 PN ST (All versions), SIMATIC ET 200S (All versions), SIMATIC ET 200SP IM 155-6 PN BA (All versions), SIMATIC ET 200SP IM 155-6 PN HA (All versions), SIMATIC ET 200SP IM 155-6 PN HF (All versions < V4.2.2), SIMATIC ET 200SP IM 155-6 PN HS (All versions), SIMATIC ET 200SP IM 155-6 PN ST (All versions), SIMATIC ET 200SP IM 155-6 PN/2 HF (All versions < V4.2.2), SIMATIC ET 200SP IM 155-6 PN/3 HF (All versions < V4.2.1), SIMATIC ET 200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0) (All versions), SIMATIC ET 200pro (All versions), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions), SIMATIC HMI Comfort Panels 4" - 22" (All versions), SIMATIC HMI KTP Mobile Panels (All versions), SIMATIC PN/PN Coupler (All versions), SIMATIC PROFINET Driver (All versions < V2.1), SIMATIC S7-1200 CPU family (incl. F) (All versions), SIMATIC S7-1500 CPU family (incl. F) (All versions < V2.0), SIMATIC S7-300 CPU family (incl. F) (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-400 V6 (incl F) and below (All versions), SIMATIC S7-400H V6 (All versions < V6.0.9), SIMATIC S7-410 V8 (All versions), SIMATIC WinAC RTX (F) 2010 (All versions < SIMATIC WinAC RTX 2010 SP3), SINAMICS DCM (All versions < V1.5 HF1), SINAMICS DCP (All versions), SINAMICS G110M V4.7 (PN Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G120 V4.7 (PN Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G130 V4.7 (Control Unit) (All versions), SINAMICS G150 (Control Unit) (All versions), SINAMICS GH150 V4.7 (Control Unit) (All versions), SINAMICS GL150 V4.7 (Control Unit) (All versions), SINAMICS GM150 V4.7 (Control Unit) (All versions), SINAMICS S110 (Control Unit) (All versions), SINAMICS S120 V4.7 (Control Unit) (All versions), SINAMICS S150 (Control Unit) (All versions), SINAMICS SL150 V4.7 (Control Unit) (All versions), SINAMICS SM120 V4.7 (Control Unit) (All versions), SINUMERIK 828D (All versions < V4.8 SP5), SINUMERIK 840D sl (All versions). Affected devices contain a	2019-10-10	not yet calculated	<a href="#">CVE-2019-10936</a> <a href="#">CONFIRM</a>

	vulnerability that allows an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large amount of specially crafted UDP packets are sent to device. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- multiple_products	A vulnerability has been identified in CP1604 (All versions < V2.8), CP1616 (All versions < V2.8), Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller (All versions < V4.1.1 Patch 05), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200 (All versions < V4.5.0 Patch 01), Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P (All versions < V4.5.0), SCALANCE X-200IRT (All versions < V5.2.1), SIMATIC ET 200M (All versions), SIMATIC ET 200S (All versions), SIMATIC ET 200ecoPN (except 6ES7148-6JD00-0AB0 and 6ES7146-6FF00-0AB0) (All versions), SIMATIC ET 200pro (All versions), SIMATIC PN/PN Coupler 6ES7158-3AD01-0XA0 (All versions), SIMATIC S7-300 CPU family (incl. F) (All versions), SIMATIC S7-400 (incl. F) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC WinAC RTX (F) 2010 (All versions < SIMATIC WinAC RTX 2010 SP3), SIMOTION (All versions), SINAMICS DCM (All versions < V1.5 HF1), SINAMICS DCP (All versions), SINAMICS G110M V4.7 (Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G120 V4.7 (Control Unit) (All versions < V4.7 SP10 HF5), SINAMICS G130 V4.7 (Control Unit) (All versions < V4.7 HF29), SINAMICS G150 (Control Unit) (All versions < V4.8), SINAMICS GH150 V4.7 (Control Unit) (All versions), SINAMICS GL150 V4.7 (Control Unit) (All versions), SINAMICS GM150 V4.7 (Control Unit) (All versions), SINAMICS S110 (Control Unit) (All versions), SINAMICS S120 V4.7 (Control Unit and CBE20) (All versions < V4.7 HF34), SINAMICS S150 (Control Unit) (All versions < V4.8), SINAMICS SL150 V4.7 (Control Unit) (All versions), SINAMICS SM120 V4.7 (Control Unit) (All versions), SINUMERIK 828D (All versions < V4.8 SP5), SINUMERIK 840D sl (All versions). An attacker with network access to an affected product may cause a Denial-of-Service condition by breaking the real-time synchronization (IRT) of the affected installation. The security vulnerability could be exploited by an unauthenticated attacker with network access to the affected installation. No user interaction is required to exploit this security vulnerability. The vulnerability impacts the availability of the affected installations.	2019-10-10	not yet calculated	<a href="#">CVE-2019-10923</a> <a href="#">CONFIRM</a>
siemens -- simatic_it_uadm	A vulnerability has been identified in SIMATIC IT UADM (All versions < V1.3). An authenticated remote attacker with network access to port 1434/tcp of SIMATIC IT UADM could potentially recover a password that can be used to gain read and write access to the related TeamCenter station. The security vulnerability could be exploited only if the attacker is authenticated. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises the confidentiality of the targeted system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2019-10-10	not yet calculated	<a href="#">CVE-2019-13929</a> <a href="#">CONFIRM</a>
siemens -- simatic_winac_rtx(f)_2010	A vulnerability has been identified in SIMATIC WinAC RTX (F) 2010 (All versions). Affected versions of the software contain a vulnerability that could allow an unauthenticated attacker to trigger a denial-of-service condition. The vulnerability can be triggered if a large HTTP request is sent to the executing service. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the service provided by the software. At the time of advisory publication no public exploitation of this security vulnerability was known.	2019-10-10	not yet calculated	<a href="#">CVE-2019-13921</a> <a href="#">CONFIRM</a>
signal -- private_messenger	The Signal Private Messenger application before 4.47.7 for Android allows a caller to force a call to be answered, without callee user interaction, via a connect message. The existence of the call is noticeable to the callee; however, the audio channel may be open before the callee can block eavesdropping.	2019-10-04	not yet calculated	<a href="#">CVE-2019-17191</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sma_solar_technology -- sunny_webbox	An attacker could send a malicious link to an authenticated operator, which may allow remote attackers to perform actions with the permissions of the user on the Sunny WebBox Firmware Version 1.6 and prior. This device uses IP addresses to maintain communication after a successful login, which would increase the	2019-10-09	not yet calculated	<a href="#">CVE-2019-13529</a> <a href="#">MISC</a>



	ease of exploitation.			<a href="#">MISC</a>
socomec -- diris_a-40_devices	Password disclosure in the web interface on socomec DIRIS A-40 devices before 48250501 allows a remote attacker to get full access to a device via the /password.json URI.	2019-10-09	not yet calculated	<a href="#">CVE-2019-15859</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate (SI, MB, 840D) firmware through 1.71.00.1225. A CGI script is vulnerable to command injection via a maliciously crafted form parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2019-15051</a> <a href="#">MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate SI 1.60.01. A maintenance script, that is executable via sudo, is vulnerable to file path injection. This enables the Attacker to write files with superuser privileges in specific locations.	2019-10-10	not yet calculated	<a href="#">CVE-2019-11526</a> <a href="#">MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate SI 1.60.01. A CGI script is vulnerable to command injection with a maliciously crafted url parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2019-11527</a> <a href="#">MISC</a>
softing -- uagate_si	An issue was discovered in Softing uaGate SI 1.60.01. A system default path for executables is user writable.	2019-10-10	not yet calculated	<a href="#">CVE-2019-11528</a> <a href="#">MISC</a>
softland -- file_sharing_wizard	A Structured Exception Handler (SEH) based buffer overflow in File Sharing Wizard 1.5.0 26-8-2008 allows remote unauthenticated attackers to execute arbitrary code via the HTTP DELETE method, a similar issue to CVE-2019-16724 and CVE-2010-2331.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17415</a> <a href="#">MISC</a>
solarwinds -- dameware_mini_remote_client	The Solarwinds Dameware Mini Remote Client agent v12.1.0.89 supports smart card authentication which can allow a user to upload an executable to be executed on the DWRC.exe host. An unauthenticated, remote attacker can request smart card login and upload and execute an arbitrary executable run under the Local System account.	2019-10-08	not yet calculated	<a href="#">CVE-2019-3980</a> <a href="#">MISC</a>
sophos -- cyberoamos	A shell injection vulnerability on the Sophos Cyberoam firewall appliance with CyberoamOS before 10.6.6 MR-6 allows remote attackers to execute arbitrary commands via the Web Admin and SSL VPN consoles.	2019-10-11	not yet calculated	<a href="#">CVE-2019-17059</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
swagger -- swagger_ui	A Cascading Style Sheets (CSS) injection vulnerability in Swagger UI before 3.23.11 allows attackers to use the Relative Path Overwrite (RPO) technique to perform CSS-based input field value exfiltration, such as exfiltration of a CSRF token value. In other words, this product intentionally allows the embedding of untrusted JSON data from remote servers, but it was not previously known that <style>@import within the JSON data was a functional attack method.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17495</a> <a href="#">MISC</a> <a href="#">MISC</a>
syslog -- rsyslog	An issue was discovered in Rsyslog v8.1908.0. contrib/pmcisconames/pmcisconames.c has a heap overflow in the parser for Cisco log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon), but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.	2019-10-07	not yet calculated	<a href="#">CVE-2019-17042</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
tbeu -- matio	Mat_VarReadNextInfo4 in mat4.c in MATIO 1.5.17 omits a certain '' character, leading to a heap-based buffer over-read in strdup_vprintf when uninitialized memory is accessed.	2019-10-12	not yet calculated	<a href="#">CVE-2019-17533</a> <a href="#">MISC</a> <a href="#">MISC</a>
tinytcl -- vino	tinytcl Vino through 2017-12-15 allows remote attackers to cause a denial of service ("vn_get_string error: Resource temporarily unavailable" error and daemon crash) via a long URL.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17414</a> <a href="#">MISC</a>
tracker_software -- pdf-xchange_editor	Tracker PDF-XChange Editor before 8.0.330.0 has an NTLM SSO hash theft vulnerability using crafted FDF or XFDF files (a related issue to CVE-2018-4993). For example, an NTLM hash is sent for a link to \\192.168.0.2\C\$\file.pdf without user interaction.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17497</a> <a href="#">MISC</a>

v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the communication to the web service is unencrypted via http. An attacker is able to intercept and sniff communication to the web service.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17218 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. Password authentication uses MD5 to hash passwords. Cracking is possible with minimal effort.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17216 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no bruteforce protection (e.g., lockout) established. An attacker might be able to bruteforce the password to authenticate on the device.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17215 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. There is no CSRF protection established on the web service.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17217 MISC</a>
v-zug -- combi-steam_mslq_devices	An issue was discovered on V-Zug Combi-Steam MSLQ devices before Ethernet R07 and before WLAN R05. By default, the device does not enforce any authentication. An adjacent attacker is able to use the network interface without proper access control.	2019-10-06	not yet calculated	<a href="#">CVE-2019-17219 MISC</a>
vmware -- multiple_products	ESXi, Workstation, Fusion, VMRC and Horizon Client contain a use-after-free vulnerability in the virtual sound device. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.5.	2019-10-10	not yet calculated	<a href="#">CVE-2019-5527 CONFIRM</a>
vmware -- workstation_and_fusion	VMware Workstation and Fusion contain a network denial-of-service vulnerability due to improper handling of certain IPv6 packets. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 4.7.	2019-10-10	not yet calculated	<a href="#">CVE-2019-5535 CONFIRM</a>
wordpress -- wordpress	The ThemeMakers Almera Responsive Portfolio theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9487 MISC</a>
wordpress -- wordpress	The ThemeMakers GamesTheme Premium theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9490 MISC</a>
wordpress -- wordpress	The ThemeMakers SmartIT Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9492 MISC</a>
wordpress -- wordpress	The buddypress-activity-plus plugin before 1.6.2 for WordPress has CSRF with resultant directory traversal via the wp-admin/admin-ajax.php bpf_b_photos[] parameter in a bpf_b_remove_temp_images action.	2019-10-07	not yet calculated	<a href="#">CVE-2015-9455 MISC</a>
wordpress -- wordpress	The history-collection plugin through 1.1.1 for WordPress has directory traversal via the download.php var parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9470 MISC</a>
wordpress -- wordpress	The pretty-link plugin before 1.6.8 for WordPress has PrioLinksController::list_links SQL injection via the group parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9457 MISC</a>
wordpress -- wordpress	The RobotCPA plugin 5 for WordPress has directory traversal via the f.php l parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9480 EXPLOIT-DB</a>
wordpress -- wordpress	The ACF-Frontend-Display plugin through 2015-07-03 for WordPress has arbitrary file upload via an action=upload request to js/blueimp-jQuery-File-Upload-d45deb1/server/php/index.php.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9479 MISC</a>
wordpress -- wordpress	The booking-system plugin before 2.1 for WordPress has DOPBSPBackEndTranslation: display SQL injection via the language parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9460 MISC</a>
wordpress -- wordpress	The incoming-links plugin before 0.9.10b for WordPress has referrers.php XSS via the Referer HTTP header.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9472 MISC</a>

				<a href="#">MISC</a>
wordpress -- wordpress	The wti-like-post plugin before 1.4.3 for WordPress has WtiLikePostProcessVote SQL injection via the HTTP_CLIENT_IP, HTTP_X_FORWARDED_FOR, HTTP_X_FORWARDED, HTTP_FORWARDED_FOR, or HTTP_FORWARDED variable.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9466</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The dzs-zoomsounds plugin through 2.0 for WordPress has admin/upload.php arbitrary file upload.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9471</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The s3bubble-amazon-s3-audio-streaming plugin 2.0 for WordPress has directory traversal via he adverts/assets/plugins/ultimate/content/downloader.php path parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9463</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The s3bubble-amazon-s3-html-5-video-with-adverts plugin 0.7 for WordPress has directory traversal via he adverts/assets/plugins/ultimate/content/downloader.php path parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9464</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
wordpress -- wordpress	The awesome-filterable-portfolio plugin before 1.9 for WordPress has afp_get_new_category_page SQL injection via the cat_id parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9462</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The content-grabber plugin 1.0 for WordPress has XSS via obj_field_name or obj_field_id.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9469</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The yet-another-stars-rating plugin before 0.9.1 for WordPress has yasr_get_multi_set_values_and_field SQL injection via the set_id parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9465</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Axioma Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9486</a> <a href="#">MISC</a>
wordpress -- wordpress	The estrutura-basica theme through 2015-09-13 for WordPress has directory traversal via the scripts/download.php arquivo parameter.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9473</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Invento Responsive Gallery/Architecture Template component through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9483</a> <a href="#">MISC</a>
wordpress -- wordpress	The animate-it plugin before 2.3.6 for WordPress has CSRF in edsanimate.php.	2019-10-10	not yet calculated	<a href="#">CVE-2019-17386</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Goodnex Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9489</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Almera Responsive Portfolio Site Template component through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9488</a> <a href="#">MISC</a>
wordpress -- wordpress	The ThemeMakers Accio Responsive Parallax One Page Site Template component through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9485</a> <a href="#">MISC</a>
wordpress -- wordpress	The Simpolio theme 1.3.2 for WordPress has insufficient restrictions on option updates.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9474</a> <a href="#">MISC</a>
	The ThemeMakers Accio One Page Parallax Responsive theme			

wordpress -- wordpress	through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9484 MISC</a>
wordpress -- wordpress	The ThemeMakers Car Dealer / Auto Dealer Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9482 MISC</a>
wordpress -- wordpress	The ThemeMakers Diplomat   Political theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9481 MISC</a>
wordpress -- wordpress	The Vernissage theme 1.2.8 for WordPress has insufficient restrictions on option updates.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9477 MISC</a>
wordpress -- wordpress	The Teardrop theme 1.8.1 for WordPress has insufficient restrictions on option updates.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9476 MISC</a>
wordpress -- wordpress	The Pont theme 1.5 for WordPress has insufficient restrictions on option updates.	2019-10-10	not yet calculated	<a href="#">CVE-2015-9475 MISC</a>
wordpress -- wordpress	The ThemeMakers Blessing Premium Responsive theme through 2015-05-15 for WordPress allows remote attackers to obtain sensitive information (such as user_login, user_pass, and user_email values) via a direct request for the wp-content/uploads/tmm_db_migrate/wp_users.dat URI.	2019-10-11	not yet calculated	<a href="#">CVE-2015-9491 MISC</a>
yealink -- multiple_phones	Yealink phones through 2019-08-04 do not properly check user roles in POST requests. Consequently, the default User account (with a password of user) can make admin requests via HTTP.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14656 MISC</a>
yealink -- multiple_phones	Yealink phones through 2019-08-04 have an issue with OpenVPN file upload. They execute tar as root to extract files, but do not validate the extraction directory. Creating a tar file with .././.././ allows replacement of almost any file on a phone. This leads to password replacement and arbitrary code execution as root.	2019-10-08	not yet calculated	<a href="#">CVE-2019-14657 MISC</a>
zabbix -- zabbix	An issue was discovered in zabbix.php? action=dashboard.view&dashboardid=1 in Zabbix through 4.4. An attacker can bypass the login page and access the dashboard page, and then create a Dashboard, Report, Screen, or Map without any Username/Password (i.e., anonymously). All created elements (Dashboard/Report/Screen/Map) are accessible by other users and by an admin.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17382 MISC</a>
zoho_manageengine -- datasecurity_plus	An issue was discovered in Zoho ManageEngine DataSecurity Plus before 5.0.1 5012. An exposed service allows a basic user ("Operator" access level) to access the configuration file of the mail server (except for the password).	2019-10-09	not yet calculated	<a href="#">CVE-2019-17112 MISC</a>
zyxel -- nbg-418n_router	wan.htm page on Zyxel NBG-418N v2 with firmware version V1.00(AARP.9)C0 can be accessed directly without authentication, which can lead to disclosure of information about the WAN, and can also be leveraged by an attacker to modify data fields of the page.	2019-10-09	not yet calculated	<a href="#">CVE-2019-17354 MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)





From: [Security Management Weekly](#)  
To: [rcortez@SUNNYVALE.CA.GOV](mailto:rcortez@SUNNYVALE.CA.GOV)  
Subject: Security Management Weekly - October 11, 2019  
Date: Friday, October 11, 2019 11:46:04 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



Banner



Advertising/Sponsorship Opportunities | Professional Edition

### Lead Story

#### For Business Continuity, Accept the Unexpected

Security Management Magazine August 2019 Issue

It is one thing to expect the unexpected. It is quite another to accept the unexpected. Denial is a powerful thing, and even the best of us can be convinced that our plans are comprehensive and our preparedness complete. [\(More\)](#)

### Top Security News

#### Only a Locked Door Stopped a Massacre at a German Synagogue

From "Only a Locked Door Stopped a Massacre at a German Synagogue"  
*New York Times (10/11/19) Schuetze, Christopher; Eddy, Melissa*

Were it not for a dark wooden door, the authorities say, Stephan Balliet may have succeeded in carrying out a massacre of Jews he had planned to broadcast live around the world. He chose Yom Kippur, knowing the synagogue in Halle, Germany, would be full. But during every service, the thick, narrow door, its outside handle removed, was locked from the inside. On Wednesday, it spared the lives of 51 Jews from the area and a group of young, international visitors, including 10 Americans, who had come to be with them on the holiest day on the Jewish calendar. Horst Seehofer, the country's interior minister, vowed to increase security measures, including extending laws that would allow the authorities to monitor digital communication to help prevent further threats such as those, they say, posed by Balliet, who was arrested after fleeing the scene in Halle, in eastern Germany. In a hate-filled screed he published online, Balliet, 27, made clear that he had chosen his target hoping to kill as many Jews as possible. Footage from a camera that he had strapped to the helmet he wore showed him planting explosives that appeared not to detonate, in an attempt to breach the synagogue door. Jewish leaders demanded on Thursday to know why their appeals for increased police presence around the synagogue had been ignored. While Jewish institutions in most large cities in Germany have a round-the-clock police detail, that was absent in Halle.

Share ☐ ☐ ☐ | [Web Link](#)

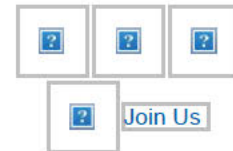


#### [WEBINAR] Shining a Light on Domestic Violence within Workplace Violence Prevention Programs

The connection between workplace violence and domestic violence is real. Research shows that 40% of women killed in the workplace were slain by a relative or domestic partner. Though a difficult,

October 11, 2019

#### Follow Us



#### Calendar of Events

##### UPCOMING EVENTS: Webinars

- [Brand Integrity, Supply Chain and Distribution Channel Security as a Means to Grow Market Share \(October 16\)](#)
- [Reputation Management: Security's Role During a Crisis \(November 6\)](#)

##### Classroom Programs

- [Active Assailant \(November 4-5\)](#)
- [Crisis Management \(November 4-5\)](#)
- [Violence Assessment and Intervention \(November 4-5\)](#)
- [Facility Security Design \(November 4-5\)](#)

[Global Events](#)  
[More Classroom Programs](#)  
[More Webinars](#)

highly sensitive issue, HR and security professionals can't turn a blind eye to partner abuse in workplace violence prevention programs. Join experts from the Hillard Heintze Threat + Violence Risk Management and Law Enforcement Consulting practices for a webinar discussing how you can incorporate domestic violence awareness and management into violence prevention programs.

[REGISTER NOW](#)

## ASIS News

### New in 2019...Security Leaders Mentoring Program

ASIS International is committed to promoting a program of mentorship within our community and to ensuring the standard of excellence for which our profession is known. The goal of the Security Leaders Mentoring Program is to foster mentoring relationships between security professionals, through which advice is shared with those aspiring to enhance their careers or advance within or transition to the security industry.

This program is presented by the ASIS Professional Development Council Mentoring Committee and is an exclusive ASIS member benefit. [Learn more about becoming a Mentor or Mentee today!](#)

Share    | [Web Link](#)



## Top Security News

### Turkish Forces Push Deeper Into Syria as Kurds Fight Back

From "Turkish Forces Push Deeper Into Syria as Kurds Fight Back"  
*Washington Post (10/11/19) Fahim, Kareem; Cunningham, Erin*

Turkey defied mounting international criticism Thursday as it deepened its offensive against Kurdish fighters in northeast Syria, while deadly rocket fire from inside Syria menaced Turkish towns. The escalating violence sent thousands of civilians on both sides of the border fleeing their homes, and aid agencies warned of a humanitarian crisis, with the United Nations reporting more than 70,000 people already displaced in northeast Syria. The Syrian National Army, a group of rebel factions backed by Turkey, said it had seized a dozen villages in northeast Syria as part of the ground offensive. Kurdish authorities in northern Syria said as many as 10 civilians were killed by Turkish forces, while mortar and rocket fire from Syria left six people dead inside Turkey, local officials said. At the U.N. Security Council, Turkey came under harsh criticism from European ambassadors, who warned of an ensuing humanitarian crisis and the revival of Islamic State militants. But the council failed to agree on a statement condemning Turkey's military operation. Tens of thousands of Islamic State members and their families were detained in northeast Syria after the SDF earlier this year seized the last of the territory held by the militant group. Diplomats and military experts have warned that the offensive could undermine security at the prisons and camps, allowing the Islamist militants to escape.

Share    | [Web Link](#)



As network infrastructure grows progressively more complex, IT alerting systems become critical to minimizing downtime. IT alerting systems provide organizations with the power to reduce the workload of IT personnel while improving the accuracy, responsiveness, and preparedness of the organization as a whole. [Download this free resource](#) to learn how to get started integrating an IT alerting solution or optimizing your current one.



---

### Missile Attack Suspected After Iranian Oil Tanker Explosion, State-Owned Firm Says

From "Missile Attack Suspected After Iranian Oil Tanker Explosion, State-Owned Firm Says"

NBCNews.com (10/11/19) Arouzi, Ali; Khodadadi, Amin Hossein; Smith, Saphora

Iran's national oil company said two explosions hit one of its tankers 60 miles from the Saudi port city of Jiddah on Friday, ratcheting up tension in the volatile region. An explosion set the vessel on fire and caused heavy damage to its tanks, with oil spilling into the Red Sea, according to Iran's state-run news agency (IRNA) and Iran's Students News Agency (ISNA). A spokesperson for Iran's National Oil Company — a government-owned firm run by the Petroleum Ministry — said that the first explosion hit the tanker's hull at around 5 a.m., with a second one striking within 30 minutes. The company said it was still trying to determine the cause but suspected a missile attack. IRNA said that all crew on board were safe and the vessel was in a stable condition. The agency did not say whom Iranian officials suspect of launching the alleged projectiles. Earlier this year, the United States accused Iran of attacking oil tankers in the Gulf of Oman, a stretch of water that separates Oman and the United Arab Emirates from Iran. Tehran has denied it was behind the attacks. The report also follows strikes on a key Saudi oil site in September which the U.S. also blamed on Iran. Tehran also denied being responsible for these attacks, although Iran-backed Houthi rebels claimed them.

Share    | [Web Link](#)



### Apple Removes App That Helps Hong Kong Protesters Track the Police

From "Apple Removes App That Helps Hong Kong Protesters Track the Police"  
New York Times (10/11/19)

Apple removed an app this week that enabled protesters in Hong Kong to track the police, a day after facing intense criticism from Chinese state media for it. Apple said it was withdrawing the app, HKmap.live, from its App Store just days after approving it because the authorities in Hong Kong said protesters were using it to attack the police in the semiautonomous city. A day earlier, People's Daily, the flagship newspaper of the Chinese Communist Party, published an editorial accusing Apple of aiding "rioters" in Hong Kong. "Letting poisonous software have its way is a betrayal of the Chinese people's feelings," said the article, which was written under a pseudonym that translates into "Calming the Waves." Timothy Cook, Apple's chief executive, said in an email to employees on Thursday that the company had removed the app after receiving "credible information" from the authorities and people in Hong Kong "that the app was being used maliciously to target individual officers for violence and to victimize individuals and property where no police are present." As a result, he said, the app violated Apple rules and local laws. With its reversal, Apple joined a growing list of corporations that are trying to navigate the fraught political situation between China and Hong Kong, where antigovernment protests have unfolded for months. Supporters of the app have argued that it helps Hong Kong residents avoid clashes between the police and protesters.

Share    | [Web Link](#)



**Traveling Abroad Soon? Get an Internet of Things (IoT) Data Roaming SIM to data-power your Security Gadgets!**

**Order your Dual Global Mobile® - USA & Global Roaming IoT DATA Smart SIM** which comes standard with permanent +1US & +44 UK Phone numbers in ONE SIM with DATA (unlimited bundled

package), VOICE & SMS, covers 230+ countries to browse, place and receive calls and sms; Free Incoming Calls in 120+ countries: the US, Canada, Mexico, the UK most of Europe, Middle East, Australia, New Zealand, Japan, etc. No monthly, quarterly or yearly fee, No connection fee! Visit: [sales.dualglobalmobile.us](mailto:sales.dualglobalmobile.us) or [www.dualglobalmobile.us](http://www.dualglobalmobile.us)

### **FBI Sounds Alarm About Chinese Intellectual Property Theft on U.S. Campuses**

From "FBI Sounds Alarm About Chinese Intellectual Property Theft on U.S. Campuses"

*Fox Business (10/06/19) Conner, Paul*

A review of emails indicated that the FBI has repeatedly warned U.S. universities about visiting researchers stealing intellectual property on behalf of China. "When we go to the universities, what we're trying to do is highlight the risk to them without discouraging them from welcoming the researchers and students from a country like China," said Assistant Attorney General John Demers. The emails underscore the extent of U.S. concerns that universities, as recruiters of foreign talent and incubators of cutting-edge research, are particularly vulnerable targets. Agents have lectured at seminars, briefed administrators in campus meetings and distributed pamphlets with cautionary tales of trade secret theft. "Existentially, we look at China as our greatest threat from an intelligence perspective, and they succeeded significantly in the last decade from stealing our best and brightest technology," said William Evanina, the U.S. government's chief counterintelligence official. The warnings come as Chinese students continue to play a significant role on U.S. campuses. A third of all international students in the United States are Chinese, according to the 2018 OpenDoors Report. About 363,341 students from China attended classes at American higher education institutions last year. The number of Chinese students has been increasing steadily since the 2012-13 school year when the number of Chinese students in the U.S. was more than 235,000. Chinese contribute about \$13 billion annually to the economy, according to NAFSA: Association of International Educators.

Share    | [Web Link](#)



### **For Healthcare Workers, the Risk of Violence Is Part of the Job**

From "For Healthcare Workers, the Risk of Violence Is Part of the Job"

*Philadelphia Inquirer (10/08/19) Carter, Andy*

Statistics show that workplace violence resulting in time off from work is four times more likely in healthcare and social assistance sectors than in private industry, highlighting the dangers faced by healthcare staff every day. Healthcare professionals are well aware of the rising tide of violence, and have taken some steps to decrease the threat to staff and patients. Staff are being instructed to report violent incidents, and many workplaces are offering training in de-escalation techniques to stop a potentially violent outbreak in its tracks. And many hospitals have incorporated rapid response teams, individuals available on call 24/7 who can defuse tense situations and secure healthcare facilities to ensure safety and security for all. In some states, lawmakers are introducing bills to improve safety and security in healthcare offices. Pennsylvania, for example, has introduced several bills that would increase the penalty for assault on a healthcare practitioner and enhance privacy measures for healthcare workers.

Share    | [Web Link](#) - May Require Paid Subscription

### **Iranian Attacks Expose Vulnerability of Campaign Email Accounts**

From "Iranian Attacks Expose Vulnerability of Campaign Email Accounts"

*The Hill (10/08/19) Miller, Maggie*



Recent Iranian cyberattacks on a U.S. presidential campaign stressed the vulnerability of email accounts as the 2020 elections approach, with Microsoft disclosing that one group tried to access the accounts of not only the campaign, but also accounts linked to journalists and former and current U.S. officials. Former Obama administration official Tom Kellermann said campaigns should ensure "modern cybersecurity technologies" are being used to safeguard endpoints, and that "websites and mobile apps should be tested for vulnerabilities and hardened accordingly." U.S. political campaigns are seen as especially vulnerable to cyberattacks because many of them are focusing their attention and resources elsewhere. "We encourage all Americans to be vigilant and on guard against this and other cyber threats -- scrutinize emails, reset passwords routinely, maintain up-to-date antivirus and operating system patches, and enable multi-factor authentication," said Christopher Krebs, director for the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.

Share    | [Web Link](#)

### **Phishing Attempts Increase 400 Percent, Many Malicious URLs Found on Trusted Domains**

From "Phishing Attempts Increase 400 Percent, Many Malicious URLs Found on Trusted Domains"

*Help Net Security (10/09/19)*

One out of every 50 URLs are malicious, nearly one-third of phishing sites use HTTPS, and Windows 7 exploits have grown 75 percent since January, according to a new Webroot report. Phishing lures have become more personalized as hackers use stolen data for more than just account takeover, and the report highlights the importance of user education. In addition, the report found that 24 percent of malicious URLs are hosted on trusted domains because hackers known trusted domain URLs raise less suspicion among users and are more difficult for security measures to block. Said Webroot's Tyler Moffitt, "Businesses and consumers need to be aware of and continually educate themselves about these evolving methods and risks to protect their data and devices."

Share    | [Web Link](#)

### **No One Could Prevent Another 'WannaCry-style' Attack, Says DHS Official**

From "No One Could Prevent Another 'WannaCry-style' Attack, Says DHS Official"

*TechCrunch (10/06/19) Whittaker, Zack*

The U.S. government may not be able to prevent another global cyberattack like WannaCry, a senior cybersecurity official has said. Jeanette Manfra, the assistant director for cybersecurity for Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), said that the 2017 WannaCry cyberattack, which saw hundreds of thousands of computers around the world infected with ransomware, was uniquely challenging because it spread so quickly. "I don't know that we could ever prevent something like that," said Manfra, referring to another WannaCry-style attack. "We just have something that completely manifests itself as a worm. I think the original perpetrators didn't expect probably that sort of impact," she added. The WannaCry cyberattack was the first major global security incident in years. Hackers believed to be associated with North Korea used a set of highly classified hacking tools that only weeks earlier had been stolen from the National Security Agency and published online. The tools allowed anyone who used them to infect thousands of vulnerable computers with a backdoor. That backdoor was used to deliver the WannaCry payload, which locked out users from their own files unless they paid a ransom. Making matters worse, WannaCry had wormable properties, allowing it to spread across a network and making it difficult to contain. Manfra said "bad things are going to happen," but that efforts to mobilize government and the private sector can help combat cyberattacks as they emerge.

Share    | [Web Link](#)



### **As Ecuador Protests Grow, President Moves Government Out of the Capital**

From "As Ecuador Protests Grow, President Moves Government Out of the Capital"

*Washington Post (10/08/19) Krygier, Rachele*

Ecuadoran President Lenin Moreno moved his government out of the capital as protests against his austerity measures continued to grow on Tuesday. Thousands converged on Quito for a sixth day of demonstrations, and the state-run oil company suspended operations at three oil fields in the Amazon region after they were "taken" by "individuals not affiliated with the operation," the Energy Ministry said. Local media outlets showed protesters setting fires, blocking streets, and pushing into the National Assembly building. Security forces deployed tear gas to disperse crowds. One person has died, dozens have been injured, and more than 500 arrested in the demonstrations that began after Moreno withdrew a fuel subsidy that helped Ecuadorans buy gasoline. Authorities have reported vandalism of government facilities and looting; they have declared a state of emergency and deployed security forces. The suspension of oil field operations has cut the nation's production by 12 percent, the Energy Ministry said. Iván Ontaneda, minister of production, commerce and investment, told reporters the country has lost \$1.4 billion over six days of protests. Moreno has called for dialogue but says he won't reverse his austerity measures. He accuses his predecessor, Rafael Correa, whom he once served as vice president, of stirring opposition against him. In a national address Monday night, Moreno said he was moving the government from Quito to the port city of Guayaquil.

Share   | [Web Link](#)

### **Assailant Live-Streamed Attempted Attack on German Synagogue**

From "Assailant Live-Streamed Attempted Attack on German Synagogue"

*New York Times (10/10/19) Eddy, Melissa; Gladstone, Rick; Hsu, Tiffany*

A heavily armed gunman with a live-streaming head camera tried to storm a synagogue in eastern Germany on Wednesday as congregants observed the holiest day in Judaism. Stopped by a locked door, he killed two people outside and wounded two others. Hours later the police announced the arrest of a suspect in the assault in the city of Halle, one of the most brazen in a string of recent attacks aimed at Jews in Germany. The methodology of the assailant bore a striking resemblance to the rampage by a far-right extremist against two mosques in Christchurch, New Zealand, more than six months ago, in which he broadcast his killings live on social media. Fifty-one people died in that attack. Like the Christchurch killer, the Halle assailant recorded himself, in a 35-minute video of shooting, mayhem and hateful language. In accented English, he identified himself as Anon, denied the Holocaust, denounced feminists and immigrants, then declared: "The root of all these problems is the Jew." He then drove to Halle's Humboldt Street synagogue, showing the arsenal of weapons in his car. While trying unsuccessfully to enter the synagogue, which was locked, he fired at a woman passing by who had spoken to him, hitting her in the back. After other failed attempts to enter the synagogue, including shooting at the door, he drove to a kebab shop and started shooting. He returned to his car, shot over the roof, and drove off.

Share   | [Web Link](#)

### **NSA Warns of Vulnerabilities in Multiple VPN Services**

From "NSA Warns of Vulnerabilities in Multiple VPN Services"

*NextGov.com (10/08/19) Corrigan, Jack*

International hackers are taking advantage of bugs in older versions of the virtual private network (VPN) applications produced by Pulse Secure, Fortinet, and Palo Alto Networks. The vulnerability in the Pulse Secure product allows nefarious actors to remotely execute code and download files, as well as intercept encrypted network traffic, while the bugs in the other two systems allow for remote code execution, according to the National Security Agency (NSA). Meanwhile, the U.K.'s National Cyber Security Center published its own warning

about the vulnerabilities on Oct. 2, stating that the exploits could allow hackers to download user credentials. The NSA recommends that users should upgrade to the latest version of the VPN software, and then reset their credentials before reconnecting to the network. The agency also listed a handful of other protective measures users can take to prevent malicious actors from infiltrating their devices.

Share    | [Web Link](#)

#### **Data Breach at Russian ISP Impacts 8.7 Million Customers**

From "Data Breach at Russian ISP Impacts 8.7 Million Customers"  
*ZDNet (10/07/19) Cimpanu, Catalin*

Russian media has recently reported that 8.7 million people's data has been compromised and sold online after Internet service provider Beeline suffered a data breach. The personal data reportedly contains such information as full names, phone numbers, and addresses. Beeline, which has clients in Russia, Asia, and Australia, admitted that the breach took place in 2017, but it did not make any details public until now. The company also said that the stolen data pertained only to Russian customers who had signed up for home broadband connections before November 2016.

Share    | [Web Link](#)

#### **Data Breach Exposes Nearly 1,000 Kaiser Permanente Patients' Information**

From "Data Breach Exposes Nearly 1,000 Kaiser Permanente Patients' Information"  
*ABC10 (10/03/19) Habegger, Becca*

Kaiser Permanente has alerted its members in Northern California to a data breach that may have exposed their personal information. In total, some 990 Sacramento-area Kaiser Permanente members had their information exposed in the breach, which took place in mid-August. According to the company, an unknown and unauthorized individual gained access to the system for approximately 13 hours when he or she broke into an authorized health service provider's email. The hacker snooped on patients' protected health information, including names, medical record numbers, age, gender, provider name, provider comments, diagnosis, medical history, and more. Angela Anderson, Kaiser Permanente Northern California regional compliance director and privacy and security officer, said that the breach was immediately corrected when the company discovered it, adding that there is no "evidence that the information was viewed, used or copied." While Kaiser Permanente found out about the breach on Aug. 19, it did not notify patients until Sept. 27, prompting questions about why it took so long. The healthcare group said it had followed proper reporting procedures.

Share    | [Web Link](#)

#### **The Lack of Cybersecurity Talent Is a 'National Security Threat,' Says DHS Official**

From "The Lack of Cybersecurity Talent Is a 'National Security Threat,' Says DHS Official"  
*Tech Crunch (10/03/19) Shieber, Jonathan*

Jeanette Manfra, the assistant director for cybersecurity for Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), said at a conference that the shortage of cybersecurity talent in the United States constitutes a national security threat. Manfra said that the CISA is prioritizing training new cybersecurity professionals, adding that the talent woes are not confined to the government, but have also constricted the private sector. As a result, Homeland Security is exploring introducing cybersecurity to students in grades K-12, hoping that early exposure will spark more interest in the subject and close the cybersecurity talent gap. Manfra further said that cybersecurity in the country can be tightened if the government and the tech community come together to collaborate on cybersecurity measures. For example, Manfra suggested that the government could pay for scholarships for cybersecurity professionals who



would then spend three to five years working in government before being free to move over to the private sector. Homeland Security is also hoping that the cost of effective cybersecurity defenses will go down in the future, allowing local and state governments to adequately protect themselves against ransomware attacks.

Share    | [Web Link](#)

News summaries © copyright 2019 [SmithBucklin](#)



#### **ASIS INTERNATIONAL**

If you have questions, please contact Member Services at [asis@asisonline.org](mailto:asis@asisonline.org) or +1.703.519.6200, or via 1625 Prince Street, Alexandria, VA 22314 USA.

[Log in to manage your privacy settings.](#) | [Unsubscribe SM Weekly](#)

ASIS International values the privacy and integrity of our members, partners, attendees, exhibitors, and sponsors, and we do not sell your contact information, nor do we provide it to third-party vendors for distribution. [View privacy policy.](#)

From: [Security Management Weekly](#)  
To: [rcortez@SUNNYVALE.CA.GOV](mailto:rcortez@SUNNYVALE.CA.GOV)  
Subject: Security Management Weekly - September 20, 2019  
Date: Friday, September 20, 2019 11:46:13 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



Banner



Advertising/Sponsorship Opportunities | Professional Edition

### Lead Story

#### For Business Continuity, Accept the Unexpected

Security Management Magazine August 2019 Issue

It is one thing to expect the unexpected. It is quite another to accept the unexpected. Denial is a powerful thing, and even the best of us can be convinced that our plans are comprehensive and our preparedness complete. [\(More\)](#)

### Top Security News

#### Iran Warns Against War as U.S. and Saudi Weigh Response to Oil Attack

From "Iran Warns Against War as U.S. and Saudi Weigh Response to Oil Attack" *Reuters (09/19/19) Khalid, Tuqa; Kalin, Stephen*

Iran warned U.S. President Donald Trump on Thursday against being dragged into all-out war in the Middle East following an attack on Saudi Arabian oil facilities which Washington and Riyadh blame on Tehran. U.S. Secretary of State Mike Pompeo has described the weekend strike that initially halved Saudi oil output as an act of war and has been discussing possible retaliation with Saudi Arabia and other Gulf allies. Trump on Wednesday struck a cautious note, saying there were many options short of war with Iran, which denies involvement in the Sept. 14 strikes. He ordered more sanctions on Tehran. Iran's foreign minister responded by asserting that the Islamic Republic "won't blink" if it has to defend itself against any U.S. or Saudi military strike, which he said would lead to "all-out war." Saudi Arabia, which called the assault a "test of global will," on Wednesday displayed what it described as remnants of 25 Iranian drones and missiles used in the strike, saying it was undeniable evidence of Iranian aggression. The United Arab Emirates on Thursday followed its ally Saudi Arabia in announcing it was joining a global maritime security coalition that Washington has been trying to build since a series of explosions on oil tankers in Gulf waters in recent months that were also blamed on Tehran. Pompeo, who arrived in the UAE from Saudi Arabia on Thursday, welcomed the move, saying "Recent events underscore the importance of protecting global commerce and freedom of navigation."

Share | [Web Link](#)

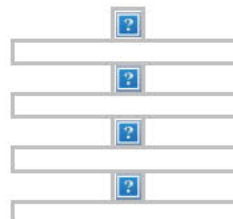
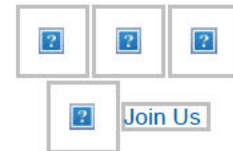


#### Would your employees know what to do in an active shooter situation?

Think. React. Survive.™ Active Assailant Awareness and Response training is a new approach to active assailant education. Developed

September 20, 2019

### Follow Us



### Calendar of Events

#### UPCOMING EVENTS: Webinars

- [Reputation Management: Security's Role During a Crisis \(November 6\)](#)

#### Classroom Programs

- [Making the Business Case for Security \(September 29-October 4th\)](#)
- [Active Assailant \(November 4-5\)](#)
- [Crisis Management \(November 4-5\)](#)
- [Violence Assessment and Intervention \(November 4-5\)](#)
- [Facility Security Design \(November 4-5\)](#)

[Global Events](#)  
[More Classroom Programs](#)  
[More Webinars](#)

by security risk management experts at Hillard Heintze, this online training teaches participants to calmly think and react within the chaos of an unexpected attack. Because it can be accessed via your learning management system, all employees are able to gain skills that will help them make critical decisions in what may be only minutes or seconds. [Learn More](#)

## ASIS News

---

### New in 2019...Security Leaders Mentoring Program

ASIS International is committed to promoting a program of mentorship within our community and to ensuring the standard of excellence for which our profession is known. The goal of the Security Leaders Mentoring Program is to foster mentoring relationships between security professionals, through which advice is shared with those aspiring to enhance their careers or advance within or transition to the security industry.

This program is presented by the ASIS Professional Development Council Mentoring Committee and is an exclusive ASIS member benefit. [Learn more about becoming a Mentor or Mentee today!](#)

Share    | [Web Link](#)



## Top Security News

---

### New Jersey Man Charged With Terrorism Offenses for Targeting Landmarks Like the Statue of Liberty, the White House, and Fenway Park

From "New Jersey Man Charged With Terrorism Offenses for Targeting Landmarks Like the Statue of Liberty, the White House, and Fenway Park" *Associated Press (09/19/19) Neumeister, Larry*

A New Jersey man who allegedly photographed or recorded video of landmarks including the the White House and Boston's Fenway Park as potential terrorism targets in the early to mid-2000s has been charged with terror offenses by authorities who say he was working on behalf of Hezbollah's Islamic Jihad Organization. Alexei Saab, 42, of Morristown, N.J., was arrested July 9 after being questioned during 11 separate sessions with FBI agents since the spring. During interviews, Saab told agents he took photographs of buildings and locations including the Prudential Center in Boston and the Capitol Building and the White House in Washington, D.C. A video of Fenway Park that authorities say was recovered from one of Saab's electronic devices was included in the complaint. Authorities say Saab took surveillance at dozens of locations in New York City, including the United Nations, the Statue of Liberty, Rockefeller Center, Times Square, the Empire State Building and airports, tunnels, and bridges and provided information on those locations to the Islamic Jihad Organization. Besides surveillance activities in the United States, authorities said he also operated abroad, including gathering intelligence for Hezbollah in Istanbul, Turkey. Authorities said Saab joined Hezbollah in 1996 and attended training in 1999, where he learned about firearms, including how to handle military assault rifles and grenades. In 2004 and 2005, he was trained in explosives in Lebanon, they said. Saab entered the United States legally in November 2000 and became a citizen in 2008.

Share    | [Web Link](#)



### Stopper® Station Button for Emergencies

STI's easy-to-use multipurpose Stopper Station push button covers a wide range of applications, and allows a user to perform an



effective and confident action when needed. Offered in red, green, yellow, white, blue or orange with standard or custom labeling. Optional illumination can be used as a status light, indicating activation, and allows the button to be easily located in a dark corridor. Multiple activation choices, including weather resistant. Several tough polycarbonate protective covers available. UL/cUL Listed, ADA Compliant.

### **Secret FBI Subpoenas Scoop Up Personal Data From Scores of Companies**

From "Secret FBI Subpoenas Scoop Up Personal Data From Scores of Companies"

*New York Times (09/20/19) Valentino-DeVries, Jennifer*

The FBI has used secret subpoenas to obtain personal data from far more companies than previously disclosed, newly released documents show. The requests, which the FBI says are critical to its counterterrorism efforts, have raised privacy concerns for years but have been associated mainly with tech companies, but records now show how far beyond Silicon Valley the practice extends — encompassing scores of banks, credit agencies, cellphone carriers, and even universities. The demands can include a variety of information, including usernames, locations, IP addresses, and records of purchases. They do not require a judge's approval and usually come with a gag order, leaving them shrouded in secrecy. Fewer than 20 entities, most of them tech companies, have ever revealed that they have received the subpoenas, known as national security letters. The documents were obtained by the Electronic Frontier Foundation through a Freedom of Information Act lawsuit. The credit agencies Equifax, Experian and TransUnion received a large number of the letters in the filing. So did financial institutions like Bank of America, Western Union and even the Federal Reserve Bank of New York. Other companies included major cellular providers such as AT&T and Verizon, as well as tech giants like Google and Facebook, which have acknowledged receiving the letters in the past. The FBI determined that information on the roughly 750 letters could be disclosed under a 2015 law, the USA Freedom Act, that requires the government to review the secrecy orders "at appropriate intervals."

Share   | [Web Link](#)



### **U.S. Seeks Tighter Security Reviews of Foreign Tech Investments**

From "U.S. Seeks Tighter Security Reviews of Foreign Tech Investments"

*Bloomberg (09/17/19) Sink, Justin; Niquette, Mark*

Foreign investors who want to put money into U.S. businesses that rely on sensitive technology, infrastructure, and data could face greater national-security scrutiny under proposed rules released Tuesday by the Trump administration. The proposed regulations seek to implement a 2018 law that gave an inter-agency review panel known as the Committee on Foreign Investment in the United States greater authority to examine foreign transactions. The new rules expand the timeline and scope of covered transactions. The proposed rules would apply to investments in U.S. businesses with critical technology subject to export controls or other regulations, as well as emerging technologies that the Commerce Department will identify. Critical infrastructure includes telecommunications, energy and transportation, and sensitive personal data includes geolocation, financial, or health-related information that may be exploited at the risk of national security, including data related to targeted populations such military personnel, a Treasury official said. The regulations do not target any particular country, the official said. A limited list of exempted countries is expected to be published when the rule is published in February. Regulators balanced the country's national-security needs against a global business environment that has built a pipeline of foreign money into U.S. companies. Restricting that flow could scare off foreign money that has been a lifeline to such companies as Silicon Valley startups and biotech enterprises.

Industry officials concerned about the implementation said potential regulatory overreach could overwhelm Treasury staff with new filings.

Share    | [Web Link](#)

### **Lawmakers Want to Bring Back Top White House Cybersecurity Post**

From "Lawmakers Want to Bring Back Top White House Cybersecurity Post"  
*Washington Post* (09/19/19) Marks, Joseph

With a new official set to take the reins of the Trump White House's national security strategy, some Democratic lawmakers are pushing for cybersecurity to get more top-level attention. Just hours after President Trump named former hostage negotiator Robert C. O'Brien as his new national security adviser, House Homeland Security Committee Chairman Bennie G. Thompson (D-Miss.) and Sen. Mark Warner (D-Va.), the top Democrat on the Senate Intelligence Committee, both called on O'Brien to reinstate the White House cybersecurity coordinator role eliminated by O'Brien's predecessor, John Bolton. By eliminating the cybersecurity coordinator's job while the government is struggling to repel Russian efforts to hack the 2020 election, Chinese theft of American companies' intellectual property and a surge in private-sector data breaches, Bolton and Trump left the nation dangerously underprotected, the lawmakers said. Bolton's stated reason for eliminating the job in May 2018 was that it duplicated work already being done by policy wonks on the National Security Council. But critics said that vastly underestimated how important cybersecurity is to multiple parts of the government. Within months of Bolton's actions lawmakers had launched multiple efforts to force Trump to reinstate the job. As a result of eliminating the job, Bolton was able to largely run White House cybersecurity policy himself — including pushing a strategy to more consistently hack back against U.S. adversaries.

Share    | [Web Link](#)



### **Tech Execs Tell Lawmakers They're Acting Faster on Extremist Content**

From "Tech Execs Tell Lawmakers They're Acting Faster on Extremist Content"  
*Los Angeles Times* (09/19/19)

Executives from Facebook, Google, and Twitter have told lawmakers that they are getting better at quickly identifying and removing violent extremist content from their social media platforms. Testifying before the Senate Commerce Committee, the executives said they are throwing money at improving the technology to find extremist content and remove it. They also said they are increasingly reaching out to law enforcement to alert them about a potential threat to public safety based on dangerous or violent social media posts. Derek Slater, Google's director of information policy, said that 87 percent of the nine million videos removed from YouTube in the second quarter were found by artificial intelligence, and that many of the videos were taken down before they could accumulate even one view. Slater said that Google decided to be proactive about reaching out to law enforcement in the aftermath of the February 2018 Parkland school shooting. Facebook, meanwhile, is planning to work with law enforcement agencies to train its artificial intelligence to detect extremist content. The social media site was widely criticized earlier this year when a shooter in New Zealand live-streamed his attack and Facebook could not detect the violence in the video. And Nick Pickles, Twitter's director of public policy strategy, said the social media platform proactively suspends accounts for promoting terrorism.

Share    | [Web Link](#) - May Require Paid Subscription

### **London Police and Facebook Move to Stop Live Streaming of Terror Attacks**

From "London Police and Facebook Move to Stop Live Streaming of Terror Attacks"  
*Reuters* (09/17/19)



London police and Facebook said on Tuesday they plan to share resources to stop the live streaming of terrorist attacks like that in Christchurch, New Zealand, earlier this year. The Metropolitan Police will share video of its firearms officers training with Facebook to help the company develop technology to identify the live streaming of an attack on its platform. Social media companies are under increasing pressure to act after a gunman killed 51 people in the New Zealand attack and live-streamed it on Facebook. The carnage was seen fewer than 200 times during the live broadcast, Facebook said in March, but copies of the footage were widely distributed on the platform as well as on Twitter, YouTube, and Facebook-owned WhatsApp and Instagram in the following hours. The police said the footage would be captured on body cameras attached to firearms officers as they carried out their regular training and then shared with Facebook. The video will also be provided to the government for use by other companies developing technology to stop the live streaming of violence on the internet. Britain's top counter-terrorism police officer Neil Basu said Facebook was trying to create technology that could help identify firearms attacks in their early stages and potentially help police across the world in responding.

“

Share    | [Web Link](#)

### **Ecuador Investigates Data Breach of Up to 20 Million People**

From "Ecuador Investigates Data Breach of Up to 20 Million People"  
*New York Times (09/18/19) Karasz, Palko; Kurmanaev, Anatoly*

Ecuador has begun an investigation into a massive data breach in which the personal data of up to 20 million people, more than the country's population, was made available online. The inquiry began after vpnMentor, an internet security firm, alerted the authorities to the enormous security failure, which included the exposure of the data of adults and children, both dead and alive. Ecuador has a population of over 16 million people. A statement from the attorney general on Monday did not indicate whether anyone had gained access to the data while it had been vulnerable. Ecuadorean officials said in a statement on Tuesday that they had detained a man identified as William Roberto G., whom they described as the legal representative of Novaestrat, a small online data consulting firm in the city of Esmeraldas. The attorney general's office said the company, which was founded by former top telecommunication officials, was suspected of being responsible for the information breach. Names, social security numbers, and contact information were among the elements contained in the exposed files. Other sections of the database contained employment information, including job titles and salaries, and bank details, such as account numbers and current balances. The data appeared to come from Ecuadorean government registries, an automobile association and a state-owned bank. It was discovered on an unsecured server in Miami. The breach was closed on Sept. 11, the company's report said.

Share    | [Web Link](#)

### **American Airlines Mechanic Charged With Sabotaging Plane Accused of Having ISIS Videos**

From "American Airlines Mechanic Charged With Sabotaging Plane Accused of Having ISIS Videos"  
*CBSNews.com (09/18/19) Van Cleave, Kris*

An American Airlines mechanic charged with sabotaging a plane is now accused of having ties to terrorists. According to prosecutors, Abdul-Majeed Marouf Ahmed Alani shared videos stored on his phone of ISIS murders. Family of Alani were in court as a federal judge deemed him a danger and a flight risk, citing new evidence of potential terrorist sympathies in denying the 60-year-old mechanic bail. Alani on July 17 allegedly super glued styrofoam inside the nose of an American Airlines 737, interfering with the plane's navigation system, prompting an alert stopping pilots from taking off. At the time, 150 people were on board but no one was hurt. Alani said he was upset about stalled contract talks which had affected him financially. Alani is an Iraqi born naturalized U.S. citizen, who prosecutors now claim shared videos stored on his cell phone of



ISIS murders, made statements wishing Allah would use "divine powers" to harm non-Muslims, had recently sent money to someone in Iraq and has a brother there, who may have ties to the Islamic State. Alani's lawyer said he did not intentionally put people in danger, because the plane had backup systems. Alani passed regular background checks. So far, he has not been charged with any terror-related offenses.

Share    | [Web Link](#)

### **Facebook Contractors Have Been Listening to 'Hey Portal'**

From "Facebook Contractors Have Been Listening to 'Hey Portal'"  
*Bloomberg (09/18/19) Wagner, Kurt; Gurman, Mark*

Facebook, which last month said it stopped using humans to review and transcribe users' voice messages, will resume that practice for some audio collected from its Portal video-calling device. Facebook confirmed Wednesday that it is collecting audio from Portal users who make a request from the device using the command "Hey Portal." By default, those commands were recorded and stored on Facebook servers, and some of them were transcribed by contractors working with the company to improve the software algorithms used to understand the commands, according to Andrew Bosworth, Facebook's head of hardware. That practice was paused last month at the same time Messenger stopped using humans to transcribe messages. "We paused human review of the 'Hey Portal' voice interactions last month while we worked on a plan that gave people more transparency and control, including a way to turn it off," Bosworth said in a statement. Portal is now reinstating human audio transcriptions but will offer consumers an option to turn off that service in a new version of its Portal software, which will be distributed to existing devices and its updated Portal lineup shipping in October. The Messenger transcriptions are separate, Bosworth added, and that program is still on pause.

Share    | [Web Link](#)

### **The Ransomware Crisis Is Going to Get A Lot Worse**

From "The Ransomware Crisis Is Going to Get A Lot Worse"  
*ZDNet (09/15/19) Ranger, Steve*

Ransomware attacks have emerged in recent years as a serious security threat for towns, cities, corporations, and even nations. Ransomware is a favored method of attack from both cybercriminal gangs and hostile nation-states, with both groups looking to cash in on the chaos surrounding a successful attack. Indeed, in recent years high-profile attacks have originated in North Korea and in Russia, and cybercriminals who wrote a ransomware strain said they were retiring after racking up \$2 billion in profits. The surge in ransomware attacks is only going to get worse in the future. Businesses are still collecting data on customers but not adequately protecting it, providing a tempting target for cybercriminals. Meanwhile, companies and their insurers have shown themselves willing to pay ransoms for encrypted data, yet another incentive for malicious actors to strike. While some simple training policies can reduce the likelihood of a company falling victim to a ransomware attack, in some cases increasingly sophisticated attacks will prove too much for companies.

Share    | [Web Link](#)

### **Companies Still Unprepared for GDPR Rule Changes and Potential EU Data Breaches**

From "Companies Still Unprepared for GDPR Rule Changes and Potential EU Data Breaches"  
*TechRepublic (09/16/19) Greig, Jonathan*

A new Ponemon Institute study found that nearly half of organizations surveyed experienced at least one personal data breach that was required to be reported under the General Data Protection Regulation (GDPR) in the last year. However, just 39 percent of U.S. firms and 45 percent of European Union companies actually reported a discovered breach to a GDPR regulator. In every country polled, 25 percent of respondents on average reported a very low level of

preparedness and confidence to deal with GDPR rules about data breaches. More than 50 percent of U.S. companies said they have applied GDPR rules to both U.S. and EU employees while just 43 percent of EU companies are doing the same.

Share    | [Web Link](#)

### **Hackers to Target U.S. Satellite in Security Test**

From "Hackers to Target U.S. Satellite in Security Test"

*The National (United Arab Emirates) (09/18/19) Peachey, Paul*

The United States is offering ethical hackers the chance to try to access a U.S. satellite and demonstrate whether there are significant weaknesses to satellite security that hostile nation-states could exploit. The United States issued the offer after an ethical hackers' convention at the end of the summer revealed there are a handful of security loopholes in the data systems of F-15 fighter jets. The offer invites hackers to try to break a satellite's security systems and turn an earth-facing camera to point at the moon instead. The U.S. Air Force will handle the submissions, vet promising candidates, and invite the best of the best to another ethical hackers' convention next year for a live contest. Space assets, including satellites, have become increasingly important, as any future conflict with another world power would likely take place partially in space. Satellites provide important battlefield information to commanding officers and help shape war strategy. US intelligence officials believe that Russia and China are developing military space teams and building anti-satellite weapons to target U.S. assets and challenge U.S. supremacy in space.

Share    | [Web Link](#)

### **Minnesota Police Arrest Man in Synagogue Fire**

From "Minnesota Police Arrest Man in Synagogue Fire"

*New York Times (09/16/19) Smith, Mitch*

Police in Duluth, Minnesota said on Sunday that they had a man in custody on suspicion of first-degree arson in connection with the fire that destroyed a Duluth synagogue last week. But the police said they had not found evidence to suggest that the crime was motivated by hatred or bias. The fire, reported early in the morning on Sept. 9, tore through the 118-year-old Adas Israel Congregation synagogue near downtown Duluth. One firefighter was injured while combating the fire, which largely destroyed the building. The police identified the suspect as Matthew Amiot, 36, a Duluth resident with an arrest record and no permanent address. He was being held without bail on Sunday, awaiting an initial court appearance. The fire attracted wide attention in part because it came at a time when anti-Semitic crimes and rhetoric have been on the rise nationally. City officials said investigators had gone door to door at nearby apartments to seek witnesses, and had reviewed hundreds of hours of surveillance video. The federal Bureau of Alcohol, Tobacco, Firearms and Explosives helped in the Duluth investigation, a standard practice for fires at religious sites. Shawn Krizaj, the city's fire chief, said that no signs of accelerants were found at the scene.

Share    | [Web Link](#)

### **Americans Failing to Act on Cyber Risk Concerns, Chubb Survey Finds**

From "Americans Failing to Act on Cyber Risk Concerns, Chubb Survey Finds"

*Insurance Journal (09/18/19)*

Chubb's Third Annual Cyber Report concludes that although Americans are concerned about cybersecurity, many have failed to take the preventive steps to protect themselves from a cyberattack. Eight in 10 Americans continue to be concerned about a cyber breach, yet only 41 percent use cybersecurity software and 31 percent regularly change their passwords. These numbers are virtually unchanged from 2018. Fran O'Brien, Division President of Personal Risk Services Chubb North America, says the lack of cybersecurity action is because people think it's too time consuming. "But implementing cyber safeguards today will save time and financial resources tomorrow, should a breach occur," she notes. Businesses are not much better about cybersecurity. While a consistent



number of individuals (75 percent and 70 percent) say that their company has "excellent" or "good" cybersecurity practices in place from 2018 and 2019, many companies continue to fail to implement the most basics safeguards. Chubb says this "education gap" means employees and individuals cannot spot incoming attacks — while 54 percent of respondents correctly defined ransomware, this was the only common form of attack that a majority of individuals could correctly identify. According to Chubb, the continued failure to implement cybersecurity safeguards means a breach is inevitable, but just 10 percent of respondents report having a cyber insurance policy in place. According to Chubb's online study, individuals don't recognize the value of individual pieces of personal data.

Share    | [Web Link](#)

News summaries © copyright 2019 [SmithBucklin](#)



#### **ASIS INTERNATIONAL**

If you have questions, please contact Member Services at [asis@asisonline.org](mailto:asis@asisonline.org) or +1.703.519.6200, or via 1625 Prince Street, Alexandria, VA 22314 USA.

[Log in to manage your privacy settings.](#) | [Unsubscribe SM Weekly](#)

ASIS International values the privacy and integrity of our members, partners, attendees, exhibitors, and sponsors, and we do not sell your contact information, nor do we provide it to third-party vendors for distribution. [View privacy policy.](#)

**From:** [CLA Public Section](#)  
**To:** [John Nagel](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, September 20, 2019 3:17:04 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive](#) (882,252 articles)



[North America](#) | [Global](#)

**USA**

[North America](#)

**Construction**



**Texas Legislative Roundup: Newly Enacted Construction-Related Laws** [Texas](#)

**Adams and Reese LLP**

As of September 1, 2019, all bills enacted in the 2019 Texas legislative session are now in effect. Several of the newly enacted laws impact the...

**Delaware Court Of Chancery Denies Motion To Dismiss Merger Agreement Breach Claims Even Though Defendant Paid The Contractual Termination Fee**

[Delaware](#)

**Shearman & Sterling LLP**

On September 9, 2019, Vice Chancellor Joseph R. Slight III of the Delaware Court of Chancery denied Essendant Inc.'s motion to dismiss an action for...

**Illinois Sets Limits on Retainage Withheld on Private Construction Projects**

[Illinois](#)

**Lewis Rice LLC**

On August 20, 2019, Illinois Governor J. B. Pritzker signed SB 1636 (Public Act 101-0432), which limits the amount of retainage that can be withheld...

**FM Radio Construction Permit and License FCC Applications Moving to New**

## Database Next Week

### Wilkinson Barker Knauer LLP

If you have a commercial or noncommercial FM radio station, an LPFM or an FM translator, and are looking to file an FCC application to seek a...

## Can Florida's Construction Sites Be Hurricane-Proofed?

Florida

### Akerman LLP

One of the biggest threats during a hurricane is windborne debris, and its potential to cause severe property damage and personal injury. Trees...

## Employee Benefits & Pensions



## Payers, Providers, and Patients - Oh My!: Removal under ERISA

Audio

### Crowell & Moring LLP

Payers, Providers, and Patients - Oh My! Is Crowell & Moring's biweekly health care podcast, discussing legal and regulatory issues that affect...

## Say Whaaat? The Sixth Circuit Debates "Corpus Linguistics" as a Tool for Statutory Interpretation

### Bradley Arant Boult Cummings LLP

A seemingly routine Sixth Circuit appeal involving the interpretation of the federal Employee Retirement Income Security Act statute (ERISA) recently...

## Mass. Appeals Court Upholds Somerville's Union Square Revitalization Plan

Massachusetts

### Pierce Atwood LLP

In 2012, the City of Somerville, the Somerville Redevelopment Authority (SRA), and the Massachusetts Department of Housing and Community Development...

## ERISA Arbitration Looks Safer; Ninth Circuit Reverses District Court, Sends Fiduciary Dispute to Arbitration

### Step toe & Johnson LLP

The US Court of Appeals for the Ninth Circuit's recent reversal of the district court's decision in Dorman v. Charles Schwab & Co. has finally opened...

## Sunshine ... on my controlled group makes me happy

### Holland & Hart LLP

The controlled group rules under the IRC are possibly one of the driest and most technical areas in benefits practice, but mistakes in controlled...

## The Impact of ERISA on the Massachusetts Paid Family and Medical Leave Law

Massachusetts

### Mintz

Massachusetts Paid Family and Medical Leave, M.G.L. c. 175M ("MAPFML") establishes a system of paid leave of up to 12 weeks for birth, adoption or...

## Mandatory Arbitration: The Next Frontier for ERISA Retirement Plans?



## **Mayer Brown**

On August 20, 2019, a Ninth Circuit panel in *Dorman v. Schwab*, No. 18-15281, reversed the district court's denial of Schwab's motion to...

---

## **The Check is in the Mail—Or Not**

### **Seyfarth Shaw LLP**

The IRS recently issued somewhat helpful guidance to plan administrators on what to do about the constant problem of uncashed benefit checks from...

---

## **It May Be a Global Economy, but ERISA Wants You to Keep Your Plan Assets in the United States**

### **Morgan Lewis**

Enacted in 1974, ERISA celebrates its 45th Birthday this year. A lot has changed in those 45 years. While ERISA has kept up with the changes at time...

---

## **PBGC's Multiemployer Insurance Program Faces Insolvency, While Single-Employer Program Improves**

### **McDermott Will & Emery**

The Pension Benefit Guaranty Corporation (PBGC) recently issued a press release announcing that the Multiemployer Insurance Program remains in a dire...

---

## **Upcoming Deadline for 403(b) Plan Document Restatements**

### **Venable LLP**

Many colleges and universities provide retirement benefits through a 403(b) plan. The IRS has set a deadline of March 31, 2020 for 403(b) plans to be...

---

## **Considerations for October 1, 2019 Massachusetts Paid Family and Medical Leave Tax**

[Massachusetts](#)

### **Burns & Levinson LLP**

Beginning on October 1, most employers in Massachusetts will be required to withhold tax to fund Massachusetts Paid Family and Medical Leave benefits...

---

## **Will New York Be The Next Gig Economy Battlefield?**

[New York](#)

### **Fisher Phillips**

"Anything you can do, I can do better." That's essentially the sentiment floating around Albany these days as New York lawmakers look enviously...

---

## **Employment & Labor**



## **Employment & Labor in Utah**

[Utah](#)

### **Holland & Hart LLP**

A structured guide in employment and labor in Utah

---

## **Employment & Labor in Nevada**

[Nevada](#)

### **Holland & Hart LLP**

A structured guide to employment & labor law in Nevada...

---

## **Employment & Labor in Colorado** Colorado

### **Holland & Hart LLP**

A structured guide to employment and labor law in Colorado

---

## **Employment & Labor in New Jersey** New Jersey

### **Drinker Biddle & Reath LLP**

A structured guide to employment and labor law in New Jersey

---

## **Oil and gas occupational health and safety labour issues in the USA**

### **Morgan Lewis**

A structured guide to oil and gas health and safety labour issues in the USA

---

## **Hiring and wage & hour law in Arizona** Arizona

### **Ogletree Deakins**

A structured guide to hiring and wage & hour law in Arizona...

---

## **Employment & Labor in Vermont** Vermont

### **Downs Rachlin Martin PLLC**

A structured guide to employment and labor law in Vermont.

---

## **More Good News From The Board: NLRB Scraps The Clear And Unmistakable Waiver Standard For The Contract Coverage Test When Deciding Unilateral Change Cases**

### **Sheppard Mullin Richter & Hampton LLP**

A flurry of critical cases have issued out of the NLRB over the past two weeks. The latest is the Board's decision in MV Transportation, 368 NLRB No...

---

## **New DOL Opinion Letter - No Delaying Designating FMLA Leave, Even When A Collective Bargaining Agreement Provides Otherwise**

### **Jackson Lewis PC**

On September 10, 2019, the Department of Labor issued an FMLA opinion letter stating that an employer may not delay designating paid leave as FMLA...

---

## **California's Small Business Harassment Prevention Training Deadlines Extended**

California

### **Fenwick & West LLP**

California Governor Gavin Newsom on Aug. 30 signed into law a bill that extends the deadline for small businesses (five or more employees) to...

---

## **The State AG Report Weekly Update September 12, 2019**

### **Cozen O'Connor**

50 AGs, led by Texas AG Ken Paxton, announced an investigation into Google over allegedly anticompetitive behavior in violation of state and fed...

---

## **Global investigations around the world: Hong Kong**



## **Global Investigations Review**

Several global banks have been under investigation by the US Securities and Exchange Commission for potential violations of the US Foreign Corrupt...

---

## **California lawmakers enact ABC test with no carveout for gig companies**

California

### **Fisher Phillips**

Negotiations continued right up until the end, but when the dust settled on California's newest employment law, gig economy companies were not spared...

---

## **The Future of The EEO-1: What Does EEOC's Information Collection Really Mean?**

### **Jackson Lewis PC**

As we previously reported , EEOC has filed notice asking for renewed approval to collect EEO-1 Component 1 race, gender and ethnicity workforce data...

---

## **California Law Eliminates Email Reporting for Serious Workplace Accidents**

California

### **Beveridge & Diamond PC**

At the end of August, California Governor Newsom signed AB 1804, a law that alters the method by which employers are to report serious occupational...

---

## **Employers May Not Have To Retain Racists, Sexists And Belligerently Disobedient Employees After All-The NLRB Appears Ready To Rethink Its Positions On Controversial Discipline-Related Doctrines**

### **Sheppard Mullin Richter & Hampton LLP**

It is lawful to discipline and even discharge an employee for making inappropriate or offensive remarks in the workplace. Indeed, current...

---

## **CDC Seeks Additional Comment on Proposed NIOSH Project That Will Survey Engineered Nanomaterial Occupational Safety and Health Practices**

### **Bergeson & Campbell PC**

The Centers for Disease Control and Prevention (CDC) published a Federal Register Notice on September 11, 2019, to provide an additional 30-day...

---

## **California Senate Passes Hotly Contested AB 5 Independent Contractor Bill**

California

### **Seyfarth Shaw LLP**

The California Senate passed a landmark bill, Assembly Bill 5 ("AB 5"), on the evening of September 10, 2019, which could impact businesses'...

---

## **Deadline for sexual harassment prevention training extended to January 1, 2021 for some employees**

California

### **Atkinson Andelson Loya Ruud & Romo**

On August 30, 2019, California Governor Gavin Newsom signed urgency legislation to extend the deadline to provide certain employees required sexual...

---

## **The DOL's New Fiduciary Rule: What Are Some Likely Outcomes?**

### **Hall Benefits Law**

The Department of Labor (DOL) is set to finalize its new fiduciary rule by the end of 2019. The rule covers those giving advice regarding retirement...

---

## **Upcoming Deadline for New York Anti-Harassment Training**

New York

### **Hogan Lovells**

Every employer in New York State should keep an eye on the October 9th, 2019 deadline for employers to adopt and provide mandatory anti-harassment...

---

## **The NLRB Nixes Union Gerrymandering And Establishes A Three Step Test For Voting Unit Determinations**

### **Sheppard Mullin Richter & Hampton LLP**

In the organizing context, the scope of a potential bargaining unit is everything-it determines which employees' votes will count towards...

---

## **United States Employment Update: Summer 2019**

New York

### **Herbert Smith Freehills LLP**

It's been a busy summer for employment law changes, and there are a number of upcoming compliance deadlines which may impact your business. These...

---

## **U.S. Department of Labor Releases Three New Opinion Letters**

### **Goldberg Segalla LLP**

There are three new opinion letters from the U.S. Department of Labor (DOL), which interpret and provide clarity to federal labor laws. These new...

---

## **North Carolina Appellate Decisions Reach Different Conclusions With Regard to Disqualification for Unemployment Benefits Due to Misconduct**

North Carolina

### **Parker Poe Adams & Bernstein LLP**

Under N.C. Gen. Stat. § 96-14.6, individuals are disqualified from receiving unemployment benefits if they are discharged due to misconduct...

---

## **New Jersey's Wage Theft Act Dramatically Increases Potential Penalties for Employers Over Wage and Hour Violations**

New Jersey

### **Saiber LLC**

The Wage Theft Act in New Jersey creates new dangers for employers in the wage and hour landscape and will likely lead to a significant increase in...

---

## **Fall to bring more than just foliage for New York employers**

New York

### **Reed Smith LLP**

New York lawmakers had a busy summer overhauling many of the State's existing workplace laws. Many of the newly enacted changes, as well as others...

---

## **Ohio Federal Judge Crafts An Unprecedented Class Action Mechanism To Bring Relief To Counties And Cities Struggling To Address Opioid Crisis**

Ohio

### **Seyfarth Shaw LLP**



Seyfarth Synopsis: In complex class actions, courts have looked to Rule 23 to authorize class actions either for trial, or for approval of a...

---

### **HAL are you ADA compliant? Recent suits raise questions about digital kiosk compliance under ADA**

**Eversheds Sutherland (US) LLP**

A recent spate of suits against several major retailers has raised questions about whether self-service checkouts and other kiosks must comply with...

---

### **NLRB Creates New 3-Step Analysis for Unit Determinations**

**Littler Mendelson PC**

On September 9, 2019, the National Labor Relations Board (NLRB) issued its decision in *The Boeing Company*, 368 NLRB No. 67 (2019), clarifying an...

---

### **Washington State's New Restrictions on Noncompetition Agreements** Washington

**Cooley LLP**

On May 8, Governor Jay Inslee of Washington State signed into law Engrossed Substitute House Bill 1450, which dramatically alters the state's law...

---

### **Three Major Workplace Bills to Land on Gov. Gavin Newsom's Desk** California

**Sheppard Mullin Richter & Hampton LLP**

Following the launch of the so-called "MeToo" movement, the California Legislature (controlled by a Democratic supermajority) has aggressively...

---

### **AB 5 Update: California Legislature Passes Final Bill on September 11, 2019**

California

**Littler Mendelson PC**

On September 11, 2019, the California Legislature passed Assembly Bill 5 (AB 5). The bill entirely redefines the standard for determining whether a...

---

### **Beltway Buzz, September 13, 2019**

**Ogletree Deakins**

They're Baaaack. Congress is back in session this week, and my commute once again came to a grinding halt. With roughly three months of scheduled...

---

### **Robot Tax Rebuttal**

**Womble Bond Dickinson (US) LLP**

Automation can perform both routine physical activities as well as cognitive capabilities. This capability development has made policymakers and the...

---

### **Ninth Circuit Rejects Lamar Dawson's Bid to Revive Lawsuit**

**Goldberg Segalla LLP**

On August 12, 2019, a panel of Ninth Circuit judges rejected Lamar Dawson's bid to revive a proposed class action lawsuit, which claimed that the...

---

### **#No Filter: Terminating an Employee for Social Media Posts - Part 2**

**Cozen O'Connor**

Prior to the advent of social media and especially the #MeToo movement, employers were generally comfortable drawing a bright line between what...

---

#### **Recent Case Updates Involving the Illinois BIPA** Illinois

##### **Bilzin Sumberg**

The Illinois Biometric Information Privacy Act (BIPA) regulates private businesses' collection, retention, disclosure, destruction, etc. Of...

---

#### **Salary History Bans Continue to Gain Momentum Across the Country (AL, IL, NJ, NY, MO, OH) (US)**

##### **Squire Patton Boggs**

The list of states and cities implementing prohibitions on employer salary history inquiries continues to grow. On June 10, 2019, Alabama enacted the...

---

#### **Good News, You Get Cake ... But No Icing**

##### **Graydon Head & Ritchey LLP**

Since March we have taken on the self-imposed duty to keep you updated on the ever changing status of the EEO-1 data collection. So much so that by...

---

#### **Employees Seeking ADA Accommodations Do Not Have to Make Formal Request**

##### **Parker Poe Adams & Bernstein LLP**

Employees or applicants with disabling medical conditions must place the employer on notice of such condition in order to claim protection under the...

---

#### **A Collective Bargaining Agreement's Management Rights Clause Is No Longer Meaningless**

##### **Vinson & Elkins LLP**

One of the biggest complaints that you will hear from employers with unionized workforces is that it is so difficult to implement minor policy...

---

#### **Ninth Circuit Holds that OSHA Respiratory Protection Standard Requires Employers to Evaluate Potentially Harmful Atmospheres to Determine Whether Respirators are Required**

##### **Keller and Heckman LLP**

In a recent case, Seward Ship's Drydock, Inc.,<sup>[1]</sup> the US Court of Appeals for the Ninth Circuit held that § 1910.134(d) of the OSHA Respiratory...

---

#### **California Lawmakers Send AB5 to Governor's Desk** California

##### **O'Melveny & Myers LLP**

The California Legislature has passed legislation designed to make it much more difficult for companies—including but not limited to those in the...

---

#### **You Can't Go Home Again: Employee's Telework Accommodation Unreasonable, Seventh Circuit Rules**

##### **Jackson Lewis PC**

The Department of Housing and Urban Development ("HUD") did not fail to accommodate a disabled lawyer by rejecting her request to work from home



and...

---

**Calif. App. Court (2nd Dist) Upholds Denial of Class Cert Based on Survey and Statistical Sampling** [California](#)

**Maurice Wutscher LLP**

The Court of Appeal for the Second District of California affirmed an order denying class certification in a wage and hour litigation, holding that...

---

**California Employment Law Notes** [California](#)

**Proskauer Rose LLP**

In the most recent chapter of the ongoing saga regarding the enforceability of arbitration agreements in California, the California Supreme Court has...

---

**New California Law Disrupts Franchise Relationships** [California](#)

**Bryan Cave Leighton Paisner LLP**

Winter is coming for franchisors in California. Last year, the California Supreme Court decided to hold California businesses liable for the violation...

---

**Seventh Circuit Affirms NLRB in Upholding Discharge of Fast and Furious Employee for Highway Misconduct**

**Littler Mendelson PC**

In Local 702, International Brotherhood of Electrical Workers, AFL-CIO v. National Labor Relations Board and Consolidated Communications, the U.S...

---

**California Passes Sweeping New Law Limiting Employer Use Of Independent Contractors (US)** [California](#)

**Squire Patton Boggs**

AB 5, and its "ABC test," expected to have greatest impact in "gig economy" jobs, but impact certain to be even more widely felt After a summer of...

---

**New York City Amends Human Rights Law to Extend Protections to Freelancers and Independent Contractors** [New York](#)

**Littler Mendelson PC**

In recent years both New York State and New York City have actively amended their anti-discrimination laws to expand worker protections. For example...

---

**Arbitration Agreements 101: they require - you guessed it - agreement.**

**Baker Sterchi Cowden & Rice LLC**

The Eighth Circuit has issued a reminder to those seeking to bind employees and consumers to arbitrate future disagreements: don't gloss over...

---

**Illinois's new employment law landscape** [Illinois](#)

**Reed Smith LLP**

A series of bill signings by Illinois Governor J.B. Pritzker have enacted sweeping changes to the landscape of employment law in Illinois. In...

---



## California Sexual Harassment Prevention Training Deadline Extended One Year

California

### Ogletree Deakins

On August 30, 2019, California Governor Gavin Newsom signed Senate Bill (SB) 778 into law, thereby giving employers more time to comply with the...

---

## Applying Epic Systems, The NLRB Adopts Employer-Friendly Arbitration Stance

### Baker McKenzie

As previously detailed here, the U.S. Supreme Court's 2018 Epic Systems decision established that requiring employees to waive their right to pursue...

---

## Another Win for Employer Property Rights: NLRB Loosens Discrimination Definition

### Barnes & Thornburg LLP

Earlier this week, the National Labor Relations Board gave employers another victory in the area of property rights. I recently blogged on a case...

---

## AB 5 Passed! Law on Worker Classification is Changed Again

California

### Leech Tishman Fuscaldo & Lampl LLC

The storyline surrounding California's law concerning independent contractors continues to have many twists and turns. We previously went into detail...

---

## California Supreme Court Rejects Workplace Arbitration Agreement

California

### Barnes & Thornburg LLP

Continuing the trend of California decisions rejecting arbitration of workplace disputes, the California Supreme Court recently rejected an...

---

## California Senate Passes AB 5, Codifying Dynamex Decision

California

### Cooley LLP

On September 10, by a vote of 29-11, the California Senate passed legislation known as AB 5 - a law codifying the "ABC test" from the landmark...

---

## What's in a day? The Full bench of the Federal Court hands down decision in Mondelez AMWU [2019] FCAFC 138

### Russell Kennedy

In August the Full Bench of the Federal Court handed down a decision regarding the meaning of a 'day' for the purpose of personal/carer's leave under...

---

## California Passes Landmark Employment Legislation Redefining Employee Versus Independent Contractor

California

### Duane Morris LLP

The main change: To qualify as an independent contractor, the worker must be performing work that is outside the usual course of the employer's...

---

## Parental Leave Continuation Policy Rejected

Florida

### Goldberg Segalla LLP

Case management is such an important task for litigators. We must plan how best to utilize the allotted and often limited time provided for each case...

---

### **California AB 5 Changes the Landscape for Use of Contractors** California

#### **Sidley Austin LLP**

On September 10, the California Senate passed Assembly Bill 5 (AB 5). The California Assembly passed AB 5 on September 11, and Gov. Gavin Newsom is...

---

### **Majority of CCPA Amendment Bills Passed by California Legislature** California

#### **Hunton Andrews Kurth LLP**

California marked the end of the 2019 legislative session this past Friday, September 13, by passing five out of six pending bills to amend the...

---

### **EEOC Explains How Employers Can Record Non-Binary Employees on EEO-1 Report**

#### **Nelson Mullins Riley & Scarborough LLP**

Covered employers must file their EEO-1 Reports with the EEOC by September 30, 2019. This year will be the first year, however, that employers who...

---

### **Wage and Hour Win for Employers: The California Supreme Court Limits PAGA's Threat to Employers** California

#### **Procopio Cory Hargreaves & Savitch LLP**

The California Supreme Court has provided some much-needed relief to California employers who routinely face Private Attorneys General Act ("PAGA") ...

---

### **CCPA Amendment Effort Largely Fizzles Out: Only Modest Changes Enacted (But Employment Info Is Granted a Partial One-Year Reprieve)** California

#### **Paul Hastings LLP**

The California State Legislature's session ended this weekend after passing a modest selection of amendments to the California Consumer Privacy Act...

---

### **Dear Littler: Do We Have to Provide the Kitchen Sink (Literally!) to Lactating Employees?**

#### **Littler Mendelson PC**

Dear Littler: A long-term San Francisco-based employee with our company is returning soon from maternity leave. In discussing her return date, she...

---

### **Latest California Consumer Privacy Act Amendments Impact Business Compliance Initiatives** California

#### **Pepper Hamilton LLP**

On September 13, the final day of its legislative session, the California Legislature approved five amendments to the California Consumer Privacy Act...

---

### **Top Five Labor Law Developments for August 2019**



### **Jackson Lewis PC**

The National Labor Relations Board (NLRB) found an employer did not violate the National Labor Relations Act (NLRA) by misclassifying its employees...

---

### **From The Jetsons to Reality, or Almost: What Employers Need to Know About Robots and AI in the Workplace**

#### **K&L Gates**

Many readers will remember The Jetsons - a futuristic world in which sophisticated robots in both the home and the workplace had the ability to do...

---

### **Limitations Challenge on Railroad Worker's FELA Claim Denied** Illinois

#### **Goldberg Segalla LLP**

The plaintiff Theresa Romcoe filed suit under the Federal Employers' Liability Act (FELA) against the defendants, Illinois Central Railroad Company...

---

### **California Passes Landmark Bill Restricting Classification of Contract Workers**

California

#### **Skadden Arps Slate Meagher & Flom LLP**

As of September 11, 2019, the California Senate and Assembly had both passed an Employment Bill (AB5) that, if signed by Gov. Gavin Newsom, would...

---

### **Washington Employers Must Provide Break Time and Space for Employees to Express Breast Milk** Washington

#### **Ogletree Deakins**

As of July 28, 2019, Washington employers with 15 or more employees are required to provide reasonable break time for employees to express breast...

---

### **CCPA Update: Legislature Amends the CCPA to Exclude Employee Data, B2B Communications for One Year** California

#### **Kelley Drye & Warren LLP**

Last week, the California legislature voted to send five amendments to the CCPA to the California governor's desk. The amendments include a one-year...

---

### **Fifth Circuit Hands Employers a Big Win, Rules Day Rates Can Satisfy the Salary Basis Under the Highly Compensated Employee Exemption**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: Employers were handed a big win recently when the U.S. Court of Appeals for the Fifth Circuit held that a day rate can satisfy the...

---

### **Countdown to Compliance: EEO-1 Component 2 Submissions Due September 30**

#### **Epstein Becker Green**

The U.S. Equal Employment Opportunity Commission ("EEOC") recently announced that its 2019 EEO-1 Component 2 portal is now open and accepting...

---

### **HSA Contributions are not Earnings for Purposes of Wage Garnishment**

#### **Kilpatrick Townsend & Stockton LLP**

The Department of Labor's Wage and Hour Division (WHD) released Letter

CCPA2019-I on September 10, 2019 (the letter)...

---

### **California's Independent Contractor Bill Signed Into Law—What's Next for Employers?** [California](#)

#### **Winston & Strawn LLP**

Today, California Governor Gavin Newsom signed into law a controversial bill that will expand last year's landmark California Supreme Court decision...

---

### **Easily "Shocked"? At Least for Wage Claims, California Supreme Court Lowers Standard for Unconscionability in Arbitration Agreements** [California](#)

#### **Littler Mendelson PC**

In *OTO, L.L.C. v. Kho*, the California Supreme Court refused to enforce an employee's arbitration agreement on the basis that it was unconscionable...

---

### **EEOC Pay Data Collection: One and Done?**

#### **Barnes & Thornburg LLP**

Employers required to file EEO-1 reports still face a September 30 deadline to submit "Component 2" pay data for 2017 and 2018. EEO-1 forms must be...

---

### **California Legislature Finalizes CCPA Amendments for 2019** [California](#)

#### **Jenner & Block LLP**

After having to suspend their final legislative session day on Friday, September 13, 2019, on Saturday, September 14, the California Legislature...

---

### **What California's New AB 5 Law Means for Employers** [California](#)

#### **Fenwick & West LLP**

California Governor Gavin Newsom on Sept. 18 signed into law Assembly Bill 5, landmark legislation which codifies, and significantly expands, the...

---

### **NLRB Issues Reprieve for Unionized Employers Seeking to Make Unilateral Changes**

#### **Littler Mendelson PC**

Many employers loathe the prospect of unionization due to the potential of a union hampering such employer's ability to make operational changes to...

---

### **NLRB Seeks Public Comment on Offensive Language in the Workplace**

#### **Bass, Berry & Sims PLC**

Can language in the workplace, even if uttered during otherwise protected conduct, lose its "protected" status under the National Labor Relations Act...

---

### **Governor Signs AB5 Into Law — Reshaping California's Independent Contractor Classification Landscape** [California](#)

#### **Payne & Fears LLP**

Today, Governor Gavin Newsom signed California Assembly Bill 5 ("AB5"), controversial legislation which will have a substantial impact on California...

---



## **Back Wages Not Recoverable In PAGA-Only Action, California Supreme Court Says in Arbitration Dispute Ruling** California

### **Barnes & Thornburg LLP**

On Sept. 12, 2019, the California Supreme Court issued a major decision in ZB, N.A. V. Superior Court of California related to the remedies available...

---

## **California Governor Says Gig Unions Are On The Way As He Signs ABC Test Into Law** California

### **Fisher Phillips**

California Governor Gavin Newsom wasted little time by signing AB 5 into law earlier today, and his signing statement should cause quite a few...

---

## **With the Enactment of AB 5, Many Independent Contractors Will Become Employees** California

### **Paul Hastings LLP**

As expected, Governor Newsom has signed AB 5, which will mandate the reclassification of many independent contractors into employees under California...

---

## **I can't drive 55 - or classify my workers**

### **Holland & Hart LLP**

Making correct classifications between independent contractors and employees is not getting simpler with flexible, geographically-distributed...

---

## **What is a Good-Faith Job Search Effort? Michigan Legislature Considers New Bill** Michigan

### **Foster Swift Collins & Smith PC**

MCL 418.301(5) sets forth the four requirements a claimant must satisfy in order to qualify for workers' compensation wage loss benefits. The...

---

## **California Adopts Strict Independent Contractor Test in New Bill** California

### **Pepper Hamilton LLP**

On September 11, the California Assembly passed AB 5, a bill that codifies and expands the application of the strict independent contractor test (the...

---

## **The ABC Test is Here to Stay: California Governor Signs AB 5** California

### **Ogletree Deakins**

On September 18, 2019, Governor Gavin Newsom signed Assembly Bill (AB) 5, which codifies last year's Supreme Court of California decision...

---

## **Employee Liability for Corporate Misconduct--Elizabeth Warren Style: Can Negligence Become Criminal?**

### **Morvillo Abramowitz Grand Iason & Anello PC**

Since the last financial crisis and the resulting increased scrutiny on business entities, companies involved in suspected corporate misconduct...

---



## **Supreme Court Denies Plaintiffs the Ability to Seek Recovery of Unpaid Wages Under PAGA** California

### **Atkinson Andelson Loya Ruud & Romo**

On September 12, 2019, the California Supreme Court decided in a unanimous decision that in a Private Attorneys General Act (PAGA) action seeking to...

---

## **OSHA Appoints New Director of Directorate of Construction (DOC).**

### **Fisher Phillips**

To almost everyone's delight, OSHA has filled the vital position of the Director of the Directorate of Construction (DOC). The DOC Director position...

---

## **CCPA Amendments Update: The More Things Change, the More They Stay the Same**

### **Troutman Sanders LLP**

Over the past year, nearly twenty amendments were introduced to modify the California Consumer Privacy Act of 2018 ("CCPA"). Now that the deadline to...

---

## **Space for Agility: The Rise of the Flexible Workplace**

### **Baker McKenzie**

The footprint of flexible workplaces continues to expand as more and more global businesses embrace the modern workforce and the ever increasing...

---

## **Now What? Practical Tips for Navigating California Post-A.B. 5** California

### **Littler Mendelson PC**

In the coming weeks—or perhaps even days—California Governor Gavin Newsom is expected to sign into law sweeping legislation—Assembly Bill 5 (A.B....

---

## **Caution: Ban Ahead - The Rise in Bans on Salary History Inquiries Requires Employer Diligence**

### **Nexsen Pruet**

A seemingly innocuous interview question is now illegal to ask job applicants in numerous jurisdictions, and the number of jurisdictions implementing...

---

## **Prepare to Implement Paid Family and Medical Leave Under New Massachusetts Law** Massachusetts

### **Holland & Knight LLP**

Massachusetts employers should make their final preparations for the Massachusetts Paid Family and Medical Leave (PFML) program in advance of the Oct...

---

## **New Jersey Passes Law Prohibiting Employers from Requesting Applicant's Salary History** New Jersey

### **Nelson Mullins Riley & Scarborough LLP**

New Jersey recently enacted a new law prohibiting employers from seeking or relying on a job applicant's salary history. The law, which will take...

---

## **Can You Be “Regarded as” Disabled Based on a Potential Future Disability?**

**Jackson Lewis PC**

This certainly sounds futuristic. (Pun intended.) Still, in a case just decided by the Eleventh Circuit Court of Appeals, *EEOC v. STME, LLC*, the EEOC...

---

## **Illinois Outlaws Questions about Job Applicants’ Prior Salaries** Illinois

**Jackson Lewis PC**

Beginning September 29, 2019, it will be against the law in Illinois for employers to ask job applicants about their prior salaries or wage history...

---

## **An Employer’s Bargaining Table Complaints as to Poor Business Conditions Is Not a Claim of Poverty Entitling a Union to Business Sensitive Information**

**Sheppard Mullin Richter & Hampton LLP**

While bargaining, unions often demand that employers produce information relevant to the bargaining process so that the union may fulfill its duties...

---

## **Additional Insight on Applying the Non-Quantitative Limitations under MHPAEA**

**Graydon Head & Ritchey LLP**

We wrote a blog post last year on the proposed FAQs addressing the Mental Health Parity and Addiction Equity Act of 2008 (MHPAEA), specifically as it...

---

## **Benefits Odds and Ends to Start the Fall**

**Nelson Mullins Riley & Scarborough LLP**

With the passing of summer and the children back in school, it is time to get to work and check on benefit compliance items that you may have missed...

---

## **E.D.N.Y.: Class certification evidence must be admissible**

**Kilpatrick Townsend & Stockton LLP**

In a prior post, we reported on the Ninth Circuit’s decision in *Sali v. Corona Regional Medical Center*, 889 F.3d 623 (9th Cir. 2018) that class...

---

## **Lessons in Drafting and Implementing an Enforceable Mandatory Arbitration Agreement** California

**Ford & Harrison LLP**

Recently, the California Supreme Court invalidated a mandatory arbitration agreement in *OTO, LLC v. Kho* (August 29, 2019) finding the agreement was...

---

## **Gainful Employment- October 1 Data Reporting Deadline for 2018-2019**

**Duane Morris LLP**

On July 1, 2019, the U.S. Department of Education published a final rule rescinding the Department’s gainful employment (GE) regulations (2014 Rule)...

---

## **State Law Round-Up: Wage Theft Laws (MN, NJ) and Restrictions on Non-Compete Agreements (ME, MD, NH, OR, RI, WA) (US)**

**Squire Patton Boggs**

In response to Minnesota’s wage theft law, which we previously reported about here, the city of Minneapolis has passed its own wage...



---

## **Employee Agreements: A Method for Mitigating ERISA Fiduciary Exposure?**

### **Hall Benefits Law**

Employment agreements cover a wide range of topics, from setting the compensation terms to protecting a company's intellectual property rights. It's...

---

## **Are Federal Judges Growing Tired Of Attorneys' Fees-Driven Wage-Hour Class Actions?**

### **Epstein Becker Green**

A number of years ago - 20 perhaps - someone shared with me a study that was conducted by a major university where participants were asked which...

---

## **Implementing Illinois' AI Video Interview Act: Five Steps Employers Can Take to Address Hidden Questions and Integrate Policies with Existing Employment Laws**

Illinois

### **Littler Mendelson PC**

In a 2019 survey Littler conducted of over 1,300 in-house counsel, HR professionals and C-suite executives, more than 35% responded that their...

---

## **NLRB Alters Longstanding Bargaining Rights Doctrine**

### **Morgan, Brown & Joy LLP**

In a major change of labor law doctrine, the National Labor Relations Board ("the Board"), in *MV Transportation, Inc.*, 368 N.L.R.B. No. 66 (September...

---

## **Employee Fraud Not a Condition for an Employer's/Insurer's Recoupment of Overpayment**

Michigan

### **Foster Swift Collins & Smith PC**

The Michigan Court of Appeals recently issued a decision which addresses the rights of employers/insurance companies to obtain reimbursement for...

---

## **2 Steps Forward, 1 Step Back: California Supreme Court Nixes Plaintiffs' Ability to Recover Unpaid Wages Under PAGA, but Forecloses Defendants' Path to Arbitration**

California

### **Greenberg Traurig LLP**

On Sept. 12, 2019, the California Supreme Court in *ZB, N.A. V. Superior Court of San Diego County* (Lawson) delivered a victory for California...

---

## **Michigan Employers Act Before the Payroll Fraud Enforcement Unit Comes Knocking**

Michigan

### **Barnes & Thornburg LLP**

Michigan employers who retain independent contractors are beginning to find themselves under scrutiny from the attorney general's newly established...

---

## **MediaBytes - the last month on MediaWrites: Instagram, Airbnb, and an employment law update**

Video

### **Bird & Bird**

In our third instalment of our new video series MediaBytes, Katrina Baxter talks to

the authors of some recent posts which have been stimulating...

---

### **Winter is Coming: Tips for Cold Weather Work and Avoiding Hazards**

**Goldberg Segalla LLP**

As the seasons begin to change, winter weather creates hazardous worksite conditions. Winter brings snow, ice, wind chills, and persistent...

---

### **Never Too Late to Arbitrate? Tips on Getting Your Agreement On**

**Bradley Arant Boult Cummings LLP**

Do your employees sign arbitration agreements? If so, do your arbitration agreements prevent employees from joining class actions against your...

---

### **Anti-Harassment Training Requirements State-by-State Survey**

**Legal Research Center Inc**

This survey examines the laws of every state for workplace sexual harassment training requirements. Laws of selected municipal governments are also...

---

### **California Codifies Employee Classification Standards**

California

**Shearman & Sterling LLP**

On September 10, 2019, the California State Senate passed Assembly Bill 5 (AB 5) effectively requiring certain workers previously operating as...

---

### **Employers Gain Flexibility to Regulate Nonemployee Access to Property under the NLRA**

**Littler Mendelson PC**

On September 6, 2019, the National Labor Relations Board (NLRB or Board) issued its decision in Kroger Limited Partnership I Mid-Atlantic, 368 NLRB...

---

### **Peace for Piece-Rate Employers in Washington**

Washington

**Sheppard Mullin Richter & Hampton LLP**

On September 5, 2019, the Washington Supreme Court issued a huge win for all non-agricultural employers who pay commission or piece-rate pay to their...

---

### **Background Check Best Practices After 5th Circ. EEOC Ruling**

**Butler Snow LLP**

For the last seven years, employers have cautiously approached consideration of applicants' criminal conviction records due to guidance issued by the...

---

### **California Law Impacts All Categories of Independent Contractors - Not Just Gig Workers - What Your Business Needs to Do Now**

California

**Mintz**

The California legislature has now passed AB 5 and, if Governor Gavin Newsom signs the bill into law as expected, California will effectively ban...

---

### **Employers: You Have Two Weeks to Comply New EEO-1 Reports Component 2 Data Due September 30th**

**Newmeyer Dillion**



In case you haven't already heard, on July 1, 2019, the Equal Employment Opportunity Commission ("EEOC") released guidelines and set a deadline for...

---

### **'Go Back to Where You Came From': Employer Liability When Workers Say Xenophobic Things**

**Butler Snow LLP**

President Donald Trump's recent Tweet suggesting that four Democratic congresswomen should "go back and help fix the totally broken and crime...

---

### **Part 24 of "The Restricting Covenant" Series: Choice of Law and Covenants Not to Compete**

[California](#)

[Delaware](#)

**Drinker Biddle & Reath LLP**

There are many notable east coast-West Coast rivalries. In sports (Celtics versus Lakers basketball), in leisure (Atlantic versus Pacific beaches)...

---

### **California Supreme Court Holds That Employees Cannot Recover Allegedly Unpaid Wages in Lawsuits Brought Under PAGA**

[California](#)

**Epstein Becker Green**

We have frequently written about California's Private Attorneys General Act ("PAGA"), a unique statute that allows private individuals to file suit...

---

### **Court: 2013 CADA Amendments Give More Remedies to State Employees**

[Colorado](#)

**Holland & Hart LLP**

On April 4, 2019, the Colorado Court of Appeals issued its decision in Houchin v. Denver Health and Hospital Authority, holding that under 2013...

---

### **California Consumer Privacy Act (CCPA) - Amendment Update**

[California](#)

**Bradley Arant Boult Cummings LLP**

Cybersecurity and Privacy Alert The dust has finally settled in the California State Legislature and the big winner for amendments to the CCPA is...

---

### **National Labor Relations Board Reopens Rules Related to Union Activity**

**Parker Poe Adams & Bernstein LLP**

The National Labor Relations Board continues its efforts to revisit earlier decisions that expanded protections for employees engaged in concerted or...

---

### **Who Are Independent (Contractors)? Throw Your Hands Up At Me!**

[California](#)

**Seyfarth Shaw LLP**

Seyfarth Synopsis: California's hotly contested and closely followed AB 5 independent contractor bill, which would extend the ABC test beyond Wage...

---

### **Michigan Considers a Statutory PTSD Presumption Among First Responders**

[Michigan](#)

[Minnesota](#)

**Foster Swift Collins & Smith PC**

On April 17, 2019, three Michigan State Representatives introduced House Bill



No. 4473 to the Michigan House of Representatives Committee on...

---

### **Is forwarding jerry falwell Jr.'s e-mails a crime?**

#### **Graydon Head & Ritchey LLP**

I saw an interesting article about some controversy at Liberty University and its president Jerry Falwell, Jr. It seems Mr. Falwell is confused about...

---

### **A checklist for drafting Section 457(f) plans for tax-exempt employers**

#### **Thompson Coburn LLP**

Section 457(f) of the Internal Revenue Code ("Code") governs "ineligible" deferred compensation plans or arrangements maintained by tax-exempt...

---

### **California Legislature Passes CCPA Amendments and Privacy Bills** California

#### **Covington & Burling LLP**

Last week, after months of negotiation and speculation, the California legislature passed bills amending the California Consumer Privacy Act ("CCPA")...

---

### **Greater Access to Mental Health Care is on the Horizon**

#### **Mintz**

Employers and retail giants alike are increasingly inserting mental health into the broader, public conversation around individual health care and...

---

### **Important cases for business from the Supreme Court's October 2018 term-Annual Report 2018-2019**

#### **Hunton Andrews Kurth LLP**

The Supreme Court declined to overrule Auer and Seminole Rock, which require courts to defer to a federal agency's reasonable interpretation of its...

---

### **Latest Department of Labor Opinion Letter Addresses the FLSA's Retail/Service Establishment Employee Exemption**

#### **Epstein Becker Green**

The U.S. Department of Labor's Wage and Hour Division ("WHD") continues to issue guidance at a rapid pace, releasing a new opinion letter regarding...

---

### **Second Circuit Rules Against Plaintiff in AutoZone Case and Allows Nixing of her Deposition**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In affirming summary judgment in favor of AutoZone, the Second Circuit rules that a sales associate did not provide enough...

---

### **Independent Contractor "ABC Test" May Soon Be Codified to Apply to Claims Made Under the California Labor and Unemployment Insurance Codes, With Some Exceptions** California

#### **Gordon Rees Scully Mansukhani**

Governor Newsom is expected to sign a bill that may have far-reaching impact on employers who classify and use independent contractors. Assembly Bill...

---

## **DOL Reiterates Employers May Not Delay FMLA Leave**

### **Michael Best & Friedrich LLP**

In an opinion letter issued earlier this week, the Department of Labor addressed whether an employer may delay designation of FMLA leave if its...

---

## **NLRB Puts a Finer Point on Its Community of Interest Test with a New Three-Step Analysis**

### **Proskauer Rose LLP**

Still hard at work as we head into mid-September, the National Labor Relations Board, in a 3-1 decision (Chairman Ring and Members Kaplan and Emanuel...

---

## **"Stud-shaming" may be sex harassment, court says**

### **Constangy Brooks Smith & Prophete LLP**

Showing, again, that workplace gossip can get you sued. I really feel that the employer will win this case, for reasons I'll discuss below, but first...

---

## **Best Practices for Plan Sponsors #11**

### **Drinker Biddle & Reath LLP**

This is the eleventh in a series of articles about Best Practices for Plan Sponsors. To be clear, "best practices" are not the same as legal...

---

## **EEOC Will Not Seek to Renew Component 2 (Pay and Hours Data) Requirements for Future EEO-1 Reports**

### **Proskauer Rose LLP**

The EEOC announced today, September 12, 2019, that it "is not seeking to renew Component 2 of the EEO-1" in a notice published on the Federal...

---

## **Be Prepared for New Federal Overtime Rule Regarding Salary**

### **Holland & Knight LLP**

New federal overtime rules are coming that will impact who qualifies as an exempt employee. Early preparation will avoid challenges when the new rules...

---

## **NLRB sides with Kroger's action to remove union representatives from company property**

### **Porter Wright Morris & Arthur LLP**

On Sept. 6, 2019, the National Labor Relations Board (NLRB) granted a significant win to employers, ruling that businesses can lawfully limit the...

---

## **FMLA Covers Parental Attendance at IEP Meetings**

### **Haynsworth Sinkler Boyd PA**

As students return to school, employers should be mindful of a new U.S. Department of Labor opinion letter impacting when a parent may use qualifying...

---

## **Labor Board Adopts 'Contract Coverage' Standard in Unilateral Change Cases, Overturns Precedent**

### **Jackson Lewis PC**

The National Labor Relations Board (NLRB) has made it easier for employers to



defend against unfair labor practice charges alleging a unilateral...

---

## **NLRB Continues Trend to Protect Employer Property Rights**

### **Ogletree Deakins**

Coming on the heels of its decision in Bexar County Performing Arts Center Foundation d/b/a Tobin Center for the Performing Arts, 368 NLRB No. 46...

---

## **The ABC Test May Soon Be Law in California: What Employers Need to Know**

California

### **Ogletree Deakins**

On September 11, 2019, the California Assembly passed a bill codifying last year's Supreme Court of California decision establishing a new test to...

---

## **No more EEO-1 comp data, EEOC proposes**

### **Constangy Brooks Smith & Prophete LLP**

What a colossal waste this has been. The Equal Employment Opportunity Commission issued a Notice, published in yesterday's Federal Register...

---

## **CA Supreme Court Rules That Employees Cannot Recover Unpaid Wages Through PAGA**

California

### **Baker & Hostetler LLP**

California's Supreme Court has cut off an area of significant potential exposure for California employers by ruling that employees cannot recover...

---

## **California Supreme Court Rejects Claim for Unpaid Wages under PAGA**

California

### **Jackson Lewis PC**

Putting an end to employees' backdoor attempts to recover unpaid wages in Private Attorneys General Act-only actions under California Labor Code...

---

## **California Supreme Court Delivers PAGA Win for Employers**

California

### **Mintz**

In a significant victory for California employers who use arbitration agreements, the California Supreme Court ruled (ZB, N.A. et al. v. Superior...

---

## **Important EEO-1 Component 2 Deadline Approaching This Month**

### **Mintz**

An important deadline approaches for those employers required to file the EEO-1 survey - which generally includes employers with at least 100...

---

## **Could A Mistake by Your Company Nurse Lead to Civil Liability in North Carolina?**

North Carolina

### **Fisher Phillips**

Employers have long operated under the premise that the North Carolina Workers' Compensation Act provides the exclusive remedy for workers injured on...

---

## **California Worker Misclassification Bill Closer to Enactment**

California

### **Jackson Lewis PC**

The California Assembly has passed a bill that would require workers to be classified as employees if the employer exerts control over how the...

---

### **California Supreme Court Limits Potential Recovery Under PAGA** California

#### **Hunton Andrews Kurth LLP**

Yesterday, the California Supreme Court issued its highly-anticipated decision in ZB, N.A. V. Lawson bringing some welcomed good news for California...

---

### **EEOC Presses Pause on Collection of EEO-1 Pay Data After This Year's September 30 Reporting Deadline (US)**

#### **Squire Patton Boggs**

As we have previously reported here, companies with at least 100 employees must collect and report 2017 and 2018 employee pay data information, broken...

---

### **How Safe Is That Harbor? The Impact of the Defend Trade Secrets Act's Whistleblower Immunity Provision on a Trade Secret Owner's Ability to Protect Its Trade Secrets**

#### **Pepper Hamilton LLP**

Imagine that your company has just commenced an internal compliance investigation in response to an allegation that the company is violating various...

---

### **Employers Should be Prepared for the Challenges of the 2019 Hurricane Season**

#### **Ford & Harrison LLP**

As Hurricane Dorian, the first hurricane of the 2019 Atlantic season, bears down on Florida, the approaching storm serves as a...

---

### **The NLRB Acknowledges The Inevitable And Adopts The Contract Coverage Test**

#### **Baker McKenzie**

This week, the National Labor Relations Board finally came to its senses and adopted the contract coverage test for cases alleging an employer had...

---

### **NLRB Holds Misclassifying of Employees Is Not a Violation**

#### **Fox Rothschild LLP**

Misclassification of employees as independent contractors "does not violate the [National Labor Relations] Act," the NLRB held last month. The...

---

### **EEOC Won't Require Employers to Produce EEO-1 Component 2 Data After This Year**

#### **Holland & Knight LLP**

As mentioned in previous Holland & Knight alerts, employers are required, by Sept. 30, 2019, to produce to the U.S. Equal Employment Opportunity...

---

### **CA bill would limit use of independent contractors** California

#### **Constangy Brooks Smith & Prophete LLP**

As many of you may have heard, the California Legislature has passed a major piece of legislation regarding independent contractors. Assembly Bill 5...



---

## **AB 5, Codifying Dynamex and Broadening the ABC Test's Application, Passes California Legislature** California

### **Ford & Harrison LLP**

After months of debate and negotiations, the California State Legislature passed the controversial AB 5 on Wednesday, September 11, 2019, bringing it...

---

## **California Supreme Court Limits PAGA Penalties** California

### **Gordon Rees Scully Mansukhani**

Employers in California have reason to rejoice as the California Supreme Court just issued a landmark ruling: employees can no longer recover...

---

## **NLRB Changes Course on Unilateral Employer Action Standard**

### **Ford & Harrison LLP**

In a 3-1 decision, the National Labor Relations Board (NLRB or the Board) reversed long-held Board precedent regarding when...

---

## **California Supreme Court Hands Employers A Rare Victory, Trims Bloated PAGA Claims** California

### **Proskauer Rose LLP**

Yesterday, the California Supreme Court held that private litigants may not recover unpaid wages under the Labor Code Private Attorneys General Act...

---

## **Colorado Employees Lose it Over Use-It-Or-Lose-It Vacation Policies** Colorado

### **Bryan Cave Leighton Paisner LLP**

Colorado employees are pushing back against the recent decision allowing use-it-or-lose vacation policies in Colorado...

---

## **Better protection for gig economy workers ?** California

### **Freshfields Bruckhaus Deringer**

Increased rights for gig workers continue to be a hot topic around the world. The EU might soon launch new initiatives as Nicolas Schmit, EU...

---

## **Landmark Bill Passes: California Codifies "ABC" Test for Worker Classification**

California

### **Proskauer Rose LLP**

On Thursday, September 12th, the California State Assembly passed Assembly Bill 5 ("AB 5"), the controversial new law that codifies the three-factor...

---

## **NLRB Adopts Management-Friendly Standard on Unilateral Employer Actions**

### **Michael Best & Friedrich LLP**

Unionized businesses should take note of the National Labor Relations Board's ("Board") recent decision in MV Transportation, Inc, where the Board...

---

## **He's Not MY Employee... Or Is He?**

### **Fox Rothschild LLP**



Engaging independent contractors instead of hiring employees is enticing&hellip; no overtime pay, benefits, tax withholdings, FICA obligations or...

---

## **California Supreme Court Hands Employers A Rare Victory, Trims Bloated PAGA Claims** [California](#)

### **Proskauer Rose LLP**

Last week, the California Supreme Court held that private litigants may not recover unpaid wages under the Labor Code Private Attorneys General Act...

---

## **How Much Will AB 5 Really Change California Law?** [California](#)

### **Ogletree Deakins**

The answer is not as much as you may think. Much of the recent media coverage of California's Assembly Bill 5 (AB 5) suggests that the bill...

---

## **Summer Vacation Is Definitely Over At The NLRB (US)**

### **Squire Patton Boggs**

Between August 29 and September 10, the National Labor Relations Board ("NLRB" or "Board") issued four decisions that resolve important issues that...

---

## **Wage Claims After OTO v. Kho: Are Arbitration Agreements Enforceable?**

[California](#)

### **Paul Hastings LLP**

The California Supreme Court recently addressed&mdash;again&mdash;the enforceability of an arbitration agreement of an employee who sought to recover...

---

## **Eighth Circuit Affirms Single Captioned Theatre Performance for Hearing Impaired not Good Enough Under ADA**

### **Baker Sterchi Cowden & Rice LLC**

Title III of the Americans with Disabilities Act specifically prohibits discrimination on the basis of disability in the activities of places of...

---

## **Non-Exempt Employees Traveling for Work: How to Manage the Time Clock**

### **Ford & Harrison LLP**

There may be instances where non-exempt employees are required to travel for business. This is a common practice in the fashion industry where...

---

## **Third Circuit Affirms \$4.5 Million Verdict in Favor of Exotic Dancers**

### **Baker & Hostetler LLP**

A significant amount of wage and hour class/collective jurisprudence has developed around the issue of whether exotic dancers are employees or...

---

## **New California Law Will Reshape Worker Classifications** [California](#)

### **Fox Rothschild LLP**

On Sept. 18, Gov. Gavin Newsom signed AB-5 into law, drastically altering how millions of Californians are paid and vastly complicating the legal...

---

## **The Controversial ABC Test From Dynamex Is Codified In Law — California's Gig Economy Braces For Change** California

**Baker McKenzie**

Today California Governor Gavin Newsom signed a landmark bill making it more difficult for companies to engage independent contractors. (See our...

---

## **NLRB Tips Scales in Favor of Employers When Drawing Distinctions Between Claims of "Inability to Pay" Versus "Competitive Disadvantage," and "Surface" Versus "Hard" Bargaining**

**Proskauer Rose LLP**

In recent weeks, the National Labor Relations Board has issued several employer-friendly decisions, and its September 13 decision in Arlington Metals...

---

## **Postmates Will Deliver Benefits To Gig Workers**

**Fisher Phillips**

Good news for Postmates delivery drivers...and for gig economy businesses across the country. The company recently announced that it would offer...

---

## **MV Transportation Inc. - NLRB rules on employer unilateral action**

**Dinsmore & Shohl LLP**

On Sept. 10, 2019, the National Labor Relations Board (NLRB) issued the MV Transportation decision and adopted the contract coverage standard in...

---

## **California Employers Cheer Rare PAGA Victory** California

**Cozen O'Connor**

The California Supreme Court recently handed down an increasingly rare win for employers and the defense bar with its September 12 decision in Z.B...

---

## **Ninth Circuit Sides With Web Scrapers**

**Sidley Austin LLP**

For years, companies seeking to block web scrapers from collecting the information on their website would invoke the Computer Fraud and Abuse Act...

---

## **Access to Private Property: Labor Board Rules Girl Scout Cookies and Union Protesters are Different**

**Jackson Lewis PC**

A nonemployee's solicitation for charitable or civic causes on an employer's property is not the equivalent of a nonemployee union representative's...

---

## **Will the Middleman Get Stuck with the Bill?** Pennsylvania

**Goldberg Segalla LLP**

From the manufacturer to the distributor to the retailer, most products pass through numerous hands before reaching the consumer. If a defect causes...

---

## **The Practical NLRB Advisor: Summer 2019**

**Ogletree Deakins**

Ogletree Deakins' Traditional Labor Relations Practice Group is pleased to



announce the publication of the summer 2019 issue of the Practical NLRB...

---

### **NLRB Tunes Up Appropriate Standard in Determining Bargaining Unit of Mechanics at Boeing**

**Holland & Knight LLP**

In its decision, The Boeing Company, the National Labor Relations Board clarifies what constitutes an "appropriate" bargaining unit under the...

---

### **Implementing Individual Arbitration Agreements Does Not Violate NLRA, Even If Done After Collective Action is Filed**

**Spencer Fane LLP**

As previously discussed on Spencer Fane Human Resource Solutions, an employer can lawfully require its employees to sign individual arbitration...

---

### **Urgent Reminder: Employers Have Until September 30 to Submit Eeo-1 Pay Data**

**Vorys Sater Seymour and Pease LLP**  
As we previously reported, the Equal Employment Opportunity Commission (EEOC) has been ordered to collect to employers' EEO-1 Component 2 compensation...

---

### **Divorce and Space Crimes**

**Burns & Levinson LLP**

The First Crime in Space! Recent headlines from The New York Times and other prominent news agencies drew in readers stating that the first crime in...

---

### **Eighth Circuit affirms working overtime can be essential job function**

**Reed Smith LLP**

Overtime work is essential in many industries. As a result, employers frequently structure job roles to require mandatory overtime. Although...

---

### **The Women of Amazon Studios' The Boys Offer Lessons on Title VII Retaliation**

**Ford & Harrison LLP**

Piggybacking off my colleague Tim Reed's recent post providing the background/plot and discussing employer liability issues in Amazon Studios'...

---

### **California to Codify Dynamex**

California

**K&L Gates**

The California Legislature has passed Assembly Bill 5 ("AB 5"), which if signed by Governor Gavin Newsom, will codify the California Supreme Court's...

---

Law Department Management



---

### **A Guide to Corporate Taxation**

**Wolters Kluwer Legal & Regulatory**

The reduction of the corporate tax rate was one of the most significant provisions of the historic Tax Cuts and Jobs Act of 2017...

---

**Legal project management challenges: what to look for vs. what you don't expect!**

**Legisway by WoltersKluwer**

The legal department is expected to be a true business partner, helping the business achieve their goals, creating value and keeping a keen eye on...

Public



**Corporate income and franchise taxes in Rhode Island**

Rhode Island

**Adler Pollock & Sheehan**

A structured guide to corporate income and franchise taxes in Rhode Island

**State and Local Taxes in Colorado**

Colorado

**Holland & Hart LLP**

A structured guide to state and local tax law in Colorado

**State and Local Taxes in Rhode Island**

Rhode Island

**Adler Pollock & Sheehan**

A structured guide to state and local taxes in Rhode Island

**Trade controls and foreign investment reviews involving China continue to expand**

Video

**Hogan Lovells**

Against the backdrop of China's growing economic, political and military influence worldwide, the United States is reassessing its economic...

**Emerging Technologies Washington Update- Sep 12, 2019**

District of Columbia

**McGuireWoods Consulting LLC**

This Week: DOT report updates status of automated vehicle, drone regulations; California legislature passes worker classification legislation; House...

**CCPA Security FAQs: Do businesses have to report data breaches to the state of California?**

California

**Bryan Cave Leighton Paisner LLP**

While the CCPA does not require that companies report data breaches to the state of California, California's data breach notification statute, enacted...

**Policy and Political Outlook from Venable's Government Affairs Group**

**Venable LLP**

Congress is back in session, and Venable's Government Affairs Group has assessed the top priorities for the remainder of the 116th Congress...

**Will California Be the First to Ban Fur Sales Statewide?**

California

**Duane Morris LLP**

The California legislature has passed a bill to ban the sale of new fur products anywhere within the state. The bill would make it unlawful to "sell...



## **Sidley perspectives on M&A and Corporate Governance**

### **Sidley Austin LLP**

In exploring a potential public company sale, target boards rightly focus on the amount and type of consideration offered by potential buyers and the...

---

## **Less Than a Month to Go Until Nevada Privacy Law Effective Date** Nevada

### **Baker & Hostetler LLP**

As discussed in our previous blog post on the topic, Nevada's amendments to its privacy law are set to go into effect Oct. 1, 2019...

---

## **NCGA Week in Review- Sep 13, 2019** North Carolina

### **McGuireWoods Consulting LLC**

Members of the North Carolina General Assembly headed back to work this week after taking a few days off following the Labor Day holiday. Many were...

---

## **Lessons Learned: A High-Profile FARA Acquittal at Trial Provides Guidance for Both the Government and Targets of Future Investigations** Washington

### **Vinson & Elkins LLP**

On September 4, a federal jury took only a few hours to return a verdict of "not guilty" for Washington, D.C. attorney and former White House Counsel...

---

## **Municipalities and School Systems: Educate Your Employees** Connecticut

### **Robinson & Cole LLP**

The pace and number of cyber-attacks against municipalities and school systems is staggering and likes of which we have never seen. Municipalities...

---

## **A Syllabus for Regulating Student Data Privacy?**

### **Davis Wright Tremaine LLP**

The start of the new school year is approaching and a number of education vendors have already received their homework assignments. U.S. Senators...

---

## **Republican Retirements Provide Insights into 2020 Election Cycle—and Beyond**

### **Brownstein Hyatt Farber Schreck LLP**

One of the precursors of the Democratic wave that swept the House of Representatives in 2018 was the near-record number of House Republicans who...

---

## **NC Legislative Update: September 13, 2019** North Carolina

### **Nexsen Pruet**

Legislators returned to Raleigh for what turned into a contentious week with new legislative districts in the works, and an unexpected budget veto...

---

## **Commissioner Bob Adler Elected Vice-Chairman of the CPSC, Making Him Acting Chairman of the Agency**

### **Mintz**

Late this afternoon it was confirmed that Commissioner Bob Adler was elected



Vice-Chairman of the CPSC. Because there is no permanent CPSC Chairman at...

---

### **The Inevitability Challenge**

#### **Covington & Burling LLP**

The Government of the Islamic Republic of Iran has, on account of its dismal human rights record and decades of aggression towards its neighbors...

---

### **Washington Healthcare Update- Sep 16, 2019**

[District of Columbia](#)

#### **McGuireWoods Consulting LLC**

This week in Washington: Hearing on public health impact of e-cigarettes, meeting on continuing appropriations for fiscal year 2020, and hearing on...

---

### **The Weekly Hill Update**

#### **Baker & Hostetler LLP**

Below is the Federal Policy team's weekly preview, posted when Congress is in session...

---

### **Foreign Students Subject to Training Location Site Visits**

#### **Green and Spiegel LLC**

Optional Practical Training (OPT) is a training benefit for valid F1 Student Visa holders. It has to be directly related to the student's major and...

---

### **United States Imposes Additional Sanctions on Nicaragua**

#### **Holland & Knight LLP**

The Office of Foreign Assets Control (OFAC) has expanded Executive Order 13851, relating to the sanctions on Nicaragua that block all...

---

### **Junior College Sued Over Controversial "Oklahoma Drill"**

[Pennsylvania](#)

#### **Goldberg Segalla LLP**

The Pennsylvania Supreme Court ruled on August 20, 2019, that Lackawanna Junior College had assumed a duty to care for the well-being of two of the...

---

### **California Senate Bill 206-The Immediate National Impact**

[California](#)

[South Carolina](#)

#### **Jackson Lewis PC**

While California Governor Gavin Newsom considers placing his signature on Senate Bill 206 and making his state the first state in the country to...

---

### **Golden loo still at large after artist insists it was no prank**

#### **Boodle Hatfield**

The 18-carat lavatory is a work by Italian artist Maurizio Cattelan. Called 'America', it was plumbed into the water system at Blenheim Palace so...

---

### **California NCAA Athletes Inch Closer to Earning Compensation**

[California](#)

#### **Goldberg Segalla LLP**

The closely followed bill would allow college athletes to enjoy the capital gained

from their name, images, and likeness. Under current NCAA rules...

---

## **DOD's Cybersecurity Maturity Model Certification and Draft CMMC Model Framework**

**Thompson Hine LLP**

DOD has released its draft CMMC model framework, including detailed new cybersecurity requirements...

---

## **PH Money Matters: This Week in Washington - September 16, 2019**

Washington

**Paul Hastings LLP**

On Tuesday, the President announced via Twitter that he had fired his third national security adviser, John Bolton, as he "disagreed..."

---

## **PH Money Matters: This Week in Washington - September 9, 2019**

Washington

**Paul Hastings LLP**

Over the weekend, the President announced via Twitter that he had canceled a secret meeting with Taliban leaders and Afghanistan's...

---

## **Keep Calm and Carry On - When Immigration Uncertainty Becomes the New Normal**

**Hunton Andrews Kurth LLP**

The UK could leave the EU in 6 weeks, or there may be another delay like the one we saw in April. Brexit watchers have likened the UK to a cat that...

---

## **Education Policy Update- Sep 17, 2019**

**McGuireWoods Consulting LLC**

Education reform was the focus of the legislative session, as Gov. Henry McMaster promised. With the support of the governor, the House quickly...

---

## **Marketer Sparks Outrage for its School Shooting Themed Line of Clothing**

**Frankfurt Kurnit Klein & Selz PC**

Fashion brand Bstroy sparked outrage after featuring a line of school shooting themed sweatshirts during a fashion show. The sweatshirts, which appear...

---

## **Court Provides Further Clarification on Inverse Condemnation Liability**

California

**Nossaman LLP**

We recently reported on the California Supreme Court's decision in Oroville which provided a relaxed standard for public agencies facing inverse...

---

## **Summer 2019 Top antitrust & competition stories**

**Linklaters LLP**

Barely a day has gone by this summer without news of another competition investigation, market study or report involving one of the Big Four Google...

---

## **Global investigations around the world: USA**

**Global Investigations Review**

There is never a shortage of high-profile corporate investigations in the United



States. Since 2000, at least 26 of the US Fortune 100 corporations...

---

**NFHS Argues Paying Student-Athletes Will Erode School Spirit at All Levels**  
**Goldberg Segalla LLP**

On August 23, 2019, the National Federation of State High School Associations (NFHS) asked the Ninth Circuit to grant leave and allow it to file an...

---

**Enforcement proceedings against sovereign states in USA**

**Quinn Emanuel Urquhart & Sullivan LLP**

An overview of key considerations when bringing enforcement proceedings against sovereign states in the courts of USA, including the extent of sovereign immunity, state assets subject to enforcement and service of process.



## Global

### Construction



**ES: Nuevo proceso de licitación pública internacional para el Aeropuerto Internacional de El Salvador "San Óscar Arnulfo Romero y Galdámez"**

**Arias**

Nuevo proceso de licitación pública internacional para el financiamiento, diseño, ampliación, construcción, equipamiento, mejora del mantenimiento y...

### Employment & Labor



**Employment & labour law in Sweden**

**Wigge & Partners**

A structured guide to the recognition and enforcement of foreign judgments in Sweden

---

**Business Immigration in Austria**

**Oberhammer Rechtsanwälte**

A structured guide to business immigration laws in Austria

---

**Employment & labour law in India**

**Kochhar & Co**

A structured guide to employment & labour law in India

---

**Business Immigration in Canada**

**Segal Immigration Law**

A structured guide to business immigration laws in Canada

---

**Oil and gas occupational health and safety labour issues in Nigeria**

**Udo Udoma & Belo-Osagie**

A structured guide to oil and gas health and safety labour issues in Nigeria

---

**Employment & labour law in Nigeria****Udo Udoma & Belo-Osagie**

A structured guide to employment and labour law in Nigeria

---

**Employment & labour law in France****Flichy Grangé Avocats**

A structured guide to employment and labour law in France

---

**Business visitor visas in Canada****Segal Immigration Law**

A structured guide to short-term business visitor visas in Canada

---

**Employment & labour law in Italy****Trifirò & Partners Avvocati**

A structured guide to employment and labour law in Italy

---

**Recruitment and wage & hour law in Germany****Vangard**

A structured guide to background checks, recruitment and wage & hour law in Germany

---

**Business Immigration in Turkey****Bener Law Office**

A structured guide to business immigration laws in Turkey

---

**UK + Comments from other countries - Global Climate Strike: five key questions for employers****Ius Laboris**

On Friday 20 September 2019, an unprecedented 'Global Climate Strike' is set to take place. Millions of employees across the world are being invited...

Law Department Management

**No success without a successor****Latin Lawyer**

Given the strategic value of GCs in today's business environment, succession planning has become of vital importance for the continued success of any...

---

**Tackling Culture in Different Sectors****Allen & Overy LLP**

"What is the difference between a bank, a national sports team and a car manufacturer? When it comes to deep cultural failings leading to widespread...

Public

**Anti-corruption & Bribery in France**

## **Reed Smith LLP**

A structured guide to anti-corruption and bribery in France

---

### **No-deal Brexit: The basics**

#### **Kilburn & Strode LLP**

The UK is set to leave the European Union on 31 October 2019 ('Exit Day'). However, the UK will continue to be party to fundamental IP treaties and...

---

### **The new Singapore Convention: Some practical issues to consider now**

#### **Herbert Smith Freehills LLP**

As has been well publicised, the new Singapore Convention seeks to establish a global enforcement regime for settlement agreements resulting from...

---

## **Other top stories**

**Employment & Labor in Wyoming**

---

**State and Local Taxes in Illinois**

---

**The Directors' Handbook**

---

**Renewable Energy in the USA**

---

**EEOC Announces It Will Not Collect Compensation Data Next Year**

---

**3 Reasons RFPs are the Secret Answer to Your Law Department's AFA Woes**

---

**"Oh AG, Please Don't Let Me Be Misunderstood": Breaking Down Common CCPA Myths**

---

**Tax on Inbound Investment in the USA**

---

**Can Employers get a Grip on Griping? Not all Gripes are Created Equal...**

---

**2019 Year-End Tax Planning Preview**

---

## **International developments**

**Construction in Australia**

---

**UK & EU Data Protection Bulletin: Summer 2019 Highlights**

---

**UK & EU Data Protection Bulletin: Summer 2019 Highlights**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---



---

## Brexit: Temporary Permissions and Contract Continuity

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law

[Contact Lexology](#)

[About Lexology](#)



© 2006-2019 Globe Business Media Group

**From:** [CLA Public Section](#)  
**To:** [Melissa Tronquet](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, September 20, 2019 3:14:01 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive](#) (882,252 articles)



[North America](#) | [Global](#)

**USA**

[North America](#)

[Employee Benefits & Pensions](#)



**Payers, Providers, and Patients - Oh My!: Removal under ERISA** [Audio](#)

**Crowell & Moring LLP**

Payers, Providers, and Patients - Oh My! Is Crowell & Moring's biweekly health care podcast, discussing legal and regulatory issues that affect...

**Say Whaaat? The Sixth Circuit Debates "Corpus Linguistics" as a Tool for Statutory Interpretation**

**Bradley Arant Boult Cummings LLP**

A seemingly routine Sixth Circuit appeal involving the interpretation of the federal Employee Retirement Income Security Act statute (ERISA) recently...

**Mass. Appeals Court Upholds Somerville's Union Square Revitalization Plan**

[Massachusetts](#)

**Pierce Atwood LLP**

In 2012, the City of Somerville, the Somerville Redevelopment Authority (SRA), and the Massachusetts Department of Housing and Community Development...

**ERISA Arbitration Looks Safer; Ninth Circuit Reverses District Court, Sends Fiduciary Dispute to Arbitration**

### **Steptoe & Johnson LLP**

The US Court of Appeals for the Ninth Circuit's recent reversal of the district court's decision in *Dorman v. Charles Schwab & Co.* has finally opened...

---

### **Sunshine ... on my controlled group makes me happy**

#### **Holland & Hart LLP**

The controlled group rules under the IRC are possibly one of the driest and most technical areas in benefits practice, but mistakes in controlled...

---

### **The Impact of ERISA on the Massachusetts Paid Family and Medical Leave Law**

Massachusetts

#### **Mintz**

Massachusetts Paid Family and Medical Leave, M.G.L c. 175M ("MAPFML") establishes a system of paid leave of up to 12 weeks for birth, adoption or...

---

### **Mandatory Arbitration: The Next Frontier for ERISA Retirement Plans?**

#### **Mayer Brown**

On August 20, 2019, a Ninth Circuit panel in *Dorman v. Schwab*, No. 18-15281, reversed the district court's denial of Schwab's motion to...

---

### **The Check is in the Mail—Or Not**

#### **Seyfarth Shaw LLP**

The IRS recently issued somewhat helpful guidance to plan administrators on what to do about the constant problem of uncashed benefit checks from...

---

### **It May Be a Global Economy, but ERISA Wants You to Keep Your Plan Assets in the United States**

#### **Morgan Lewis**

Enacted in 1974, ERISA celebrates its 45th Birthday this year. A lot has changed in those 45 years. While ERISA has kept up with the changes at time...

---

### **PBGC's Multiemployer Insurance Program Faces Insolvency, While Single-Employer Program Improves**

#### **McDermott Will & Emery**

The Pension Benefit Guaranty Corporation (PBGC) recently issued a press release announcing that the Multiemployer Insurance Program remains in a dire...

---

### **Upcoming Deadline for 403(b) Plan Document Restatements**

#### **Venable LLP**

Many colleges and universities provide retirement benefits through a 403(b) plan. The IRS has set a deadline of March 31, 2020 for 403(b) plans to be...

---

### **Considerations for October 1, 2019 Massachusetts Paid Family and Medical Leave Tax**

Massachusetts

#### **Burns & Levinson LLP**

Beginning on October 1, most employers in Massachusetts will be required to



withhold tax to fund Massachusetts Paid Family and Medical Leave benefits...

## Will New York Be The Next Gig Economy Battlefield? New York

**Fisher Phillips**

"Anything you can do, I can do better." That's essentially the sentiment floating around Albany these days as New York lawmakers look enviously...

### Employment & Labor



## Employment & Labor in Utah Utah

**Holland & Hart LLP**

A structured guide in employment and labor in Utah

## Employment & Labor in Colorado Colorado

**Holland & Hart LLP**

A structured guide to employment and labor law in Colorado

## Hiring and wage & hour law in Arizona Arizona

**Ogletree Deakins**

A structured guide to hiring and wage & hour law in Arizona...

## Employment & Labor in Vermont Vermont

**Downs Rachlin Martin PLLC**

A structured guide to employment and labor law in Vermont.

## Employment & Labor in Nevada Nevada

**Holland & Hart LLP**

A structured guide to employment & labor law in Nevada...

## Employment & Labor in New Jersey New Jersey

**Drinker Biddle & Reath LLP**

A structured guide to employment and labor law in New Jersey

## Oil and gas occupational health and safety labour issues in the USA

**Morgan Lewis**

A structured guide to oil and gas health and safety labour issues in the USA

## More Good News From The Board: NLRB Scraps The Clear And Unmistakable Waiver Standard For The Contract Coverage Test When Deciding Unilateral Change Cases

**Sheppard Mullin Richter & Hampton LLP**

A flurry of critical cases have issued out of the NLRB over the past two weeks. The latest is the Board's decision in MV Transportation, 368 NLRB No...

## New DOL Opinion Letter - No Delaying Designating FMLA Leave, Even When A Collective Bargaining Agreement Provides Otherwise

### **Jackson Lewis PC**

On September 10, 2019, the Department of Labor issued an FMLA opinion letter stating that an employer may not delay designating paid leave as FMLA...

---

### **California's Small Business Harassment Prevention Training Deadlines Extended**

California

#### **Fenwick & West LLP**

California Governor Gavin Newsom on Aug. 30 signed into law a bill that extends the deadline for small businesses (five or more employees) to...

---

### **The State AG Report Weekly Update September 12, 2019**

#### **Cozen O'Connor**

50 AGs, led by Texas AG Ken Paxton, announced an investigation into Google over allegedly anticompetitive behavior in violation of state and fed...

---

### **Upcoming Deadline for New York Anti-Harassment Training**

New York

#### **Hogan Lovells**

Every employer in New York State should keep an eye on the October 9th, 2019 deadline for employers to adopt and provide mandatory anti-harassment...

---

### **Global investigations around the world: Hong Kong**

#### **Global Investigations Review**

Several global banks have been under investigation by the US Securities and Exchange Commission for potential violations of the US Foreign Corrupt...

---

### **CDC Seeks Additional Comment on Proposed NIOSH Project That Will Survey Engineered Nanomaterial Occupational Safety and Health Practices**

#### **Bergeson & Campbell PC**

The Centers for Disease Control and Prevention (CDC) published a Federal Register Notice on September 11, 2019, to provide an additional 30-day...

---

### **Deadline for sexual harassment prevention training extended to January 1, 2021 for some employees**

California

#### **Atkinson Andelson Loya Ruud & Romo**

On August 30, 2019, California Governor Gavin Newsom signed urgency legislation to extend the deadline to provide certain employees required sexual...

---

### **California Senate Passes Hotly Contested AB 5 Independent Contractor Bill**

California

#### **Seyfarth Shaw LLP**

The California Senate passed a landmark bill, Assembly Bill 5 ("AB 5"), on the evening of September 10, 2019, which could impact businesses'...

---

### **The DOL's New Fiduciary Rule: What Are Some Likely Outcomes?**

#### **Hall Benefits Law**

The Department of Labor (DOL) is set to finalize its new fiduciary rule by the end of 2019. The rule covers those giving advice regarding retirement...



---

## California lawmakers enact ABC test with no carveout for gig companies

California

### Fisher Phillips

Negotiations continued right up until the end, but when the dust settled on California's newest employment law, gig economy companies were not spared...

---

## The Future of The EEO-1: What Does EEOC's Information Collection Really Mean?

### Jackson Lewis PC

As we previously reported, EEOC has filed notice asking for renewed approval to collect EEO-1 Component 1 race, gender and ethnicity workforce data...

---

## Arbitration Agreements 101: they require - you guessed it - agreement.

### Baker Sterchi Cowden & Rice LLC

The Eighth Circuit has issued a reminder to those seeking to bind employees and consumers to arbitrate future disagreements: don't gloss over...

---

## California Law Eliminates Email Reporting for Serious Workplace Accidents

California

### Beveridge & Diamond PC

At the end of August, California Governor Newsom signed AB 1804, a law that alters the method by which employers are to report serious occupational...

---

## Illinois's new employment law landscape

Illinois

### Reed Smith LLP

A series of bill signings by Illinois Governor J.B. Pritzker have enacted sweeping changes to the landscape of employment law in Illinois. In...

---

## Employers May Not Have To Retain Racists, Sexists And Belligerently Disobedient Employees After All-The NLRB Appears Ready To Rethink Its Positions On Controversial Discipline-Related Doctrines

### Sheppard Mullin Richter & Hampton LLP

It is lawful to discipline and even discharge an employee for making inappropriate or offensive remarks in the workplace. Indeed, current...

---

## California Sexual Harassment Prevention Training Deadline Extended One Year

California

### Ogletree Deakins

On August 30, 2019, California Governor Gavin Newsom signed Senate Bill (SB) 778 into law, thereby giving employers more time to comply with the...

---

## Applying Epic Systems, The NLRB Adopts Employer-Friendly Arbitration Stance

### Baker McKenzie

As previously detailed here, the U.S. Supreme Court's 2018 Epic Systems decision established that requiring employees to waive their right to pursue...

---

## **Another Win for Employer Property Rights: NLRB Loosens Discrimination Definition**

### **Barnes & Thornburg LLP**

Earlier this week, the National Labor Relations Board gave employers another victory in the area of property rights. I recently blogged on a case...

---

## **AB 5 Passed! Law on Worker Classification is Changed Again** California

### **Leech Tishman Fuscaldo & Lampl LLC**

The storyline surrounding California's law concerning independent contractors continues to have many twists and turns. We previously went into detail...

---

## **California Supreme Court Rejects Workplace Arbitration Agreement** California

### **Barnes & Thornburg LLP**

Continuing the trend of California decisions rejecting arbitration of workplace disputes, the California Supreme Court recently rejected an...

---

## **California Senate Passes AB 5, Codifying Dynamex Decision** California

### **Cooley LLP**

On September 10, by a vote of 29-11, the California Senate passed legislation known as AB 5 - a law codifying the "ABC test" from the landmark...

---

## **What's in a day? The Full bench of the Federal Court hands down decision in Mondelez AMWU [2019] FCAFC 138**

### **Russell Kennedy**

In August the Full Bench of the Federal Court handed down a decision regarding the meaning of a 'day' for the purpose of personal/carer's leave under...

---

## **California Passes Landmark Employment Legislation Redefining Employee Versus Independent Contractor** California

### **Duane Morris LLP**

The main change: To qualify as an independent contractor, the worker must be performing work that is outside the usual course of the employer's...

---

## **Parental Leave Continuation Policy Rejected** Florida

### **Goldberg Segalla LLP**

Case management is such an important task for litigators. We must plan how best to utilize the allotted and often limited time provided for each case...

---

## **California AB 5 Changes the Landscape for Use of Contractors** California

### **Sidley Austin LLP**

On September 10, the California Senate passed Assembly Bill 5 (AB 5). The California Assembly passed AB 5 on September 11, and Gov. Gavin Newsom is...

---

## **Majority of CCPA Amendment Bills Passed by California Legislature** California

### **Hunton Andrews Kurth LLP**



California marked the end of the 2019 legislative session this past Friday, September 13, by passing five out of six pending bills to amend the...

---

### **EEOC Explains How Employers Can Record Non-Binary Employees on EEO-1 Report**

**Nelson Mullins Riley & Scarborough LLP**

Covered employers must file their EEO-1 Reports with the EEOC by September 30, 2019. This year will be the first year, however, that employers who...

---

### **Wage and Hour Win for Employers: The California Supreme Court Limits PAGA's Threat to Employers** [California](#)

**Procopio Cory Hargreaves & Savitch LLP**

The California Supreme Court has provided some much-needed relief to California employers who routinely face Private Attorneys General Act ("PAGA")

...

---

### **CCPA Amendment Effort Largely Fizzles Out: Only Modest Changes Enacted (But Employment Info Is Granted a Partial One-Year Reprieve)** [California](#)

**Paul Hastings LLP**

The California State Legislature's session ended this weekend after passing a modest selection of amendments to the California Consumer Privacy Act...

---

### **Dear Littler: Do We Have to Provide the Kitchen Sink (Literally!) to Lactating Employees?**

**Littler Mendelson PC**

Dear Littler: A long-term San Francisco-based employee with our company is returning soon from maternity leave. In discussing her return date, she...

---

### **Latest California Consumer Privacy Act Amendments Impact Business Compliance Initiatives** [California](#)

**Pepper Hamilton LLP**

On September 13, the final day of its legislative session, the California Legislature approved five amendments to the California Consumer Privacy Act...

---

### **Top Five Labor Law Developments for August 2019**

**Jackson Lewis PC**

The National Labor Relations Board (NLRB) found an employer did not violate the National Labor Relations Act (NLRA) by misclassifying its employees...

---

### **From The Jetsons to Reality, or Almost: What Employers Need to Know About Robots and AI in the Workplace**

**K&L Gates**

Many readers will remember The Jetsons - a futuristic world in which sophisticated robots in both the home and the workplace had the ability to do...

---

### **The NLRB Nixes Union Gerrymandering And Establishes A Three Step Test For Voting Unit Determinations**

### **Sheppard Mullin Richter & Hampton LLP**

In the organizing context, the scope of a potential bargaining unit is everything-it determines which employees' votes will count towards...

---

### **Limitations Challenge on Railroad Worker's FELA Claim Denied** Illinois

#### **Goldberg Segalla LLP**

The plaintiff Theresa Romcoe filed suit under the Federal Employers' Liability Act (FELA) against the defendants, Illinois Central Railroad Company...

---

### **United States Employment Update: Summer 2019** New York

#### **Herbert Smith Freehills LLP**

It's been a busy summer for employment law changes, and there are a number of upcoming compliance deadlines which may impact your business. These...

---

### **California Passes Landmark Bill Restricting Classification of Contract Workers**

California

#### **Skadden Arps Slate Meagher & Flom LLP**

As of September 11, 2019, the California Senate and Assembly had both passed an Employment Bill (AB5) that, if signed by Gov. Gavin Newsom, would...

---

### **Washington Employers Must Provide Break Time and Space for Employees to Express Breast Milk** Washington

#### **Ogletree Deakins**

As of July 28, 2019, Washington employers with 15 or more employees are required to provide reasonable break time for employees to express breast...

---

### **U.S. Department of Labor Releases Three New Opinion Letters**

#### **Goldberg Segalla LLP**

There are three new opinion letters from the U.S. Department of Labor (DOL), which interpret and provide clarity to federal labor laws. These new...

---

### **CCPA Update: Legislature Amends the CCPA to Exclude Employee Data, B2B Communications for One Year** California

#### **Kelley Drye & Warren LLP**

Last week, the California legislature voted to send five amendments to the CCPA to the California governor's desk. The amendments include a one-year...

---

### **Fifth Circuit Hands Employers a Big Win, Rules Day Rates Can Satisfy the Salary Basis Under the Highly Compensated Employee Exemption**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: Employers were handed a big win recently when the U.S. Court of Appeals for the Fifth Circuit held that a day rate can satisfy the...

---

### **North Carolina Appellate Decisions Reach Different Conclusions With Regard to Disqualification for Unemployment Benefits Due to Misconduct** North Carolina

#### **Parker Poe Adams & Bernstein LLP**



Under N.C. Gen. Stat. § 96-14.6, individuals are disqualified from receiving unemployment benefits if they are discharged due to misconduct...

---

**Countdown to Compliance: EEO-1 Component 2 Submissions Due September 30**  
**Epstein Becker Green**

The U.S. Equal Employment Opportunity Commission (“EEOC”) recently announced that its 2019 EEO-1 Component 2 portal is now open and accepting...

---

**Can You Be “Regarded as” Disabled Based on a Potential Future Disability?**  
**Jackson Lewis PC**

This certainly sounds futuristic. (Pun intended.) Still, in a case just decided by the Eleventh Circuit Court of Appeals, EEOC v. STME, LLC, the EEOC...

---

**New Jersey’s Wage Theft Act Dramatically Increases Potential Penalties for Employers Over Wage and Hour Violations** New Jersey

**Saiber LLC**

The Wage Theft Act in New Jersey creates new dangers for employers in the wage and hour landscape and will likely lead to a significant increase in...

---

**Illinois Outlaws Questions about Job Applicants’ Prior Salaries** Illinois

**Jackson Lewis PC**

Beginning September 29, 2019, it will be against the law in Illinois for employers to ask job applicants about their prior salaries or wage history...

---

**An Employer’s Bargaining Table Complaints as to Poor Business Conditions Is Not a Claim of Poverty Entitling a Union to Business Sensitive Information**

**Sheppard Mullin Richter & Hampton LLP**

While bargaining, unions often demand that employers produce information relevant to the bargaining process so that the union may fulfill its duties...

---

**Additional Insight on Applying the Non-Quantitative Limitations under MHPAEA**  
**Graydon Head & Ritchey LLP**

We wrote a blog post last year on the proposed FAQs addressing the Mental Health Parity and Addiction Equity Act of 2008 (MHPAEA), specifically as it...

---

**Fall to bring more than just foliage for New York employers** New York

**Reed Smith LLP**

New York lawmakers had a busy summer overhauling many of the State’s existing workplace laws. Many of the newly enacted changes, as well as others...

---

**Benefits Odds and Ends to Start the Fall**  
**Nelson Mullins Riley & Scarborough LLP**

With the passing of summer and the children back in school, it is time to get to work and check on benefit compliance items that you may have missed...

---

**E.D.N.Y.: Class certification evidence must be admissible**  
**Kilpatrick Townsend & Stockton LLP**



In a prior post, we reported on the Ninth Circuit's decision in *Sali v. Corona Regional Medical Center*, 889 F.3d 623 (9th Cir. 2018) that class...

---

### **Ohio Federal Judge Crafts An Unprecedented Class Action Mechanism To Bring Relief To Counties And Cities Struggling To Address Opioid Crisis**

Ohio

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In complex class actions, courts have looked to Rule 23 to authorize class actions either for trial, or for approval of a...

---

### **Lessons in Drafting and Implementing an Enforceable Mandatory Arbitration Agreement**

California

#### **Ford & Harrison LLP**

Recently, the California Supreme Court invalidated a mandatory arbitration agreement in *OTO, LLC v. Kho* (August 29, 2019) finding the agreement was...

---

### **HAL are you ADA compliant? Recent suits raise questions about digital kiosk compliance under ADA**

#### **Eversheds Sutherland (US) LLP**

A recent spate of suits against several major retailers has raised questions about whether self-service checkouts and other kiosks must comply with...

---

### **Gainful Employment- October 1 Data Reporting Deadline for 2018-2019**

#### **Duane Morris LLP**

On July 1, 2019, the U.S. Department of Education published a final rule rescinding the Department's gainful employment (GE) regulations (2014 Rule)...

---

### **NLRB Creates New 3-Step Analysis for Unit Determinations**

#### **Littler Mendelson PC**

On September 9, 2019, the National Labor Relations Board (NLRB) issued its decision in *The Boeing Company*, 368 NLRB No. 67 (2019), clarifying an...

---

### **State Law Round-Up: Wage Theft Laws (MN, NJ) and Restrictions on Non-Compete Agreements (ME, MD, NH, OR, RI, WA) (US)**

#### **Squire Patton Boggs**

In response to Minnesota's wage theft law, which we previously reported about here, the city of Minneapolis has passed its own wage...

---

### **Employee Agreements: A Method for Mitigating ERISA Fiduciary Exposure?**

#### **Hall Benefits Law**

Employment agreements cover a wide range of topics, from setting the compensation terms to protecting a company's intellectual property rights. It's...

---

### **Washington State's New Restrictions on Noncompetition Agreements**

Washington

#### **Cooley LLP**

On May 8, Governor Jay Inslee of Washington State signed into law Engrossed Substitute House Bill 1450, which dramatically alters the state's law...

---

## **Are Federal Judges Growing Tired Of Attorneys' Fees-Driven Wage-Hour Class Actions?**

**Epstein Becker Green**

A number of years ago - 20 perhaps - someone shared with me a study that was conducted by a major university where participants were asked which...

---

## **Three Major Workplace Bills to Land on Gov. Gavin Newsom's Desk** California

**Sheppard Mullin Richter & Hampton LLP**

Following the launch of the so-called "MeToo" movement, the California Legislature (controlled by a Democratic supermajority) has aggressively...

---

## **AB 5 Update: California Legislature Passes Final Bill on September 11, 2019**

California

**Littler Mendelson PC**

On September 11, 2019, the California Legislature passed Assembly Bill 5 (AB 5). The bill entirely redefines the standard for determining whether a...

---

## **Implementing Illinois' AI Video Interview Act: Five Steps Employers Can Take to Address Hidden Questions and Integrate Policies with Existing Employment Laws** Illinois

**Littler Mendelson PC**

In a 2019 survey Littler conducted of over 1,300 in-house counsel, HR professionals and C-suite executives, more than 35% responded that their...

---

## **Beltway Buzz, September 13, 2019**

**Ogletree Deakins**

They're Baaaack. Congress is back in session this week, and my commute once again came to a grinding halt. With roughly three months of scheduled...

---

## **Robot Tax Rebuttal**

**Womble Bond Dickinson (US) LLP**

Automation can perform both routine physical activities as well as cognitive capabilities. This capability development has made policymakers and the...

---

## **NLRB Alters Longstanding Bargaining Rights Doctrine**

**Morgan, Brown & Joy LLP**

In a major change of labor law doctrine, the National Labor Relations Board ("the Board"), in *MV Transportation, Inc.*, 368 N.L.R.B. No. 66 (September...

---

## **Employee Fraud Not a Condition for an Employer's/Insurer's Recoupment of Overpayment** Michigan

**Foster Swift Collins & Smith PC**

The Michigan Court of Appeals recently issued a decision which addresses the rights of employers/insurance companies to obtain reimbursement for...

---

## **Ninth Circuit Rejects Lamar Dawson's Bid to Revive Lawsuit**

**Goldberg Segalla LLP**



On August 12, 2019, a panel of Ninth Circuit judges rejected Lamar Dawson's bid to revive a proposed class action lawsuit, which claimed that the...

---

## **2 Steps Forward, 1 Step Back: California Supreme Court Nixes Plaintiffs' Ability to Recover Unpaid Wages Under PAGA, but Forecloses Defendants' Path to Arbitration**

California

### **Greenberg Traurig LLP**

On Sept. 12, 2019, the California Supreme Court in *ZB, N.A. V. Superior Court of San Diego County (Lawson)* delivered a victory for California...

---

## **#No Filter: Terminating an Employee for Social Media Posts - Part 2**

### **Cozen O'Connor**

Prior to the advent of social media and especially the #MeToo movement, employers were generally comfortable drawing a bright line between what...

---

## **Michigan Employers Act Before the Payroll Fraud Enforcement Unit Comes Knocking**

Michigan

### **Barnes & Thornburg LLP**

Michigan employers who retain independent contractors are beginning to find themselves under scrutiny from the attorney general's newly established...

---

## **Recent Case Updates Involving the Illinois BIPA**

Illinois

### **Bilzin Sumberg**

The Illinois Biometric Information Privacy Act (BIPA) regulates private businesses' collection, retention, disclosure, destruction, etc. Of...

---

## **MediaBytes - the last month on MediaWrites: Instagram, Airbnb, and an employment law update**

Video

### **Bird & Bird**

In our third instalment of our new video series MediaBytes, Katrina Baxter talks to the authors of some recent posts which have been stimulating...

---

## **Salary History Bans Continue to Gain Momentum Across the Country (AL, IL, NJ, NY, MO, OH) (US)**

### **Squire Patton Boggs**

The list of states and cities implementing prohibitions on employer salary history inquiries continues to grow. On June 10, 2019, Alabama enacted the...

---

## **Winter is Coming: Tips for Cold Weather Work and Avoiding Hazards**

### **Goldberg Segalla LLP**

As the seasons begin to change, winter weather creates hazardous worksite conditions. Winter brings snow, ice, wind chills, and persistent...

---

## **Good News, You Get Cake ... But No Icing**

### **Graydon Head & Ritchey LLP**

Since March we have taken on the self-imposed duty to keep you updated on the ever changing status of the EEO-1 data collection. So much so that by...

---

**Employees Seeking ADA Accommodations Do Not Have to Make Formal Request**  
**Parker Poe Adams & Bernstein LLP**

Employees or applicants with disabling medical conditions must place the employer on notice of such condition in order to claim protection under the...

---

**A Collective Bargaining Agreement's Management Rights Clause Is No Longer Meaningless**

**Vinson & Elkins LLP**

One of the biggest complaints that you will hear from employers with unionized workforces is that it is so difficult to implement minor policy...

---

**Never Too Late to Arbitrate? Tips on Getting Your Agreement On**  
**Bradley Arant Boult Cummings LLP**

Do your employees sign arbitration agreements? If so, do your arbitration agreements prevent employees from joining class actions against your...

---

**Anti-Harassment Training Requirements State-by-State Survey**  
**Legal Research Center Inc**

This survey examines the laws of every state for workplace sexual harassment training requirements. Laws of selected municipal governments are also...

---

**Ninth Circuit Holds that OSHA Respiratory Protection Standard Requires Employers to Evaluate Potentially Harmful Atmospheres to Determine Whether Respirators are Required**

**Keller and Heckman LLP**

In a recent case, *Seward Ship's Drydock, Inc.*, [1] the US Court of Appeals for the Ninth Circuit held that § 1910.134(d) of the OSHA Respiratory...

---

**California Codifies Employee Classification Standards**

California

**Shearman & Sterling LLP**

On September 10, 2019, the California State Senate passed Assembly Bill 5 (AB 5) effectively requiring certain workers previously operating as...

---

**California Lawmakers Send AB5 to Governor's Desk**

California

**O'Melveny & Myers LLP**

The California Legislature has passed legislation designed to make it much more difficult for companies—including but not limited to those in the...

---

**Employers Gain Flexibility to Regulate Nonemployee Access to Property under the NLRA**

**Littler Mendelson PC**

On September 6, 2019, the National Labor Relations Board (NLRB or Board) issued its decision in *Kroger Limited Partnership I Mid-Atlantic*, 368 NLRB...

---

**You Can't Go Home Again: Employee's Telework Accommodation Unreasonable, Seventh Circuit Rules**



### **Jackson Lewis PC**

The Department of Housing and Urban Development (“HUD”) did not fail to accommodate a disabled lawyer by rejecting her request to work from home and...

---

### **Peace for Piece-Rate Employers in Washington** Washington

#### **Sheppard Mullin Richter & Hampton LLP**

On September 5, 2019, the Washington Supreme Court issued a huge win for all non-agricultural employers who pay commission or piece-rate pay to their...

---

### **Calif. App. Court (2nd Dist) Upholds Denial of Class Cert Based on Survey and Statistical Sampling** California

#### **Maurice Wutscher LLP**

The Court of Appeal for the Second District of California affirmed an order denying class certification in a wage and hour litigation, holding that...

---

### **Background Check Best Practices After 5th Circ. EEOC Ruling**

#### **Butler Snow LLP**

For the last seven years, employers have cautiously approached consideration of applicants' criminal conviction records due to guidance issued by the...

---

### **California Employment Law Notes** California

#### **Proskauer Rose LLP**

In the most recent chapter of the ongoing saga regarding the enforceability of arbitration agreements in California, the California Supreme Court has...

---

### **California Law Impacts All Categories of Independent Contractors - Not Just Gig Workers - What Your Business Needs to Do Now** California

#### **Mintz**

The California legislature has now passed AB 5 and, if Governor Gavin Newsom signs the bill into law as expected, California will effectively ban...

---

### **Employers: You Have Two Weeks to Comply New EEO-1 Reports Component 2 Data Due September 30th**

#### **Newmeyer Dillion**

In case you haven't already heard, on July 1, 2019, the Equal Employment Opportunity Commission (“EEOC”) released guidelines and set a deadline for...

---

### **New California Law Disrupts Franchise Relationships** California

#### **Bryan Cave Leighton Paisner LLP**

Winter is coming for franchisors in California. Last year, the California Supreme Court decided to hold California businesses liable for the violation...

---

### **‘Go Back to Where You Came From’: Employer Liability When Workers Say Xenophobic Things**

#### **Butler Snow LLP**



President Donald Trump's recent Tweet suggesting that four Democratic congresswomen should "go back and help fix the totally broken and crime...

---

### **Seventh Circuit Affirms NLRB in Upholding Discharge of Fast and Furious Employee for Highway Misconduct**

**Littler Mendelson PC**

In *Local 702, International Brotherhood of Electrical Workers, AFL-CIO v. National Labor Relations Board and Consolidated Communications*, the U.S...

---

### **California Passes Sweeping New Law Limiting Employer Use Of Independent Contractors (US)**

California

**Squire Patton Boggs**

AB 5, and its "ABC test," expected to have greatest impact in "gig economy" jobs, but impact certain to be even more widely felt After a summer of...

---

### **Part 24 of "The Restricting Covenant" Series: Choice of Law and Covenants Not to Compete**

California

Delaware

**Drinker Biddle & Reath LLP**

There are many notable east coast-West Coast rivalries. In sports (Celtics versus Lakers basketball), in leisure (Atlantic versus Pacific beaches)...

---

### **California Supreme Court Holds That Employees Cannot Recover Allegedly Unpaid Wages in Lawsuits Brought Under PAGA**

California

**Epstein Becker Green**

We have frequently written about California's Private Attorneys General Act ("PAGA"), a unique statute that allows private individuals to file suit...

---

### **Court: 2013 CADA Amendments Give More Remedies to State Employees**

Colorado

**Holland & Hart LLP**

On April 4, 2019, the Colorado Court of Appeals issued its decision in *Houchin v. Denver Health and Hospital Authority*, holding that under 2013...

---

### **New York City Amends Human Rights Law to Extend Protections to Freelancers and Independent Contractors**

New York

**Littler Mendelson PC**

In recent years both New York State and New York City have actively amended their anti-discrimination laws to expand worker protections. For example...

---

### **California Consumer Privacy Act (CCPA) - Amendment Update**

California

**Bradley Arant Boult Cummings LLP**

Cybersecurity and Privacy Alert The dust has finally settled in the California State Legislature and the big winner for amendments to the CCPA is...

---

### **National Labor Relations Board Reopens Rules Related to Union Activity**

**Parker Poe Adams & Bernstein LLP**

The National Labor Relations Board continues its efforts to revisit earlier decisions that expanded protections for employees engaged in concerted or...

---

### **Who Are Independent (Contractors)? Throw Your Hands Up At Me!**

California

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: California's hotly contested and closely followed AB 5 independent contractor bill, which would extend the ABC test beyond Wage...

---

### **Michigan Considers a Statutory PTSD Presumption Among First Responders**

Michigan

Minnesota

#### **Foster Swift Collins & Smith PC**

On April 17, 2019, three Michigan State Representatives introduced House Bill No. 4473 to the Michigan House of Representatives Committee on...

---

### **Is forwarding jerry falwell Jr.'s e-mails a crime?**

#### **Graydon Head & Ritchey LLP**

I saw an interesting article about some controversy at Liberty University and its president Jerry Falwell, Jr. It seems Mr. Falwell is confused about...

---

### **A checklist for drafting Section 457(f) plans for tax-exempt employers**

#### **Thompson Coburn LLP**

Section 457(f) of the Internal Revenue Code ("Code") governs "ineligible" deferred compensation plans or arrangements maintained by tax-exempt...

---

### **California Legislature Passes CCPA Amendments and Privacy Bills**

California

#### **Covington & Burling LLP**

Last week, after months of negotiation and speculation, the California legislature passed bills amending the California Consumer Privacy Act ("CCPA")...

---

### **Greater Access to Mental Health Care is on the Horizon**

#### **Mintz**

Employers and retail giants alike are increasingly inserting mental health into the broader, public conversation around individual health care and...

---

### **Important cases for business from the Supreme Court's October 2018 term- Annual Report 2018-2019**

#### **Hunton Andrews Kurth LLP**

The Supreme Court declined to overrule Auer and Seminole Rock, which require courts to defer to a federal agency's reasonable interpretation of its...

---

### **Latest Department of Labor Opinion Letter Addresses the FLSA's Retail/Service Establishment Employee Exemption**

#### **Epstein Becker Green**

The U.S. Department of Labor's Wage and Hour Division ("WHD") continues to issue guidance at a rapid pace, releasing a new opinion letter regarding...

---

### **Second Circuit Rules Against Plaintiff in AutoZone Case and Allows Nixing of**



## **her Deposition**

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: In affirming summary judgment in favor of AutoZone, the Second Circuit rules that a sales associate did not provide enough...

---

## **HSA Contributions are not Earnings for Purposes of Wage Garnishment**

### **Kilpatrick Townsend & Stockton LLP**

The Department of Labor's Wage and Hour Division (WHD) released Letter CCPA2019-I on September 10, 2019 (the letter)...

---

## **California's Independent Contractor Bill Signed Into Law—What's Next for Employers?**

California

### **Winston & Strawn LLP**

Today, California Governor Gavin Newsom signed into law a controversial bill that will expand last year's landmark California Supreme Court decision...

---

## **Easily "Shocked"? At Least for Wage Claims, California Supreme Court Lowers Standard for Unconscionability in Arbitration Agreements**

California

### **Littler Mendelson PC**

In OTO, L.L.C. V. Kho, the California Supreme Court refused to enforce an employee's arbitration agreement on the basis that it was unconscionable...

---

## **EEOC Pay Data Collection: One and Done?**

### **Barnes & Thornburg LLP**

Employers required to file EEO-1 reports still face a September 30 deadline to submit "Component 2" pay data for 2017 and 2018. EEO-1 forms must be...

---

## **California Legislature Finalizes CCPA Amendments for 2019**

California

### **Jenner & Block LLP**

After having to suspend their final legislative session day on Friday, September 13, 2019, on Saturday, September 14, the California Legislature...

---

## **What California's New AB 5 Law Means for Employers**

California

### **Fenwick & West LLP**

California Governor Gavin Newsom on Sept. 18 signed into law Assembly Bill 5, landmark legislation which codifies, and significantly expands, the...

---

## **NLRB Issues Reprieve for Unionized Employers Seeking to Make Unilateral Changes**

### **Littler Mendelson PC**

Many employers loathe the prospect of unionization due to the potential of a union hampering such employer's ability to make operational changes to...

---

## **NLRB Seeks Public Comment on Offensive Language in the Workplace**

### **Bass, Berry & Sims PLC**

Can language in the workplace, even if uttered during otherwise protected conduct, lose its "protected" status under the National Labor Relations Act...

---

## **Governor Signs AB5 Into Law — Reshaping California's Independent Contractor Classification Landscape** [California](#)

### **Payne & Fears LLP**

Today, Governor Gavin Newsom signed California Assembly Bill 5 ("AB5"), controversial legislation which will have a substantial impact on California...

---

## **Back Wages Not Recoverable In PAGA-Only Action, California Supreme Court Says in Arbitration Dispute Ruling** [California](#)

### **Barnes & Thornburg LLP**

On Sept. 12, 2019, the California Supreme Court issued a major decision in ZB, N.A. V. Superior Court of California related to the remedies available...

---

## **California Governor Says Gig Unions Are On The Way As He Signs ABC Test Into Law** [California](#)

### **Fisher Phillips**

California Governor Gavin Newsom wasted little time by signing AB 5 into law earlier today, and his signing statement should cause quite a few...

---

## **With the Enactment of AB 5, Many Independent Contractors Will Become Employees** [California](#)

### **Paul Hastings LLP**

As expected, Governor Newsom has signed AB 5, which will mandate the reclassification of many independent contractors into employees under California...

---

## **I can't drive 55 - or classify my workers**

### **Holland & Hart LLP**

Making correct classifications between independent contractors and employees is not getting simpler with flexible, geographically-distributed...

---

## **What is a Good-Faith Job Search Effort? Michigan Legislature Considers New Bill** [Michigan](#)

### **Foster Swift Collins & Smith PC**

MCL 418.301(5) sets forth the four requirements a claimant must satisfy in order to qualify for workers' compensation wage loss benefits. The...

---

## **California Adopts Strict Independent Contractor Test in New Bill** [California](#)

### **Pepper Hamilton LLP**

On September 11, the California Assembly passed AB 5, a bill that codifies and expands the application of the strict independent contractor test (the...

---

## **The ABC Test is Here to Stay: California Governor Signs AB 5** [California](#)

### **Ogletree Deakins**

On September 18, 2019, Governor Gavin Newsom signed Assembly Bill (AB) 5, which codifies last year's Supreme Court of California decision...

---



## **Employee Liability for Corporate Misconduct--Elizabeth Warren Style: Can Negligence Become Criminal?**

**Morvillo Abramowitz Grand Iason & Anello PC**

Since the last financial crisis and the resulting increased scrutiny on business entities, companies involved in suspected corporate misconduct...

---

## **Supreme Court Denies Plaintiffs the Ability to Seek Recovery of Unpaid Wages Under PAGA** California

**Atkinson Andelson Loya Ruud & Romo**

On September 12, 2019, the California Supreme Court decided in a unanimous decision that in a Private Attorneys General Act (PAGA) action seeking to...

---

## **OSHA Appoints New Director of Directorate of Construction (DOC).**

**Fisher Phillips**

To almost everyone's delight, OSHA has filled the vital position of the Director of the Directorate of Construction (DOC). The DOC Director position...

---

## **CCPA Amendments Update: The More Things Change, the More They Stay the Same**

**Troutman Sanders LLP**

Over the past year, nearly twenty amendments were introduced to modify the California Consumer Privacy Act of 2018 ("CCPA"). Now that the deadline to...

---

## **Space for Agility: The Rise of the Flexible Workplace**

**Baker McKenzie**

The footprint of flexible workplaces continues to expand as more and more global businesses embrace the modern workforce and the ever increasing...

---

## **Now What? Practical Tips for Navigating California Post-A.B. 5** California

**Littler Mendelson PC**

In the coming weeks—or perhaps even days—California Governor Gavin Newsom is expected to sign into law sweeping legislation—Assembly Bill 5 (A.B....

---

## **Caution: Ban Ahead - The Rise in Bans on Salary History Inquiries Requires Employer Diligence**

**Nexsen Pruet**

A seemingly innocuous interview question is now illegal to ask job applicants in numerous jurisdictions, and the number of jurisdictions implementing...

---

## **Prepare to Implement Paid Family and Medical Leave Under New Massachusetts Law** Massachusetts

**Holland & Knight LLP**

Massachusetts employers should make their final preparations for the Massachusetts Paid Family and Medical Leave (PFML) program in advance of the Oct...

---



## **New Jersey Passes Law Prohibiting Employers from Requesting Applicant's Salary History** New Jersey

### **Nelson Mullins Riley & Scarborough LLP**

New Jersey recently enacted a new law prohibiting employers from seeking or relying on a job applicant's salary history. The law, which will take...

---

## **Independent Contractor "ABC Test" May Soon Be Codified to Apply to Claims Made Under the California Labor and Unemployment Insurance Codes, With Some Exceptions** California

### **Gordon Rees Scully Mansukhani**

Governor Newsom is expected to sign a bill that may have far-reaching impact on employers who classify and use independent contractors. Assembly Bill...

---

## **DOL Reiterates Employers May Not Delay FMLA Leave**

### **Michael Best & Friedrich LLP**

In an opinion letter issued earlier this week, the Department of Labor addressed whether an employer may delay designation of FMLA leave if its...

---

## **NLRB Puts a Finer Point on Its Community of Interest Test with a New Three-Step Analysis**

### **Proskauer Rose LLP**

Still hard at work as we head into mid-September, the National Labor Relations Board, in a 3-1 decision (Chairman Ring and Members Kaplan and Emanuel...

---

## **"Stud-shaming" may be sex harassment, court says**

### **Constangy Brooks Smith & Prophete LLP**

Showing, again, that workplace gossip can get you sued. I really feel that the employer will win this case, for reasons I'll discuss below, but first...

---

## **Best Practices for Plan Sponsors #11**

### **Drinker Biddle & Reath LLP**

This is the eleventh in a series of articles about Best Practices for Plan Sponsors. To be clear, "best practices" are not the same as legal...

---

## **CA bill would limit use of independent contractors** California

### **Constangy Brooks Smith & Prophete LLP**

As many of you may have heard, the California Legislature has passed a major piece of legislation regarding independent contractors. Assembly Bill 5...

---

## **AB 5, Codifying Dynamex and Broadening the ABC Test's Application, Passes California Legislature** California

### **Ford & Harrison LLP**

After months of debate and negotiations, the California State Legislature passed the controversial AB 5 on Wednesday, September 11, 2019, bringing it...

---

## **EEOC Will Not Seek to Renew Component 2 (Pay and Hours Data) Requirements**

## for Future EEO-1 Reports

### **Proskauer Rose LLP**

The EEOC announced today, September 12, 2019, that it “is not seeking to renew Component 2 of the EEO-1” in a notice published on the Federal...

---

## **California Supreme Court Limits PAGA Penalties** California

### **Gordon Rees Scully Mansukhani**

Employers in California have reason to rejoice as the California Supreme Court just issued a landmark ruling: employees can no longer recover...

---

## **NLRB Changes Course on Unilateral Employer Action Standard**

### **Ford & Harrison LLP**

In a 3-1 decision, the National Labor Relations Board (NLRB or the Board) reversed long-held Board precedent regarding when...

---

## **California Supreme Court Hands Employers A Rare Victory, Trims Bloated PAGA Claims** California

### **Proskauer Rose LLP**

Yesterday, the California Supreme Court held that private litigants may not recover unpaid wages under the Labor Code Private Attorneys General Act...

---

## **Colorado Employees Lose it Over Use-It-Or-Lose-It Vacation Policies** Colorado

### **Bryan Cave Leighton Paisner LLP**

Colorado employees are pushing back against the recent decision allowing use-it-or-lose vacation policies in Colorado...

---

## **Better protection for gig economy workers ?** California

### **Freshfields Bruckhaus Deringer**

Increased rights for gig workers continue to be a hot topic around the world. The EU might soon launch new initiatives as Nicolas Schmit, EU...

---

## **Landmark Bill Passes: California Codifies “ABC” Test for Worker Classification**

California

### **Proskauer Rose LLP**

On Thursday, September 12th, the California State Assembly passed Assembly Bill 5 (“AB 5”), the controversial new law that codifies the three-factor...

---

## **NLRB Adopts Management-Friendly Standard on Unilateral Employer Actions**

### **Michael Best & Friedrich LLP**

Unionized businesses should take note of the National Labor Relations Board’s (“Board”) recent decision in MV Transportation, Inc, where the Board...

---

## **He’s Not MY Employee... Or Is He?**

### **Fox Rothschild LLP**

Engaging independent contractors instead of hiring employees is enticing&hellip; no overtime pay, benefits, tax withholdings, FICA obligations or...

---



## **California Supreme Court Hands Employers A Rare Victory, Trims Bloated PAGA Claims**

California

### **Proskauer Rose LLP**

Last week, the California Supreme Court held that private litigants may not recover unpaid wages under the Labor Code Private Attorneys General Act...

---

## **How Much Will AB 5 Really Change California Law?**

California

### **Ogletree Deakins**

The answer is not as much as you may think. Much of the recent media coverage of California's Assembly Bill 5 (AB 5) suggests that the bill...

---

## **Be Prepared for New Federal Overtime Rule Regarding Salary**

### **Holland & Knight LLP**

New federal overtime rules are coming that will impact who qualifies as an exempt employee. Early preparation will avoid challenges when the new rules...

---

## **Summer Vacation Is Definitely Over At The NLRB (US)**

### **Squire Patton Boggs**

Between August 29 and September 10, the National Labor Relations Board ("NLRB" or "Board") issued four decisions that resolve important issues that...

---

## **NLRB sides with Kroger's action to remove union representatives from company property**

### **Porter Wright Morris & Arthur LLP**

On Sept. 6, 2019, the National Labor Relations Board (NLRB) granted a significant win to employers, ruling that businesses can lawfully limit the...

---

## **FMLA Covers Parental Attendance at IEP Meetings**

### **Haynsworth Sinkler Boyd PA**

As students return to school, employers should be mindful of a new U.S. Department of Labor opinion letter impacting when a parent may use qualifying...

---

## **Wage Claims After OTO v. Kho: Are Arbitration Agreements Enforceable?**

California

### **Paul Hastings LLP**

The California Supreme Court recently addressed—and again—the enforceability of an arbitration agreement of an employee who sought to recover...

---

## **Labor Board Adopts 'Contract Coverage' Standard in Unilateral Change Cases, Overturns Precedent**

### **Jackson Lewis PC**

The National Labor Relations Board (NLRB) has made it easier for employers to defend against unfair labor practice charges alleging a unilateral...

---

## **NLRB Continues Trend to Protect Employer Property Rights**

### **Ogletree Deakins**

Coming on the heels of its decision in Bexar County Performing Arts Center Foundation d/b/a Tobin Center for the Performing Arts, 368 NLRB No. 46...

---

## **The ABC Test May Soon Be Law in California: What Employers Need to Know**

California

### **Ogletree Deakins**

On September 11, 2019, the California Assembly passed a bill codifying last year's Supreme Court of California decision establishing a new test to...

---

## **No more EEO-1 comp data, EEOC proposes**

### **Constangy Brooks Smith & Prophete LLP**

What a colossal waste this has been. The Equal Employment Opportunity Commission issued a Notice, published in yesterday's Federal Register...

---

## **CA Supreme Court Rules That Employees Cannot Recover Unpaid Wages Through PAGA**

California

### **Baker & Hostetler LLP**

California's Supreme Court has cut off an area of significant potential exposure for California employers by ruling that employees cannot recover...

---

## **California Employers Cheer Rare PAGA Victory**

California

### **Cozen O'Connor**

The California Supreme Court recently handed down an increasingly rare win for employers and the defense bar with its September 12 decision in Z.B...

---

## **California Supreme Court Rejects Claim for Unpaid Wages under PAGA**

California

### **Jackson Lewis PC**

Putting an end to employees' backdoor attempts to recover unpaid wages in Private Attorneys General Act-only actions under California Labor Code...

---

## **California Supreme Court Delivers PAGA Win for Employers**

California

### **Mintz**

In a significant victory for California employers who use arbitration agreements, the California Supreme Court ruled (ZB, N.A. et al. v. Superior...

---

## **Ninth Circuit Sides With Web Scrapers**

### **Sidley Austin LLP**

For years, companies seeking to block web scrapers from collecting the information on their website would invoke the Computer Fraud and Abuse Act...

---

## **Important EEO-1 Component 2 Deadline Approaching This Month**

### **Mintz**

An important deadline approaches for those employers required to file the EEO-1 survey - which generally includes employers with at least 100...

---

## **Could A Mistake by Your Company Nurse Lead to Civil Liability in North Carolina?**

North Carolina



---

**Fisher Phillips**

Employers have long operated under the premise that the North Carolina Workers' Compensation Act provides the exclusive remedy for workers injured on...

---

**Access to Private Property: Labor Board Rules Girl Scout Cookies and Union Protesters are Different****Jackson Lewis PC**

A nonemployee's solicitation for charitable or civic causes on an employer's property is not the equivalent of a nonemployee union representative's...

---

**Will the Middleman Get Stuck with the Bill?** Pennsylvania**Goldberg Segalla LLP**

From the manufacturer to the distributor to the retailer, most products pass through numerous hands before reaching the consumer. If a defect causes...

---

**California Worker Misclassification Bill Closer to Enactment** California**Jackson Lewis PC**

The California Assembly has passed a bill that would require workers to be classified as employees if the employer exerts control over how the...

---

**California Supreme Court Limits Potential Recovery Under PAGA** California**Hunton Andrews Kurth LLP**

Yesterday, the California Supreme Court issued its highly-anticipated decision in ZB, N.A. V. Lawson bringing some welcomed good news for California...

---

**The Practical NLRB Advisor: Summer 2019****Ogletree Deakins**

Ogletree Deakins' Traditional Labor Relations Practice Group is pleased to announce the publication of the summer 2019 issue of the Practical NLRB...

---

**EEOC Presses Pause on Collection of EEO-1 Pay Data After This Year's September 30 Reporting Deadline (US)****Squire Patton Boggs**

As we have previously reported here, companies with at least 100 employees must collect and report 2017 and 2018 employee pay data information, broken...

---

**NLRB Tunes Up Appropriate Standard in Determining Bargaining Unit of Mechanics at Boeing****Holland & Knight LLP**

In its decision, The Boeing Company, the National Labor Relations Board clarifies what constitutes an "appropriate" bargaining unit under the...

---

**How Safe Is That Harbor? The Impact of the Defend Trade Secrets Act's Whistleblower Immunity Provision on a Trade Secret Owner's Ability to Protect Its Trade Secrets**



### **Pepper Hamilton LLP**

Imagine that your company has just commenced an internal compliance investigation in response to an allegation that the company is violating various...

---

### **Employers Should be Prepared for the Challenges of the 2019 Hurricane Season**

#### **Ford & Harrison LLP**

As Hurricane Dorian, the first hurricane of the 2019 Atlantic season, bears down on Florida, the approaching storm serves as a...

---

### **Implementing Individual Arbitration Agreements Does Not Violate NLRA, Even If Done After Collective Action is Filed**

#### **Spencer Fane LLP**

As previously discussed on Spencer Fane Human Resource Solutions, an employer can lawfully require its employees to sign individual arbitration...

---

### **Urgent Reminder: Employers Have Until September 30 to Submit EEO-1 Pay Data**

#### **Vorys Sater Seymour and Pease LLP**

As we previously reported, the Equal Employment Opportunity Commission (EEOC) has been ordered to collect to employers' EEO-1 Component 2 compensation...

---

### **The NLRB Acknowledges The Inevitable And Adopts The Contract Coverage Test**

#### **Baker McKenzie**

This week, the National Labor Relations Board finally came to its senses and adopted the contract coverage test for cases alleging an employer had...

---

### **NLRB Holds Misclassifying of Employees Is Not a Violation**

#### **Fox Rothschild LLP**

Misclassification of employees as independent contractors "does not violate the [National Labor Relations] Act," the NLRB held last month. The...

---

### **Divorce and Space Crimes**

#### **Burns & Levinson LLP**

The First Crime in Space! Recent headlines from The New York Times and other prominent news agencies drew in readers stating that the first crime in...

---

### **EEOC Won't Require Employers to Produce EEO-1 Component 2 Data After This Year**

#### **Holland & Knight LLP**

As mentioned in previous Holland & Knight alerts, employers are required, by Sept. 30, 2019, to produce to the U.S. Equal Employment Opportunity...

---

### **Eighth Circuit affirms working overtime can be essential job function**

#### **Reed Smith LLP**

Overtime work is essential in many industries. As a result, employers frequently structure job roles to require mandatory overtime. Although...

---

## **The Women of Amazon Studios' The Boys Offer Lessons on Title VII Retaliation** **Ford & Harrison LLP**

Piggybacking off my colleague Tim Reed's recent post providing the background/plot and discussing employer liability issues in Amazon Studios'...

---

## **California to Codify Dynamex** California

### **K&L Gates**

The California Legislature has passed Assembly Bill 5 ("AB 5"), which if signed by Governor Gavin Newsom, will codify the California Supreme Court's...

---

## **Eighth Circuit Affirms Single Captioned Theatre Performance for Hearing Impaired not Good Enough Under ADA**

### **Baker Sterchi Cowden & Rice LLC**

Title III of the Americans with Disabilities Act specifically prohibits discrimination on the basis of disability in the activities of places of...

---

## **Non-Exempt Employees Traveling for Work: How to Manage the Time Clock**

### **Ford & Harrison LLP**

There may be instances where non-exempt employees are required to travel for business. This is a common practice in the fashion industry where...

---

## **Third Circuit Affirms \$4.5 Million Verdict in Favor of Exotic Dancers**

### **Baker & Hostetler LLP**

A significant amount of wage and hour class/collective jurisprudence has developed around the issue of whether exotic dancers are employees or...

---

## **New California Law Will Reshape Worker Classifications** California

### **Fox Rothschild LLP**

On Sept. 18, Gov. Gavin Newsom signed AB-5 into law, drastically altering how millions of Californians are paid and vastly complicating the legal...

---

## **The Controversial ABC Test From Dynamex Is Codified In Law — California's Gig Economy Braces For Change** California

### **Baker McKenzie**

Today California Governor Gavin Newsom signed a landmark bill making it more difficult for companies to engage independent contractors. (See our...

---

## **NLRB Tips Scales in Favor of Employers When Drawing Distinctions Between Claims of "Inability to Pay" Versus "Competitive Disadvantage," and "Surface" Versus "Hard" Bargaining**

### **Proskauer Rose LLP**

In recent weeks, the National Labor Relations Board has issued several employer-friendly decisions, and its September 13 decision in Arlington Metals...

---

## **Postmates Will Deliver Benefits To Gig Workers**

### **Fisher Phillips**

Good news for Postmates delivery drivers...and for gig economy businesses



across the country. The company recently announced that it would offer...

---

### **MV Transportation Inc. - NLRB rules on employer unilateral action**

#### **Dinsmore & Shohl LLP**

On Sept. 10, 2019, the National Labor Relations Board (NLRB) issued the MV Transportation decision and adopted the contract coverage standard in...

---

## **Environment & Climate Change**



---

### **Oil and gas environmental protection laws in the USA**

#### **Morgan Lewis**

A structured guide to oil and gas environmental protection laws in the USA

---

### **Industry Update: New Statewide Commercial Cannabis Regulations in California Create Opportunities for Savvy Investors**

California

#### **Venable LLP**

Following the State of California's legalization of adult-use cannabis in November 2016, cannabis regulations have been growing like weeds (pun...

---

### **The roundup on toxic pesticides - regulatory divergence, growing litigation**

#### **Leigh Day**

In August last year, Monsanto was ordered to pay nearly \$290 million compensation to Dewayne Johnson, a 46 year old groundskeeper from California who...

---

### **SCAQMD's Historic RECLAIM Program Sunset Faces Questions on the Horizon**

California

#### **Hunton Andrews Kurth LLP**

The South Coast Air Quality Management District's (SCAQMD or the District) Regional Clean Air Incentives Market (RECLAIM) made history as...

---

### **California Legislature Passes Housing Crisis Act of 2019 and Rent Control Bill, Among Others**

California

#### **Holland & Knight LLP**

A handful of important state laws related to housing have been passed by the California legislature, including the Housing Crisis Act of 2019 (SB...

---

### **SEC Proposes to Modernize Disclosures of Business, Legal Proceedings and Risk Factors Under Regulation S-K**

#### **Cahill Gordon & Reindel LLP**

On August 8, 2019, the Securities and Exchange Commission (the "SEC") issued a release (the "Release")<sup>1</sup> proposing amendments to Regulation S-K Items...

---

### **Long-Awaited Repeal Rule Ends Patchwork of WOTUS Implementation**

#### **Hunton Andrews Kurth LLP**

Which Waters of the US (WOTUS) rule applies to my project? For four years, that has been a recurring question with a complicated, ever-changing...

---

## **EPA Repeals Obama Rule Defining Waters of the U.S.**

### **Bracewell LLP**

On Thursday, September 12, EPA General Counsel Matt Leopold announced EPA's final rule repealing the 2015 Waters of the United States ("WOTUS") Rule...

---

## **EPA Criticized By Academics: Identifying Susceptible Populations**

### **Bergeson & Campbell PC**

On August 29, 2019, an article titled Population susceptibility: A vital consideration in chemical risk evaluation under the Lautenberg Toxic...

---

## **The 2015 WOTUS Rule Is Repealed**

### **Breazeale Sachse & Wilson LLP**

The EPA and the Corps of Engineers have taken the first of two steps to repeal and replace the definition of 'waters of the United States'...

---

## **EPA Updates FY 2018-2022 Strategic Plan**

### **Bergeson & Campbell PC**

On September 9, 2019, the U.S. Environmental Protection Agency (EPA) announced an update to its Fiscal Year (FY) 2018-2022 Strategic Plan. According...

---

## **New Regulations Reform Implementation of Endangered Species Act**

### **Beveridge & Diamond PC**

Long-sought reforms to Endangered Species Act (ESA) implementation have arrived. On August 27, 2019, the U.S. Fish and Wildlife Service (FWS) and U.S...

---

## **No Defense Owed to Insured for Mediation Involving Environmental Contamination**

Illinois

### **Goldberg Segalla LLP**

The Illinois Appellate Court recently held that the term "suit" in a commercial general liability policy does not include a pre-suit mediation...

---

## **EPA Evaluating Application for Experimental Pesticide to Combat Mosquitos**

### **Taft Stettinius & Hollister LLP**

EPA recently received an application for an experimental use permit that would allow Oxitec, a British biotechnology company, to study the use of...

---

## **Superfund Task Force Final Report: A Superset of Recommendations**

### **Beveridge & Diamond PC**

On September 9, EPA's Superfund Task Force released its final report on recommendations to improve the Superfund program. This eighty-page document...

---

## **The Weekly Hill Update**

### **Baker & Hostetler LLP**



Below is the Federal Policy team's weekly preview, posted when Congress is in session...

---

### **Effective Date of New State Wetland Definition and Permitting Procedures**

California

#### **Procopio Cory Hargreaves & Savitch LLP**

Earlier this year, we published two articles monitoring the implementation of the new State Wetland Definition and Procedures for Dischargers of...

---

### **Déjà Vu: EPA, Army Corps Take First Step to Redefine "Waters of the U.S."**

#### **Beveridge & Diamond PC**

Last week EPA and the U.S. Army Corps of Engineers announced that they again will be taking the first step in the long-awaited rulemaking process to...

---

### **First Import Permit Issued for Sport Hunted Threatened Lion Trophy**

#### **Duane Morris LLP**

For the first time since the United States protected lions under the Endangered Species Act ("ESA") in 2016, the Fish and Wildlife Service ("FWS")...

---

### **Earthjustice Claims EPA Fails to Disclose Information about New Chemical Substances**

#### **Bergeson & Campbell PC**

On September 3, 2019, Earthjustice filed with the U.S. Environmental Protection Agency (EPA) a notice of intent to sue EPA under Section 20(a)(2) of...

---

### **It Has Been A Busy Year For the TSCA Risk Assessment Process**

#### **Squire Patton Boggs**

As 2019 moves into its closing months, US EPA activity under the amended Toxic Substances Control Act (TSCA) remains front and center. As part of US...

---

### **Fish and Wildlife Service Delists Fosskett speckled dace**

#### **Nossaman LLP**

On September 13, 2019, the U.S. Fish and Wildlife Service (Service) posted a final rule removing the Fosskett speckled dace (*Rhinichthys osculus* ssp.)...

---

### **Monthly Update for September 2019**

#### **Bergeson & Campbell PC**

On August 19, 2019, the U.S. Environmental Protection Agency (EPA) announced that it seeks comment on manufacturer requests for the risk evaluations...

---

### **Circular Economy and Pollution Reduction Act Stalls in California Legislature**

California

#### **Keller and Heckman LLP**

The Circular Economy and Pollution Reduction Act, SB-54/AB-1080, did not pass the California State Legislature before the 2019/2020 legislative...

---



## **Report Recommends Changes to US EPA's General Permit for Industrial Stormwater Discharges Ahead of Reissuance**

### **Squire Patton Boggs**

Stormwater permitting requirements for many industrial facilities are set forth in US EPA's Multi-Sector General Permit for Stormwater Discharges...

---

## **EPA Taps Public for Comment on Water Reuse Plans**

### **Goldberg Segalla LLP**

The plan outlines ways that the EPA can work with state and local governments to promote water reuse and support research into new Technologies. Due...

---

## **CDCR's Inaction In Failing To Maintain Historic Former Hotel Not A "Project" Subject To CEQA, Holds First District**

California

### **Miller Starr Regalia**

In a short published opinion filed September 13, 2019, the First District Court of Appeal (Div. 4) affirmed the trial court's judgment denying a...

---

## **Nota Bene Episode 50: Who is Filling the International Divergence in Climate Change Regulation? with Nico van Aelstyn**

### **Sheppard Mullin Richter & Hampton LLP**

With crucial existing environmental regulations being threatened with rollbacks by the government and the Earth's sustainability becoming more dire...

---

## **Transfer-Based Exclusion Upheld: Court Discards "Discard" Argument**

### **Nelson Mullins Riley & Scarborough LLP**

A thoughtful, practical opinion seems to provide the EPA with a tutorial on promulgating a defensible regulation. On July 2, 2019, the U.S. Court of...

---

## **Earthjustice Notifies EPA of Intent to Sue for Failure to Disclose Information about New Chemical Substances**

### **Bergeson & Campbell PC**

On September 3, 2019, Earthjustice filed with the U.S. Environmental Protection Agency (EPA) a notice of intent (NOI) to sue EPA under Section...

---

## **EPA Researches Carbon Nanotubes in 3D Printing Filament**

### **Bergeson & Campbell PC**

The September 10, 2019, issue of the U.S. Environmental Protection Agency's (EPA) Science Matters newsletter includes an article entitled "Keeping up...

---

## **Natural Gas Pipeline One Step Closer to Reality For Residents of New York**

New

York

### **Goldberg Segalla LLP**

The United States Federal Energy Regulation Commission (FERC) has issued an order holding that the New York Department of Environmental Conservation...

---

## **Are We Living in the Golden Age of Cooperation or Not? The Implications of SEC Chair Jay Clayton's Recent Comments Challenging Perceptions of Cross-Border**

## **Collaboration in FCPA Enforcement**

### **K&L Gates**

In a speech to the Economic Club of New York on September 9, Securities and Exchange Commission ("SEC") Chair Jay Clayton lamented foreign...

---

## **Politics Trumps Economics? Trump's Revocation of California's Waiver Under the Clean Air Act**

California

### **Sheppard Mullin Richter & Hampton LLP**

Today President Trump announced on Twitter that the U.S. was revoking California's waiver under the Clean Air Act (CAA) which allowed it to impose...

---

## **Project Tundra Awarded \$9.8 Million for Research and Development**

### **Eversheds Sutherland (US) LLP**

The U.S. Department of Energy announced that it will provide \$9.8 million for Front-End Engineering and Design work for Project Tundra and the Energy...

---

## **SEC Proposes Rule Changes for Business Description, Legal Proceedings and Risk Factors Disclosures**

### **Manatt Phelps & Phillips LLP**

Aiming to modernize the description of business, legal proceedings and risk factor disclosures that registrants are required to make pursuant to...

---

## **Internet & Social Media**



## **stay ADvised: What's New This Week, August 26**

### **Davis Wright Tremaine LLP**

In what appears to be becoming routine at the Federal Trade Commission (FTC), the agency recently brought an(other) enforcement action against a...

---

## **Ninth Circuit Upholds Amazon.com's Cost-Sharing Valuation**

### **Ropes & Gray LLP**

On August 16, 2019, the Ninth Circuit upheld Amazon's cost-sharing arrangement and valuation of its intangible assets, affirming the Tax Court's 2017...

---

## **NIST Privacy Framework Draft Released**

### **Robinson & Cole LLP**

The National Institute of Standards and Technology (NIST) recently released its draft Privacy Framework: A Tool for Improving Privacy through...

---

## **Mr. T Sues Popular Marijuana Website**

### **Goldberg Segalla LLP**

On August 22, 2019, Laurence Tureaud, most commonly known as Mr. T, sued Leafly, a digital cannabis company. In his lawsuit, Mr. T claimed that...

---

## **District court allows majority of privacy invasion class action claims to proceed against social media company**

California

### **Buckley LLP**



On September 9, the U.S. District Court for the Northern District of California granted in part and denied in part a social media company's motion to...

---

### **Your Smartphone: Friend or Foe?**

**Duane Morris LLP**

Wherever we go these days, whether at work, at home, in restaurants, outside, or practically anywhere else, people reflexively go to their...

---

### **OIG Approves Per-Click Fee Arrangement for Online Healthcare Directory**

**Epstein Becker Green**

On September 10, 2019, the Office of Inspector General of the Department of Health and Human Services ("OIG") published Advisory Opinion 19-04. In...

---

### **Facing Fines—The Mechanics of Facebook's Reportedly Forthcoming FTC Settlement**

**Allen & Overy LLP**

On April 24, 2019, Facebook announced to investors that it expects to set aside an amount between \$3 billion and \$5 billion in relation to the...

---

### **New Jersey Fantasy Sports Operator Settles with State**

[New Jersey](#)

**Klein Moynihan Turco LLP**

On August 16, 2019, fantasy sports operator SportsHub Games Network, Inc. ("SportsHub") and the New Jersey Attorney General entered into a Consent...

---

### **Scraping the Web: Practical Implications From the hiQ v. LinkedIn Opinion**

**Jones Day**

In a highly anticipated decision, the Ninth Circuit ruled on September 9, 2019, that scraping data from the public portions of a website likely does...

---

### **Alibaba Opens Online Marketplace to U.S.-Based Businesses**

**Vorys Sater Seymour and Pease LLP**

Alibaba Group, which operates the online marketplace Alibaba.com, recently announced that it will now allow U.S.-based businesses to sell on the...

---

### **Privacy Regulators Turning Up the Heat: Major Fines for Data Breaches and Privacy Violations This Summer**

**Bennett Jones LLP**

Summer 2019 saw a flurry of major fines levied against large corporations for data breaches and other privacy violations. Ranging from a €460,000...

---

### **Rhode Island Expands Electronic Money Transfer Licensing Requirements to Certain Cryptocurrency Service Providers**

[Rhode Island](#)

**Troutman Sanders LLP**

Rhode Island has amended its electronic money transfer law to require state licensing for certain entities providing cryptocurrency or "virtual..."

---

### **Update From LitLand: "Hey Google, Are You Listening?"**

[California](#)

[Illinois](#)

## **Davis Wright Tremaine LLP**

LitLand is a monthly feature that reviews developments in litigation as they relate to privacy matters and highlight any past, current, and future...

---

### **Just How Far Does California's New IoT Security Law Reach?** [California](#)

#### **Baker & Hostetler LLP**

On January 1, 2020, California's new Internet of Things (IoT) Security Law goes into effect. The law is the first IoT-specific security law in the...

---

### **OTA & Travel Distribution Update: TripAdvisor continues to defend claims of fake reviews; Booking.com and others create travel sustainability pact; Vacasa strikes direct connect deal with Google**

#### **Garvey Schubert Barer**

Fall has definitely arrived here in the Pacific Northwest. This week's OTA & Travel Distribution Update is below and...

---

### **Nevada's New Privacy Law Will Go Into Effect Next Month: Are You Ready?**

#### **Squire Patton Boggs**

The Nevada Privacy of Information Collected on the Internet from Consumers Act (NPICICA) applies to operators of commercial websites and online...

---

### **Business Roundtable Proposes Framework for Consumer Privacy Legislation**

#### **Covington & Burling LLP**

On September 10, 2019, 51 members of the Business Roundtable sent a letter to congressional leaders advocating principles for a national consumer...

---

### **The Ninth Circuit Takes On Web Scraping**

#### **Saiber LLC**

"Web scraping" involves the use of software to collect data from the internet, which can then be sold to other users. On September 9, 2019, the...

---

### **Episode 278: Will international trade law prevent the US from regulating the security of the Internet of Things?** [California](#) [Audio](#)

#### **Step toe & Johnson LLP**

Joel Trachtman thinks it's a near certainty that the WTO agreements will complicate US efforts to head off an IoT cybersecurity meltdown, and there's...

---

### **Ninth Circuit's LinkedIn Decision Does Not Greenlight the Unauthorized Webscraping of Public Websites**

#### **Morrison & Foerster LLP**

A recent decision from the Ninth Circuit Court of Appeals in a dispute between LinkedIn and hiQ Labs has spotlighted the thorny legal issues involved...

---

### **New Decision Raises Questions About FTC's Restitution Power**

#### **Manatt Phelps & Phillips LLP**

A recent decision from the U.S. Court of Appeals for the Seventh Circuit could have a significant impact on the efforts of the Federal Trade...



---

## California Legislature Passes Amendments to Privacy Law California

### O'Melveny & Myers LLP

In a flurry of activity on the last day of the legislative session, on September 13, 2019, California passed several amendments to the California...

---

## Facebook launches its own Supreme Court

### Shepherd and Wedderburn LLP

The challenge of hate speech and illegal content has been written about here before. Give people the ability to express their view and they will...

---

## Website Law Alert - A Defense That May Succeed Against an ADA Non-Compliance Suit

### Cowan Liebowitz & Latman PC

A ruling from the United States District Court for the Southern District of New York has opened the door for a website owner to successfully defend a...

---

## TINA Not Playing Around With YouTube Kidfluencer

### Manatt Phelps & Phillips LLP

A popular YouTube channel for kids is the subject of a new complaint filed by Truth in Advertising (TINA) with the Federal Trade Commission (FTC)...

---

## CCPA Privacy FAQs: If a website participates in behavioral advertising, does Nevada privacy law require that it disclose that it is "selling" consumers' information? California Nevada

### Bryan Cave Leighton Paisner LLP

On May 29, 2019, Nevada became the first state to pass legislation emulating portions of the CCPA when it adopted Senate Bill No. 220...

---

## HHS Issues Favorable Advisory Opinion for Online Healthcare Directory Charging Per-Click Fees

### Robinson & Cole LLP

On September 5, 2019, the Department of Health and Human Services (HHS) Office of the Inspector General (OIG) issued OIG Advisory Opinion 19-04 (...)

---

## FDA Announces Public Meeting to Discuss "A New Era of Smarter Food Safety"

### Keller and Heckman LLP

FDA will hold a public meeting on October 21, 2019 to hear from a broad cross-section of stakeholders on their new food safety approach, called "A...

---

## The Human Touch of Web Accessibility

### Akerman LLP

Automation is the way of the future . . . Or so we thought. Make no mistake, the technology at our fingertips is powerful. As we increasingly rely on...

---

## Compliance Tips From the Largest COPPA Settlement Ever

### Manatt Phelps & Phillips LLP

---



In a record-setting deal with the Federal Trade Commission (FTC) and the New York State Office of the Attorney General, YouTube agreed to pay a total...

## Internet of Things Strategies for the Energy Sector

### Mintz

Whether thinking about managing oil and gas, water or other infrastructure facilities, or considering industrial efficiency, robotics and automation...

## Legal Practice



## A Guide to Corporate Taxation

### Wolters Kluwer Legal & Regulatory

The reduction of the corporate tax rate was one of the most significant provisions of the historic Tax Cuts and Jobs Act of 2017...

## Best Practices for Successful Fee Collection Pennsylvania

### Goldberg Segalla LLP

Ask any lawyer who routinely represents CPAs: "What is the No. 1 mistake CPAs make that gets them into trouble with their clients?" The answer almost...

## Discovery Counsel Vital In All Phases Of Mass Tort Litigation

### Nelson Mullins Riley & Scarborough LLP

A "virtual law team" is a collaborative and technology-based team of lawyers selected for specific tasks in defending a single client's litigation. In...

## Court Adopts A Favorable Privilege Standard But Unfavorable Work Product Standard: Part II

### McGuireWoods LLP

Last week's Privilege Point described a Northern District of Illinois decision which applied the favorable "one of the significant purposes"...

## What you need to know about Missouri's updated discovery rules Missouri

### Thompson Coburn LLP

On July 10th, Governor Mike Parson signed into law Senate Bill 224, which passed the Senate on a final 23-9 vote shortly before the end of the 2019...

## Global investigations around the world: USA

### Global Investigations Review

There is never a shortage of high-profile corporate investigations in the United States. Since 2000, at least 26 of the US Fortune 100 corporations...

## Projects & Procurement



## Vultures circling as bill to expand CFCA to tax looms in legislature California

### McDermott Will & Emery

Legislators in Sacramento are mulling over one of the most (if not the most) troubling state and local tax bills of the past decade. AB 1270...

---

**Video: Government Contractors: FedBizOpps To Be Rolled Into Beta.SAM.Gov Starting November 2019**

**Kilpatrick Townsend & Stockton LLP**

The Federal Business Opportunities (FedBizOpps) website is an aggregation site of government opportunities valued at greater than \$25,000...

---

**California False Claims Act Bill to Include Tax Fraud Fails** California

**Troutman Sanders LLP**

On August 30, the California Senate Appropriations Committee failed to approve A.B. 1270 which would extend the California False Claims Act to include...

---

**HUD's FHA Lender Annual Certification Statements May Significantly Reduce FHA Lender Risk of False Claims Act Liability**

**Jenner & Block LLP**

September 13, 2019 is the deadline for comments on HUD's proposed changes to FHA Lender Annual Certification Statements. The most significant changes...

---

**Eleventh Circuit Rejects Expert Challenge to Clinical Judgment Decision in Hospice False Claims Act Litigation**

**Dykema Gossett PLLC**

On September 9, 2019, the U.S. Court of Appeals for the Eleventh Circuit issued an important decision for health care providers, especially those in...

---

**Eleventh Circuit Says Difference of Opinion Does Not Establish Falsity in False Claims Act Case**

**Pepper Hamilton LLP**

On September 9, in a setback for AseraCare but an overall win for hospice providers, the Eleventh Circuit affirmed a Northern District of Alabama...

---

**GSA Requiring "Bilateral" Modification to All Multiple Award Schedule Contracts to Prohibit Use of Huawei/ZTE Equipment**

**Crowell & Moring LLP**

The General Services Administration ("GSA") has announced its intention to initiate in September 2019 a mass "bilateral" modification of all GSA...

---

**Eleventh Circuit rejects reliance on statistical sampling and requires proof of objective falsity for each claim pursued under the FCA**

**DLA Piper**

This week, the Eleventh Circuit significantly raised the burden for DOJ and qui tam plaintiffs asserting False Claims Act claims under a false...

---

**NIA "In Search of a SpaceX for Nuclear" Talk on the Hill**

**Hogan Lovells**

On Wednesday Nuclear Innovation Alliance (NIA) hosted a meeting on the Hill about how to enhance the development of nuclear energy by finding its...

---



### **11th Circuit: Difference in Opinion Not Enough for FCA Liability**

#### **Latham & Watkins LLP**

The 11th Circuit's long-awaited AseraCare opinion requires more than mere disagreement regarding clinical judgment to prove falsity under the False...

---

### **3rd Circuit: FCA does not guarantee an in-person hearing before dismissal**

#### **Buckley LLP**

On September 12, the U.S. Court of Appeals for the Third Circuit held that the False Claims Act (FCA) does not guarantee relators an automatic...

---

### **On the Effective Use of Liquidating Agreements**

California

#### **Seyfarth Shaw LLP**

Congress enacted the Contract Disputes Act of 1978 (CDA) to “provide a fair, balanced, and comprehensive statutory system of legal and administrative...

---

### **Third Circuit Holds FCA Qui Tam Plaintiffs Not Entitled to Automatic Hearing on Government Motion to Dismiss**

#### **Dinsmore & Shohl LLP**

On Thursday, September 12, the Third Circuit decided United States ex rel. Chang v. Children’s Advocacy Center of Delaware, No. 18-2311. In a...

---

### **Eleventh Circuit Endorses Objective Falsehood Standard for False Claims Cases Concerning Physician Judgment of Hospice Eligibility**

#### **Robinson & Cole LLP**

In a 3-0 decision issued September 9, 2019, the U.S. Court of Appeals for the Eleventh Circuit affirmed a three-year-old district court ruling in...

---

### **The Eleventh Circuit’s Recent AseraCare Decision Raises the Bar for Establishing Falsity in False Claims Act Cases Involving a Medical Provider’s Clinical Judgment**

#### **Winston & Strawn LLP**

In a noteworthy decision issued last week, the Eleventh Circuit Court of Appeals held that a claim cannot be deemed “false” under the False Claims...

---

### **Will an Unappealing Trend in Battlefield Contractor Suits Continue? Following A Pattern of Appellate Indecision—Fueled by the Government’s Equivocal Litigation Stances—the Fourth Circuit Mulls En Banc Review**

#### **Covington & Burling LLP**

It’s often said that hard cases make bad law. In the realm of contractor-on-the-battlefield lawsuits, hard cases seem to be making no law—at least at...

---

### **Magnolia LNG to Supply Proposed Vietnamese Power Plant**

#### **Eversheds Sutherland (US) LLP**

Magnolia LNG’s parent company, Liquefied Natural Gas Limited, and Delta Offshore Energy (DeltaOE) have announced an alliance with the Bac Lieu...

---

**US - Government procurement: Australia added as WTO GPA country in the FAR.**

## **Baker McKenzie**

On September 10, 2019, the Department of Defense (DOD), General Services Administration (GSA), and National Aeronautics and Space Administration...

Public



### **Corporate income and franchise taxes in Rhode Island**

Rhode Island

#### **Adler Pollock & Sheehan**

A structured guide to corporate income and franchise taxes in Rhode Island

### **State and Local Taxes in Colorado**

Colorado

#### **Holland & Hart LLP**

A structured guide to state and local tax law in Colorado

### **State and Local Taxes in Rhode Island**

Rhode Island

#### **Adler Pollock & Sheehan**

A structured guide to state and local taxes in Rhode Island

### **Trade controls and foreign investment reviews involving China continue to expand**

Video

#### **Hogan Lovells**

Against the backdrop of China's growing economic, political and military influence worldwide, the United States is reassessing its economic...

### **Emerging Technologies Washington Update- Sep 12, 2019**

District of Columbia

#### **McGuireWoods Consulting LLC**

This Week: DOT report updates status of automated vehicle, drone regulations; California legislature passes worker classification legislation; House...

### **CCPA Security FAQs: Do businesses have to report data breaches to the state of California?**

California

#### **Bryan Cave Leighton Paisner LLP**

While the CCPA does not require that companies report data breaches to the state of California, California's data breach notification statute, enacted...

### **Policy and Political Outlook from Venable's Government Affairs Group**

#### **Venable LLP**

Congress is back in session, and Venable's Government Affairs Group has assessed the top priorities for the remainder of the 116th Congress...

### **Will California Be the First to Ban Fur Sales Statewide?**

California

#### **Duane Morris LLP**

The California legislature has passed a bill to ban the sale of new fur products anywhere within the state. The bill would make it unlawful to "sell..."

### **Sidley perspectives on M&A and Corporate Governance**



### **Sidley Austin LLP**

In exploring a potential public company sale, target boards rightly focus on the amount and type of consideration offered by potential buyers and the...

---

### **Less Than a Month to Go Until Nevada Privacy Law Effective Date**

Nevada

### **Baker & Hostetler LLP**

As discussed in our previous blog post on the topic, Nevada's amendments to its privacy law are set to go into effect Oct. 1, 2019...

---

### **NCGA Week in Review- Sep 13, 2019**

North Carolina

### **McGuireWoods Consulting LLC**

Members of the North Carolina General Assembly headed back to work this week after taking a few days off following the Labor Day holiday. Many were...

---

### **Lessons Learned: A High-Profile FARA Acquittal at Trial Provides Guidance for Both the Government and Targets of Future Investigations**

Washington

### **Vinson & Elkins LLP**

On September 4, a federal jury took only a few hours to return a verdict of "not guilty" for Washington, D.C. attorney and former White House Counsel...

---

### **Municipalities and School Systems: Educate Your Employees**

Connecticut

### **Robinson & Cole LLP**

The pace and number of cyber-attacks against municipalities and school systems is staggering and likes of which we have never seen. Municipalities...

---

### **A Syllabus for Regulating Student Data Privacy?**

### **Davis Wright Tremaine LLP**

The start of the new school year is approaching and a number of education vendors have already received their homework assignments. U.S. Senators...

---

### **Republican Retirements Provide Insights into 2020 Election Cycle—and Beyond**

### **Brownstein Hyatt Farber Schreck LLP**

One of the precursors of the Democratic wave that swept the House of Representatives in 2018 was the near-record number of House Republicans who...

---

### **NC Legislative Update: September 13, 2019**

North Carolina

### **Nexsen Pruet**

Legislators returned to Raleigh for what turned into a contentious week with new legislative districts in the works, and an unexpected budget veto...

---

### **Commissioner Bob Adler Elected Vice-Chairman of the CPSC, Making Him Acting Chairman of the Agency**

### **Mintz**

Late this afternoon it was confirmed that Commissioner Bob Adler was elected Vice-Chairman of the CPSC. Because there is no permanent CPSC Chairman



at...

---

### **The Inevitability Challenge**

#### **Covington & Burling LLP**

The Government of the Islamic Republic of Iran has, on account of its dismal human rights record and decades of aggression towards its neighbors...

---

### **Washington Healthcare Update- Sep 16, 2019** District of Columbia

#### **McGuireWoods Consulting LLC**

This week in Washington: Hearing on public health impact of e-cigarettes, meeting on continuing appropriations for fiscal year 2020, and hearing on...

---

### **Foreign Students Subject to Training Location Site Visits**

#### **Green and Spiegel LLC**

Optional Practical Training (OPT) is a training benefit for valid F1 Student Visa holders. It has to be directly related to the student's major and...

---

### **United States Imposes Additional Sanctions on Nicaragua**

#### **Holland & Knight LLP**

The Office of Foreign Assets Control (OFAC) has expanded Executive Order 13851, relating to the sanctions on Nicaragua that block all...

---

### **Junior College Sued Over Controversial "Oklahoma Drill"** Pennsylvania

#### **Goldberg Segalla LLP**

The Pennsylvania Supreme Court ruled on August 20, 2019, that Lackawanna Junior College had assumed a duty to care for the well-being of two of the...

---

### **California Senate Bill 206-The Immediate National Impact** California South Carolina

#### **Jackson Lewis PC**

While California Governor Gavin Newsom considers placing his signature on Senate Bill 206 and making his state the first state in the country to...

---

### **Golden loo still at large after artist insists it was no prank**

#### **Boodle Hatfield**

The 18-carat lavatory is a work by Italian artist Maurizio Cattelan. Called 'America', it was plumbed into the water system at Blenheim Palace so...

---

### **California NCAA Athletes Inch Closer to Earning Compensation** California

#### **Goldberg Segalla LLP**

The closely followed bill would allow college athletes to enjoy the capital gained from their name, images, and likeness. Under current NCAA rules...

---

### **DOD's Cybersecurity Maturity Model Certification and Draft CMMC Model Framework**

#### **Thompson Hine LLP**

DOD has released its draft CMMC model framework, including detailed new

cybersecurity requirements...

---

**PH Money Matters: This Week in Washington - September 16, 2019** Washington

**Paul Hastings LLP**

On Tuesday, the President announced via Twitter that he had fired his third national security adviser, John Bolton, as he “disagreed...

---

**PH Money Matters: This Week in Washington - September 9, 2019** Washington

**Paul Hastings LLP**

Over the weekend, the President announced via Twitter that he had canceled a secret meeting with Taliban leaders and Afghanistan’s...

---

**Keep Calm and Carry On - When Immigration Uncertainty Becomes the New Normal**

**Hunton Andrews Kurth LLP**

The UK could leave the EU in 6 weeks, or there may be another delay like the one we saw in April. Brexit watchers have likened the UK to a cat that...

---

**Education Policy Update- Sep 17, 2019**

**McGuireWoods Consulting LLC**

Education reform was the focus of the legislative session, as Gov. Henry McMaster promised. With the support of the governor, the House quickly...

---

**Marketer Sparks Outrage for its School Shooting Themed Line of Clothing**

**Frankfurt Kurnit Klein & Selz PC**

Fashion brand Bstroy sparked outrage after featuring a line of school shooting themed sweatshirts during a fashion show. The sweatshirts, which appear...

---

**Court Provides Further Clarification on Inverse Condemnation Liability** California

**Nossaman LLP**

We recently reported on the California Supreme Court’s decision in Oroville which provided a relaxed standard for public agencies facing inverse...

---

**Summer 2019 Top antitrust & competition stories**

**Linklaters LLP**

Barely a day has gone by this summer without news of another competition investigation, market study or report involving one of the Big Four Google...

---

**NFHS Argues Paying Student-Athletes Will Erode School Spirit at All Levels**

**Goldberg Segalla LLP**

On August 23, 2019, the National Federation of State High School Associations (NFHS) asked the Ninth Circuit to grant leave and allow it to file an...

---

**Enforcement proceedings against sovereign states in USA**

**Quinn Emanuel Urquhart & Sullivan LLP**

An overview of key considerations when bringing enforcement proceedings against sovereign states in the courts of USA, including the extent of sovereign



immunity, state assets subject to enforcement and service of process.



## Global

### Employment & Labor



#### Employment & labour law in Sweden

##### **Wigge & Partners**

A structured guide to the recognition and enforcement of foreign judgments in Sweden

#### Business Immigration in Austria

##### **Oberhammer Rechtsanwälte**

A structured guide to business immigration laws in Austria

#### Employment & labour law in India

##### **Kochhar & Co**

A structured guide to employment & labour law in India

#### Business Immigration in Canada

##### **Segal Immigration Law**

A structured guide to business immigration laws in Canada

#### Oil and gas occupational health and safety labour issues in Nigeria

##### **Udo Udoma & Belo-Osagie**

A structured guide to oil and gas health and safety labour issues in Nigeria

#### Employment & labour law in Nigeria

##### **Udo Udoma & Belo-Osagie**

A structured guide to employment and labour law in Nigeria

#### Employment & labour law in France

##### **Flichy Grangé Avocats**

A structured guide to employment and labour law in France

#### Business visitor visas in Canada

##### **Segal Immigration Law**

A structured guide to short-term business visitor visas in Canada

#### Employment & labour law in Italy

##### **Trifirò & Partners Avvocati**

A structured guide to employment and labour law in Italy

#### Recruitment and wage & hour law in Germany

## **Vangard**

A structured guide to background checks, recruitment and wage & hour law in Germany

---

## **Business Immigration in Turkey**

### **Bener Law Office**

A structured guide to business immigration laws in Turkey

---

## **UK + Comments from other countries - Global Climate Strike: five key questions for employers**

### **Ius Laboris**

On Friday 20 September 2019, an unprecedented 'Global Climate Strike' is set to take place. Millions of employees across the world are being invited...

## **Environment & Climate Change**



## **Renewable Energy in Armenia**

### **Concern Dialog Law Firm**

A structured guide to renewable energy in Armenia

---

## **Environment and climate change in Switzerland**

### **Pestalozzi Attorneys at Law**

A structured guide to environment and climate change laws in Switzerland

---

## **Renewable Energy in Brazil**

### **Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados**

A structured guide to renewable energy in Brazil

---

## **Environment and climate change in the United Kingdom**

### **Linklaters LLP**

A structured guide to environment and climate change laws in the United Kingdom

---

## **September 'Global Climate Strikes': what employers need to consider**

### **MinterEllison**

Global climate protests on 20 September pose reputational risks for businesses if they do not prepare to manage a number of issues...

---

## **Climate change - a plain language guide for business**

### **MinterEllison**

We explore some of the background to issues that businesses face when addressing climate change...

---

## **Energy Report August 2019**

### **George Etomi & Partners**

In Nigeria, the challenges associated with electricity access from the national grid have given rise to innovative ways of structuring reliable power...

## Internet & Social Media



### Digital Business in Sweden

#### Mannheimer Swartling

A structured guide to digital business in Sweden

### The impact of the GDPR outside the EU

#### Ius Laboris

Since its entry into force in May 2018, the GDPR has had a significant impact on data protection policy and enforcement beyond the EU. This review by...

### WIPO Arbitration and Mediation Center Issues First Decision under UA-DRP

#### PETOŠEVIĆ

Following the entry into force of the .UA Domain-Name Dispute-Resolution Policy (UA-DRP) on March 19, 2019, the WIPO Arbitration and Mediation Center...

### Impact of digital disruption worldwide

#### Gowling WLG

In our latest report, Tides of Disruption: How to navigate business transformation, we highlight key markets and their current readiness for digital...

## Projects & Procurement



### ES: Nuevo proceso de licitación pública internacional para el Aeropuerto Internacional de El Salvador "San Óscar Arnulfo Romero y Galdámez"

#### Arias

Nuevo proceso de licitación pública internacional para el financiamiento, diseño, ampliación, construcción, equipamiento, mejora del mantenimiento y...

## Public



### Anti-corruption & Bribery in France

#### Reed Smith LLP

A structured guide to anti-corruption and bribery in France

### No-deal Brexit: The basics

#### Kilburn & Strode LLP

The UK is set to leave the European Union on 31 October 2019 ('Exit Day'). However, the UK will continue to be party to fundamental IP treaties and...

### The new Singapore Convention: Some practical issues to consider now

#### Herbert Smith Freehills LLP

As has been well publicised, the new Singapore Convention seeks to establish a global enforcement regime for settlement agreements resulting from...

## Other top stories



**Employment & Labor in Wyoming**

---

**State and Local Taxes in Illinois**

---

**The Directors' Handbook**

---

**Renewable Energy in the USA**

---

**Data & Privacy News - 12 September 2019**

---

**EEOC Announces It Will Not Collect Compensation Data Next Year**

---

**3 Reasons RFPs are the Secret Answer to Your Law Department's AFA Woes**

---

**"Oh AG, Please Don't Let Me Be Misunderstood": Breaking Down Common CCPA Myths**

---

**Tax on Inbound Investment in the USA**

---

**Can Employers get a Grip on Griping? Not all Gripes are Created Equal...**

---

## **International developments**

**Renewable Energy in the United Kingdom**

---

**Lawyers misguided attempt at office romance goes awry resulting in damages of \$170,000**

---

**Time to weed out knotweed - is Europe leading the way?**

---

**Time to weed out knotweed - is Europe leading the way?**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

**Brexit: Temporary Permissions and Contract Continuity**

---

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law

[Contact Lexology](#)

[About Lexology](#)





From: [US-CERT](mailto:US-CERT)  
To: [tmca.mis@sunnyvale.ca.gov](mailto:tmca.mis@sunnyvale.ca.gov)  
Subject: Vulnerability Summary for the Week of September 2, 2019  
Date: Monday, September 09, 2019 9:33:56 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## Vulnerability Summary for the Week of September 2, 2019

09/09/2019 06:49 AM EDT

Original release date: September 9, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alfresco -- alfresco	An issue was discovered in Alfresco Community Edition versions 6.0 and lower. An unauthenticated, remote attacker could authenticate to Alfresco's Solr Web Admin Interface. The vulnerability is due to the presence of a default private key that is present in all default installations. An attacker could exploit this vulnerability by using the extracted private key and bundling it into a PKCS12. A successful exploit could allow the attacker to gain information about the target system (e.g., OS type, system file locations, Java version, Solr version, etc.) as well as the ability to launch further attacks by leveraging the access to Alfresco's Solr Web Admin Interface.	2019-09-05	7.5	<a href="#">CVE-2019-14222 MISC</a>
alfresco -- alfresco	An issue was discovered in Alfresco Community Edition 5.2.201707. By leveraging multiple components in the Alfresco Software applications, an exploit chain was observed that allows an attacker to achieve remote code execution on the victim machine. The attacker must upload malicious Solr configuration files and then receive a JMX connection from the victim, and serve a Java object that results in deserialization and code execution.	2019-09-05	9.0	<a href="#">CVE-2019-14224 MISC</a>
artifex -- ghostscript	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass -dSAFER restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	2019-09-06	7.5	<a href="#">CVE-2019-14813 CONFIRM CONFIRM</a>
asus -- precision_touchpad	AsusPTPFilter.sys on Asus Precision TouchPad 11.0.0.25 hardware has a Pool Overflow associated with the \AsusTP device, leading to a DoS or potentially privilege escalation via a crafted DeviceIoControl call.	2019-09-04	7.5	<a href="#">CVE-2019-10709 MISC MISC</a>
broadcom -- ca_client_automation	An access vulnerability in CA Common Services DIA of CA Technologies Client Automation 14 and Workload Automation AE 11.3.5, 11.3.6 allows a remote attacker to execute arbitrary code.	2019-09-06	7.5	<a href="#">CVE-2019-13656 MISC</a>
cisco -- jabber	A vulnerability in Cisco Jabber Client Framework (JCF) for Mac Software, installed as part of the Cisco Jabber for Mac client, could allow an authenticated, local attacker to execute arbitrary code on an affected device. The vulnerability is due to improper file level permissions on an affected device when it is running Cisco JCF for Mac Software. An attacker could exploit this vulnerability by authenticating to the affected device and executing arbitrary code or potentially modifying certain configuration files. A successful exploit could allow the attacker to execute arbitrary code or modify certain configuration files on the device using the privileges of the installed Cisco JCF for Mac Software.	2019-09-04	7.2	<a href="#">CVE-2019-12645 CISCO</a>
cisco -- nx-os	A vulnerability in the Network Time Protocol (NTP) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to excessive use of system resources when the affected device is logging a drop action for received MODE_PRIVATE (Mode 7) NTP packets. An attacker could exploit this vulnerability by flooding the device with a steady stream of Mode 7 NTP packets. A successful exploit could allow the attacker to cause high CPU and memory usage on the affected device, which could cause internal system processes to restart or cause the affected device to unexpectedly reload. Note: The NTP feature is enabled by default.	2019-08-30	7.8	<a href="#">CVE-2019-1967 CISCO</a>
cisco -- unified_computing_system	A vulnerability in a specific CLI command within the local management (local-mgmt) context for Cisco UCS Fabric Interconnect Software could allow an authenticated, local attacker to gain elevated privileges as the root user on an affected device. The vulnerability is due to extraneous subcommand options present for a specific CLI command within the local-mgmt context. An attacker could exploit this vulnerability by authenticating to an affected device, entering the local-mgmt context, and issuing a specific CLI command and submitting user input. A successful exploit could allow the attacker to execute arbitrary operating system commands as root on an affected device. The attacker would need to have valid user credentials for the device.	2019-08-30	7.2	<a href="#">CVE-2019-1966 CISCO</a>
cisco -- webex_teams	A vulnerability in the Cisco Webex Teams client for Windows could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected system. This vulnerability is due to improper restrictions on software logging features used by the application on Windows operating systems. An attacker could exploit this vulnerability by convincing a targeted user to visit a website designed	2019-09-04	9.3	<a href="#">CVE-2019-1939 CISCO</a>

	to submit malicious input to the affected application. A successful exploit could allow the attacker to cause the application to modify files and execute arbitrary commands on the system with the privileges of the targeted user.			
egain -- chat	eGain Chat 15.0.3 allows unrestricted file upload.	2019-09-04	7.5	<a href="#">CVE-2019-13976</a> MISC
eventum_project -- eventum	Controller/ListController.php in Eventum 3.5.0 is vulnerable to Deserialization of Untrusted Data. Fixed in version 3.5.2.	2019-09-05	7.5	<a href="#">CVE-2018-11569</a> MISC
exim -- exim	Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash.	2019-09-06	10.0	<a href="#">CVE-2019-15846</a> MISC MLIST MLIST MLIST MLIST MLIST MLIST MLIST FEDORA FEDORA BUGTRAQ GENTOO UBUNTU DEBIAN CERT-VN MISC
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350648, 12.0-RELEASE before 12.0-RELEASE-p9, 11.3-STABLE before r350650, 11.3-RELEASE before 11.3-RELEASE-p2, and 11.2-RELEASE before 11.2-RELEASE-p13, the ICMPv6 input path incorrectly handles cases where an MLDv2 listener query packet is internally fragmented across multiple mbufs. A remote attacker may be able to cause an out-of-bounds read or write that may cause the kernel to attempt to access an unmapped page and subsequently panic.	2019-08-30	7.5	<a href="#">CVE-2019-5608</a> CONFIRM
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350828, 12.0-RELEASE before 12.0-RELEASE-p10, 11.3-STABLE before r350829, 11.3-RELEASE before 11.3-RELEASE-p3, and 11.2-RELEASE before 11.2-RELEASE-p14, a missing check in the function to arrange data in a chain of mbufs could cause data returned not to be contiguous. Extra checks in the Pv6 stack could catch the error condition and trigger a kernel panic, leading to a remote denial of service.	2019-08-30	7.8	<a href="#">CVE-2019-5611</a> MISC BUGTRAQ CONFIRM
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r351264, 12.0-RELEASE before 12.0-RELEASE-p10, 11.3-STABLE before r351265, 11.3-RELEASE before 11.3-RELEASE-p3, and 11.2-RELEASE before 11.2-RELEASE-p14, the kernel driver for /dev/midistat implements a read handler that is not thread-safe. A multi-threaded program can exploit races in the handler to copy out kernel memory outside the boundaries of midistat's data buffer.	2019-08-30	7.8	<a href="#">CVE-2019-5612</a> CONFIRM
fusionpbx -- fusionpbx	FusionPBX 4.4.8 allows an attacker to execute arbitrary system commands by submitting a malicious command to the service_edit.php file (which will insert the malicious command into the database). To trigger the command, one needs to call the services.php file via a GET request with the service id followed by the parameter a=start to execute the stored command.	2019-09-05	9.0	<a href="#">CVE-2019-15029</a> MISC MISC MISC
google -- android	NVIDIA Tegra contains a vulnerability in BootRom where a user with kernel level privileges can write an arbitrary value to an arbitrary physical address	2019-09-06	7.2	<a href="#">CVE-2018-6240</a> MISC
google -- android	In ihevcd_ref_list of ihevcd_ref_list.c in Android 10, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	9.3	<a href="#">CVE-2019-2108</a> MISC
google -- android	In GateKeeper::MintAuthToken of gatekeeper.cpp in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-2115</a> MISC
google -- android	In SensorManager::assertStateLocked of SensorManager.cpp in Android 7.1.1, 7.1.2, 8.0, 8.1, and 9, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-2174</a> MISC
google -- android	In ihevcd_parse_buffering_period_sei of ihevcd_parse_headers.c in Android 8.0, 8.1 and 9, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	9.3	<a href="#">CVE-2019-2176</a> MISC
google -- android	In rw_t4t_sm_read_ndef of rw_t4t in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC service with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-2178</a> MISC
google -- android	In readArgumentList of zygoter java in Android 10, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-9254</a> MISC
hanwha-security -- srn-472s_firmware	An issue was discovered in NVR WebViewer on Hanwha Techwin SRN-472s 1.07_190502 devices, and other SRN-x devices before 2019-05-03. A system crash and reboot can be achieved by submitting a long username in excess of 117 characters. The username triggers a buffer overflow in the main process controlling operation of the DVR system, rendering services unavailable during the reboot operation. A repeated attack affects availability as long as the attacker has network access to the device.	2019-09-05	7.8	<a href="#">CVE-2019-12223</a> MISC MISC MISC
libreoffice -- libreoffice	LibreOffice has a feature where documents can specify that pre-installed macros can be executed on various script events such as mouse-over, document-open etc. Access is intended to be restricted to scripts under the share/Scripts/python, user/Scripts/python sub-directories of the LibreOffice install. Protection was added, to address CVE-2019-9852, to avoid a directory traversal attack where scripts in arbitrary locations on the file system could be executed by employing a URL encoding attack to defeat the path verification step. However this protection	2019-09-06	7.5	<a href="#">CVE-2019-9854</a> CONFIRM

	could be bypassed by taking advantage of a flaw in how LibreOffice assembled the final script URL location directly from components of the passed in path as opposed to solely from the sanitized output of the path verification step. This issue affects: Document Foundation LibreOffice 6.2 versions prior to 6.2.7; 6.3 versions prior to 6.3.1.			
libreoffice -- libreoffice	LibreOffice is typically bundled with LibreLogo, a programmable turtle vector graphics script, which can execute arbitrary python commands contained with the document it is launched from. LibreOffice also has a feature where documents can specify that pre-installed scripts can be executed on various document script events such as mouse-over, etc. Protection was added to block calling LibreLogo from script event handlers. However a Windows 8.3 path equivalence handling flaw left LibreOffice vulnerable under Windows that a document could trigger executing LibreLogo via a Windows filename pseudonym. This issue affects: Document Foundation LibreOffice 6.2 versions prior to 6.2.7; 6.3 versions prior to 6.3.1.	2019-09-06	7.5	<a href="#">CVE-2019-9855</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.14.11. A double free may be caused by the function allocate_trace_buffer in the file kernel/trace/trace.c.	2019-09-04	7.2	<a href="#">CVE-2017-18595</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	A backporting error was discovered in the Linux stable/longterm kernel 4.4.x through 4.4.190, 4.9.x through 4.9.190, 4.14.x through 4.14.141, 4.19.x through 4.19.69, and 5.2.x through 5.2.11. Misuse of the upstream "x86/ptrace: Fix possible spectre-v1 in ptrace_get_debugreg()" commit reintroduced the Spectre vulnerability that it aimed to eliminate. This occurred because the backport process depends on cherry picking specific commits, and because two (correctly ordered) code lines were swapped.	2019-09-04	7.5	<a href="#">CVE-2019-15902</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobjects() in net/core/net-sysfs.c, which will cause denial of service.	2019-09-04	7.8	<a href="#">CVE-2019-15916</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.5. There is a use-after-free issue when hci_uart_register_dev() fails in hci_uart_set_proto() in drivers/bluetooth/hci_ldisc.c.	2019-09-04	7.2	<a href="#">CVE-2019-15917</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.10. SMB2_negotiate in fs/cifs/smb2pdu.c has an out-of-bounds read because data structures are incompletely updated after a change from smb30 to smb21.	2019-09-04	7.2	<a href="#">CVE-2019-15918</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.10. SMB2_write in fs/cifs/smb2pdu.c has a use-after-free.	2019-09-04	7.2	<a href="#">CVE-2019-15919</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.10. SMB2_read in fs/cifs/smb2pdu.c has a use-after-free. NOTE: this was not fixed correctly in 5.0.10; see the 5.0.11 Changelog, which documents a memory leak.	2019-09-04	7.2	<a href="#">CVE-2019-15920</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.2.3. An out of bounds access exists in the function hclge_tm_sched_mode_vnet_base_cfg in the file drivers/net/ethernet/hisilicon/hns3/hns3pf/hclge_tm.c.	2019-09-04	7.2	<a href="#">CVE-2019-15925</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.2.3. Out of bounds access exists in the functions ath6kl_wmi_pstream_timeout_event_rx and ath6kl_wmi_cac_event_rx in the file drivers/net/wireless/ath/ath6kl/wmi.c.	2019-09-04	9.4	<a href="#">CVE-2019-15926</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.20.2. An out-of-bounds access exists in the function build_audio_procunit in the file sound/usb/mixer.c.	2019-09-04	7.2	<a href="#">CVE-2019-15927</a> <a href="#">MISC</a> <a href="#">MISC</a>
nagios -- nagios_xi	Nagios XI before 5.6.6 allows remote command execution as root. The exploit requires access to the server as the nagios user, or access as the admin user via the web interface. The getprofile.sh script, invoked by downloading a system profile (profile.php?cmd=download), is executed as root via a passwordless sudo entry; the script executes check_plugin, which is owned by the nagios user. A user logged into Nagios XI with permissions to modify plugins, or the nagios user on the server, can modify the check_plugin executable and insert malicious commands to execute as root.	2019-09-05	9.0	<a href="#">CVE-2019-15949</a> <a href="#">MISC</a>
opencsc_project -- opencsc	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Bitstring in decode_bit_string in libopencsc/asn1.c.	2019-09-05	7.5	<a href="#">CVE-2019-15945</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencsc_project -- opencsc	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Octet string in asn1_decode_entry in libopencsc/asn1.c.	2019-09-05	7.5	<a href="#">CVE-2019-15946</a> <a href="#">MISC</a> <a href="#">MISC</a>
pengutronix -- barebox	Pengutronix barebox through 2019.08.1 has a remote buffer overflow in nfs_readlink_reply in net/nfs.c because a length field is directly used for a memcpy.	2019-09-05	7.5	<a href="#">CVE-2019-15937</a> <a href="#">MISC</a>
pengutronix -- barebox	Pengutronix barebox through 2019.08.1 has a remote buffer overflow in nfs_readlink_req in fs/nfs.c because a length field is directly used for a memcpy.	2019-09-05	7.5	<a href="#">CVE-2019-15938</a> <a href="#">MISC</a>
restaurant_reservations_project -- restaurant_reservations	The nd-restaurant-reservations plugin before 1.5 for WordPress has no requirement for nd_rst_import_settings_php_function authentication.	2019-08-30	7.5	<a href="#">CVE-2019-15819</a> <a href="#">MISC</a> <a href="#">MISC</a>
sonatype -- nexus_repository_manager	The Nexus Yum Repository Plugin in v2 is vulnerable to Remote Code Execution when instances using CommandLineExecutor java are supplied vulnerable data, such as the Yum Configuration Capability.	2019-09-03	9.0	<a href="#">CVE-2019-5475</a> <a href="#">MISC</a>
symfonyextensions -- rich_text_formatter	The Rich Text Formatter (Redactor) extension through v1.1.1 for Symphony CMS has an Unauthenticated arbitrary file upload vulnerability in content.fileupload.php and content.imageupload.php.	2019-09-05	7.5	<a href="#">CVE-2019-13187</a> <a href="#">MISC</a> <a href="#">MISC</a>
totaljs -- total_js_cms	An issue was discovered in Total.js CMS 12.0.0. An authenticated user with the widgets privilege can gain achieve Remote Command Execution (RCE) on the remote server by creating a malicious widget with a special tag containing JavaScript code that will be evaluated server side. In the process of evaluating the tag by the back-end, it is possible to escape the sandbox object by using the following payload: <script total>global.process.mainModule.require(child_process).exec(RCE);</script>	2019-09-05	9.0	<a href="#">CVE-2019-15954</a> <a href="#">MISC</a> <a href="#">MISC</a>
varnish-cache -- varnish	An issue was discovered in Varnish Cache before 6.0.4 LTS, and 6.1.x and 6.2.x before 6.2.1. An HTTP/1 parsing failure allows a remote attacker to trigger an assert by sending crafted HTTP/1 requests. The assert will cause an automatic	2019-09-03	7.8	<a href="#">CVE-2019-15892</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>



	restart with a clean cache, which makes it a Denial of Service attack.			DEBIAN
wpbrigade -- loginpress	The LoginPress plugin before 1.1.4 for WordPress has SQL injection via an import of settings.	2019-09-03	7.5	<a href="#">CVE-2019-15872</a> MISC
wpserveur -- wps_child_theme_generator	The wps-child-theme-generator plugin before 1.2 for WordPress has classes/helpers.php directory traversal.	2019-08-30	7.5	<a href="#">CVE-2019-15822</a> MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has an action=confirmation protection bypass.	2019-08-30	7.5	<a href="#">CVE-2019-15823</a> MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has an adminhash protection bypass.	2019-08-30	7.5	<a href="#">CVE-2019-15824</a> MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has an action=rp&key&login protection bypass.	2019-08-30	7.5	<a href="#">CVE-2019-15825</a> MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has a protection bypass via wp-login.php in the Referer field.	2019-08-30	7.5	<a href="#">CVE-2019-15826</a> MISC
xiaoyi -- yi_m1_mirrorless_camera_firmware	An exploitable authentication bypass vulnerability exists in the Bluetooth Low Energy (BLE) authentication module of YI M1 Mirrorless Camera V3 2-cn. An attacker can send a set of BLE commands to trigger this vulnerability, resulting in sensitive data leakage (e.g., personal photos). An attacker can also control the camera to record or take a picture after bypassing authentication.	2019-09-06	8.3	<a href="#">CVE-2019-13953</a> MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web -- photo_gallery	The photo-gallery plugin before 1.2.42 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2015-9380</a> MISC
abus -- secvest_wireless_alarm_system_fuaa50000_firmware	An issue was discovered on ABUS Secvest FUA50000 3.01.01 devices. Due to an insufficient implementation of jamming detection, an attacker is able to suppress correctly received RF messages sent between wireless peripheral components, e.g., wireless detectors or remote controls, and the ABUS Secvest alarm central. An attacker is able to perform a "reactive jamming" attack. The reactive jamming simply detects the start of a RF message sent by a component of the ABUS Secvest wireless alarm system, for instance a wireless motion detector (FUBW50000) or a remote control (FUBE50014 or FUBE50015), and overlays it with random data before the original RF message ends. Thereby, the receiver (alarm central) is not able to properly decode the original transmitted signal. This enables an attacker to suppress correctly received RF messages of the wireless alarm system in an unauthorized manner, for instance status messages sent by a detector indicating an intrusion.	2019-09-03	5.0	<a href="#">CVE-2019-14261</a> MISC FULLDISC BUGTRAQ
airbrake -- airbrake_ruby	The Airbrake Ruby notifier 4.2.3 for Airbrake mishandles the blacklist_keys configuration option and consequently may disclose passwords to unauthorized actors. This is fixed in 4.2.4 (also, 4.2.2 and earlier are unaffected).	2019-09-06	5.0	<a href="#">CVE-2019-16060</a> MISC
apache -- commons_compress	The file name encoding algorithm used internally in Apache Commons Compress 1.15 to 1.18 can get into an infinite loop when faced with specially crafted inputs. This can lead to a denial of service attack if an attacker can choose the file names inside of an archive created by Compress.	2019-08-30	5.0	<a href="#">CVE-2019-12402</a> MISC
artifex -- ghostscript	A flaw was found in, ghostscript versions prior to 9.28, in the pdf_hook_DSC_Creator procedure where it did not properly secure its privileged calls, enabling scripts to bypass -dSAFER restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	2019-09-03	6.8	<a href="#">CVE-2019-14811</a> CONFIRM
bitcoin -- bitcoin-qt	In Bitcoin Core 0.18.0, bitcoin-qt stores wallet.dat data unencrypted in memory. Upon a crash, it may dump a core file. If a user were to mishandle a core file, an attacker can reconstruct the user's wallet.dat file, including their private keys, via a grep "6231 0500" command.	2019-09-05	5.0	<a href="#">CVE-2019-15947</a> MISC
blynk -- blynk-library	An exploitable information disclosure vulnerability exists in the packet-parsing functionality of Blynk-Library v0.6.1. A specially crafted packet can cause an unauthenticated strncpy, resulting in information disclosure. An attacker can send a packet to trigger this vulnerability.	2019-09-05	5.0	<a href="#">CVE-2019-5065</a> MISC
bold-themes -- bold_page_builder	The bold-page-builder plugin before 2.3.2 for WordPress has no protection against modifying settings and importing data.	2019-08-30	5.0	<a href="#">CVE-2019-15821</a> MISC
canon -- print	The ContentProvider in the Canon PR NT.jp.co.canon.bsd.ad.pixmaprint 2.5.5 application for Android does not properly restrict canon.i.j.printer.capability.data data access. This allows an attacker's malicious application to obtain sensitive information including factory passwords for the administrator web interface and WPA2-PSK key.	2019-09-05	4.3	<a href="#">CVE-2019-14339</a> MISC
	A vulnerability in the authorization module of Cisco Content Security			

cisco -- content_security_management_appliance	Management Appliance (SMA) Software could allow an authenticated, remote attacker to gain out-of-scope access to email. The vulnerability exists because the affected software does not correctly implement role permission controls. An attacker could exploit this vulnerability by using a custom role with specific permissions. A successful exploit could allow the attacker to access the spam quarantine of other users.	2019-09-04	4.0	<a href="#">CVE-2019-12635</a> <a href="#">CISCO</a>
cisco -- finesse	A vulnerability in Cisco Finesse could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on an affected system. The vulnerability exists because the affected system does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to access the system and perform unauthorized actions.	2019-09-04	5.0	<a href="#">CVE-2019-12632</a> <a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability exists because the web-based management interface of the affected device does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-09-04	4.3	<a href="#">CVE-2019-12644</a> <a href="#">CISCO</a>
cisco -- network_level_service	A vulnerability in the "plug-and-play" services component of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper access restrictions on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to access running configuration information about devices managed by the IND, including administrative credentials.	2019-09-04	5.0	<a href="#">CVE-2019-1976</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.	2019-08-30	5.0	<a href="#">CVE-2019-1968</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the implementation of the Simple Network Management Protocol (SNMP) Access Control List (ACL) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to perform SNMP polling of an affected device, even if it is configured to deny SNMP traffic. The vulnerability is due to an incorrect length check when the configured ACL name is the maximum length, which is 32 ASCII characters. An attacker could exploit this vulnerability by performing SNMP polling of an affected device. A successful exploit could allow the attacker to perform SNMP polling that should have been denied. The attacker has no control of the configuration of the SNMP ACL name.	2019-08-30	5.0	<a href="#">CVE-2019-1969</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability within the Endpoint Learning feature of Cisco Nexus 9000 Series Switches running in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an endpoint device in certain circumstances. The vulnerability is due to improper endpoint learning when packets are received on a specific port from outside the ACI fabric and destined to an endpoint located on a border leaf when Disable Remote Endpoint Learning has been enabled. This can result in a Remote (XR) entry being created for the impacted endpoint that will become stale if the endpoint migrates to a different port or leaf switch. This results in traffic not reaching the impacted endpoint until the Remote entry can be relearned by another mechanism.	2019-08-30	4.3	<a href="#">CVE-2019-1977</a> <a href="#">CISCO</a>
cisco -- unified_contact_center_express	A vulnerability in Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on a targeted system. The vulnerability is due to improper validation of user-supplied input on the affected system. An attacker could exploit this vulnerability by sending the user of the web application a crafted request. If the request is processed, the attacker could access the system and perform unauthorized actions.	2019-09-04	5.0	<a href="#">CVE-2019-12633</a> <a href="#">CISCO</a>
convertplug -- convertplus	The ConvertPlus plugin before 3.4.5 for WordPress has an unintended account creation (with the none role) via a request for variants.	2019-09-03	5.0	<a href="#">CVE-2019-15863</a> <a href="#">MISC</a>
custom_404_pro_project -- custom_404_pro	The custom-404-pro plugin before 3.2.8 for WordPress has reflected XSS, a different vulnerability than CVE-2019-14789.	2019-08-30	4.3	<a href="#">CVE-2019-15838</a> <a href="#">MISC</a> <a href="#">MISC</a>
dell -- emc_enterprise_copy_data_management	Dell EMC Enterprise Copy Data Management (eCDM) versions 1.0, 1.1, 2.0, 2.1, and 3.0 contain a certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim's data in transit.	2019-09-03	5.8	<a href="#">CVE-2019-3751</a> <a href="#">MISC</a>
dell -- emc_unity_operating_environment	Dell EMC Unity Operating Environment versions prior to 5.0.0.0.5.116, Dell EMC UnityVSA versions prior to 5.0.0.0.5.116 and Dell EMC VNXe3200 versions prior to 3.1.10.9946299 contain a reflected cross-site scripting vulnerability on the cas/logout page. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to supply malicious HTML or Java Script code to Unisphere, which is then reflected back to the victim and executed by the web browser.	2019-09-03	4.3	<a href="#">CVE-2019-3754</a> <a href="#">CONFIRM</a>
egain -- chat	eGain Chat 15.0.3 allows HTML Injection.	2019-09-04	4.3	<a href="#">CVE-2019-13975</a> <a href="#">MISC</a>
eng -- knowage	In Knowage through 6.1.1, an unauthenticated user can bypass access	2019-09-05	5.0	<a href="#">CVE-2019-13188</a>

	controls and access the entire application.			MISC
eng -- knowage	In Knowage through 6.1.1, the sign up page does not invalidate a valid CAPTCHA token. This allows for CAPTCHA bypass in the signup page.	2019-09-05	5.0	<a href="#">CVE-2019-13190</a> MISC
epignosishq -- efront_lms	A code execution vulnerability exists in Epignosis eFront LMS v5.2.12. A specially crafted web request can cause unsafe deserialization potentially resulting in PHP code being executed. An attacker can send a crafted web parameter to trigger this vulnerability.	2019-09-05	6.5	<a href="#">CVE-2019-5069</a> MISC
epignosishq -- efront_lms	An exploitable SQL injection vulnerability exists in the unauthenticated portion of eFront LMS, versions v5.2.12 and earlier. Specially crafted web request to login page can cause SQL injections, resulting in data compromise. An attacker can use a browser to trigger these vulnerabilities, and no special tools are required.	2019-09-05	6.4	<a href="#">CVE-2019-5070</a> MISC
espressif -- esp-idf	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 allows the installation of a zero Pairwise Master Key (PMK) after the completion of any EAP authentication method, which allows attackers in radio range to replay, decrypt, or spoof frames via a rogue access point.	2019-09-04	4.8	<a href="#">CVE-2019-12587</a> MISC MISC MISC
estronics -- es_file_explorer_file_manager	The master-password feature in the ES File Explorer File Manager application 4.2.0.1.3 for Android can be bypassed via a com.estronics.android.pop.fip.ESFtpShortcut intent, leading to remote FTP access to the entirety of local storage.	2019-09-05	5.0	<a href="#">CVE-2019-11380</a> MISC
estsoft -- alsee	A memory corruption vulnerability exists in the PSD parsing functionality of ALSee v5.3 ~ v8.39. A specially crafted PSD file can cause an out of bounds write vulnerability resulting in code execution. By persuading a victim to open a specially-crafted .PSD file, an attacker could execute arbitrary code.	2019-08-30	6.8	<a href="#">CVE-2019-12810</a> CONFIRM
ezautomation -- ez_plc_editor	An attacker could use a specially crafted project file to corrupt the memory and execute code under the privileges of the EZ PLC Editor Versions 1.8.41 and prior.	2019-09-04	6.8	<a href="#">CVE-2019-13522</a> MISC
ezautomation -- ez_touch_editor	An attacker could use a specially crafted project file to overflow the buffer and execute code under the privileges of the EZ Touch Editor Versions 2.1.0 and prior.	2019-09-04	6.8	<a href="#">CVE-2019-13518</a> MISC
f5 -- big-ip_access_policy_manager	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges.	2019-09-04	6.5	<a href="#">CVE-2019-6646</a> MISC
facebook -- facebook_for_woocommerce	The facebook-for-woocommerce plugin before 1.9.14 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15840</a> MISC
facebook -- facebook_for_woocommerce	The facebook-for-woocommerce plugin before 1.9.15 for WordPress has CSRF via ajax_woo_infobanner_post_click, ajax_woo_infobanner_post_xout, or ajax_fb_toggle_visibility.	2019-08-30	6.8	<a href="#">CVE-2019-15841</a> MISC
ffmpeg -- ffmpeg	FFmpeg through 4.2 has a "Conditional jump or move depends on uninitialised value" issue in h2645_parse because alloc_rbsp_buffer in libavcodec/h2645_parse.c mishandles rbsp_buffer.	2019-09-05	6.8	<a href="#">CVE-2019-15942</a> MISC
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350619, 12.0-RELEASE before 12.0-RELEASE-p9, 11.3-STABLE before r350619, 11.3-RELEASE before 11.3-RELEASE-p2, and 11.2-RELEASE before 11.2-RELEASE-p13, the bhyve e1000 device emulation used a guest-provided value to determine the size of the on-stack buffer without validation when TCP segmentation offload is requested for a transmitted packet. A misbehaving bhyve guest could overwrite memory in the bhyve process on the host.	2019-08-30	6.4	<a href="#">CVE-2019-5609</a> CONFIRM
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350637, 12.0-RELEASE before 12.0-RELEASE-p9, 11.3-STABLE before r350638, 11.3-RELEASE before 11.3-RELEASE-p2, and 11.2-RELEASE before 11.2-RELEASE-p13, the bsnmp library is not properly validating the submitted length from a type-length-value encoding. A remote user could cause an out-of-bounds read or trigger a crash of the software such as bsnmpd resulting in a denial of service.	2019-08-30	5.0	<a href="#">CVE-2019-5610</a> MISC BUGTRAQ CONFIRM
freedesktop -- poppler	Poppler before 0.76.0 has an integer overflow in Parser: makeStream in Parser cc.	2019-09-05	6.8	<a href="#">CVE-2018-21009</a> MISC
freetype -- freetype	FreeType before 2.6.1 has a heap-based buffer over-read in T1_Get_Private_Dict in type1/t1parse.c.	2019-09-03	6.8	<a href="#">CVE-2015-9381</a> MISC MLIST MISC
freetype -- freetype	FreeType before 2.6.1 has a buffer over-read in skip_comment in psaux/psobjs.c because ps_parser_skip_PS_token is mishandled in an FT_New_Memory_Face operation.	2019-09-03	4.3	<a href="#">CVE-2015-9382</a> MISC MLIST MISC
freetype -- freetype	FreeType before 2.6.2 has a heap-based buffer over-read in tt_cmap14_validate in sfnt/ttmap.c.	2019-09-03	4.3	<a href="#">CVE-2015-9383</a> MISC MLIST MISC
glyphandcog -- xpdfreader	Xpdf 2.00 allows a SIGSEGV in XRef::constructXRef in XRef.cc. NOTE: 2.00 is a version from November 2002.	2019-09-03	4.3	<a href="#">CVE-2019-15860</a> MISC
gnu -- gcc	The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.	2019-09-02	5.0	<a href="#">CVE-2019-15847</a> MISC
google -- android	In execTransact of Binder.java in Android 7.1.1, 7.1.2, 8.0, 8.1, and 9, there is a possible local execution of arbitrary code in a privileged process due to a memory overwrite. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	4.6	<a href="#">CVE-2019-2123</a> MISC

google -- android	In checkAccess of SliceManagerService.java in Android 9, there is a possible permissions check bypass due to incorrect order of arguments. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	4.4	<a href="#">CVE-2019-2175</a> MISC
google -- android	In isPreferred of HidProfile.java in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible device type confusion due to a permissions bypass. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	6.8	<a href="#">CVE-2019-2177</a> MISC
google -- android	In NDEF_MsgValidate of ndef_utils in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	4.3	<a href="#">CVE-2019-2179</a> MISC
google -- android	In binder_transaction of binder.c in the Android kernel, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	6.9	<a href="#">CVE-2019-2181</a> MISC
grafana -- grafana	In Grafana 2.x through 6.x before 6.3.4, parts of the HTTP API allow unauthenticated use. This makes it possible to run a denial of service attack against the server running Grafana.	2019-09-03	5.0	<a href="#">CVE-2019-15043</a> CONFIRM MISC CONFIRM FEDORA FEDORA
ibm -- intelligent_operations_center	BM Intelligent Operations Center V5.1.0 - V5.2.0, IBM Intelligent Operations Center for Emergency Management V5.1.0 - V5.1.0.6, and IBM Water Operations for Watermatics V5.1.0 - V5.2.1.1 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 161201.	2019-09-05	5.0	<a href="#">CVE-2019-4321</a> CONFIRM XF
ibm -- jazz_for_service_management	BM Jazz for Service Management 1.1.3 is vulnerable to HTTP header injection, caused by incorrect trust in the HTTP Host header during caching. By sending a specially crafted HTTP GET request, a remote attacker could exploit this vulnerability to inject arbitrary HTTP headers, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-force ID: 158976.	2019-09-05	4.3	<a href="#">CVE-2019-4186</a> XF CONFIRM
instagram-php-api_project -- instagram-php-api	cosenary Instagram-PHP-API (aka Instagram PHP API V2), as used in the UserPro plugin through 4.9.32 for WordPress, has XSS via the example/success.php_error_description parameter.	2019-09-04	4.3	<a href="#">CVE-2019-14470</a> MISC MISC MISC EXPLOIT-DB
jetbrains -- teamcity	JetBrains TeamCity 2019.1 and 2019.1.1 allows cross-site scripting (XSS), potentially making it possible to send an arbitrary HTTP request to a TeamCity server under the name of the currently logged-in user.	2019-09-05	4.3	<a href="#">CVE-2019-15848</a> CONFIRM
knowage-suite -- knowage	In Knowage through 6.1.1, an authenticated user that accesses the users page will obtain all user password hashes.	2019-09-05	4.0	<a href="#">CVE-2019-13349</a> MISC
knowage-suite -- knowage	In Knowage through 6.1.1, an unauthenticated user can enumerated valid usernames via the ChangePwdServlet page.	2019-09-05	5.0	<a href="#">CVE-2019-14278</a> MISC
lenovo -- xclarity_administrator	An XML External Entity (XXE) processing vulnerability was reported in Lenovo XClarity Administrator (LXCA) prior to version 2.5.0, Lenovo XClarity Integrator (LXCI) for Microsoft System Center prior to version 7.7.0, and Lenovo XClarity Integrator (LXCI) for VMware vCenter prior to version 6.1.0 that could allow information disclosure.	2019-09-03	5.0	<a href="#">CVE-2019-6179</a> MISC
lenovo -- xclarity_administrator	A reflected cross-site scripting (XSS) vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow a crafted URL, if visited, to cause JavaScript code to be executed in the user's web browser. The JavaScript code is not executed on LXCA itself.	2019-09-03	4.3	<a href="#">CVE-2019-6181</a> MISC
lenovo -- xclarity_administrator	A stored CSV Injection vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow an administrative user to store malformed data in LXCA Jobs and Event Log data, that could result in crafted formulas stored in an exported CSV file. The crafted formula is not executed on LXCA itself.	2019-09-03	4.0	<a href="#">CVE-2019-6182</a> MISC
libexpat_project -- libexpat	In libexpat before 2.2.8, crafted XML input could fool the parser into changing from DTD parsing to document parsing too early; a consecutive call to XML_GetCurrentLineNumber (or XML_GetCurrentColumnNumber) then resulted in a heap-based buffer over-read.	2019-09-04	5.0	<a href="#">CVE-2019-15903</a> MISC MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.16.7. A use-after-free can be caused by the function rsi_mac80211_detach in the file drivers/net/wireless/rsi/rsi_91x_mac80211.c.	2019-09-04	4.9	<a href="#">CVE-2018-21008</a> MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.6. There is a memory leak issue when idr_alloc() fails in genl_register_family() in net/netlink/genetlink.c.	2019-09-04	4.6	<a href="#">CVE-2019-15921</a> MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a pf data structure if alloc_disk fails in drivers/block/paride/pf.c.	2019-09-04	4.9	<a href="#">CVE-2019-15922</a> MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a cd data structure if alloc_disk fails in drivers/block/paride/pf.c.	2019-09-04	4.9	<a href="#">CVE-2019-15923</a> MISC MISC
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.11. fm10k_init_module in drivers/net/ethernet/intel/fm10k/fm10k_main.c has a NULL pointer dereference because there is no -ENOMEM upon an	2019-09-04	4.9	<a href="#">CVE-2019-15924</a> MISC

	alloc_workqueue failure.			MISC
login_or_logout_menu_item_project -- login_or_logout_menu_item	The login-or-logout-menu-item plugin before 1.2.0 for WordPress has no requirement for lolmi_save_settings authentication.	2019-08-30	5.8	CVE-2019-15820 MISC MISC MISC
memcached -- memcached	memcached 1.5.16, when UNIX sockets are used, has a stack-based buffer over-read in conn_to_str in memcached.c.	2019-08-30	5.0	CVE-2019-15026 CONFIRM CONFIRM MLIST
mongodb -- mongodb	An unprivileged user or program on Microsoft Windows which can create OpenSSL configuration files in a fixed location may cause utility programs shipped with MongoDB server versions less than 4.0.11, 3.6.14, and 3.4.22 to run attacker defined code as the user running the utility.	2019-08-30	6.8	CVE-2019-2390 CONFIRM
mulesoft -- api_gateway	Directory Traversal in APIkit, HTTP connector, and OAuth2 Provider components in MuleSoft Mule Runtime 3.2.0 and higher released before August 1 2019, MuleSoft Mule Runtime 4.1.0 and higher released before August 1 2019, and all versions of MuleSoft API Gateway released before August 1 2019 allow remote attackers to read files accessible to the Mule process.	2019-08-30	5.0	CVE-2019-15630 MISC
nagios -- log_server	Nagios Log Server before 2.0.8 allows Reflected XSS via the username on the Login page.	2019-09-03	4.3	CVE-2019-15898 MISC MISC
naver -- cloud_explorer	NDrive(1.2.2) sys in Naver Cloud Explorer has a stack-based buffer overflow, which allows attackers to cause a denial of service when reading data from IOCTL handle.	2019-09-03	5.0	CVE-2019-13156 CONFIRM
onkyo -- tx-nr686_firmware	Directory traversal vulnerability on ONKYO TX-NR686 1030-5000-1040-0010 A/V Receiver devices allows remote attackers to read arbitrary files via a .. (dot dot) and %2f to the default URL.	2019-08-30	5.0	CVE-2019-6113 MISC
opencv -- opencv	An issue was discovered in OpenCV 4.1.0. There is a divide-by-zero error in cv::HOGDescriptor::getDescriptorSize in modules/objdetect/src/hog.cpp.	2019-09-05	5.0	CVE-2019-15939 MISC MISC
profilegrid -- profilegrid	The profilegrid-user-profiles-groups-and-communities plugin before 2.8.6 for WordPress has remote code execution via an wp-admin/admin-ajax.php request with the action=pm_template_preview&html=<?php substring followed by PHP code.	2019-09-03	6.5	CVE-2019-15873 MISC MISC
rancher -- rancher	Rancher 2 through 2.2.4 is vulnerable to a Cross-Site WebSocket Hijacking attack that allows an exploiter to gain access to clusters managed by Rancher. The attack requires a victim to be logged into a Rancher server, and then to access a third-party site hosted by the exploiter. Once that is accomplished, the exploiter is able to execute commands against the cluster's Kubernetes API with the permissions and identity of the victim.	2019-09-04	4.3	CVE-2019-13209 MISC CONFIRM
realestateconnected -- easy_property_listings	The easy-property-listings plugin before 3.4 for WordPress has XSS.	2019-08-30	4.3	CVE-2019-15817 MISC MISC
samba -- samba	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.	2019-09-03	6.4	CVE-2019-10197 CONFIRM BUGTRAQ CONFIRM UBUNTU DEBIAN MISC
saplica -- sentrifugo	Sentrifugo 3.2 lacks CSRF protection. This could lead to an attacker tricking the administrator into executing arbitrary code at index.php/dashboard/viewprofile via a crafted HTML page.	2019-09-06	6.8	CVE-2019-16059 MISC
sentrifugo -- sentrifugo	Multiple file upload restriction bypass vulnerabilities in Sentrifugo 3.2 could allow authenticated users to execute arbitrary code via a webshell.	2019-09-04	6.5	CVE-2019-15813 EXPLOIT-DB
shaosina -- sina_extension_for_elementor	The sina-extension-for-elementor plugin before 2.2.1 for WordPress has local file inclusion.	2019-08-30	5.0	CVE-2019-15839 MISC MISC MISC
simple_mail_address_encoder_project -- simple_mail_address_encoder	The simple-mail-address-encoder plugin before 1.7 for WordPress has reflected XSS.	2019-08-30	4.3	CVE-2019-15833 MISC
statichttpserver_project -- statichttpserver	A path traversal vulnerability in <= v0.9.7 of statichttpserver npm module allows attackers to list files in arbitrary folders.	2019-09-03	5.0	CVE-2019-5480 MISC
symantec -- advanced_secure_gateway	The ASG/ProxySG FTP proxy WebFTP mode allows intercepting FTP connections where a user accesses an FTP server via a ftp:// URL in a web browser. A stored cross-site scripting (XSS) vulnerability in the WebFTP mode allows a remote attacker to inject malicious JavaScript code in ASG/ProxySG's web listing of a remote FTP server. Exploiting the vulnerability requires the attacker to be able to upload crafted files to the remote FTP server. Affected versions: ASG 6.6 and 6.7 prior to 6.7.4.2; ProxySG 6.5 prior to 6.5.10.15, 6.6, and 6.7 prior to 6.7.4.2.	2019-08-30	4.3	CVE-2018-18370 CONFIRM
symantec -- advanced_secure_gateway	The ASG/ProxySG FTP proxy WebFTP mode allows intercepting FTP connections where a user accesses an FTP server via a ftp:// URL in a web browser. An information disclosure vulnerability in the WebFTP mode allows a malicious user to obtain plaintext authentication credentials for a remote FTP server from the ASG/ProxySG's web listing of the FTP server. Affected versions: ASG 6.6 and 6.7 prior to 6.7.4.2; ProxySG 6.5 prior to 6.5.10.15, 6.6, and 6.7 prior to 6.7.4.2.	2019-08-30	4.0	CVE-2018-18371 CONFIRM
	An information disclosure vulnerability in the Management Center (MC)			



symantec -- management_center	REST API 2.0, 2.1, and 2.2 prior to 2.2.2.1 allows a malicious authenticated user to obtain passwords for external backup and CPL policy import servers that they might not otherwise be authorized to access.	2019-08-30	4.0	<a href="#">CVE-2019-9697</a> <a href="#">CONFIRM</a>
symantec -- reporter	An information disclosure vulnerability in Symantec Reporter web UI 10.3 prior to 10.3.2.5 allows a malicious authenticated administrator user to obtain passwords for external SMTP, FTP, FTPS, LDAP, and Cloud Log Download servers that they might not otherwise be authorized to access. The malicious administrator user can also obtain the passwords of other Reporter web UI users.	2019-08-30	4.0	<a href="#">CVE-2019-12753</a> <a href="#">CONFIRM</a>
totaljs -- total_js_cms	An issue was discovered in Total js CMS 12.0.0. An authenticated user with the Pages privilege can conduct a path traversal attack (..) to include html files that are outside the permitted directory. Also, if a page contains a template directive, then the directive will be server side processed. Thus, if a user can control the content of a html file, then they can inject a payload with a malicious template directive to gain Remote Command Execution. The exploit will work only with the html extension.	2019-09-05	6.5	<a href="#">CVE-2019-15952</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
totaljs -- total_js_cms	An issue was discovered in Total js CMS 12.0.0. An authenticated user with limited privileges can get access to a resource that they do not own by calling the associated API. The product correctly manages privileges only for the front-end resource path, not for API requests. This leads to vertical and horizontal privilege escalation.	2019-09-05	6.5	<a href="#">CVE-2019-15953</a> <a href="#">MISC</a> <a href="#">MISC</a>
totaljs -- total_js_cms	An issue was discovered in Total js CMS 12.0.0. A low privilege user can perform a simple transformation of a cookie to obtain the random values inside it. If an attacker can discover a session cookie owned by an admin, then it is possible to brute force it with $O(n)=2n$ instead of $O(n)=n^x$ complexity, and steal the admin password.	2019-09-05	4.0	<a href="#">CVE-2019-15955</a> <a href="#">MISC</a> <a href="#">MISC</a>
totemo -- totemomail	Cross-site scripting (XSS) vulnerability in the 'Certificate' feature of totemomail 6.0.0 build 570 allows remote attackers to inject arbitrary web script or HTML.	2019-08-30	4.3	<a href="#">CVE-2018-15510</a> <a href="#">MISC</a>
totemo -- totemomail	Cross-site scripting (XSS) vulnerability in the 'Notification template' feature of totemomail 6.0.0 build 570 allows remote attackers to inject arbitrary web script or HTML.	2019-08-30	4.3	<a href="#">CVE-2018-15511</a> <a href="#">MISC</a>
totemo -- totemomail	Cross-site scripting (XSS) vulnerability in the 'Authorisation Service' feature of totemomail 6.0.0 build 570 allows remote attackers to inject arbitrary web script or HTML.	2019-08-30	4.3	<a href="#">CVE-2018-15512</a> <a href="#">MISC</a>
totemo -- totemomail	Log viewer in totemomail 6 0 0 build 570 allows access to session Ds of high privileged users by leveraging access to a read-only auditor role.	2019-08-30	5.0	<a href="#">CVE-2018-15513</a> <a href="#">MISC</a>
tribulant -- one_click_ssl	The one-click-ssl plugin before 1.4.7 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15828</a> <a href="#">MISC</a> <a href="#">MISC</a>
uclouvain -- openjpeg	OpenJPEG before 2.3.1 has a heap buffer overflow in color_apply_icc_profile in bin/common/color.c.	2019-09-05	6.8	<a href="#">CVE-2018-21010</a> <a href="#">MISC</a>
webcraftic -- simple_301_redirects	The simple-301-redirects-addon-bulk-uploader plugin through 1.2.4 for WordPress has no requirement for authentication for action=bulk301export or action=bulk301clearlist.	2019-08-30	5.8	<a href="#">CVE-2019-15818</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
webcraftic -- woody_ad_snippets	admin/includes/class.import.snippet.php in the "Woody ad snippets" plugin before 2.2.5 for WordPress allows unauthenticated options import, as demonstrated by storing an XSS payload for remote code execution.	2019-09-03	4.3	<a href="#">CVE-2019-15858</a> <a href="#">MISC</a> <a href="#">MISC</a>
webp_converter_for_media_project -- webp_converter_for_media	The webp-converter-for-media plugin before 1 0 3 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15834</a> <a href="#">MISC</a> <a href="#">MISC</a>
wp-buy -- visitor_traffic_real_time_statistics	The visitors-traffic-real-time-statistics plugin before 1.12 for WordPress has CSRF in the settings page.	2019-08-30	6.8	<a href="#">CVE-2019-15831</a> <a href="#">MISC</a> <a href="#">MISC</a>
wp-buy -- visitor_traffic_real_time_statistics	The visitors-traffic-real-time-statistics plugin before 1.13 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15832</a> <a href="#">MISC</a> <a href="#">MISC</a>
wp_better_permaLinks_project -- wp_better_permaLinks	The wp-better-permaLinks plugin before 3.0.5 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15835</a> <a href="#">MISC</a> <a href="#">MISC</a>
wpaffiliatemanager -- affiliates_manager	The affiliates-manager plugin before 2 6 6 for WordPress has CSRF.	2019-09-03	6.8	<a href="#">CVE-2019-15868</a> <a href="#">MISC</a> <a href="#">MISC</a>
wpbrigade -- loginpress	The LoginPress plugin before 1.1.4 for WordPress has no capability check for updates to settings.	2019-09-03	4.0	<a href="#">CVE-2019-15871</a> <a href="#">MISC</a> <a href="#">MISC</a>
wpexpertdeveloper -- wp_private_content_plus	The wp-private-content-plus plugin before 2.0 for WordPress has no protection against option changes via save_settings_page and other save_functions.	2019-08-30	5.0	<a href="#">CVE-2019-15816</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
bitwise-it -- webp_express	The webp-express plugin before 0.14.8 for WordPress has stored XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15837</a> MISC MISC
bootstrapped -- wp_ultimate_recipe	The wp-ultimate-recipe plugin before 3.12.7 for WordPress has stored XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15836</a> MISC MISC
espressif -- arduino-esp32	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 processes EAP Success messages before any EAP method completion or failure, which allows attackers in radio range to cause a denial of service (crash) via a crafted message.	2019-09-04	3.3	<a href="#">CVE-2019-12586</a> MISC MISC MISC
f5 -- container_ingress_service	On version 1.9.0, if DEBUG logging is enabled, F5 Container Ingress Service (CIS) for Kubernetes and Red Hat OpenShift (k8s-bigip-ctlr) log files may contain BIG-IP secrets such as SSL Private Keys and Private key Passphrases as provided as inputs by an AS3 Declaration.	2019-09-04	1.9	<a href="#">CVE-2019-6648</a> MISC
freedesktop -- systemd	In systemd 240, bus_open_system_watch_bind_with_description in shared/bus-util.c (as used by systemd-resolved to connect to the system D-Bus instance), calls sd_bus_set_trusted, which disables access controls for incoming D-Bus messages. An unprivileged user can exploit this by executing D-Bus methods that should be restricted to privileged users, in order to change the system's DNS resolver settings.	2019-09-04	2.1	<a href="#">CVE-2019-15718</a> MISC MISC MISC FEDORA FEDORA
google -- android	In Google Assistant in Android 9, there is a possible permissions bypass that allows the Assistant to take a screenshot of apps with FLAG_SECURE. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	2.1	<a href="#">CVE-2019-2103</a> MISC
google -- android	In ComposeActivityEmailExternal of ComposeActivityEmailExternal.java in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible way to silently attach files to an email due to a confused deputy. This could lead to local information disclosure.	2019-09-05	2.1	<a href="#">CVE-2019-2124</a> MISC
google -- android	In ippSetValueTag of ipp.c in Android 8.0, 8.1 and 9, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure from the printer service with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	2.1	<a href="#">CVE-2019-2180</a> MISC
greentree-labs -- gallery_photoblocks	The photoblocks-grid-gallery plugin before 1.1.33 for WordPress has wp-admin/admin.php?page=photoblocks-edit&id= XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15829</a> MISC MISC
ibm -- business_automation_workflow	IBM Business Automation Workflow V18.0.0.0 through V18.0.0.2 and IBM Business Process Manager V8.6.0.0 through V8.6.0.0 Cumulative Fix 2018 03, V8.5.7.0 through V8.5.7.0 Cumulative Fix 2017 06, and V8.5.6.0 through V8.5.6.0 CF2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 158415.	2019-09-05	3.5	<a href="#">CVE-2019-4149</a> XF CONFIRM
icegram -- icegram	The icegram plugin before 1.10.29 for WordPress has ig_cat_list XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15830</a> MISC MISC MISC
lenovo -- xclarity_administrator	A stored cross-site scripting (XSS) vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow an administrative user to cause JavaScript code to be stored in LXCA which may then be executed in the user's web browser. The JavaScript code is not executed on LXCA itself.	2019-09-03	3.5	<a href="#">CVE-2019-6180</a> MISC
mongodb -- mongodb	Incorrect scoping of kill operations in MongoDB Server's packaged SysV init scripts allow users with write access to the PID file to insert arbitrary PIDs to be killed when the root user stops the MongoDB process via SysV init. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.11; v3.6 versions prior to 3.6.14; v3.4 versions prior to 3.4.22.	2019-08-30	3.3	<a href="#">CVE-2019-2389</a> CONFIRM
onesignal -- onesignal-free-web-push-notifications	The onesignal-free-web-push-notifications plugin before 1.17.8 for WordPress has XSS via the subdomain parameter.	2019-08-30	3.5	<a href="#">CVE-2019-15827</a> MISC MISC MISC
philips -- hdi_4000_firmware	In Philips HDI 4000 Ultrasound Systems, all versions running on old, unsupported operating systems such as Windows 2000, the HDI 4000 Ultrasound System is built on an old operating system that is no longer supported. Thus, any unmitigated vulnerability in the old operating system could be exploited to affect this product.	2019-09-04	3.6	<a href="#">CVE-2019-10988</a> MISC
redhat -- virtualization_host	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE is unique from CVE-2019-1071, CVE-2019-1073.	2019-09-03	2.1	<a href="#">CVE-2019-1125</a> REDHAT MISC
sentrifugo -- sentrifugo	Multiple stored XSS vulnerabilities in Sentrifugo 3.2 could allow authenticated users to inject arbitrary web script or HTML.	2019-09-04	3.5	<a href="#">CVE-2019-15814</a> EXPLOIT-DB
smanos -- w100_firmware	Smanos W100 1.0.0 devices have Insecure Permissions, exploitable by an attacker on the same Wi-Fi network.	2019-09-05	3.3	<a href="#">CVE-2019-13361</a> MISC
symantec -- vip	Symantec My VIP portal, previous version which has already been auto updated, was susceptible to a cross-site scripting (XSS) exploit, which is a type of issue that can enable attackers to inject client-side scripts into web pages viewed by other users or potentially bypass access controls such as the same-origin policy.	2019-08-30	3.5	<a href="#">CVE-2019-12754</a> CONFIRM
tiktok -- tiktok	The TikTok (formerly Musical.ly) application 12.2.0 for Android and iOS performs unencrypted transmission of images, videos, and likes. This allows an attacker to extract private sensitive information by sniffing network traffic.	2019-09-04	3.3	<a href="#">CVE-2019-14319</a> MISC MISC
xilinx -- zynq_ultrascale+_mpsoc_firmware	A weakness was found in Encrypt Only boot mode in Zynq UltraScale+ devices. This could lead to an adversary being able to modify the control fields of the boot image leading to an incorrect secure boot behavior.	2019-09-03	2.1	<a href="#">CVE-2019-5478</a> MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alfresco -- alfresco_community_edition	An issue was discovered in Alfresco Community Edition versions below 5.2.6, 6.0.N and 6.1.N. The Alfresco Share application is vulnerable to an Open Redirect attack via a crafted POST request. By manipulating the POST parameters, an attacker can redirect a victim to a malicious website over any protocol the attacker desires (e.g., http, https, ftp, smb, etc.).	2019-09-06	not yet calculated	<a href="#">CVE-2019-14223</a> <a href="#">MISC</a>
artifex -- ghostscript	A flaw was found in, ghostscript versions prior to 9.28, in the .pdfexectoken and other procedures where it did not properly secure its privileged calls, enabling scripts to bypass -dSAFER restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	2019-09-03	not yet calculated	<a href="#">CVE-2019-14817</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
becton_dickinson_and_company -- pyxis_es_and_pyxis_enterprise_server_with_windows_server	In Pyxis ES Versions 1.3.4 through to 1.6.1 and Pyxis Enterprise Server, with Windows Server Versions 4.4 through 4.12, a vulnerability has been identified where existing access privileges are not restricted in coordination with the expiration of access based on active directory user account changes when the device is joined to an AD domain.	2019-09-06	not yet calculated	<a href="#">CVE-2019-13517</a> <a href="#">MISC</a>
challenge_healthcare -- change_healthcare_cardiology_and_horizon_cardiology_and_mckesson_cardiology	A vulnerability was found in McKesson Cardiology product 13.x and 14.x. Insecure file permissions in the default installation may allow an attacker with local system access to execute unauthorized arbitrary code.	2019-09-06	not yet calculated	<a href="#">CVE-2018-18630</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-806_devices	D-Link D R-806 devices allow remote attackers to execute arbitrary shell commands via a trailing substring of an HTTP header that has "SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/" at the beginning.	2019-09-06	not yet calculated	<a href="#">CVE-2019-10891</a> <a href="#">MISC</a>
d-link -- dir-806_devices	hnapi_main in /htdocs/cgi-bin on D-link D R-806 v1.0 devices has a stack-based buffer overflow via a long HTTP header that has "SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/" at the beginning.	2019-09-06	not yet calculated	<a href="#">CVE-2019-10892</a> <a href="#">MISC</a>
dasan_zhone_solutions -- znid_gpon_2426a_eu_devices	Multiple Cross-Site Scripting (XSS) issues in the web interface on DASAN Zhone ZNID GPON 2426A EU version S3.1.285 devices allow a remote attacker to execute arbitrary JavaScript via manipulation of an unsanitized GET parameter: /zhndnsdisplay cmd (name), /wlsecrefresh.wl (wlWscCfgMethod, wl_wsc_reg).	2019-09-05	not yet calculated	<a href="#">CVE-2019-10677</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
datalogic -- av7000_linear_barcode_scanner	Datalogic AV7000 Linear barcode scanner all versions prior to 4.6.0.0 is vulnerable to authentication bypass, which may allow an attacker to remotely execute arbitrary code.	2019-08-30	not yet calculated	<a href="#">CVE-2019-13526</a> <a href="#">MISC</a>
eclipse -- spotless_eclipse-wtp_and_eclipse-cdt_and_eclipse_groovy	In all versions prior to version 3.9.6 for eclipse-wtp, all versions prior to version 9.4.4 for eclipse-cdt, and all versions prior to version 3.0.1 for eclipse-groovy, Spotless was resolving dependencies over an insecure channel (http). If the build occurred over an insecure connection, a malicious user could have performed a Man-in-the-Middle attack during the build and alter the build artifacts that were produced. In case that any of these artifacts were compromised, any developers using these could be altered. **Note:** In order to validate that this artifact was not compromised, the maintainer would need to confirm that none of the artifacts published to the registry were not altered with. Until this happens, we can not guarantee that this artifact was not compromised even though the probability that this happened is low.	2019-09-05	not yet calculated	<a href="#">CVE-2019-10753</a> <a href="#">MISC</a>
espressif -- esp8266_nonos_sdk	The client 802.11 mac implementation in Espressif ESP8266_NONOS_SDK 2.2.0 through 3.1.0 does not validate correctly the RSN AuthKey suite list count in beacon frames, probe responses, and association responses, which allows attackers in radio range to cause a denial of service (crash) via a crafted message.	2019-09-04	not yet calculated	<a href="#">CVE-2019-12588</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file.	2019-09-04	not yet calculated	<a href="#">CVE-2019-6643</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken.	2019-09-04	not yet calculated	<a href="#">CVE-2019-6645</a> <a href="#">MISC</a>
	Similar to the issue identified in CVE-2018-12120, on			

f5 -- big-ip	versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible.	2019-09-04	not yet calculated	<a href="#">CVE-2019-6644</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system.	2019-09-04	not yet calculated	<a href="#">CVE-2019-6647</a> <a href="#">MISC</a>
facebook -- hhvm	Insufficient boundary checks when processing M_SOFx markers from JPEG headers in the GD extension could allow access to out-of-bounds memory via a maliciously constructed invalid JPEG input. This issue affects HHVM versions prior to 3.30.9, all versions between 4.0.0 and 4.8.3, all versions between 4.9.0 and 4.15.2, and versions 4.16.0 to 4.16.3, 4.17.0 to 4.17.2, 4.18.0 to 4.18.1, 4.19.0, 4.20.0 to 4.20.1.	2019-09-06	not yet calculated	<a href="#">CVE-2019-11926</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
facebook -- hhvm	Insufficient boundary checks when processing the JPEG APP12 block marker in the GD extension could allow access to out-of-bounds memory via a maliciously constructed invalid JPEG input. This issue affects HHVM versions prior to 3.30.9, all versions between 4.0.0 and 4.8.3, all versions between 4.9.0 and 4.15.2, and versions 4.16.0 to 4.16.3, 4.17.0 to 4.17.2, 4.18.0 to 4.18.1, 4.19.0, 4.20.0 to 4.20.1.	2019-09-06	not yet calculated	<a href="#">CVE-2019-11925</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
google -- android	In the Android kernel in i2c driver there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9454</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the touchscreen driver there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9451</a> <a href="#">MISC</a>
google -- android	In the Android kernel in sync debug fs driver there is a kernel pointer leak due to the usage of printf with %p. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9444</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the FingerTipS touchscreen driver there is a possible out of bounds write due to a missing bounds check. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9448</a> <a href="#">MISC</a>
google -- android	In the Android kernel in FingerTipS touchscreen driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9449</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the kernel MMU code there is a possible execution path leaving some kernel text and rodata pages writable. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-2182</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the FingerTipS touchscreen driver there is a possible use-after-free due to improper locking. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9447</a> <a href="#">MISC</a>
google -- android	In the Android kernel in F2FS driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9445</a> <a href="#">MISC</a>
google -- android	In the Android kernel in Pixel C USB monitor driver there is a possible OOB write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9456</a> <a href="#">MISC</a>
google -- android	In the Android kernel in F2FS touch driver there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9453</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the FingerTipS touchscreen driver there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9450</a> <a href="#">MISC</a>

google -- android	In the Android kernel in the FingerTipS touchscreen driver there is a possible out of bounds write due to improper input validation. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9446</a> <a href="#">MISC</a>
google -- android	In the Android kernel in SEC_TS touch driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9452</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the video driver there is a kernel pointer leak due to a WARN_ON statement. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9455</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the v53L0 driver there is a possible out of bounds write due to a permissions bypass. This could lead to local escalation of privilege due to a set_fs() call without restoring the previous limit with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9443</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is a possible out of bounds write due to improper input validation. This could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9441</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the video driver there is a use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9458</a> <a href="#">MISC</a>
google -- android	In the Android kernel in ELF file loading there is possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9457</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9274</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the bootloader there is a possible secure boot bypass. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9436</a> <a href="#">MISC</a>
google -- android	In the Android kernel in unifi and r8180 WiFi drivers there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9270</a> <a href="#">MISC</a>
google -- android	In the Android kernel in sdcardsfs there is a possible violation of the separation of data between profiles due to shared mapping of obb files. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9345</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the synaptics_dsx_htc touchscreen driver there is a possible out of bounds write due to a use after free. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9276</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is a use after free due to improper locking. This could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9275</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the synaptics_dsx_htc touchscreen driver there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9273</a> <a href="#">MISC</a>
google -- android	In the Android kernel in Bluetooth there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9426</a> <a href="#">MISC</a>
google -- android	In the Android kernel in VPN routing there is a possible information disclosure. This could lead to remote information disclosure by an adjacent network attacker with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9461</a> <a href="#">MISC</a>
	In the Android kernel in the FingerTipS touchscreen			



google -- android	driver there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9248</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the f2fs driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9245</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is a race condition due to insufficient locking. This could lead to a use-after-free which could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9271</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System privileges required. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9442</a> <a href="#">MISC</a>
if.svnadmin -- if.svnadmin	if.SVNAdmin through 1.6.2 allows svnadmin/usercreate.php CSRF to create a user.	2019-09-06	not yet calculated	<a href="#">CVE-2019-15128</a> <a href="#">MISC</a>
intramaps -- mapcontrol	A SQL injection vulnerability in IntraMaps MapControl 8 allows attackers to execute arbitrary SQL commands via the /ApplicationEngine/Search/Refine/Set page.	2019-09-05	not yet calculated	<a href="#">CVE-2019-13191</a> <a href="#">MISC</a>
larvit -- larvitbase_api	An unintended require vulnerability in <v0.5.5 larvitbase-api may allow an attacker to load arbitrary non-production code (JavaScript file).	2019-09-03	not yet calculated	<a href="#">CVE-2019-5479</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/nbd.c does not check the nla_nest_start_noflag return value.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16089</a> <a href="#">MISC</a>
mautic -- mautic	An issue was discovered in Mautic 2.13.1. There is Stored XSS via the authorUrl field in config.json.	2019-09-06	not yet calculated	<a href="#">CVE-2018-11198</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
opensc -- pam_p11	An issue was discovered in the pam_p11 component 0.2.0 and 0.3.0 for OpenSC. If a smart card creates a signature with a length longer than 256 bytes, this triggers a buffer overflow. This may be the case for RSA keys with 4096 bits depending on the signature scheme.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16058</a> <a href="#">MISC</a>
php -- php	A type confusion vulnerability in the merge_param() function of php_http_params.c in PHP's pecl-http extension 3.1.0beta2 (PHP 7) and earlier as well as 2.6.0beta2 (PHP 5) and earlier allows attackers to crash PHP and possibly execute arbitrary code via crafted HTTP requests.	2019-09-06	not yet calculated	<a href="#">CVE-2016-7398</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
python -- python	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16056</a> <a href="#">MISC</a> <a href="#">MISC</a>
qemu -- qemu	libslirp 4.0.0, as used in QEMU 4.1.0, has a use-after-free in ip_reass in ip_input.c.	2019-09-06	not yet calculated	<a href="#">CVE-2019-15890</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an invalid read in readOHDRHeaderMessageDataLayout in hdf/dataobject.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16094</a> <a href="#">MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an invalid read in getDimension in hrtf/reader.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16095</a> <a href="#">MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an out-of-bounds read in directblockRead in hdf/fractalhead.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16091</a> <a href="#">MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has a NULL pointer dereference in getHrtf in hrtf/reader.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16092</a> <a href="#">MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an invalid write in readOHDRHeaderMessageDataLayout in hdf/dataobject.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16093</a> <a href="#">MISC</a>

tyto_software -- sahi_pro	An issue was discovered in Tyto Sahi Pro 6 x through 8.0.0. TestRunner_Non_distributed (and distributed end points) does not have any authentication mechanism. This allow an attacker to execute an arbitrary script on the remote Sahi Pro server. There is also a password-protected web interface intended for remote access to scripts. This web interface lacks server-side validation, which allows an attacker to create/modify/delete a script remotely without any password. Chaining both of these issues results in remote code execution on the Sahi Pro server.	2019-09-06	not yet calculated	<a href="#">CVE-2019-15102</a> <a href="#">MISC</a>
valve -- counter-strike_global_offensive	In Counter-Strike: Global Offensive before 8/29/2019, community game servers can display unsafe HTML in a disconnection message.	2019-09-05	not yet calculated	<a href="#">CVE-2019-15944</a> <a href="#">MISC</a>
wordpress -- wordpress	The easy-pdf-restaurant-menu-upload plugin before 1.1 2 for WordPress has XSS.	2019-08-30	not yet calculated	<a href="#">CVE-2019-15842</a> <a href="#">MISC</a>
wordpress -- wordpress	The breadcrumbs-by-menu plugin before 1.0.3 for WordPress has CSRF.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15865</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The crelly-slider plugin before 1 3 5 for WordPress has arbitrary file upload via a PHP file inside a ZIP archive to wp_ajax_crellyslider_importSlider.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15866</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The slick-popup plugin before 1.7 2 for WordPress has a hardcoded OmakPass13# password for the slickpopupteam account, after a Subscriber calls a certain AJAX action.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15867</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The JobCareer theme before 2.5.1 for WordPress has stored XSS.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15869</a> <a href="#">MISC</a>
wordpress -- wordpress	The CarSpot theme before 2.1.7 for WordPress has stored XSS via the Phone Number field.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15870</a> <a href="#">MISC</a>
wordpress -- wordpress	The download-manager plugin before 2 9.94 for WordPress has XSS via the category shortcode feature, as demonstrated by the orderby or search[publish_date] parameter.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15889</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The breadcrumbs-by-menu plugin before 1.0.3 for WordPress has XSS.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15864</a> <a href="#">MISC</a> <a href="#">MISC</a>
xpdf -- xpdf	Xpdf 3 04 has a SIGSEGV in XRef::fetch in XRef.cc after many recursive calls to Catalog: countPageTree in Catalog cc.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16088</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:  
[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:  


SUBSCRIBER SERVICES:  
[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)



From: [US-CERT](mailto:US-CERT)  
To: [vsulante@ci.sunnvale.ca.us](mailto:vsulante@ci.sunnvale.ca.us)  
Subject: Vulnerability Summary for the Week of September 2, 2019  
Date: Monday, September 09, 2019 9:29:37 AM



National Cyber Awareness System:

## [Vulnerability Summary for the Week of September 2, 2019](#)

09/09/2019 06:49 AM EDT

Original release date: September 9, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alfresco -- alfresco	An issue was discovered in Alfresco Community Edition versions 6.0 and lower. An unauthenticated, remote attacker could authenticate to Alfresco's Solr Web Admin Interface. The vulnerability is due to the presence of a default private key that is present in all default installations. An attacker could exploit this vulnerability by using the extracted private key and bundling it into a PKCS12. A successful exploit could allow the attacker to gain information about the target system (e.g., OS type, system file locations, Java version, Solr version, etc.) as well as the ability to launch further attacks by leveraging the access to Alfresco's Solr Web Admin Interface.	2019-09-05	7.5	<a href="#">CVE-2019-14222</a> MISC
alfresco -- alfresco	An issue was discovered in Alfresco Community Edition 5.2.201707. By leveraging multiple components in the Alfresco Software applications, an exploit chain was observed that allows an attacker to achieve remote code execution on the victim machine. The attacker must upload malicious Solr configuration files and then receive a JMX connection from the victim, and serve a Java object that results in deserialization and code execution.	2019-09-05	9.0	<a href="#">CVE-2019-14224</a> MISC
artifex -- ghostscript	A flaw was found in ghostscript, versions 9.x before 9.28, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass -dSAFER restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	2019-09-06	7.5	<a href="#">CVE-2019-14813</a> CONFIRM CONFIRM
asus -- precision_touchpad	AsusPTPFilter.sys on Asus Precision TouchPad 11.0.0.25 hardware has a Pool Overflow associated with the \\.\\AsusTP device, leading to a DoS or potentially privilege escalation via a crafted DeviceIoControl call.	2019-09-04	7.5	<a href="#">CVE-2019-10709</a> MISC MISC
broadcom -- ca_client_automation	An access vulnerability in CA Common Services DIA of CA Technologies Client Automation 14 and Workload Automation AE 11.3.5, 11.3.6 allows a remote attacker to execute arbitrary code.	2019-09-06	7.5	<a href="#">CVE-2019-13656</a> MISC
cisco -- jabber	A vulnerability in Cisco Jabber Client Framework (JCF) for Mac Software, installed as part of the Cisco Jabber for Mac client, could allow an authenticated, local attacker to execute arbitrary code on an affected device. The vulnerability is due to improper file level permissions on an affected device when it is running Cisco JCF for Mac Software. An attacker could exploit this vulnerability by authenticating to the affected device and executing arbitrary code or potentially modifying certain configuration files. A successful exploit could allow the attacker to execute arbitrary code or modify certain configuration files on the device using the privileges of the installed Cisco JCF for Mac Software.	2019-09-04	7.2	<a href="#">CVE-2019-12645</a> CISCO
cisco -- nx-os	A vulnerability in the Network Time Protocol (NTP) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to excessive use of system resources when the affected device is logging a drop action for received MODE_PRIVATE (Mode 7) NTP packets. An attacker could exploit this vulnerability by flooding the device with a steady stream of Mode 7 NTP packets. A successful exploit could allow the attacker to cause high CPU and memory usage on the affected device, which could cause internal system processes to restart or cause the affected device to unexpectedly reload. Note: The NTP feature is enabled by default.	2019-08-30	7.8	<a href="#">CVE-2019-1967</a> CISCO
cisco -- unified_computing_system	A vulnerability in a specific CLI command within the local management (local-mgmt) context for Cisco UCS Fabric Interconnect Software could allow an authenticated, local attacker to gain elevated privileges as the root user on an affected device. The vulnerability is due to extraneous subcommand options present for a specific CLI command within the local-mgmt context. An attacker could exploit this vulnerability by authenticating to an affected device, entering the local-mgmt context, and issuing a specific CLI command and submitting user input. A successful exploit could allow the attacker to execute arbitrary operating system commands as root on an affected device. The attacker would need to have valid user credentials for the device.	2019-08-30	7.2	<a href="#">CVE-2019-1966</a> CISCO
cisco -- webex_teams	A vulnerability in the Cisco Webex Teams client for Windows could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected system. This vulnerability is due to improper restrictions on software logging features used by the application on Windows operating systems. An attacker could exploit this vulnerability by convincing a targeted user to visit a website designed to submit malicious input to the affected application. A successful exploit could allow the attacker to cause the application to modify files and execute arbitrary	2019-09-04	9.3	<a href="#">CVE-2019-1939</a> CISCO

	commands on the system with the privileges of the targeted user.			
egain -- chat	eGain Chat 15.0.3 allows unrestricted file upload.	2019-09-04	7.5	<a href="#">CVE-2019-13976</a> MISC
eventum_project -- eventum	Controller/ListController.php in Eventum 3.5.0 is vulnerable to Deserialization of Untrusted Data. Fixed in version 3.5.2.	2019-09-05	7.5	<a href="#">CVE-2018-11569</a> MISC
exim -- exim	Exim before 4.92.2 allows remote attackers to execute arbitrary code as root via a trailing backslash.	2019-09-06	10.0	<a href="#">CVE-2019-15846</a> MISC MLIST MLIST MLIST MLIST MLIST MLIST MLIST MLIST FEDORA FEDORA BUGTRAQ GENTOO UBUNTU DEBIAN CERT-VN MISC
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350648, 12.0-RELEASE before 12.0-RELEASE-p9, 11.3-STABLE before r350650, 11.3-RELEASE before 11.3-RELEASE-p2, and 11.2-RELEASE before 11.2-RELEASE-p13, the ICMPv6 input path incorrectly handles cases where an MLDv2 listener query packet is internally fragmented across multiple mbufs. A remote attacker may be able to cause an out-of-bounds read or write that may cause the kernel to attempt to access an unmapped page and subsequently panic.	2019-08-30	7.5	<a href="#">CVE-2019-5608</a> CONFIRM
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350828, 12.0-RELEASE before 12.0-RELEASE-p10, 11.3-STABLE before r350829, 11.3-RELEASE before 11.3-RELEASE-p3, and 11.2-RELEASE before 11.2-RELEASE-p14, a missing check in the function to arrange data in a chain of mbufs could cause data returned not to be contiguous. Extra checks in the Pv6 stack could catch the error condition and trigger a kernel panic, leading to a remote denial of service.	2019-08-30	7.8	<a href="#">CVE-2019-5611</a> MISC BUGTRAQ CONFIRM
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r351264, 12.0-RELEASE before 12.0-RELEASE-p10, 11.3-STABLE before r351265, 11.3-RELEASE before 11.3-RELEASE-p3, and 11.2-RELEASE before 11.2-RELEASE-p14, the kernel driver for /dev/midstat implements a read handler that is not thread-safe. A multi-threaded program can exploit races in the handler to copy out kernel memory outside the boundaries of midstat's data buffer.	2019-08-30	7.8	<a href="#">CVE-2019-5612</a> CONFIRM
fusionpbx -- fusionpbx	FusionPBX 4.4.8 allows an attacker to execute arbitrary system commands by submitting a malicious command to the service_edit.php file (which will insert the malicious command into the database). To trigger the command, one needs to call the services.php file via a GET request with the service id followed by the parameter a=start to execute the stored command.	2019-09-05	9.0	<a href="#">CVE-2019-15029</a> MISC MISC MISC
google -- android	NVIDIA Tegra contains a vulnerability in BootRom where a user with kernel level privileges can write an arbitrary value to an arbitrary physical address	2019-09-06	7.2	<a href="#">CVE-2018-6240</a> MISC
google -- android	In ihevcd_ref_list of ihevcd_ref_list.c in Android 10, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	9.3	<a href="#">CVE-2019-2108</a> MISC
google -- android	In GateKeeper::MintAuthToken of gatekeeper.cpp in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-2115</a> MISC
google -- android	In SensorManager::assertStateLocked of SensorManager.cpp in Android 7.1.1, 7.1.2, 8.0, 8.1, and 9, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-2174</a> MISC
google -- android	In ihevcd_parse_buffering_period_sei of ihevcd_parse_headers.c in Android 8.0, 8.1 and 9, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	9.3	<a href="#">CVE-2019-2176</a> MISC
google -- android	In rw_t4t_sm_read_ndef of rw_t4t in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC service with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-2178</a> MISC
google -- android	In readArgumentList of zygoter.java in Android 10, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	7.2	<a href="#">CVE-2019-9254</a> MISC
hanwha-security -- sm-472s_firmware	An issue was discovered in NVR WebViewer on Hanwah Techwin SRN-472s 1.07_190502 devices, and other SRN-x devices before 2019-05-03. A system crash and reboot can be achieved by submitting a long username in excess of 117 characters. The username triggers a buffer overflow in the main process controlling operation of the DVR system, rendering services unavailable during the reboot operation. A repeated attack affects availability as long as the attacker has network access to the device.	2019-09-05	7.8	<a href="#">CVE-2019-12223</a> MISC MISC MISC
libreoffice -- libreoffice	LibreOffice has a feature where documents can specify that pre-installed macros can be executed on various script events such as mouse-over, document-open etc. Access is intended to be restricted to scripts under the share/Scripts/python, user/Scripts/python sub-directories of the LibreOffice install. Protection was added, to address CVE-2019-9852, to avoid a directory traversal attack where scripts in arbitrary locations on the file system could be executed by employing a URL encoding attack to defeat the path verification step. However this protection could be bypassed by taking advantage of a flaw in how LibreOffice assembled the final script URL location directly from components of the passed in path as	2019-09-06	7.5	<a href="#">CVE-2019-9854</a> CONFIRM

	opposed to solely from the sanitized output of the path verification step. This issue affects: Document Foundation LibreOffice 6.2 versions prior to 6.2.7; 6.3 versions prior to 6.3.1.			
libreoffice -- libreoffice	LibreOffice is typically bundled with LibreLogo, a programmable turtle vector graphics script, which can execute arbitrary python commands contained with the document it is launched from. LibreOffice also has a feature where documents can specify that pre-installed scripts can be executed on various document script events such as mouse-over, etc. Protection was added to block calling LibreLogo from script event handlers. However a Windows 8 3 path equivalence handling flaw left LibreOffice vulnerable under Windows that a document could trigger executing LibreLogo via a Windows filename pseudonym. This issue affects: Document Foundation LibreOffice 6.2 versions prior to 6.2.7; 6.3 versions prior to 6.3.1.	2019-09-06	7.5	<a href="#">CVE-2019-9855</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.14.11. A double free may be caused by the function allocate_trace_buffer in the file kernel/trace/trace.c.	2019-09-04	7.2	<a href="#">CVE-2017-18595</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	A backporting error was discovered in the Linux stable/longterm kernel 4.4.x through 4.4.190, 4.9.x through 4.9.190, 4.14.x through 4.14.141, 4.19.x through 4.19.69, and 5.2.x through 5.2.11. Misuse of the upstream "x86/ptrace: Fix possible spectre-v1 in ptrace_get_debugreg()" commit reintroduced the Spectre vulnerability that it aimed to eliminate. This occurred because the backport process depends on cherry picking specific commits, and because two (correctly ordered) code lines were swapped.	2019-09-04	7.5	<a href="#">CVE-2019-15902</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobjects() in net/core/net-sysfs.c, which will cause denial of service.	2019-09-04	7.8	<a href="#">CVE-2019-15916</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.5. There is a use-after-free issue when hci_uart_register_dev() fails in hci_uart_set_proto() in drivers/bluetooth/hci_ldisc.c.	2019-09-04	7.2	<a href="#">CVE-2019-15917</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.10. SMB2_negotiate in fs/cifs/smb2pdu.c has an out-of-bounds read because data structures are incompletely updated after a change from smb30 to smb21.	2019-09-04	7.2	<a href="#">CVE-2019-15918</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.10. SMB2_write in fs/cifs/smb2pdu.c has a use-after-free.	2019-09-04	7.2	<a href="#">CVE-2019-15919</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.10. SMB2_read in fs/cifs/smb2pdu.c has a use-after-free. NOTE: this was not fixed correctly in 5.0.10; see the 5.0.11 Changelog, which documents a memory leak.	2019-09-04	7.2	<a href="#">CVE-2019-15920</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.2.3. An out of bounds access exists in the function hclge_tm_sched_mode_vnet_base_cfg in the file drivers/net/ethernet/hisilicon/hns3/hns3pf/hclge_tm.c.	2019-09-04	7.2	<a href="#">CVE-2019-15925</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.2.3. Out of bounds access exists in the functions ath6kl_wmi_pstream_timeout_rx and ath6kl_wmi_cac_event_rx in the file drivers/net/wireless/ath/ath6kl/wmi.c.	2019-09-04	9.4	<a href="#">CVE-2019-15926</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.20.2. An out-of-bounds access exists in the function build_audio_procnit in the file sound/usb/mixer.c.	2019-09-04	7.2	<a href="#">CVE-2019-15927</a> <a href="#">MISC</a> <a href="#">MISC</a>
nagios -- nagios_xi	Nagios XI before 5.6.6 allows remote command execution as root. The exploit requires access to the server as the nagios user, or access as the admin user via the web interface. The getprofile.sh script, invoked by downloading a system profile (profile.php?cmd=download), is executed as root via a passwordless sudo entry; the script executes check_plugin, which is owned by the nagios user. A user logged into Nagios XI with permissions to modify plugins, or the nagios user on the server, can modify the check_plugin executable and insert malicious commands to execute as root.	2019-09-05	9.0	<a href="#">CVE-2019-15949</a> <a href="#">MISC</a>
opensc_project -- opensc	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Bitstring in decode_bit_string in libopensc/asn1.c.	2019-09-05	7.5	<a href="#">CVE-2019-15945</a> <a href="#">MISC</a> <a href="#">MISC</a>
opensc_project -- opensc	OpenSC before 0.20.0-rc1 has an out-of-bounds access of an ASN.1 Octet string in asn1_decode_entry in libopensc/asn1.c.	2019-09-05	7.5	<a href="#">CVE-2019-15946</a> <a href="#">MISC</a> <a href="#">MISC</a>
pengutronix -- barebox	Pengutronix barebox through 2019.08.1 has a remote buffer overflow in nfs_readlink_reply in net/nfs.c because a length field is directly used for a memcpy.	2019-09-05	7.5	<a href="#">CVE-2019-15937</a> <a href="#">MISC</a>
pengutronix -- barebox	Pengutronix barebox through 2019.08.1 has a remote buffer overflow in nfs_readlink_req in fs/nfs.c because a length field is directly used for a memcpy.	2019-09-05	7.5	<a href="#">CVE-2019-15938</a> <a href="#">MISC</a>
restaurant_reservations_project -- restaurant_reservations	The nd-restaurant-reservations plugin before 1.5 for WordPress has no requirement for nd_rst_import_settings_php_function authentication.	2019-08-30	7.5	<a href="#">CVE-2019-15819</a> <a href="#">MISC</a> <a href="#">MISC</a>
sonatype -- nexus_repository_manager	The Nexus Yum Repository Plugin in v2 is vulnerable to Remote Code Execution when instances using CommandLineExecutor java are supplied vulnerable data, such as the Yum Configuration Capability.	2019-09-03	9.0	<a href="#">CVE-2019-5475</a> <a href="#">MISC</a>
symfonyextensions -- rich_text_formatter	The Rich Text Formatter (Redactor) extension through v1.1.1 for Symphony CMS has an Unauthenticated arbitrary file upload vulnerability in content.fileupload.php and content.imageupload.php.	2019-09-05	7.5	<a href="#">CVE-2019-13187</a> <a href="#">MISC</a> <a href="#">MISC</a>
totaljs -- total_js_cms	An issue was discovered in Total.js CMS 12.0.0. An authenticated user with the widgets privilege can gain achieve Remote Command Execution (RCE) on the remote server by creating a malicious widget with a special tag containing JavaScript code that will be evaluated server side. In the process of evaluating the tag by the back-end, it is possible to escape the sandbox object by using the following payload: <script total>global.process.mainModule.require(child_process).exec(RCE);</script>	2019-09-05	9.0	<a href="#">CVE-2019-15954</a> <a href="#">MISC</a> <a href="#">MISC</a>
varnish-cache -- varnish	An issue was discovered in Varnish Cache before 6.0.4 LTS, and 6.1.x and 6.2.x before 6.2.1. An HTTP/1 parsing failure allows a remote attacker to trigger an assert by sending crafted HTTP/1 requests. The assert will cause an automatic restart with a clean cache, which makes it a Denial of Service attack.	2019-09-03	7.8	<a href="#">CVE-2019-15892</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
				<a href="#">CVE-2019-15872</a>



wpbrigade -- loginpress	The LoginPress plugin before 1.1.4 for WordPress has SQL injection via an import of settings.	2019-09-03	7.5	MISC MISC
wpserveur -- wps_child_theme_generator	The wps-child-theme-generator plugin before 1.2 for WordPress has classes/helpers.php directory traversal.	2019-08-30	7.5	CVE-2019-15822 MISC MISC MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has an action=confirmation protection bypass.	2019-08-30	7.5	CVE-2019-15823 MISC MISC MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has an adminhash protection bypass.	2019-08-30	7.5	CVE-2019-15824 MISC MISC MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has an action=rp&key&login protection bypass.	2019-08-30	7.5	CVE-2019-15825 MISC MISC MISC
wpserveur -- wps_hide_login	The wps-hide-login plugin before 1.5.3 for WordPress has a protection bypass via wp-login.php in the Referer field.	2019-08-30	7.5	CVE-2019-15826 MISC MISC MISC
xiaoyi -- yi_m1_mirrorless_camera_firmware	An exploitable authentication bypass vulnerability exists in the Bluetooth Low Energy (BLE) authentication module of YI M1 Mirrorless Camera V3 2-cn. An attacker can send a set of BLE commands to trigger this vulnerability, resulting in sensitive data leakage (e.g., personal photos). An attacker can also control the camera to record or take a picture after bypassing authentication.	2019-09-06	8.3	CVE-2019-13953 MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web -- photo_gallery	The photo-gallery plugin before 1.2.42 for WordPress has CSRF.	2019-08-30	6.8	CVE-2015-9380 MISC MISC MISC
abus -- secvest_wireless_alarm_system_fuaa50000_firmware	An issue was discovered on ABUS Secvest FUA50000 3.01.01 devices. Due to an insufficient implementation of jamming detection, an attacker is able to suppress correctly received RF messages sent between wireless peripheral components, e.g., wireless detectors or remote controls, and the ABUS Secvest alarm central. An attacker is able to perform a "reactive jamming" attack. The reactive jamming simply detects the start of a RF message sent by a component of the ABUS Secvest wireless alarm system, for instance a wireless motion detector (FUBW50000) or a remote control (FUBE50014 or FUBE50015), and overlays it with random data before the original RF message ends. Thereby, the receiver (alarm central) is not able to properly decode the original transmitted signal. This enables an attacker to suppress correctly received RF messages of the wireless alarm system in an unauthorized manner, for instance status messages sent by a detector indicating an intrusion.	2019-09-03	5.0	CVE-2019-14261 MISC FULLDISC BUGTRAQ MISC
airbrake -- airbrake_ruby	The Airbrake Ruby notifier 4.2.3 for Airbrake mishandles the blacklist_keys configuration option and consequently may disclose passwords to unauthorized actors. This is fixed in 4.2.4 (also, 4.2.2 and earlier are unaffected).	2019-09-06	5.0	CVE-2019-16060 MISC
apache -- commons_compress	The file name encoding algorithm used internally in Apache Commons Compress 1.15 to 1.18 can get into an infinite loop when faced with specially crafted inputs. This can lead to a denial of service attack if an attacker can choose the file names inside of an archive created by Compress.	2019-08-30	5.0	CVE-2019-12402 MISC
artifex -- ghostscript	A flaw was found in, ghostscript versions prior to 9.28, in the pdf_hook_DSC_Creator procedure where it did not properly secure its privileged calls, enabling scripts to bypass -dSAFER restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	2019-09-03	6.8	CVE-2019-14811 CONFIRM
bitcoin -- bitcoin-qt	In Bitcoin Core 0.18.0, bitcoin-qt stores wallet.dat data unencrypted in memory. Upon a crash, it may dump a core file. If a user were to mishandle a core file, an attacker can reconstruct the user's wallet.dat file, including their private keys, via a grep "6231 0500" command.	2019-09-05	5.0	CVE-2019-15947 MISC MISC
blynk -- blynk-library	An exploitable information disclosure vulnerability exists in the packet-parsing functionality of Blynk-Library v0.6.1. A specially crafted packet can cause an unauthenticated strncpy, resulting in information disclosure. An attacker can send a packet to trigger this vulnerability.	2019-09-05	5.0	CVE-2019-5065 MISC
bold-themes -- bold_page_builder	The bold-page-builder plugin before 2.3.2 for WordPress has no protection against modifying settings and importing data.	2019-08-30	5.0	CVE-2019-15821 MISC MISC MISC
canon -- print	The ContentProvider in the Canon PR NT.jp.co canon.bsd.ad.pixmaprint 2.5.5 application for Android does not properly restrict canon.i.j printer.capability.data access. This allows an attacker's malicious application to obtain sensitive information including factory passwords for the administrator web interface and WPA2-PSK key.	2019-09-05	4.3	CVE-2019-14339 MISC MISC
	A vulnerability in the authorization module of Cisco Content Security Management Appliance (SMA) Software could allow an authenticated, remote attacker to gain out-of-scope access to email. The vulnerability			CVE-2019-

cisco -- content_security_management_appliance	exists because the affected software does not correctly implement role permission controls. An attacker could exploit this vulnerability by using a custom role with specific permissions. A successful exploit could allow the attacker to access the spam quarantine of other users.	2019-09-04	4.0	<a href="#">12635 CISC0</a>
cisco -- finesse	A vulnerability in Cisco Finesse could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on an affected system. The vulnerability exists because the affected system does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to a user of the web application. A successful exploit could allow the attacker to access the system and perform unauthorized actions.	2019-09-04	5.0	<a href="#">CVE-2019-12632 CISC0</a>
cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability exists because the web-based management interface of the affected device does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-09-04	4.3	<a href="#">CVE-2019-12644 CISC0</a>
cisco -- network_level_service	A vulnerability in the &ldquo;plug-and-play&rdquo; services component of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to access sensitive information on an affected device. The vulnerability is due to improper access restrictions on the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to access running configuration information about devices managed by the IND, including administrative credentials.	2019-09-04	5.0	<a href="#">CVE-2019-1976 CISC0</a>
cisco -- nx-os	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an NX-API system process to unexpectedly restart. The vulnerability is due to incorrect validation of the HTTP header of a request that is sent to the NX-API. An attacker could exploit this vulnerability by sending a crafted HTTP request to the NX-API on an affected device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition in the NX-API service; however, the NX-OS device itself would still be available and passing network traffic. Note: The NX-API feature is disabled by default.	2019-08-30	5.0	<a href="#">CVE-2019-1968 CISC0</a>
cisco -- nx-os	A vulnerability in the implementation of the Simple Network Management Protocol (SNMP) Access Control List (ACL) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to perform SNMP polling of an affected device, even if it is configured to deny SNMP traffic. The vulnerability is due to an incorrect length check when the configured ACL name is the maximum length, which is 32 ASCII characters. An attacker could exploit this vulnerability by performing SNMP polling of an affected device. A successful exploit could allow the attacker to perform SNMP polling that should have been denied. The attacker has no control of the configuration of the SNMP ACL name.	2019-08-30	5.0	<a href="#">CVE-2019-1969 CISC0</a>
cisco -- nx-os	A vulnerability within the Endpoint Learning feature of Cisco Nexus 9000 Series Switches running in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an endpoint device in certain circumstances. The vulnerability is due to improper endpoint learning when packets are received on a specific port from outside the ACI fabric and destined to an endpoint located on a border leaf when Disable Remote Endpoint Learning has been enabled. This can result in a Remote (XR) entry being created for the impacted endpoint that will become stale if the endpoint migrates to a different port or leaf switch. This results in traffic not reaching the impacted endpoint until the Remote entry can be relearned by another mechanism.	2019-08-30	4.3	<a href="#">CVE-2019-1977 CISC0</a>
cisco -- unified_contact_center_express	A vulnerability in Cisco Unified Contact Center Express (Unified CCX) could allow an unauthenticated, remote attacker to bypass access controls and conduct a server-side request forgery (SSRF) attack on a targeted system. The vulnerability is due to improper validation of user-supplied input on the affected system. An attacker could exploit this vulnerability by sending the user of the web application a crafted request. If the request is processed, the attacker could access the system and perform unauthorized actions.	2019-09-04	5.0	<a href="#">CVE-2019-12633 CISC0</a>
convertplug -- convertplus	The ConvertPlus plugin before 3.4.5 for WordPress has an unintended account creation (with the none role) via a request for variants.	2019-09-03	5.0	<a href="#">CVE-2019-15863 MISC</a>
custom_404_pro_project -- custom_404_pro	The custom-404-pro plugin before 3.2.8 for WordPress has reflected XSS, a different vulnerability than CVE-2019-14789.	2019-08-30	4.3	<a href="#">CVE-2019-15838 MISC</a>
dell -- emc_enterprise_copy_data_management	Dell EMC Enterprise Copy Data Management (eCDM) versions 1.0, 1.1, 2.0, 2.1, and 3.0 contain a certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim's data in transit.	2019-09-03	5.8	<a href="#">CVE-2019-3751 MISC</a>
dell -- emc_unity_operating_environment	Dell EMC Unity Operating Environment versions prior to 5.0.0.0.5.116, Dell EMC UnityVSA versions prior to 5.0.0.0.5.116 and Dell EMC VNXe3200 versions prior to 3.1.10.9946299 contain a reflected cross-site scripting vulnerability on the cas/logout page. A remote unauthenticated attacker could potentially exploit this vulnerability by tricking a victim application user to supply malicious HTML or Java Script code to Unisphere, which is then reflected back to the victim and executed by the web browser.	2019-09-03	4.3	<a href="#">CVE-2019-3754 CONFIRM</a>
egain -- chat	eGain Chat 15.0.3 allows HTML Injection.	2019-09-04	4.3	<a href="#">CVE-2019-13975 MISC</a>
eng -- knowage	In Knowage through 6.1.1, an unauthenticated user can bypass access controls and access the entire application.	2019-09-05	5.0	<a href="#">CVE-2019-13188 MISC</a>

eng -- knowage	In Knowage through 6.1.1, the sign up page does not invalidate a valid CAPTCHA token. This allows for CAPTCHA bypass in the signup page.	2019-09-05	5.0	<a href="#">CVE-2019-13190</a> MISC
epignoshq -- efront_lms	A code execution vulnerability exists in Epignosis eFront LMS v5.2.12. A specially crafted web request can cause unsafe deserialization potentially resulting in PHP code being executed. An attacker can send a crafted web parameter to trigger this vulnerability.	2019-09-05	6.5	<a href="#">CVE-2019-5069</a> MISC
epignoshq -- efront_lms	An exploitable SQL injection vulnerability exists in the unauthenticated portion of eFront LMS, versions v5.2.12 and earlier. Specially crafted web request to login page can cause SQL injections, resulting in data compromise. An attacker can use a browser to trigger these vulnerabilities, and no special tools are required.	2019-09-05	6.4	<a href="#">CVE-2019-5070</a> MISC
espressif -- esp-idf	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 allows the installation of a zero Pairwise Master Key (PMK) after the completion of any EAP authentication method, which allows attackers in radio range to replay, decrypt, or spoof frames via a rogue access point.	2019-09-04	4.8	<a href="#">CVE-2019-12587</a> MISC MISC MISC
estrongs -- es_file_explorer_file_manager	The master-password feature in the ES File Explorer File Manager application 4.2.0.1.3 for Android can be bypassed via a com.estrongs.android.pop.ftp.ESFTPShortcut intent, leading to remote FTP access to the entirety of local storage.	2019-09-05	5.0	<a href="#">CVE-2019-11380</a> MISC
estsoft -- alsee	A memory corruption vulnerability exists in the PSD parsing functionality of ALSee v5.3 ~ v8.39. A specially crafted PSD file can cause an out of bounds write vulnerability resulting in code execution. By persuading a victim to open a specially-crafted PSD file, an attacker could execute arbitrary code.	2019-08-30	6.8	<a href="#">CVE-2019-12810</a> CONFIRM
ezautomation -- ez_plc_editor	An attacker could use a specially crafted project file to corrupt the memory and execute code under the privileges of the EZ PLC Editor Versions 1.8.41 and prior.	2019-09-04	6.8	<a href="#">CVE-2019-13522</a> MISC
ezautomation -- ez_touch_editor	An attacker could use a specially crafted project file to overflow the buffer and execute code under the privileges of the EZ Touch Editor Versions 2.1.0 and prior.	2019-09-04	6.8	<a href="#">CVE-2019-13518</a> MISC
f5 -- big-ip_access_policy_manager	On BIG-IP 11.5.2-11.6.4 and Enterprise Manager 3.1.1, REST users with guest privileges may be able to escalate their privileges and run commands with admin privileges.	2019-09-04	6.5	<a href="#">CVE-2019-6646</a> MISC
facebook -- facebook_for_woocommerce	The facebook-for-woocommerce plugin before 1.9.14 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15840</a> MISC
facebook -- facebook_for_woocommerce	The facebook-for-woocommerce plugin before 1.9.15 for WordPress has CSRF via ajax_woo_infobanner_post_click, ajax_woo_infobanner_post_xout, or ajax_fb_toggle_visibility.	2019-08-30	6.8	<a href="#">CVE-2019-15841</a> MISC
ffmpeg -- ffmpeg	FFmpeg through 4.2 has a "Conditional jump or move depends on uninitialised value" issue in h2645_parse because alloc_rbsp_buffer in libavcodec/h2645_parse.c mishandles rbsp_buffer.	2019-09-05	6.8	<a href="#">CVE-2019-15942</a> MISC
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350619, 12.0-RELEASE before 12.0-RELEASE-p9, 11.3-STABLE before r350619, 11.3-RELEASE before 11.3-RELEASE-p2, and 11.2-RELEASE before 11.2-RELEASE-p13, the bhyve e1000 device emulation used a guest-provided value to determine the size of the on-stack buffer without validation when TCP segmentation offload is requested for a transmitted packet. A misbehaving bhyve guest could overwrite memory in the bhyve process on the host.	2019-08-30	6.4	<a href="#">CVE-2019-5609</a> CONFIRM
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r350637, 12.0-RELEASE before 12.0-RELEASE-p9, 11.3-STABLE before r350638, 11.3-RELEASE before 11.3-RELEASE-p2, and 11.2-RELEASE before 11.2-RELEASE-p13, the bsnmp library is not properly validating the submitted length from a type-length-value encoding. A remote user could cause an out-of-bounds read or trigger a crash of the software such as bsnmpd resulting in a denial of service.	2019-08-30	5.0	<a href="#">CVE-2019-5610</a> MISC BUGTRAQ CONFIRM
freedesktop -- poppler	Poppler before 0.76.0 has an integer overflow in Parser: makeStream in Parser.cc.	2019-09-05	6.8	<a href="#">CVE-2018-21009</a> MISC
freetype -- freetype	FreeType before 2.6.1 has a heap-based buffer over-read in T1_Get_Private_Dict in type1/t1parse.c.	2019-09-03	6.8	<a href="#">CVE-2015-9381</a> MISC MLIST MISC
freetype -- freetype	FreeType before 2.6.1 has a buffer over-read in skip_comment in psaux/psobjs.c because ps_parser_skip_PS_token is mishandled in an FT_New_Memory_Face operation.	2019-09-03	4.3	<a href="#">CVE-2015-9382</a> MISC MLIST MISC
freetype -- freetype	FreeType before 2.6.2 has a heap-based buffer over-read in tt_cmap14_validate in sfnt/tt cmap.c.	2019-09-03	4.3	<a href="#">CVE-2015-9383</a> MISC MLIST MISC
glyphandcog -- xpdfreader	Xpdf 2.00 allows a SIGSEGV in XRef::constructXRef in XRef.cc. NOTE: 2.00 is a version from November 2002.	2019-09-03	4.3	<a href="#">CVE-2019-15860</a> MISC
gnu -- gcc	The POWER9 backend in GNU Compiler Collection (GCC) before version 10 could optimize multiple calls of the __builtin_darn intrinsic into a single call, thus reducing the entropy of the random number generator. This occurred because a volatile operation was not specified. For example, within a single execution of a program, the output of every __builtin_darn() call may be the same.	2019-09-02	5.0	<a href="#">CVE-2019-15847</a> MISC
google -- android	In execTransact of Binder.java in Android 7.1.1, 7.1.2, 8.0, 8.1, and 9, there is a possible local execution of arbitrary code in a privileged process due to a memory overwrite. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	4.6	<a href="#">CVE-2019-2123</a> MISC
google -- android	In checkAccess of SliceManagerService.java in Android 9, there is a possible permissions check bypass due to incorrect order of arguments.	2019-09-05	4.4	<a href="#">CVE-2019-2175</a>

	This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.			<a href="#">MISC</a>
google -- android	In isPreferred of HidProfile java in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible device type confusion due to a permissions bypass. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	<a href="#">6.8</a>	<a href="#">CVE-2019-2177</a> <a href="#">MISC</a>
google -- android	In NDEF_MsgValidate of ndef_utils in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	<a href="#">4.3</a>	<a href="#">CVE-2019-2179</a> <a href="#">MISC</a>
google -- android	In binder_transaction of binder.c in the Android kernel, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2019-09-05	<a href="#">6.9</a>	<a href="#">CVE-2019-2181</a> <a href="#">MISC</a>
grafana -- grafana	In Grafana 2.x through 6.x before 6.3.4, parts of the HTTP API allow unauthenticated use. This makes it possible to run a denial of service attack against the server running Grafana.	2019-09-03	<a href="#">5.0</a>	<a href="#">CVE-2019-15043</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">FEDORA</a>
ibm -- intelligent_operations_center	BM Intelligent Operations Center V5.1.0 - V5.2.0, IBM Intelligent Operations Center for Emergency Management V5.1.0 - V5.1.0.6, and IBM Water Operations for Watermatics V5.1.0 - V5.2.1.1 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 161201.	2019-09-05	<a href="#">5.0</a>	<a href="#">CVE-2019-4321</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- jazz_for_service_management	BM Jazz for Service Management 1.1.3 is vulnerable to HTTP header injection, caused by incorrect trust in the HTTP Host header during caching. By sending a specially crafted HTTP GET request, a remote attacker could exploit this vulnerability to inject arbitrary HTTP headers, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-force ID: 158976.	2019-09-05	<a href="#">4.3</a>	<a href="#">CVE-2019-4186</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
instagram-php-api_project -- instagram-php-api	cosenary Instagram-PHP-API (aka Instagram PHP API V2), as used in the UserPro plugin through 4.9.32 for WordPress, has XSS via the example/success.php error_description parameter.	2019-09-04	<a href="#">4.3</a>	<a href="#">CVE-2019-14470</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
jetbrains -- teamcity	JetBrains TeamCity 2019.1 and 2019.1.1 allows cross-site scripting (XSS), potentially making it possible to send an arbitrary HTTP request to a TeamCity server under the name of the currently logged-in user.	2019-09-05	<a href="#">4.3</a>	<a href="#">CVE-2019-15848</a> <a href="#">CONFIRM</a>
knowage-suite -- knowage	In Knowage through 6.1.1, an authenticated user that accesses the users page will obtain all user password hashes.	2019-09-05	<a href="#">4.0</a>	<a href="#">CVE-2019-13349</a> <a href="#">MISC</a>
knowage-suite -- knowage	In Knowage through 6.1.1, an unauthenticated user can enumerated valid usernames via the ChangePwdServlet page.	2019-09-05	<a href="#">5.0</a>	<a href="#">CVE-2019-14278</a> <a href="#">MISC</a>
lenovo -- xclarity_administrator	An XML External Entity (XXE) processing vulnerability was reported in Lenovo XClarity Administrator (LXCA) prior to version 2.5.0, Lenovo XClarity Integrator (LXCI) for Microsoft System Center prior to version 7.7.0, and Lenovo XClarity Integrator (LXCI) for VMWare vCenter prior to version 6.1.0 that could allow information disclosure.	2019-09-03	<a href="#">5.0</a>	<a href="#">CVE-2019-6179</a> <a href="#">MISC</a>
lenovo -- xclarity_administrator	A reflected cross-site scripting (XSS) vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow a crafted URL, if visited, to cause JavaScript code to be executed in the user's web browser. The JavaScript code is not executed on LXCA itself.	2019-09-03	<a href="#">4.3</a>	<a href="#">CVE-2019-6181</a> <a href="#">MISC</a>
lenovo -- xclarity_administrator	A stored CSV Injection vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow an administrative user to store malformed data in LXCA Jobs and Event Log data, that could result in crafted formulas stored in an exported CSV file. The crafted formula is not executed on LXCA itself.	2019-09-03	<a href="#">4.0</a>	<a href="#">CVE-2019-6182</a> <a href="#">MISC</a>
libexpat_project -- libexpat	In libexpat before 2.2.8, crafted XML input could fool the parser into changing from DTD parsing to document parsing too early; a consecutive call to XML_GetCurrentLineNumber (or XML_GetCurrentColumnNumber) then resulted in a heap-based buffer over-read.	2019-09-04	<a href="#">5.0</a>	<a href="#">CVE-2019-15903</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.16.7. A use-after-free can be caused by the function rsi_mac80211_detach in the file drivers/net/wireless/rsi/rsi_91x_mac80211.c.	2019-09-04	<a href="#">4.9</a>	<a href="#">CVE-2018-21008</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.6. There is a memory leak issue when idr_alloc() fails in genl_register_family() in net/netlink/genetlink.c.	2019-09-04	<a href="#">4.6</a>	<a href="#">CVE-2019-15921</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a pf data structure if alloc_disk fails in drivers/block/paride/pf.c.	2019-09-04	<a href="#">4.9</a>	<a href="#">CVE-2019-15922</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.9. There is a NULL pointer dereference for a cd data structure if alloc_disk fails in drivers/block/paride/pf.c.	2019-09-04	<a href="#">4.9</a>	<a href="#">CVE-2019-15923</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.0.11. fm10k_init_module in drivers/net/ethernet/intel/fm10k/fm10k_main.c has a NULL pointer dereference because there is no -ENOMEM upon an alloc_workqueue failure.	2019-09-04	<a href="#">4.9</a>	<a href="#">CVE-2019-15924</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-</a>

login_or_logout_menu_item_project -- login_or_logout_menu_item	The login-or-logout-menu-item plugin before 1.2.0 for WordPress has no requirement for lolmi_save_settings authentication.	2019-08-30	5.8	<a href="#">15820 MISC MISC MISC</a>
memcached -- memcached	memcached 1.5.16, when UNIX sockets are used, has a stack-based buffer over-read in conn_to_str in memcached.c.	2019-08-30	5.0	<a href="#">CVE-2019-15026 CONFIRM CONFIRM MLIST</a>
mongodb -- mongodb	An unprivileged user or program on Microsoft Windows which can create OpenSSL configuration files in a fixed location may cause utility programs shipped with MongoDB server versions less than 4.0.11, 3.6.14, and 3.4.22 to run attacker defined code as the user running the utility.	2019-08-30	6.8	<a href="#">CVE-2019-2390 CONFIRM</a>
mulesoft -- api_gateway	Directory Traversal in APIKit, HTTP connector, and OAuth2 Provider components in MuleSoft Mule Runtime 3.2.0 and higher released before August 1 2019, MuleSoft Mule Runtime 4.1.0 and higher released before August 1 2019, and all versions of MuleSoft API Gateway released before August 1 2019 allow remote attackers to read files accessible to the Mule process.	2019-08-30	5.0	<a href="#">CVE-2019-15630 MISC</a>
nagios -- log_server	Nagios Log Server before 2.0.8 allows Reflected XSS via the username on the Login page.	2019-09-03	4.3	<a href="#">CVE-2019-15898 MISC MISC</a>
naver -- cloud_explorer	NDrive(1.2.2) sys in Naver Cloud Explorer has a stack-based buffer overflow, which allows attackers to cause a denial of service when reading data from IOCTL handle.	2019-09-03	5.0	<a href="#">CVE-2019-13156 CONFIRM</a>
onkyo -- tx-nr686_firmware	Directory traversal vulnerability on ONKYO TX-NR686 1030-5000-1040-0010 A/V Receiver devices allows remote attackers to read arbitrary files via a .. (dot dot) and %2f to the default URL.	2019-08-30	5.0	<a href="#">CVE-2019-6113 MISC</a>
opencv -- opencv	An issue was discovered in OpenCV 4.1.0. There is a divide-by-zero error in cv::HOGDescriptor::getDescriptorSize in modules/objdetect/src/hog.cpp.	2019-09-05	5.0	<a href="#">CVE-2019-15939 MISC MISC</a>
profilegrid -- profilegrid	The profilegrid-user-profiles-groups-and-communities plugin before 2.8.6 for WordPress has remote code execution via an wp-admin/admin-ajax.php request with the action=pn_template_preview&html=<?php substr followed by PHP code.	2019-09-03	6.5	<a href="#">CVE-2019-15873 MISC MISC</a>
rancher -- rancher	Rancher 2 through 2.2.4 is vulnerable to a Cross-Site WebSocket Hijacking attack that allows an exploiter to gain access to clusters managed by Rancher. The attack requires a victim to be logged into a Rancher server, and then to access a third-party site hosted by the exploiter. Once that is accomplished, the exploiter is able to execute commands against the cluster's Kubernetes API with the permissions and identity of the victim.	2019-09-04	4.3	<a href="#">CVE-2019-13209 MISC CONFIRM</a>
realestateconnected -- easy_property_listings	The easy-property-listings plugin before 3.4 for WordPress has XSS.	2019-08-30	4.3	<a href="#">CVE-2019-15817 MISC MISC</a>
samba -- samba	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.	2019-09-03	6.4	<a href="#">CVE-2019-10197 CONFIRM BUGTRAQ CONFIRM UBUNTU DEBIAN MISC</a>
saplica -- sentrifugo	Sentrifugo 3.2 lacks CSRF protection. This could lead to an attacker tricking the administrator into executing arbitrary code at index.php/dashboard/viewprofile via a crafted HTML page.	2019-09-06	6.8	<a href="#">CVE-2019-16059 MISC</a>
sentrifugo -- sentrifugo	Multiple file upload restriction bypass vulnerabilities in Sentrifugo 3.2 could allow authenticated users to execute arbitrary code via a webshell.	2019-09-04	6.5	<a href="#">CVE-2019-15813 EXPLOIT-DB</a>
shaosina -- sina_extension_for_elementor	The sina-extension-for-elementor plugin before 2.2.1 for WordPress has local file inclusion.	2019-08-30	5.0	<a href="#">CVE-2019-15839 MISC MISC MISC</a>
simple_mail_address_encoder_project -- simple_mail_address_encoder	The simple-mail-address-encoder plugin before 1.7 for WordPress has reflected XSS.	2019-08-30	4.3	<a href="#">CVE-2019-15833 MISC</a>
statichttpserver_project -- statichttpserver	A path traversal vulnerability in <= v0.9.7 of statichttpserver npm module allows attackers to list files in arbitrary folders.	2019-09-03	5.0	<a href="#">CVE-2019-5480 MISC</a>
symantec -- advanced_secure_gateway	The ASG/ProxySG FTP proxy WebFTP mode allows intercepting FTP connections where a user accesses an FTP server via a ftp:// URL in a web browser. A stored cross-site scripting (XSS) vulnerability in the WebFTP mode allows a remote attacker to inject malicious JavaScript code in ASG/ProxySG's web listing of a remote FTP server. Exploiting the vulnerability requires the attacker to be able to upload crafted files to the remote FTP server. Affected versions: ASG 6.6 and 6.7 prior to 6.7.4.2; ProxySG 6.5 prior to 6.5.10.15, 6.6, and 6.7 prior to 6.7.4.2.	2019-08-30	4.3	<a href="#">CVE-2018-18370 CONFIRM</a>
symantec -- advanced_secure_gateway	The ASG/ProxySG FTP proxy WebFTP mode allows intercepting FTP connections where a user accesses an FTP server via a ftp:// URL in a web browser. An information disclosure vulnerability in the WebFTP mode allows a malicious user to obtain plaintext authentication credentials for a remote FTP server from the ASG/ProxySG's web listing of the FTP server. Affected versions: ASG 6.6 and 6.7 prior to 6.7.4.2; ProxySG 6.5 prior to 6.5.10.15, 6.6, and 6.7 prior to 6.7.4.2.	2019-08-30	4.0	<a href="#">CVE-2018-18371 CONFIRM</a>
symantec -- management_center	An information disclosure vulnerability in the Management Center (MC) REST API 2.0, 2.1, and 2.2 prior to 2.2.2.1 allows a malicious authenticated user to obtain passwords for external backup and CPL policy import servers	2019-08-30	4.0	<a href="#">CVE-2019-9697 CONFIRM</a>



	that they might not otherwise be authorized to access.			
symantec -- reporter	An information disclosure vulnerability in Symantec Reporter web UI 10.3 prior to 10.3.2.5 allows a malicious authenticated administrator user to obtain passwords for external SMTP, FTP, FTPS, LDAP, and Cloud Log Download servers that they might not otherwise be authorized to access. The malicious administrator user can also obtain the passwords of other Reporter web UI users.	2019-08-30	4.0	<a href="#">CVE-2019-12753</a> CONFIRM
totaljs -- total_js_cms	An issue was discovered in Total js CMS 12.0.0. An authenticated user with the Pages privilege can conduct a path traversal attack (../) to include html files that are outside the permitted directory. Also, if a page contains a template directive, then the directive will be server side processed. Thus, if a user can control the content of a html file, then they can inject a payload with a malicious template directive to gain Remote Command Execution. The exploit will work only with the html extension.	2019-09-05	6.5	<a href="#">CVE-2019-15952</a> MISC FULLDISC MISC MISC
totaljs -- total_js_cms	An issue was discovered in Total js CMS 12.0.0. An authenticated user with limited privileges can get access to a resource that they do not own by calling the associated API. The product correctly manages privileges only for the front-end resource path, not for API requests. This leads to vertical and horizontal privilege escalation.	2019-09-05	6.5	<a href="#">CVE-2019-15953</a> MISC MISC
totaljs -- total_js_cms	An issue was discovered in Total js CMS 12.0.0. A low privilege user can perform a simple transformation of a cookie to obtain the random values inside it. If an attacker can discover a session cookie owned by an admin, then it is possible to brute force it with $O(n)=2n$ instead of $O(n)=n^x$ complexity, and steal the admin password.	2019-09-05	4.0	<a href="#">CVE-2019-15955</a> MISC MISC
totemo -- totemomail	Cross-site scripting (XSS) vulnerability in the 'Certificate' feature of totemomail 6.0.0 build 570 allows remote attackers to inject arbitrary web script or HTML.	2019-08-30	4.3	<a href="#">CVE-2018-15510</a> MISC
totemo -- totemomail	Cross-site scripting (XSS) vulnerability in the 'Notification template' feature of totemomail 6.0.0 build 570 allows remote attackers to inject arbitrary web script or HTML.	2019-08-30	4.3	<a href="#">CVE-2018-15511</a> MISC
totemo -- totemomail	Cross-site scripting (XSS) vulnerability in the 'Authorisation Service' feature of totemomail 6.0.0 build 570 allows remote attackers to inject arbitrary web script or HTML.	2019-08-30	4.3	<a href="#">CVE-2018-15512</a> MISC
totemo -- totemomail	Log viewer in totemomail 6 0 0 build 570 allows access to session Ds of high privileged users by leveraging access to a read-only auditor role.	2019-08-30	5.0	<a href="#">CVE-2018-15513</a> MISC
tribulant -- one_click_ssl	The one-click-ssl plugin before 1.4.7 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15828</a> MISC MISC
uclouvain -- openjpeg	OpenJPEG before 2.3.1 has a heap buffer overflow in color_apply_icc_profile in bin/common/color.c.	2019-09-05	6.8	<a href="#">CVE-2018-21010</a> MISC
webcraftic -- simple_301_redirects	The simple-301-redirects-addon-bulk-uploader plugin through 1.2.4 for WordPress has no requirement for authentication for action=bulk301export or action=bulk301clearlist.	2019-08-30	5.8	<a href="#">CVE-2019-15818</a> MISC MISC MISC
webcraftic -- woody_ad_snippets	admin/includes/class.import.snippet.php in the "Woody ad snippets" plugin before 2.2.5 for WordPress allows unauthenticated options import, as demonstrated by storing an XSS payload for remote code execution.	2019-09-03	4.3	<a href="#">CVE-2019-15858</a> MISC MISC
webp_converter_for_media_project -- webp_converter_for_media	The webp-converter-for-media plugin before 1 0 3 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15834</a> MISC MISC
wp-buy -- visitor_traffic_real_time_statistics	The visitors-traffic-real-time-statistics plugin before 1.12 for WordPress has CSRF in the settings page.	2019-08-30	6.8	<a href="#">CVE-2019-15831</a> MISC MISC
wp-buy -- visitor_traffic_real_time_statistics	The visitors-traffic-real-time-statistics plugin before 1.13 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15832</a> MISC MISC
wp_better_permalinks_project -- wp_better_permalinks	The wp-better-permalinks plugin before 3.0.5 for WordPress has CSRF.	2019-08-30	6.8	<a href="#">CVE-2019-15835</a> MISC MISC
wpaffiliatemanager -- affiliates_manager	The affiliates-manager plugin before 2 6 6 for WordPress has CSRF.	2019-09-03	6.8	<a href="#">CVE-2019-15868</a> MISC MISC
wpbrigade -- loginpress	The LoginPress plugin before 1.1.4 for WordPress has no capability check for updates to settings.	2019-09-03	4.0	<a href="#">CVE-2019-15871</a> MISC MISC
wpexpertdeveloper -- wp_private_content_plus	The wp-private-content-plus plugin before 2.0 for WordPress has no protection against option changes via save_settings_page and other save_ functions.	2019-08-30	5.0	<a href="#">CVE-2019-15816</a> MISC MISC MISC

[Back to top](#)

## Low Vulnerabilities

Primary	CVSS	Source & Patch
---------	------	----------------

Vendor -- Product	Description	Published	Score	Info
bitwise-it -- webp_express	The webp-express plugin before 0.14.8 for WordPress has stored XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15837</a> MISC MISC
bootstrapped -- wp_ultimate_recipe	The wp-ultimate-recipe plugin before 3.12.7 for WordPress has stored XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15836</a> MISC MISC
espressif -- arduino-esp32	The EAP peer implementation in Espressif ESP-IDF 2.0.0 through 4.0.0 and ESP8266_NONOS_SDK 2.2.0 through 3.1.0 processes EAP Success messages before any EAP method completion or failure, which allows attackers in radio range to cause a denial of service (crash) via a crafted message.	2019-09-04	3.3	<a href="#">CVE-2019-12586</a> MISC MISC MISC
f5 -- container_ingress_service	On version 1.9.0, if DEBUG logging is enable, F5 Container Ingress Service (CIS) for Kubernetes and Red Hat OpenShift (k8s-bigip-ctlr) log files may contain BIG-IP secrets such as SSL Private Keys and Private Key Passphrases as provided as inputs by an AS3 Declaration.	2019-09-04	1.9	<a href="#">CVE-2019-6648</a> MISC
freedesktop -- systemd	In systemd 240, bus_open_system_watch_bind_with_description in shared/bus-util.c (as used by systemd-resolved to connect to the system D-Bus instance), calls sd_bus_set_trusted, which disables access controls for incoming D-Bus messages. An unprivileged user can exploit this by executing D-Bus methods that should be restricted to privileged users, in order to change the system's DNS resolver settings.	2019-09-04	2.1	<a href="#">CVE-2019-15718</a> MISC MISC FEDORA FEDORA
google -- android	In Google Assistant in Android 9, there is a possible permissions bypass that allows the Assistant to take a screenshot of apps with FLAG_SECURE. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	2.1	<a href="#">CVE-2019-2103</a> MISC
google -- android	In ComposeActivityEmailExternal of ComposeActivityEmailExternal.java in Android 7.1.1, 7.1.2, 8.0, 8.1 and 9, there is a possible way to silently attach files to an email due to a confused deputy. This could lead to local information disclosure.	2019-09-05	2.1	<a href="#">CVE-2019-2124</a> MISC
google -- android	In iPPSetValueTypeTag of iPP.c in Android 8.0, 8.1 and 9, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure from the printer service with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-05	2.1	<a href="#">CVE-2019-2180</a> MISC
greentrelabs -- gallery_photoblocks	The photoblocks-grid-gallery plugin before 1.1.33 for WordPress has wp-admin/admin.php?page=photoblocks-edit&id= XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15829</a> MISC MISC
ibm -- business_automation_workflow	IBM Business Automation Workflow V18.0.0.0 through V18.0.0.2 and IBM Business Process Manager V8.6.0.0 through V8.6.0.0 Cumulative Fix 2018.03, V8.5.7.0 through V8.5.7.0 Cumulative Fix 2017.06, and V8.5.6.0 through V8.5.6.0 CF2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 158415.	2019-09-05	3.5	<a href="#">CVE-2019-4149</a> XF CONFIRM
icegram -- icegram	The icegram plugin before 1.10.29 for WordPress has ig_cat_list XSS.	2019-08-30	3.5	<a href="#">CVE-2019-15830</a> MISC MISC MISC
lenovo -- xclarity_administrator	A stored cross-site scripting (XSS) vulnerability was reported in Lenovo XClarity Administrator (LXCA) versions prior to 2.5.0 that could allow an administrative user to cause JavaScript code to be stored in LXCA which may then be executed in the user's web browser. The JavaScript code is not executed on LXCA itself.	2019-09-03	3.5	<a href="#">CVE-2019-6180</a> MISC
mongodb -- mongodb	Incorrect scoping of kill operations in MongoDB Server's packaged SysV init scripts allow users with write access to the PID file to insert arbitrary PIDs to be killed when the root user stops the MongoDB process via SysV init. This issue affects: MongoDB Inc. MongoDB Server v4.0 versions prior to 4.0.11; v3.6 versions prior to 3.6.14; v3.4 versions prior to 3.4.22.	2019-08-30	3.3	<a href="#">CVE-2019-2389</a> CONFIRM
onesignal -- onesignal-free-web-push-notifications	The onesignal-free-web-push-notifications plugin before 1.17.8 for WordPress has XSS via the subdomain parameter.	2019-08-30	3.5	<a href="#">CVE-2019-15827</a> MISC MISC MISC
philips -- hdi_4000_firmware	In Philips HDI 4000 Ultrasound Systems, all versions running on old, unsupported operating systems such as Windows 2000, the HDI 4000 Ultrasound System is built on an old operating system that is no longer supported. Thus, any unmitigated vulnerability in the old operating system could be exploited to affect this product.	2019-09-04	3.6	<a href="#">CVE-2019-10988</a> MISC
redhat -- virtualization_host	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE is unique from CVE-2019-1071, CVE-2019-1073.	2019-09-03	2.1	<a href="#">CVE-2019-1125</a> REDHAT MISC
sentrifugo -- sentrifugo	Multiple stored XSS vulnerabilities in Sentrifugo 3.2 could allow authenticated users to inject arbitrary web script or HTML.	2019-09-04	3.5	<a href="#">CVE-2019-15814</a> EXPLOIT-DB
smanos -- w100_firmware	Smanos W100 1.0.0 devices have Insecure Permissions, exploitable by an attacker on the same Wi-Fi network.	2019-09-05	3.3	<a href="#">CVE-2019-13361</a> MISC
symantec -- vip	Symantec My VIP portal, previous version which has already been auto updated, was susceptible to a cross-site scripting (XSS) exploit, which is a type of issue that can enable attackers to inject client-side scripts into web pages viewed by other users or potentially bypass access controls such as the same-origin policy.	2019-08-30	3.5	<a href="#">CVE-2019-12754</a> CONFIRM
tiktok -- tiktok	The TikTok (formerly Musical.ly) application 12.2.0 for Android and iOS performs unencrypted transmission of images, videos, and likes. This allows an attacker to extract private sensitive information by sniffing network traffic.	2019-09-04	3.3	<a href="#">CVE-2019-14319</a> MISC MISC
xilinx -- zynq_ultrascale+_mpsoc_firmware	A weakness was found in Encrypt Only boot mode in Zynq UltraScale+ devices. This could lead to an adversary being able to modify the control fields of the boot image leading to an incorrect secure boot behavior.	2019-09-03	2.1	<a href="#">CVE-2019-5478</a> MISC MISC

[Back to top](#)

Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alfresco -- alfresco_community_edition	An issue was discovered in Alfresco Community Edition versions below 5.2.6, 6.0.N and 6.1.N. The Alfresco Share application is vulnerable to an Open Redirect attack via a crafted POST request. By manipulating the POST parameters, an attacker can redirect a victim to a malicious website over any protocol the attacker desires (e.g., http, https, ftp, smb, etc.).	2019-09-06	not yet calculated	<a href="#">CVE-2019-14223</a> <a href="#">MISC</a>
artifex -- ghostscript	A flaw was found in, ghostscript versions prior to 9.28, in the .pdfexectoken and other procedures where it did not properly secure its privileged calls, enabling scripts to bypass -dSAFER restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.	2019-09-03	not yet calculated	<a href="#">CVE-2019-14817</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
becton_dickinson_and_company -- pyxis_es_and_pyxis_enterprise_server_with_windows_server	In Pyxis ES Versions 1.3.4 through to 1.6.1 and Pyxis Enterprise Server, with Windows Server Versions 4.4 through 4.12, a vulnerability has been identified where existing access privileges are not restricted in coordination with the expiration of access based on active directory user account changes when the device is joined to an AD domain.	2019-09-06	not yet calculated	<a href="#">CVE-2019-13517</a> <a href="#">MISC</a>
challenge_healthcare -- change_healthcare_cardiology_and_horizon_cardiology_and_mckesson_cardiology	A vulnerability was found in McKesson Cardiology product 13.x and 14.x. Insecure file permissions in the default installation may allow an attacker with local system access to execute unauthorized arbitrary code.	2019-09-06	not yet calculated	<a href="#">CVE-2018-18630</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dir-806_devices	D-Link D R-806 devices allow remote attackers to execute arbitrary shell commands via a trailing substring of an HTTP header that has "SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/" at the beginning.	2019-09-06	not yet calculated	<a href="#">CVE-2019-10891</a> <a href="#">MISC</a>
d-link -- dir-806_devices	hnapi_main in /htdocs/cgi-bin on D-link D R-806 v1.0 devices has a stack-based buffer overflow via a long HTTP header that has "SOAPAction: http://purenetworks.com/HNAP1/GetDeviceSettings/" at the beginning.	2019-09-06	not yet calculated	<a href="#">CVE-2019-10892</a> <a href="#">MISC</a>
dasan_zhone_solutions -- znid_gpon_2426a_eu_devices	Multiple Cross-Site Scripting (XSS) issues in the web interface on DASAN Zhone ZNID GPON 2426A EU version S3.1.285 devices allow a remote attacker to execute arbitrary JavaScript via manipulation of an unsanitized GET parameter: /zhndnsdisplay cmd (name), /wlsecfresh.wl (wlWscCfgMethod, wl_wsc_reg).	2019-09-05	not yet calculated	<a href="#">CVE-2019-10677</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
datalogic -- av7000_linear_barcode_scanner	Datalogic AV7000 Linear barcode scanner all versions prior to 4.6.0.0 is vulnerable to authentication bypass, which may allow an attacker to remotely execute arbitrary code.	2019-08-30	not yet calculated	<a href="#">CVE-2019-13526</a> <a href="#">MISC</a>
eclipse -- spotless_eclipse-wtp_and_eclipse-cdt_and_eclipse_groovy	In all versions prior to version 3.9.6 for eclipse-wtp, all versions prior to version 9.4.4 for eclipse-cdt, and all versions prior to version 3.0.1 for eclipse-groovy, Spotless was resolving dependencies over an insecure channel (http). If the build occurred over an insecure connection, a malicious user could have performed a Man-in-the-Middle attack during the build and alter the build artifacts that were produced. In case that any of these artifacts were compromised, any developers using these could be altered. **Note:** In order to validate that this artifact was not compromised, the maintainer would need to confirm that none of the artifacts published to the registry were not altered with. Until this happens, we can not guarantee that this artifact was not compromised even though the probability that this happened is low.	2019-09-05	not yet calculated	<a href="#">CVE-2019-10753</a> <a href="#">MISC</a>
espressif -- esp8266_nonos_sdk	The client 802.11 mac implementation in Espressif ESP8266_NONOS_SDK 2.2.0 through 3.1.0 does not validate correctly the RSN AuthKey suite list count in beacon frames, probe responses, and association responses, which allows attackers in radio range to cause a denial of service (crash) via a crafted message.	2019-09-04	not yet calculated	<a href="#">CVE-2019-12588</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip	On versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, 12.1.0-12.1.4.1, and 11.5.2-11.6.4, an attacker sending specifically crafted DHCPv6 requests through a BIG-IP virtual server configured with a DHCPv6 profile may be able to cause the TMM process to produce a core file.	2019-09-04	not yet calculated	<a href="#">CVE-2019-6643</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.5, 13.0.0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, FTP traffic passing through a Virtual Server with both an active FTP profile associated and connection mirroring configured may lead to a TMM crash causing the configured HA action to be taken.	2019-09-04	not yet calculated	<a href="#">CVE-2019-6645</a> <a href="#">MISC</a>
	Similar to the issue identified in CVE-2018-12120, on versions 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.2, and 12.1.0-12.1.4 BIG-IP will bind a debug			<a href="#">CVE-</a>

f5 -- big-ip	nodejs process to all interfaces when invoked. This may expose the process to unauthorized users if the plugin is left in debug mode and the port is accessible.	2019-09-04	not yet calculated	<a href="#">2019-6644 MISC</a>
f5 -- big-ip	On BIG-IP 14.1 0-14.1.0.5, 14 0 0-14.0.0.4, 13 0 0-13.1.2, 12.1.0-12.1.4.1, 11.5.2-11.6.4, when processing authentication attempts for control-plane users MCPD leaks a small amount of memory. Under rare conditions attackers with access to the management interface could eventually deplete memory on the system.	2019-09-04	not yet calculated	<a href="#">CVE-2019-6647 MISC</a>
facebook -- hhvm	Insufficient boundary checks when processing M_SOFx markers from JPEG headers in the GD extension could allow access to out-of-bounds memory via a maliciously constructed invalid JPEG input. This issue affects HHVM versions prior to 3.30.9, all versions between 4.0.0 and 4.8.3, all versions between 4.9.0 and 4.15.2, and versions 4.16.0 to 4.16.3, 4.17.0 to 4.17.2, 4.18.0 to 4.18.1, 4.19.0, 4.20.0 to 4.20.1.	2019-09-06	not yet calculated	<a href="#">CVE-2019-11926 CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
facebook -- hhvm	Insufficient boundary checks when processing the JPEG APP12 block marker in the GD extension could allow access to out-of-bounds memory via a maliciously constructed invalid JPEG input. This issue affects HHVM versions prior to 3.30.9, all versions between 4.0.0 and 4.8.3, all versions between 4.9.0 and 4.15.2, and versions 4.16.0 to 4.16.3, 4.17.0 to 4.17.2, 4.18.0 to 4.18.1, 4.19.0, 4.20.0 to 4.20.1.	2019-09-06	not yet calculated	<a href="#">CVE-2019-11925 CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
google -- android	In the Android kernel in i2c driver there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9454 MISC</a>
google -- android	In the Android kernel in the touchscreen driver there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9451 MISC</a>
google -- android	In the Android kernel in sync debug fs driver there is a kernel pointer leak due to the usage of printf with %p. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9444 MISC</a>
google -- android	In the Android kernel in the FingerTipS touchscreen driver there is a possible out of bounds write due to a missing bounds check. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9448 MISC</a>
google -- android	In the Android kernel in FingerTipS touchscreen driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9449 MISC</a>
google -- android	In the Android kernel in the kernel MMU code there is a possible execution path leaving some kernel text and rodata pages writable. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-2182 MISC</a>
google -- android	In the Android kernel in the FingerTipS touchscreen driver there is a possible use-after-free due to improper locking. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9447 MISC</a>
google -- android	In the Android kernel in F2FS driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9445 MISC</a>
google -- android	In the Android kernel in Pixel C USB monitor driver there is a possible OOB write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9456 MISC</a>
google -- android	In the Android kernel in F2FS touch driver there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9453 MISC</a>
google -- android	In the Android kernel in the FingerTipS touchscreen driver there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9450 MISC</a>
	In the Android kernel in the FingerTipS touchscreen driver there is a possible out of bounds write due to			<a href="#">CVE-</a>

google -- android	improper input validation. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9446</a> <a href="#">MISC</a>
google -- android	In the Android kernel in SEC_TS touch driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9452</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the video driver there is a kernel pointer leak due to a WARN_ON statement. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9455</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the v53L0 driver there is a possible out of bounds write due to a permissions bypass. This could lead to local escalation of privilege due to a set_fs() call without restoring the previous limit with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9443</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is a possible out of bounds write due to improper input validation. This could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9441</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the video driver there is a use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9458</a> <a href="#">MISC</a>
google -- android	In the Android kernel in ELF file loading there is possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9457</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9274</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the bootloader there is a possible secure boot bypass. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9436</a> <a href="#">MISC</a>
google -- android	In the Android kernel in unifi and r8180 WiFi drivers there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9270</a> <a href="#">MISC</a>
google -- android	In the Android kernel in sdcardfs there is a possible violation of the separation of data between profiles due to shared mapping of obb files. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9345</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the synaptics_dsx_htc touchscreen driver there is a possible out of bounds write due to a use after free. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9276</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the mnh driver there is a use after free due to improper locking. This could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9275</a> <a href="#">MISC</a>
google -- android	In the Android kernel in the synaptics_dsx_htc touchscreen driver there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9273</a> <a href="#">MISC</a>
google -- android	In the Android kernel in Bluetooth there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9426</a> <a href="#">MISC</a>
google -- android	In the Android kernel in VPN routing there is a possible information disclosure. This could lead to remote information disclosure by an adjacent network attacker with no additional execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9461</a> <a href="#">MISC</a>
	In the Android kernel in the FingerTipS touchscreen driver there is a possible out of bounds write due to a missing bounds check. This could lead to local	2019-09-	not yet	<a href="#">CVE-2019-</a>



google -- android	escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	06	calculated	<a href="#">9248 MISC</a>
google -- android	In the Android kernel in the f2fs driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9245 MISC</a>
google -- android	In the Android kernel in the mnh driver there is a race condition due to insufficient locking. This could lead to a use-after-free which could lead to escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9271 MISC</a>
google -- android	In the Android kernel in the mnh driver there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System privileges required. User interaction is not needed for exploitation.	2019-09-06	not yet calculated	<a href="#">CVE-2019-9442 MISC</a>
if.svnadmin -- if.svnadmin	if.SVNAdmin through 1.6.2 allows svnadmin/usercreate.php CSRF to create a user.	2019-09-06	not yet calculated	<a href="#">CVE-2019-15128 MISC</a>
intramaps -- mapcontrol	A SQL injection vulnerability in IntraMaps MapControl 8 allows attackers to execute arbitrary SQL commands via the /ApplicationEngine/Search/Refine/Set page.	2019-09-05	not yet calculated	<a href="#">CVE-2019-13191 MISC</a>
larvit -- larvitbase_api	An unintended require vulnerability in <v0.5.5 larvitbase-api may allow an attacker to load arbitrary non-production code (JavaScript file).	2019-09-03	not yet calculated	<a href="#">CVE-2019-5479 MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/nbd.c does not check the nla_nest_start_noflag return value.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16089 MISC</a>
mautic -- mautic	An issue was discovered in Mautic 2.13.1. There is Stored XSS via the authorUrl field in config.json.	2019-09-06	not yet calculated	<a href="#">CVE-2018-11198 MISC</a> <a href="#">CONFIRM</a>
opensc -- pam_p11	An issue was discovered in the pam_p11 component 0.2.0 and 0.3.0 for OpenSC. If a smart card creates a signature with a length longer than 256 bytes, this triggers a buffer overflow. This may be the case for RSA keys with 4096 bits depending on the signature scheme.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16058 MISC</a>
php -- php	A type confusion vulnerability in the merge_param() function of php_http_params.c in PHP's pecl-http extension 3.1.0beta2 (PHP 7) and earlier as well as 2.6.0beta2 (PHP 5) and earlier allows attackers to crash PHP and possibly execute arbitrary code via crafted HTTP requests.	2019-09-06	not yet calculated	<a href="#">CVE-2016-7398 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
python -- python	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16056 MISC</a> <a href="#">MISC</a>
qemu -- qemu	libslirp 4.0.0, as used in QEMU 4.1.0, has a use-after-free in ip_reass in ip_input.c.	2019-09-06	not yet calculated	<a href="#">CVE-2019-15890 CONFIRM</a> <a href="#">MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an invalid read in readOHDRHeaderMessageDataLayout in hdf/dataobject.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16094 MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an invalid read in getDimension in hrtf/reader.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16095 MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an out-of-bounds read in directblockRead in hdf/fractalhead.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16091 MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has a NULL pointer dereference in getHrtf in hrtf/reader.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16092 MISC</a>
symonics -- libmysofa	Symonics libmysofa 0.7 has an invalid write in readOHDRHeaderMessageDataLayout in hdf/dataobject.c.	2019-09-07	not yet calculated	<a href="#">CVE-2019-16093 MISC</a>
	An issue was discovered in Tyto Sahi Pro 6.x through 8.0.0. TestRunner_Non_distributed (and			

tyto_software -- sahi_pro	distributed end points) does not have any authentication mechanism. This allow an attacker to execute an arbitrary script on the remote Sahi Pro server. There is also a password-protected web interface intended for remote access to scripts. This web interface lacks server-side validation, which allows an attacker to create/modify/delete a script remotely without any password. Chaining both of these issues results in remote code execution on the Sahi Pro server.	2019-09-06	not yet calculated	<a href="#">CVE-2019-15102</a> <a href="#">MISC</a>
valve -- counter-strike_global_offensive	In Counter-Strike: Global Offensive before 8/29/2019, community game servers can display unsafe HTML in a disconnection message.	2019-09-05	not yet calculated	<a href="#">CVE-2019-15944</a> <a href="#">MISC</a>
wordpress -- wordpress	The easy-pdf-restaurant-menu-upload plugin before 1.1 2 for WordPress has XSS.	2019-08-30	not yet calculated	<a href="#">CVE-2019-15842</a> <a href="#">MISC</a>
wordpress -- wordpress	The breadcrumbs-by-menu plugin before 1.0.3 for WordPress has CSRF.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15865</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The crelly-slider plugin before 1 3 5 for WordPress has arbitrary file upload via a PHP file inside a ZIP archive to wp_ajax_crellyslider_importSlider.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15866</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The slick-popup plugin before 1.7 2 for WordPress has a hardcoded OmakPass13# password for the slickpopupteam account, after a Subscriber calls a certain AJAX action.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15867</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The JobCareer theme before 2.5.1 for WordPress has stored XSS.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15869</a> <a href="#">MISC</a>
wordpress -- wordpress	The CarSpot theme before 2.1.7 for WordPress has stored XSS via the Phone Number field.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15870</a> <a href="#">MISC</a>
wordpress -- wordpress	The download-manager plugin before 2 9.94 for WordPress has XSS via the category shortcode feature, as demonstrated by the orderby or search[publish_date] parameter.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15889</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The breadcrumbs-by-menu plugin before 1.0.3 for WordPress has XSS.	2019-09-03	not yet calculated	<a href="#">CVE-2019-15864</a> <a href="#">MISC</a> <a href="#">MISC</a>
xpdf -- xpdf	Xpdf 3 04 has a SIGSEGV in XRef::fetch in XRef.cc after many recursive calls to Catalog::countPageTree in Catalog.cc.	2019-09-06	not yet calculated	<a href="#">CVE-2019-16088</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)



**From:** [US-CERT](#)  
**To:** [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov)  
**Subject:** Vulnerability Summary for the Week of July 29, 2019  
**Date:** Monday, August 05, 2019 2:15:34 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## [Vulnerability Summary for the Week of July 29, 2019](#)

08/05/2019 06:36 AM EDT

Original release date: August 5, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web -- photo_gallery	A SQL injection vulnerability exists in the 10Web Photo Gallery plugin before 1.5.31 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via filemanager/model.php.	2019-07-30	<a href="#">10.0</a>	<a href="#">CVE-2019-14313</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. On the /cbs/system/ShowAdvanced.do "File Explorer" screen, it is possible to change the directory in the JavaScript code. If changed to (for example) "C:" then one can browse the whole server.	2019-07-26	<a href="#">7.8</a>	<a href="#">CVE-2019-10265</a> <a href="#">MISC</a>
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. When sending an out-of-bounds XML document to a URL, it is possible to read the file structure and even the content of files without authentication.	2019-07-26	<a href="#">7.8</a>	<a href="#">CVE-2019-10266</a> <a href="#">MISC</a> <a href="#">MISC</a>
ahsay -- cloud_backup_suite	An insecure file upload and code execution issue was discovered in Ahsay Cloud Backup Suite 8.1.0.50. It is possible to upload a file into any directory of the server. One can insert a JSP shell into the web server's directory and execute it. This leads to full access to the system, as the configured user (e.g., Administrator).	2019-07-26	<a href="#">9.0</a>	<a href="#">CVE-2019-10267</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 76.0.8 allows remote attackers to execute arbitrary code via mailing-list attachments (SEC-452).	2019-07-30	<a href="#">7.5</a>	<a href="#">CVE-2018-20863</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 allows arbitrary code execution in the context of the root account via dnssec adminbin (SEC-465).	2019-07-30	<a href="#">7.2</a>	<a href="#">CVE-2018-20869</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows SQL injection during database backups (SEC-420).	2019-08-01	<a href="#">7.5</a>	<a href="#">CVE-2018-20887</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows local users to escalate to root access because of userdata cache misparsing (SEC-479).	2019-07-30	<a href="#">7.2</a>	<a href="#">CVE-2019-14400</a> <a href="#">CONFIRM</a>
datagrid_project -- datagrid	The datagrid gem 1.0.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party.	2019-07-26	<a href="#">7.5</a>	<a href="#">CVE-2019-14281</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet	2019-07-31	<a href="#">7.5</a>	<a href="#">CVE-2019-14192</a>

	due to a net_process_received_packet integer underflow during an nc_input_packet call.			MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with an unvalidated length at nfs_readlink_reply, in the "if" block after calculating the new path length.	2019-07-31	7.5	CVE-2019-14193 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv2 case.	2019-07-31	7.5	CVE-2019-14194 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with unvalidated length at nfs_readlink_reply in the "else" block after calculating the new path length.	2019-07-31	7.5	CVE-2019-14195 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_lookup_reply.	2019-07-31	7.5	CVE-2019-14196 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv3 case.	2019-07-31	7.5	CVE-2019-14198 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet due to a net_process_received_packet integer underflow during an *udp_packet_handler call.	2019-07-31	7.5	CVE-2019-14199 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: rpc_lookup_reply.	2019-07-31	7.5	CVE-2019-14200 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_lookup_reply.	2019-07-31	7.5	CVE-2019-14201 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_readlink_reply.	2019-07-31	7.5	CVE-2019-14202 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_mount_reply.	2019-07-31	7.5	CVE-2019-14203 MISC MISC
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_umountall_reply.	2019-07-31	7.5	CVE-2019-14204 MISC MISC
discourse -- discourse	Discourse before v2.4.0.beta2 lacks a confirmation screen when logging in via an email link.	2019-07-29	7.5	CVE-2019-1020018 MISC MISC
libmodbus -- libmodbus	An issue was discovered in libmodbus before 3.0.7 and 3.1.x before 3.1.5. There is an out-of-bounds read for the MODBUS_FC_WRITE_MULTIPLE_COILS case, aka VD-1302.	2019-07-31	7.5	CVE-2019-14462 MISC MISC
libmodbus -- libmodbus	An issue was discovered in libmodbus before 3.0.7 and 3.1.x before 3.1.5. There is an out-of-bounds read for the MODBUS_FC_WRITE_MULTIPLE_REGISTERS case, aka VD-1301.	2019-07-31	7.5	CVE-2019-14463 MISC MISC
linux -- linux_kernel	In the Linux kernel before 2.6.20, there is an off-by-one bug in net/netlabel/netlabel_cipso_v4.c where it is possible to overflow the doi_def->tags[] array.	2019-07-27	7.5	CVE-2007-6762 MISC MISC MISC
linux -- linux_kernel	In the Linux kernel before 2.6.34, a range check issue in drivers/gpu/drm/radeon/atombios.c could cause an off by one (buffer overflow) problem.	2019-07-27	7.5	CVE-2010-5331 MISC MISC MISC

linux -- linux_kernel	In the Linux kernel before 2.6.37, an out of bounds array access happened in drivers/net/mlx4/port.c. When searching for a free entry in either mlx4_register_vlan() or mlx4_register_mac(), and there is no free entry, the loop terminates without updating the local variable free thus causing out of array bounds access.	2019-07-27	7.5	<a href="#">CVE-2010-5332</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 3.1, an off by one in the drivers/target/loopback/tcm_loop.c tcm_loop_make_naa_tpg() function could result in at least memory corruption.	2019-07-27	7.5	<a href="#">CVE-2011-5327</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 3.4, a buffer overflow occurs in drivers/net/wireless/iwlwifi/iwl-agn-sta.c, which will cause at least memory corruption.	2019-07-27	7.5	<a href="#">CVE-2012-6712</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 4.1.4, a buffer overflow occurs when checking userspace params in drivers/media/dvb-frontends/cx24116.c. The maximum size for a DiSEqC command is 6, according to the userspace API. However, the code allows larger values such as 23.	2019-07-27	7.5	<a href="#">CVE-2015-9289</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 4.9.6, there is an off by one in the drivers/mtd/spi-nor/cadence-quadspi.c cqspi_setup_flash() function. There are CQSPI_MAX_CHIPSELECT elements in the ->f_pdata array so the ">" should be ">=" instead.	2019-07-27	7.5	<a href="#">CVE-2016-10764</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 4.14, an out of boundary access happened in drivers/nvme/target/fc.c.	2019-07-27	7.5	<a href="#">CVE-2017-18379</a> <a href="#">MISC</a> <a href="#">MISC</a>
simple_captcha2_project -- simple_captcha2	The simple_captcha2 gem 0.2.3 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party.	2019-07-26	7.5	<a href="#">CVE-2019-14282</a> <a href="#">MISC</a> <a href="#">MISC</a>
veritas -- resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. An arbitrary command execution vulnerability allows a malicious VRP user to execute commands with root privilege within the VRP virtual machine, related to resiliency plans and custom script functionality.	2019-07-29	9.0	<a href="#">CVE-2019-14416</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
veritas -- resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. An arbitrary command execution vulnerability allows a malicious VRP user to execute commands with root privilege within the VRP virtual machine, related to DNS functionality.	2019-07-29	9.0	<a href="#">CVE-2019-14417</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. When creating a trial account, it is possible to inject XSS in the Alias field, allowing the attacker to retrieve the admin's cookie and take over the account.	2019-07-26	4.3	<a href="#">CVE-2019-10263</a> <a href="#">MISC</a>
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. With a valid administrator account, the "Move / Import / Export Users" screen has an Import Users option. This option accepts a ZIP archive containing a users.xml file that can trigger XXE.	2019-07-26	6.5	<a href="#">CVE-2019-10264</a> <a href="#">MISC</a>
ash-aio_project -- ash-aio	ASH-AIO before 2.0.0.3 allows an open redirect.	2019-07-29	5.8	<a href="#">CVE-2019-1020016</a> <a href="#">MISC</a>
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.840, File and Directory Information Exposure in filemanager allows attackers to enumerate users and check for active users of the application by reading /tmp/login.log.	2019-07-26	4.0	<a href="#">CVE-2019-13385</a> <a href="#">MISC</a> <a href="#">MISC</a>



centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, a hidden action=9 feature in filemanager2.php allows attackers to execute a shell command, i.e., obtain a reverse shell with user privilege.	2019-07-26	<a href="#">6.5</a>	<a href="#">CVE-2019-13386</a> <a href="#">MISC</a> <a href="#">MISC</a>
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, Reflected XSS in filemanager2.php (parameter fm_current_dir) allows attackers to steal a cookie or session, or redirect to a phishing website.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-13387</a> <a href="#">MISC</a> <a href="#">MISC</a>
central_dogma_project -- central_dogma	Cross-site scripting vulnerability in Central Dogma 0.17.0 to 0.40.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-6002</a> <a href="#">JVN</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 76.0.8 allows a persistent Virtual FTP accounts after removal of its associated domain (SEC-454).	2019-07-30	<a href="#">6.4</a>	<a href="#">CVE-2018-20864</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has Self XSS in the WHM Additional Backup Destination field (SEC-459).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20865</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has Stored XSS in the WHM "Reset a DNS Zone" feature (SEC-461).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20866</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has an open redirect when resetting connections (SEC-462).	2019-07-30	<a href="#">5.8</a>	<a href="#">CVE-2018-20867</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has Stored XSS in the WHM MultiPHP Manager interface (SEC-464).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20868</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows demo accounts to execute arbitrary code via the Fileman::viewfile API (SEC-444).	2019-08-01	<a href="#">6.5</a>	<a href="#">CVE-2018-20879</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows FTP access during account suspension (SEC-449).	2019-08-01	<a href="#">4.0</a>	<a href="#">CVE-2018-20883</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows Apache HTTP Server configuration injection because of DocumentRoot variable interpolation (SEC-416).	2019-08-01	<a href="#">5.0</a>	<a href="#">CVE-2018-20885</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows Remote-Stored XSS in WHM Save Theme Interface (SEC-400).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20901</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows self XSS in the WHM Backup Configuration interface (SEC-421).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20903</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows self XSS in the WHM cPAddons showsecurity Interface (SEC-357).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20910</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows code execution because "." is in @INC during a Perl syntax check of cpaddonsup (SEC-359).	2019-08-01	<a href="#">6.5</a>	<a href="#">CVE-2018-20911</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows demo accounts to execute code via awstats (SEC-362).	2019-08-01	<a href="#">6.5</a>	<a href="#">CVE-2018-20912</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 70.0.23, OpenID providers can inject arbitrary data into cPanel session files (SEC-368).	2019-08-01	<a href="#">4.9</a>	<a href="#">CVE-2018-20914</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS in WHM DNS Cluster (SEC-372).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20918</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Create Account action (SEC-373).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20919</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Edit DNS Zone action (SEC-374).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20920</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM "Delete a DNS Zone" action (SEC-375).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20921</a> <a href="#">CONFIRM</a>

cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM DNS Cleanup action (SEC-376).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20922 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Synchronize DNS Records action (SEC-377).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20923 CONFIRM</a>
cpanel -- cpanel	cPanel before 82.0.2 has Self XSS in the cPanel and webmail master templates (SEC-506).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14387 MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 allows unauthenticated file creation because Exim log parsing is mishandled (SEC-507).	2019-07-30	<a href="#">5.0</a>	<a href="#">CVE-2019-14388 MISC</a>
cpanel -- cpanel	cPanel before 80.0.22 allows remote code execution by a demo account because of incorrect URI dispatching (SEC-501).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14392 CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 allows local code execution in the context of a different cPanel account because of insecure cpphp execution (SEC-486).	2019-07-30	<a href="#">4.6</a>	<a href="#">CVE-2019-14393 CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 allows demo accounts to modify arbitrary files via the extractfile API1 call (SEC-496).	2019-07-30	<a href="#">5.0</a>	<a href="#">CVE-2019-14397 CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 allows demo accounts to execute arbitrary code via ajax_maketxt_syntax_util.pl (SEC-498).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14398 CONFIRM</a>
cpanel -- cpanel	The SSL certificate-storage feature in cPanel before 78.0.18 allows unsafe file operations in the context of the root account (SEC-477).	2019-07-30	<a href="#">6.1</a>	<a href="#">CVE-2019-14399 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows code execution via an addforward API1 call (SEC-480).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14401 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 offers an open mail relay because of incorrect domain-redirect routing (SEC-483).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14403 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows certain file-read operations in the context of the root account via the Exim virtual_user_spam router (SEC-484).	2019-07-30	<a href="#">4.9</a>	<a href="#">CVE-2019-14404 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows demo accounts to execute code via securitypolicy.cg (SEC-487).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14405 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 has stored XSS in the BoxTrapper Queue Listing (SEC-493).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14406 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 reveals internal data to OpenID providers (SEC-415).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-14407 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 allows a demo account to link with an OpenID provider (SEC-460).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-14408 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 does not properly restrict demo accounts from writing to files via the DCV UAPI (SEC-473).	2019-07-30	<a href="#">5.0</a>	<a href="#">CVE-2019-14411 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 allows certain file-write operations as shared users during connection resets (SEC-476).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-14413 CONFIRM</a>
craftcms -- craft_cms	In some circumstances, Craft 2 before 2.7.10 and 3 before 3.2.6 wasn't stripping EXIF data from user-uploaded images when it was configured to do so, potentially exposing personal/geolocation data to the public.	2019-07-26	<a href="#">5.0</a>	<a href="#">CVE-2019-14280 MISC</a> <a href="#">MISC</a>
custom_simple_rss_project -- custom_simple_rss	A CSRF vulnerability in Settings form in the Custom Simple Rss plugin 2.0.6 for WordPress allows attackers to change the plugin settings.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14327 MISC</a> <a href="#">MISC</a>
denx -- u-boot	A crafted self-referential DOS partition table will cause all Das U-Boot versions through 2019.07-rc4 to infinitely recurse, causing the stack to grow infinitely and eventually either crash or overwrite other data.	2019-07-29	<a href="#">6.4</a>	<a href="#">CVE-2019-13103 MISC</a> <a href="#">MISC</a>

denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a read of out-of-bounds data at nfs_read_reply.	2019-07-31	<a href="#">6.4</a>	<a href="#">CVE-2019-14197</a> <a href="#">MISC</a> <a href="#">MISC</a>
discourse -- discourse	Discourse before v2.4.0.beta2 lacks a confirmation screen when logging in via a user-api OTP.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020017</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	An issue was discovered in EspoCRM before 5.6.6. There is stored XSS due to lack of filtration of user-supplied data in Create Task. A malicious attacker can modify the parameter name to contain JavaScript code.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14329</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	An issue was discovered in EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create Case. A malicious attacker can modify the firstName and lastName to contain JavaScript code.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14330</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	An issue was discovered in EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create User. A malicious attacker can modify the firstName and lastName to contain JavaScript code.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14331</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	EspoCRM version 5.6.4 is vulnerable to stored XSS due to lack of filtration of user-supplied data in the api/v1/Document functionality for storing documents in the account tab. An attacker can upload a crafted file that contains JavaScript code in its name. This code will be executed when a user opens a page of any profile with this.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14349</a> <a href="#">MISC</a>
espocrm -- espocrm	EspoCRM 5.6.4 is vulnerable to stored XSS due to lack of filtration of user-supplied data in the Knowledge base. A malicious attacker can inject JavaScript code in the body parameter during api/v1/KnowledgeBaseArticle knowledge-base record creation.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14350</a> <a href="#">MISC</a>
espocrm -- espocrm	EspoCRM 5.6.4 is vulnerable to user password hash enumeration. A malicious authenticated attacker can brute-force a user password hash by 1 symbol at a time using specially crafted api/v1/User?filterList filters.	2019-07-28	<a href="#">4.0</a>	<a href="#">CVE-2019-14351</a> <a href="#">MISC</a>
exiv2 -- exiv2	Exiv2 0.27.99.0 has a heap-based buffer over-read in Exiv2::RaflImage::readMetadata() in rafimage.cpp.	2019-07-28	<a href="#">6.8</a>	<a href="#">CVE-2019-14368</a> <a href="#">MISC</a>
exiv2 -- exiv2	Exiv2::PngImage::readMetadata() in pngimage.cpp in Exiv2 0.27.99.0 allows attackers to cause a denial of service (heap-based buffer over-read) via a crafted image file.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14369</a> <a href="#">MISC</a>
exiv2 -- exiv2	In Exiv2 0.27.99.0, there is an out-of-bounds read in Exiv2::MrwImage::readMetadata() in mrwimage.cpp. It could result in denial of service.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14370</a> <a href="#">MISC</a>
flif -- flif	An issue was discovered in image_save_png in image/image-png.cpp in Free Lossless Image Format (FLIF) 0.3. Attackers can trigger a heap-based buffer over-read in libpng via a crafted flif file.	2019-07-28	<a href="#">6.8</a>	<a href="#">CVE-2019-14373</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an Integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "one byte per line" case.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14288</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "multiple bytes per line" case.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14289</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 2.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14290</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 3.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14291</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in Xpdf 4.01.01. There is an out of			<a href="#">CVE-2019-</a>

glyphandcog -- xpdfreader	bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6 case 1.	2019-07-27	4.3	<a href="#">14292</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6 case 2.	2019-07-27	4.3	<a href="#">CVE-2019-14293</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is a use-after-free in the function JPXStream::fillReadBuf at JPXStream.cc, due to an out of bounds read.	2019-07-27	4.3	<a href="#">CVE-2019-14294</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- kubernetes_engine	Jenkins Google Kubernetes Engine Plugin 0.6.2 and earlier created a temporary file containing a temporary access token in the project workspace, where it could be accessed by users with Job/Read permission.	2019-07-31	4.0	<a href="#">CVE-2019-10365</a> <a href="#">MLIST</a> <a href="#">MISC</a>
ibm -- daeja_viewone	IBM Daeja ViewONE Professional, Standard & Virtual 5.0.5 and 5.0.6 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 163620.	2019-07-30	5.5	<a href="#">CVE-2019-4456</a> <a href="#">XE</a> <a href="#">CONFIRM</a>
ibm -- storediq	IBM StoreIQ 7.6.0.0. through 7.6.0.18 could allow an authenticated user to obtain sensitive information that a privileged user should only be allowed to view. IBM X-Force ID: 158696.	2019-07-31	4.0	<a href="#">CVE-2019-4163</a> <a href="#">CONFIRM</a> <a href="#">XE</a>
ibm -- storediq	IBM StoreIQ 7.6.0.0. through 7.6.0.18 could allow a remote attacker to cause a denial of service attack using repeated requests to the server. IBM X-Force ID: 158698.	2019-07-31	5.0	<a href="#">CVE-2019-4165</a> <a href="#">CONFIRM</a> <a href="#">XE</a>
icegram -- email_subscribers_&_newsletters	An XSS vulnerability in the "Email Subscribers & Newsletters" plugin 4.1.6 for WordPress allows an attacker to inject malicious JavaScript code through a publicly available subscription form using the esfx_name wp-admin/admin-ajax.php POST parameter.	2019-07-28	4.3	<a href="#">CVE-2019-14364</a> <a href="#">MISC</a> <a href="#">MISC</a>
inveniosoftware -- invenio-app	invenio-app before 1.1.1 allows host header injection.	2019-07-29	5.8	<a href="#">CVE-2019-1020006</a> <a href="#">CONFIRM</a>
inveniosoftware -- invenio-previewer	invenio-previewer before 1.0.0a12 allows XSS.	2019-07-29	4.3	<a href="#">CVE-2019-1020019</a> <a href="#">MISC</a>
jenkins -- configuration_as_code	Missing permission checks in Jenkins Configuration as Code Plugin 1.24 and earlier in various HTTP endpoints allowed users with Overall/Read access to access the generated schema and documentation for this plugin containing detailed information about installed plugins.	2019-07-31	4.0	<a href="#">CVE-2019-10344</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.24 and earlier did not escape values resulting in variable interpolation during configuration import when exporting, allowing attackers with permission to change Jenkins system configuration to obtain the values of environment variables.	2019-07-31	5.5	<a href="#">CVE-2019-10362</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.24 and earlier did not reliably identify sensitive values expected to be exported in their encrypted form.	2019-07-31	4.0	<a href="#">CVE-2019-10363</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- m2release	A cross-site request forgery vulnerability in Jenkins Maven Release Plugin 0.14.0 and earlier in the M2ReleaseAction#doSubmit method allowed attackers to perform releases with attacker-specified options.	2019-07-31	6.8	<a href="#">CVE-2019-10359</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- maven	Jenkins Maven Integration Plugin 3.3 and earlier did not apply build log decorators to module builds, potentially revealing sensitive build variables in the build log.	2019-07-31	4.0	<a href="#">CVE-2019-10358</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- pipeline:shared_groovy_libraries	A missing permission check in Jenkins Pipeline: Shared Groovy Libraries Plugin 2.14 and earlier allowed users with Overall/Read access to obtain limited information about the content of SCM repositories referenced by global libraries.	2019-07-31	4.0	<a href="#">CVE-2019-10357</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- script_security	A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.61 and earlier related to the handling of type casts allowed attackers to execute arbitrary code in sandboxed	2019-07-31	6.5	<a href="#">CVE-2019-10355</a> <a href="#">MLIST</a>

	scripts.			<a href="#">MISC</a>
jenkins -- script_security	A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.61 and earlier related to the handling of method pointer expressions allowed attackers to execute arbitrary code in sandboxed scripts.	2019-07-31	<a href="#">6.5</a>	<a href="#">CVE-2019-10356</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- skytap_cloud_ci	Jenkins Skytap Cloud CI Plugin 2.06 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system.	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10366</a> <a href="#">MLIST</a> <a href="#">MISC</a>
kolide -- fleet	Fleet before 2.1.2 allows exposure of SMTP credentials.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020009</a> <a href="#">MISC</a>
libav -- libav	An issue was discovered in Lbav 12.3. There is an infinite loop in the function mov_probe in the file libavformat/mov.c, related to offset and tag.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14371</a> <a href="#">MISC</a>
libav -- libav	In Lbav 12.3, there is an infinite loop in the function vv_read_block_header() in the file vvdec.c.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14372</a> <a href="#">MISC</a>
libav -- libav	An issue was discovered in Lbav 12.3. Division by zero in range_decode_culshift in lbavcodec/apedec.c allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14443</a> <a href="#">MISC</a>
libsdl -- sdl2_image	An exploitable code execution vulnerability exists in the PCX image-rendering functionality of SDL2_image 2.0.4. A specially crafted PCX image can cause a heap overflow, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-5057</a> <a href="#">MISC</a>
libsdl -- sdl2_image	An exploitable code execution vulnerability exists in the XCF image rendering functionality of SDL2_image 2.0.4. A specially crafted XCF image can cause a heap overflow, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-5058</a> <a href="#">MISC</a>
libsdl -- sdl2_image	An exploitable code execution vulnerability exists in the XPM image rendering functionality of SDL2_image 2.0.4. A specially crafted XPM image can cause an integer overflow, allocating too small of a buffer. This buffer can then be written out of bounds resulting in a heap overflow, ultimately ending in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-5059</a> <a href="#">MISC</a>
libslirp_project -- libslirp	ip_reass in ip_input.c in libslirp 4.0.0 has a heap-based buffer overflow via a large packet because it mishandles a case involving the first fragment.	2019-07-29	<a href="#">6.5</a>	<a href="#">CVE-2019-14378</a> <a href="#">MLIST</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.20. drivers/phy/mscc/phy-ocelot-serdes.c has an off-by-one error with a resultant ctrl->phys out-of-bounds read.	2019-07-26	<a href="#">4.6</a>	<a href="#">CVE-2018-20854</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue() use-after-free because a certain error case is mishandled.	2019-07-26	<a href="#">4.6</a>	<a href="#">CVE-2018-20856</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.2.3, set_geometry in drivers/block/floppy.c does not validate the sect and head fields, as demonstrated by an integer overflow and out-of-bounds read. It can be triggered by an unprivileged local user when a floppy disk has been inserted. NOTE: QEMU creates the floppy device by default.	2019-07-26	<a href="#">4.6</a>	<a href="#">CVE-2019-14283</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mcpp_project -- mcpp	MCP 2.7.2 has a heap-based buffer overflow in the do_msg() function in support.c.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-14274</a> <a href="#">MISC</a>
misp -- misp	In app/webroot/js/event-graph.js in MISP 2.4.111, a stored XSS vulnerability exists in the event-graph view when a user toggles the event graph view. A malicious MISP event must be crafted in order to trigger the vulnerability.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14286</a> <a href="#">MISC</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. A sesskey (CSRF) token was not being utilised by the XML loading/unloading admin tool.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-10186</a> <a href="#">CONFIRM</a>



				<a href="#">MISC</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. Users with permission to delete entries from a glossary were able to delete entries from other glossaries they did not have direct access to.	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10187</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. Teachers in a quiz group could modify group overrides for other groups in the same quiz.	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10188</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. Teachers in an assignment group could modify group overrides for other groups in the same assignment.	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10189</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
nats -- nats_server	An integer overflow in NATS Server 2.0.0 allows a remote attacker to crash the server by sending a crafted request.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-13126</a> <a href="#">MISC</a> <a href="#">MISC</a>
open.edx -- edx-platform	edx-platform before 2015-07-20 allows code execution by privileged users because the course import endpoint mishandles .tar.gz files.	2019-07-29	<a href="#">6.5</a>	<a href="#">CVE-2015-5601</a> <a href="#">CONFIRM</a>
open.edx -- edx-platform	edx-platform before 2015-09-17 allows XSS via a team name.	2019-07-29	<a href="#">4.3</a>	<a href="#">CVE-2015-6960</a> <a href="#">CONFIRM</a>
openmpt -- libopenmpt	libopenmpt before 0.3.13 allows a crash with malformed MED files.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20860</a> <a href="#">MISC</a>
openmpt -- libopenmpt	libopenmpt before 0.4.5 allows a crash during playback due to an out-of-bounds read in XM and MT2 files.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14380</a> <a href="#">MISC</a>
parseplatform -- parse-server	parse-server before 3.4.1 allows DoS after any POST to a volatile class.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020012</a> <a href="#">MISC</a>
parseplatform -- parse-server	parse-server before 3.6.0 allows account enumeration.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020013</a> <a href="#">MISC</a>
postgresql -- postgresql	A vulnerability was found in postgresql versions 11.x prior to 11.3. Using a purpose-crafted insert to a partitioned table, an attacker can read arbitrary bytes of server memory. In the default configuration, any user can create a partitioned table suitable for this attack. (Exploit prerequisites are the same as for CVE-2018-1052).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-10129</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
pterodactyl -- panel	Pterodactyl before 0.7.14 with 2FA allows credential sniffing.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020002</a> <a href="#">CONFIRM</a>
stacktable.js_project -- stacktable.js	stacktable.js before 1.0.4 allows XSS.	2019-07-29	<a href="#">4.3</a>	<a href="#">CVE-2019-1020008</a> <a href="#">MISC</a>
sunhater -- kcfinder	A cross-site scripting (XSS) vulnerability in upload.php in SunHater KCFinder 3.20-test1, 3.20-test2, 3.12, and earlier allows remote attackers to inject arbitrary web script or HTML via the CKEditorFuncNum parameter.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14315</a> <a href="#">MISC</a>
testlink -- testlink	TestLink 1.9.19 has XSS via the error.php message parameter.	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2019-14471</a> <a href="#">MISC</a>
tridactyl_project -- tridactyl	Tridactyl before 1.16.0 allows fake key events.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020004</a> <a href="#">MISC</a>
unity -- web_player	The Unity Web Player plugin before 4.6.6f2 and 5.x before 5.0.3f2 allows attackers to read messages or access online services via a victim's credentials	2019-07-29	<a href="#">4.0</a>	<a href="#">CVE-2015-9288</a> <a href="#">CONFIRM</a>
upx_project -- upx	An Integer overflow in the getElfSections function in p_vmlnx.cpp in UPX 3.95 allows remote attackers to cause a denial of service (crash) via a skewed offset larger than the size of the PE section in a UPX packed executable, which triggers an allocation of excessive memory.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14295</a> <a href="#">MISC</a>
upx_project -- upx	canUnpack in p_vmlnx.cpp in UPX 3.95 allows remote attackers to cause a denial of service (SEGV or buffer	2019-07-27	<a href="#">6.8</a>	<a href="#">CVE-2019-14296</a>

	overflow, and application crash) or possibly have unspecified other impact via a crafted UPX packed file.			<a href="#">MISC</a>
wallaceit -- wallacepos	Cross-site request forgery in WallacePOS 1.4.3 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-3959</a> <a href="#">MISC</a>
wikindx_project -- wikindx	A cross-site scripting (XSS) vulnerability in getPagingStart() in core/lists/PAGING.php in WIKINDX through 5.8.1 allows remote attackers to inject arbitrary web script or HTML via the PagingStart parameter.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-13588</a> <a href="#">CONFIRM</a>
wpfastestcache -- wp_fastest_cache	The WP Fastest Cache plugin through 0.8.9.0 for WordPress allows remote attackers to delete arbitrary files because wp_postratings_clear_fastest_cache and rm_folder_recursively in wpFastestCache.php mishandle ../ in an HTTP Referer header.	2019-07-29	<a href="#">5.8</a>	<a href="#">CVE-2019-6726</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
xfig_project -- fig2dev	Xfig fig2dev 3.2.7a has a stack-based buffer overflow in the calc_arrow function in bound.c.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-14275</a> <a href="#">MISC</a>
yardoc -- yard	yard before 0.9.20 allows path traversal.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020001</a> <a href="#">MISC</a>
zendesk -- samlr	Zendesk Samlr before 2.6.2 allows an XML nodes comment attack such as a name_id node with user@example.com followed by <!---->, and then the attacker's domain name.	2019-07-26	<a href="#">5.0</a>	<a href="#">CVE-2018-20857</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cpanel -- cpanel	cPanel before 76.0.8 unsafely performs PostgreSQL password changes (SEC-366).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2018-20862</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The WebDAV transport feature in cPanel before 76.0.8 enables debug logging (SEC-467).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2018-20870</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in the WHM Security Questions interface (SEC-433).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20875</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in the Site Software Moderation interface (SEC-434).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20876</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in WHM Style Upload interface (SEC-437).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20877</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows stored XSS in WHM "File and Directory Restoration" interface (SEC-441).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20878</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 mishandles account suspension because of an invalid email_accounts.json file (SEC-445).	2019-08-01	<a href="#">2.1</a>	<a href="#">CVE-2018-20880</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self stored XSS on the Security Questions login page (SEC-446).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20881</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows stored XSS in the WHM File Restoration interface (SEC-367).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20884</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to read root's crontab file by leveraging ClamAV installation (SEC-408).	2019-08-01	<a href="#">2.1</a>	<a href="#">CVE-2018-20902</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows attackers to read the root accesshash via the WHM /cgi/trustclustermaster.cgi (SEC-364).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20913</a> <a href="#">CONFIRM</a>

cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Edit DNS Zone action (SEC-369).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20915</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows Stored XSS via a WHM Edit MX Entry (SEC-370).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20916</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows any user to disable Solr (SEC-371).	2019-08-01	<a href="#">2.1</a>	<a href="#">CVE-2018-20917</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 82.0.2 has stored XSS in the WHM Tomcat Manager interface (SEC-504).	2019-07-30	<a href="#">3.5</a>	<a href="#">CVE-2019-14386</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 allows local users to discover the MySQL root password (SEC-510).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14389</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 has stored XSS in the WHM Modify Account interface (SEC-512).	2019-07-30	<a href="#">3.5</a>	<a href="#">CVE-2019-14390</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 does not properly enforce Reseller package creation ACLs (SEC-514).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14391</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 80.0.5 allows unsafe file operations in the context of the root account via the fetch_ssl_certificates_for_fqdns API (SEC-489).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14394</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 uses world-readable permissions for the Queueprocd log (SEC-494).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14395</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	API Analytics adminbin in cPanel before 80.0.5 allows spoofed insertions of log data (SEC-495).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14396</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 unsafely determines terminal capabilities by using infocmp (SEC-481).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14402</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 allows arbitrary file-read operations via Passenger adminbin (SEC-466).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14409</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	Maketext in cPanel before 78.0.2 allows format-string injection in the Email store_filter UAPI (SEC-472).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14410</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	Maketext in cPanel before 78.0.2 allows format-string injection in the DCV check_domains_via_dns UAPI (SEC-474).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14412</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 78.0.2, a Userdata cache temporary file can conflict with domains (SEC-478).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2019-14414</a> <a href="#">CONFIRM</a>
dependencytrack -- dependency-track	Dependency-Track before 3.5.1 allows XSS.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2019-1020007</a> <a href="#">CONFIRM</a>
http-file-server_project -- http-file-server	Cross-site scripting (XSS) vulnerability in http-file-server (all versions) allows an attacker with access to the server file system to execute arbitrary JavaScript code in victim's browser.	2019-07-30	<a href="#">3.5</a>	<a href="#">CVE-2019-5458</a> <a href="#">MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server - Liberty Admin Center could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could send a specially-crafted HTTP request to hijack the victim's click actions or launch other client-side browser attacks. IBM X-Force ID: 160513.	2019-07-30	<a href="#">3.5</a>	<a href="#">CVE-2019-4285</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
inveniosoftware -- invenio-communities	invenio-communities before 1.0.0a20 allows XSS.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2019-1020005</a> <a href="#">MISC</a>
inveniosoftware -- invenio-records	invenio-records before 1.2.2 allows XSS.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2019-1020003</a> <a href="#">MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.24 and earlier did not properly apply masking to values expected to be hidden when	2019-07-31	<a href="#">2.1</a>	<a href="#">CVE-2019-10343</a> <a href="#">MLIST</a>

	logging the configuration being applied.			<a href="#">MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.20 and earlier did not treat the proxy password as a secret to be masked when logging or encrypted for export.	2019-07-31	<a href="#">2.1</a>	<a href="#">CVE-2019-10345</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- ec2	Jenkins Amazon EC2 Plugin 1.43 and earlier wrote the beginning of private keys to the Jenkins system log.	2019-07-31	<a href="#">2.1</a>	<a href="#">CVE-2019-10364</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- m2_release	A stored cross site scripting vulnerability in Jenkins Maven Release Plugin 0.14.0 and earlier allowed attackers to inject arbitrary HTML and JavaScript in the plugin-provided web pages in Jenkins.	2019-07-31	<a href="#">3.5</a>	<a href="#">CVE-2019-10360</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- m2release	Jenkins Maven Release Plugin 0.14.0 and earlier stored credentials unencrypted on the Jenkins master where they could be viewed by users with access to the master file system.	2019-07-31	<a href="#">2.1</a>	<a href="#">CVE-2019-10361</a> <a href="#">MLIST</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.18.7. In create_qp_common in drivers/infiniband/hw/mlx5/qp.c, mlx5_b_create_qp_resp was never initialized, resulting in a leak of stack memory to userspace.	2019-07-26	<a href="#">2.1</a>	<a href="#">CVE-2018-20855</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.2.3, drivers/block/floppy.c allows a denial of service by setup_format_params division-by-zero. Two consecutive ioctl's can trigger the bug: the first one should set the drive geometry with .sect and .rate values that make F_SECT_PER_TRACK be zero. Next, the floppy format operation should be called. It can be triggered by an unprivileged local user even when a floppy disk has not been inserted. NOTE: QEMU creates the floppy device by default.	2019-07-26	<a href="#">2.1</a>	<a href="#">CVE-2019-14284</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- outlook	A spoofing vulnerability exists in the way Microsoft Outlook for Android software parses specifically crafted email messages, aka 'Outlook for Android Spoofing Vulnerability'.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2019-1105</a> <a href="#">N/A</a>
min-http-server_project -- min-http-server	Cross-site scripting (XSS) vulnerability in min-http-server (all versions) allows an attacker with access to the server file system to execute arbitrary JavaScript code in victim's browser.	2019-07-30	<a href="#">3.5</a>	<a href="#">CVE-2019-5457</a> <a href="#">MISC</a>
open.edx -- edx-platform	edx-platform before 2015-08-17 allows XSS in the Studio listing of courses.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2015-6253</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
veeam -- one_reporter	Veeam ONE Reporter 9.5.0.3201 allows XSS via the Add/Edit Widget with a crafted Caption field to setDashboardWidget in CommonDataHandlerReadOnly.ashx.	2019-07-27	<a href="#">3.5</a>	<a href="#">CVE-2019-14297</a> <a href="#">MISC</a>
veeam -- one_reporter	Veeam ONE Reporter 9.5.0.3201 allows XSS via a crafted Description(config) field to addDashboard or editDashboard in CommonDataHandlerReadOnly.ashx.	2019-07-27	<a href="#">3.5</a>	<a href="#">CVE-2019-14298</a> <a href="#">MISC</a>
veritas -- resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. A persistent cross-site scripting (XSS) vulnerability allows a malicious VRP user to inject malicious script into another user's browser, related to resiliency plans functionality. A victim must open a resiliency plan that an attacker has access to.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2019-14415</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
wallaceit -- wallacepos	Insufficient output sanitization in WallacePOS 1.4.3 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks via a crafted sales transaction.	2019-07-31	<a href="#">3.5</a>	<a href="#">CVE-2019-3958</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3proxy -- 3proxy	webadmin.c in 3proxy before 0.8.13 has an out-of-bounds write in the admin	2019-08-	not yet	<a href="#">CVE-2019-14495</a>

	interface.	01	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
adoptopenjdk -- icedtea-web	It was found that icedtea-web though 1.7.2 and 1.8.2 did not properly sanitize paths from <jar/> elements in JNLP files. An attacker could trick a victim into running a specially crafted application and use this flaw to upload arbitrary files to arbitrary locations in the context of the user.	2019-07-31	not yet calculated	<a href="#">CVE-2019-10182</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
adoptopenjdk -- icedtea-web	It was found that icedtea-web up to and including 1.7.2 and 1.8.2 was vulnerable to a zip-slip attack during auto-extraction of a JAR file. An attacker could use this flaw to write files to arbitrary locations. This could also be used to replace the main running application and, possibly, break out of the sandbox.	2019-07-31	not yet calculated	<a href="#">CVE-2019-10185</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
adoptopenjdk -- icedtea-web	It was found that in icedtea-web up to and including 1.7.2 and 1.8.2 executable code could be injected in a JAR file without compromising the signature verification. An attacker could use this flaw to inject code in a trusted JAR. The code would be executed inside the sandbox.	2019-07-31	not yet calculated	<a href="#">CVE-2019-10181</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
advantech -- webaccess_hmi_designer	In Advantech WebAccess HMI Designer Version 2.1.9.23 and prior, processing specially crafted MCR files lacking proper validation of user supplied data may cause the system to write outside the intended buffer area, allowing remote code execution.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10961</a> <a href="#">MISC</a>
alcatel-lucent_enterprise -- 8008_cloud_edition_deskphone_voip_phone	On the Alcatel-Lucent Enterprise (ALE) 8008 Cloud Edition Deskphone VoIP phone with firmware 1.50.13, a command injection (missing input validation) issue in the password change field for the Change Password interface allows an authenticated remote attacker in the same network to trigger OS commands via shell commands in a POST request.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14260</a> <a href="#">MISC</a>
alcatel -- linkzone_mw40-v-v1.0_mw40_02.00_02_devices	The web interface of Alcatel LINKZONE MW40-V-V1.0 MW40_LU_02.00_02 devices is vulnerable to an authentication bypass that allows an unauthenticated user to have access to the web interface without knowing the administrator's password.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7163</a> <a href="#">MISC</a>
amcrest -- ip2m-841b_ip_camera	The Amcrest IP2M-841B IP camera firmware version V2.520.AC00.18.R does not require authentication to access the HTTP endpoint /videotalk. An unauthenticated, remote person can connect to this endpoint and listen to the audio the camera is capturing.	2019-07-29	not yet calculated	<a href="#">CVE-2019-3948</a> <a href="#">MISC</a> <a href="#">MISC</a>
ansible -- ansible	A flaw was discovered in the way Ansible templating was implemented in versions before 2.6.18, 2.7.12 and 2.8.2, causing the possibility of information disclosure through unexpected variable substitution. By taking advantage of unintended variable substitution the content of any variable may be disclosed.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10156</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
apache -- activemq_client	It was found that the Apache ActiveMQ client before 5.15.5 exposed a remote shutdown command in the ActiveMQConnection class. An attacker logged into a compromised broker could use this flaw to achieve denial of service on a connected client.	2019-08-01	not yet calculated	<a href="#">CVE-2015-7559</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>



apache -- solr	In Apache Solr, the DataImportHandler, an optional but popular module to pull in data from databases and other sources, has a feature in which the whole DIH configuration can come from a request's "dataConfig" parameter. The debug mode of the DIH admin screen uses this to allow convenient debugging / development of a DIH config. Since a DIH config can contain scripts, this parameter is a security risk. Starting with version 8.2.0 of Solr, use of this parameter requires setting the Java System property "enable.dih.dataConfigParam" to true.	2019-08-01	not yet calculated	<a href="#">CVE-2019-0193</a> <a href="#">CONFIRM</a>
apache -- tika	A carefully crafted or corrupt zip file can cause an OOM in Apache Tika's RecursiveParserWrapper in versions 1.7-1.21. Users should upgrade to 1.22 or later.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10088</a> <a href="#">CONFIRM</a>
apache -- tika	In Apache Tika 1.19 to 1.21, a carefully crafted 2003ml or 2006ml file could consume all available SAXParsers in the pool and lead to very long hangs. Apache Tika users should upgrade to 1.22 or later.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10093</a> <a href="#">CONFIRM</a>
apache -- tika	A carefully crafted package/compressed file that, when unzipped/uncompressed yields the same file (a quine), causes a StackOverflowError in Apache Tika's RecursiveParserWrapper in versions 1.7-1.21. Apache Tika users should upgrade to 1.22 or later.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10094</a> <a href="#">CONFIRM</a>
apache -- vcl	Apache VCL versions 2.1 through 2.5 do not properly validate cookie input when determining what node (if any) was previously selected in the privilege tree. The cookie data is then used in an SQL statement. This allows for an SQL injection attack. Access to this portion of a VCL system requires admin level rights. Other layers of security seem to protect against malicious attack. However, all VCL systems running versions earlier than 2.5.1 should be upgraded or patched. This vulnerability was found and reported to the Apache VCL project by ADLab of Venustech.	2019-07-29	not yet calculated	<a href="#">CVE-2018-11772</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apache -- vcl	Apache VCL versions 2.1 through 2.5 do not properly validate form input when processing a submitted block allocation. The form data is then used as an argument to the php built in function strtotime. This allows for an attack against the underlying implementation of that function. The implementation of strtotime at the time the issue was discovered appeared to be resistant to a malicious attack. However, all VCL systems running versions earlier than 2.5.1 should be upgraded or patched. This vulnerability was found and reported to the Apache VCL project by ADLab of Venustech.	2019-07-29	not yet calculated	<a href="#">CVE-2018-11773</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apache -- vcl	Apache VCL versions 2.1 through 2.5 do not properly validate form input when adding and removing VMs to and from hosts. The form data is then used in SQL statements. This allows for an SQL injection attack. Access to this portion of a VCL system requires admin level rights. Other layers of security seem to protect against malicious attack. However, all VCL systems running versions earlier than	2019-07-29	not yet calculated	<a href="#">CVE-2018-11774</a> <a href="#">MLIST</a> <a href="#">MLIST</a>

	2.5.1 should be upgraded or patched. This vulnerability was found and reported to the Apache VCL project by ADLab of Venustech.			
avaya -- aura_conferencing	A Cross-Site Scripting (XSS) vulnerability in the Web UI of Avaya Aura Conferencing may allow code execution and potentially disclose sensitive information. Affected versions of Avaya Aura Conferencing include all 8.x versions prior to 8.0 SP14 (8.0.14). Prior versions not listed were not evaluated.	2019-07-31	not yet calculated	<a href="#">CVE-2019-7000</a> <a href="#">CONFIRM</a>
bitdefender -- multiple_products	An issue was discovered in Bitdefender products for Windows (Bitdefender Endpoint Security Tool versions prior to 6.6.8.115; and Bitdefender Antivirus Plus, Bitdefender Internet Security, and Bitdefender Total Security versions prior to 23.0.24.120) that can lead to local code injection. A local attacker with administrator privileges can create a malicious DLL file in %SystemRoot%\System32\ that will be executed with local user privileges.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14242</a> <a href="#">CONFIRM</a>
cisco -- nexus_9000_series_aci_mode_switch_software	A vulnerability in the Link Layer Discovery Protocol (LLDP) subsystem of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an adjacent, unauthenticated attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges. The vulnerability is due to improper input validation of certain type, length, value (TLV) fields of the LLDP frame header. An attacker could exploit this vulnerability by sending a crafted LLDP packet to the targeted device. A successful exploit may lead to a buffer overflow condition that could either cause a DoS condition or allow the attacker to execute arbitrary code with root privileges. Note: This vulnerability cannot be exploited by transit traffic through the device; the crafted packet must be targeted to a directly connected interface. This vulnerability affects Cisco Nexus 9000 Series Fabric Switches in ACI mode if they are running a Cisco Nexus 9000 Series ACI Mode Switch Software release prior to 13.2(7f) or any 14.x release.	2019-07-31	not yet calculated	<a href="#">CVE-2019-1901</a> <a href="#">CISCO</a>
clmg -- clmg	Clmg through 2.6.7 has a heap-based buffer overflow in _load_bmp in Clmg.h because of erroneous memory allocation for a malformed BMP image.	2019-07-31	not yet calculated	<a href="#">CVE-2019-13568</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
clusterlabs -- fence-agents	A flaw was discovered in fence-agents, prior to version 4.3.4, where using non-ASCII characters in a guest VM's comment or other fields would cause fence_rhevm to exit with an exception. In cluster environments, this could lead to preventing automated recovery or otherwise denying service to clusters of which that VM is a member.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10153</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows arbitrary file-read operations for Webmail accounts via Branding APIs (SEC-120).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10815</a> <a href="#">MISC</a>
	cPanel before 11.52.0.13 does not prevent arbitrary file-read operations via	2019-08-	not yet	<a href="#">CVE-</a>

cpanel -- cpanel	get_information_for_applications (CPANEL-1221).	01	calculated	<a href="#">2015-9291 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows arbitrary code execution in the context of the root account because of MakeText interpolation (SEC-89).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10823 MISC</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows Webmail accounts to execute arbitrary code through forwarders (SEC-121).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10816 MISC</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows SQL Injection via the ModSecurity TailWatch log file (SEC-123).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10817 MISC</a>
cpanel -- cpanel	cPanel before 57.9999.54 incorrectly sets log-file permissions in dnsadmin-startup and spamd-startup (SEC-124).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10818 MISC</a>
cpanel -- cpanel	In cPanel before 57.9999.54, user log files become world-readable when rotated by cpanellogd (SEC-125).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10819 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows daemons to access their controlling TTYs (SEC-31).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10820 MISC</a>
cpanel -- cpanel	In cPanel before 55.9999.141, Scripts/addpop reveals a command-line password in a process list (SEC-75).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10821 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows ACL bypass for AppConfig applications via magic_revision (SEC-100).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10830 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows a POP/IMAP cPHulk bypass via account name munging (SEC-107).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10835 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows unauthenticated arbitrary code execution via DNS NS entry poisoning (SEC-90).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10824 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows attackers to bypass a Security Policy by faking static documents (SEC-92).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10825 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows attackers to bypass Two Factor Authentication via DNS clustering requests (SEC-93).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10826 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows self stored XSS in WHM Edit System Mail Preferences (SEC-96).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10827 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows arbitrary code execution because of an unsafe @INC path (SEC-97).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10828 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows arbitrary file-read operations because of a multipart form processing error (SEC-99).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10829 MISC</a>
cpanel -- cpanel	cPanel before 66.0.2 allows resellers to read other accounts' domain log files (SEC-288).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18426 CONFIRM</a>
	cPanel before 55.9999.141 does not			<a href="#">CVE-</a>

cpanel -- cpanel	perform as two-factor authentication check when possessing another account (SEC-101).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10831 MISC</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows demo-mode escape via show_template.stor (SEC-119).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10814 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows subaccounts to discover sensitive data through comet feeds (SEC-29).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10856 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows self XSS in X3 Reseller Branding Images (SEC-88).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10822 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows stored XSS in the WHM Feature Manager interface (SEC-86).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10853 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-overwrite operations in scripts/check_system_storable (SEC-78).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10845 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-chown and file-chmod operations during Roundcube database conversions (SEC-79).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10846 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-read and file-write operations via scripts/fixmailboxpath (SEC-80).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10847 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-overwrite operations in scripts/quotacheck (SEC-81).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10848 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary code execution via scripts/synccpaddonswithsqlhost (SEC-83).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10850 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary code execution because of an unsafe @INC path (SEC-46).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10837 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows self XSS in the WHM PHP Configuration editor interface (SEC-84).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10851 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 lacks ACL enforcement in the AppConfig subsystem (SEC-85).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10852 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows self XSS in the X3 Entropy Banner interface (SEC-87).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10854 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 allows jailed accounts to restore files that are outside of the jail (SEC-310).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18384 CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows unauthenticated arbitrary code execution via cpsrvd (SEC-91).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10855 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 mishandles username-based blocking for PRE requests in cPHulkd (SEC-104).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10833 MISC</a>
				<a href="#">CVE-</a>

cpanel -- cpanel	cPanel before 11.54.0.0 allows unauthenticated arbitrary code execution via DNS NS entry poisoning (SEC-64).	2019-08-01	not yet calculated	<a href="#">2016-10858 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows unauthorized password changes via Webmail API commands (SEC-65).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10859 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows unauthorized zone modification via the WHM API (SEC-66).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10860 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 allows use of an unreserved e-mail address in DNS zone SOA records (SEC-306).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18382 CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-read operations via the bin/fmq script (SEC-70).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10838 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows arbitrary file-read operations during authentication with caldav (SEC-108).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10836 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows FTP cPHulk bypass via account name munging (SEC-102).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10832 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary code execution via Maketext injection in PostgresAdmin (SEC-313).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18386 CONFIRM</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows account-suspension bypass via ftp (SEC-105).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10834 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 can perform unsafe file operations because Jailshell does not set the umask (SEC-315).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18388 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, domain log files become readable after log processing (SEC-273).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18423 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, the Apache HTTP Server configuration file is changed to world-readable when rebuilt (SEC-274).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18424 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, the cpdavd_error_log file can be created with weak permissions (SEC-280).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18425 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows user accounts to be partially created with invalid username formats (SEC-334).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18401 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary file-read operations because of the backup .htaccess modification logic (SEC-345).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18405 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows attackers to read root's crontab file during a short time interval upon enabling or disabling sqloptimizer (SEC-332).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18399 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows collisions because PostgreSQL databases can be assigned to multiple accounts (SEC-325).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18392 CONFIRM</a>



cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary code execution via Maketext injection in a Reseller style upload (SEC-314).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18387</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows string format injection in dovecot-xaps-plugin (SEC-318).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18389</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows demo accounts to create databases and users (SEC-271).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18421</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	DnsUtils in cPanel before 68.0.15 allows zone creation for hostname and account subdomains (SEC-331).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18398</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows code execution in the context of the root account because of weak permissions on incremental backups (SEC-322).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18390</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows attackers to read backup files because they are world-readable during a short time interval (SEC-323).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18391</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows self XSS during ftp account creation under addon domains (SEC-118).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10813</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 does not have a sufficient list of reserved usernames (SEC-327).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18394</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 does not preserve permissions for local backup transport (SEC-330).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18397</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary file-read operations via Exim vdomainaliases (SEC-329).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18396</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 does not block a username of postmaster, which might allow reception of private e-mail (SEC-326).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18393</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 does not block a username of ssl (SEC-328).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18395</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, EasyApache 4 conversion sets weak domlog ownership and permissions (SEC-272).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18422</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons processing (SEC-269).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18420</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 writes home-directory backups to an incorrect location (SEC-309).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18383</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows stored XSS in WHM MySQL Password Change interfaces (SEC-282).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18408</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows a bypass of the e-mail sending limit (SEC-60).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10857</a> <a href="#">MISC</a>

cpanel -- cpanel	cPanel before 68.0.15 allows unprivileged users to access restricted directories during account restores (SEC-311).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18385</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 67.9999.103, the backup system overwrites root's home directory when a mount disappears (SEC-299).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18413</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows stored XSS during a cpaddons moderated upgrade (SEC-336).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18402</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows code execution in the context of the nobody account via Mailman archives (SEC-337).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18403</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows domain data to be deleted for domains with the .lock TLD (SEC-341).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18404</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows code execution in the context of shared users via JSON-API (SEC-76).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10843</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows SQL injection during eximstats processing (SEC-276).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18406</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 does not enforce SSL hostname verification for the support-agreement download (SEC-279).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18407</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 67.9999.103, the backup interface could return a backup archive with all MySQL databases (SEC-283).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18409</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons uninstallation (SEC-266).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18419</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 67.9999.103, a user account's backup archive could contain all MySQL databases on the server (SEC-284).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18410</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The "addon domain conversion" feature in cPanel before 67.9999.103 can copy all MySQL databases to the new account (SEC-285).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18411</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows Apache HTTP Server log files to become world-readable because of mishandling on an account rename (SEC-296).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18412</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows an open redirect in /unprotected/redirect.html (SEC-300).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18414</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows local root code execution via cpdavid (SEC-333).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18400</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows code execution in the context of the mailman account because of incorrect environment-variable filtering (SEC-302).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18415</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows arbitrary file-overwrite operations during a Roundcube SQLite schema update (SEC-303).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18416</a> <a href="#">CONFIRM</a>

cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons installation (SEC-263).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18417 CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons file operations (SEC-265).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18418 CONFIRM</a>
cpanel -- cpanel	The chcpass script in cPanel before 11.54.0.4 reveals a password hash (SEC-77).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10844 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows certain file-chmod operations in scripts/secureit (SEC-82).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10849 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows certain file-read operations in bin/setup_global_spam_filter.pl (SEC-74).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10842 MISC</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to redirect web traffic (SEC-245).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18441 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows code execution by webmail and demo accounts via a store_filter API call (SEC-236).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18433 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows code execution in the context of the root account via a SET_VHOST_LANG_PACKAGE multilang adminbin call (SEC-237).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18434 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via the BoxTrapper API (SEC-238).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18435 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to read files via a Fileman::getfileactions API2 call (SEC-239).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18436 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows a Webmail account to execute code via forwarders (SEC-240).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18437 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via an ImageManager_dimensions API call (SEC-243).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18439 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows certain file-rename operations in the context of the root account via scripts/convert_roundcube_mysql2sqlite (SEC-254).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18449 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo users to execute traceroute via api2 (SEC-244).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18440 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute Cpanel::SPFUI API commands (SEC-246).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18442 CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.1 does not reliably perform suspend/unsuspend operations on accounts (CPANEL-13941).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18431 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows arbitrary file-read operations during File Restoration	2019-08-	not yet	<a href="#">CVE-2018-</a>

	(SEC-436).	01	calculated	<a href="#">20891</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute SSH API commands (SEC-248).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18444</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 does not enforce demo restrictions for SSL API calls (SEC-249).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18445</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows file-read and file-write operations for demo accounts via the SourceIPCheck API (SEC-250).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18446</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via the ClamScanner_getsocket API (SEC-251).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18447</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows certain file-read operations via a Serverinfo_manpage API call (SEC-252).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18448</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows arbitrary zone file modifications during record edits (SEC-426).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20890</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The bin/mkxhostspasswd script in cPanel before 11.54.0.4 discloses password hashes (SEC-73).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10841</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 74.0.0 allows arbitrary zone file modifications because of incorrect CAA record handling (SEC-439).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20892</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 64.0.21, Horde MySQL to SQLite conversion can leak a database password (SEC-234).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18432</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, user and group ownership may be incorrectly set when using reassign_post_terminate_cruft (SEC-294).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18430</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 does not prevent e-mail account suspensions from being applied to unowned accounts (SEC-411).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20934</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows does not preserve security policy questions across an account rename (SEC-223).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18461</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 62.0.17, addon domain conversion did not require a package for resellers (SEC-208).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18455</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows self XSS in the WHM cPAddons showsecurity interface (SEC-217).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18456</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows arbitrary file-read operations via WHM /styled/ URLs (SEC-218).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18457</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows file overwrite when renaming an account (SEC-219).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18458</a> <a href="#">CONFIRM</a>
	cPanel before 62.0.24 allows stored XSS	2019-08-	not yet	<a href="#">CVE-2017-</a>

cpanel -- cpanel	in the WHM cPAddons install interface (SEC-262).	02	calculated	<a href="#">18454 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 does not preserve supplemental groups across account renames (SEC-260).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18453 CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows arbitrary code execution during automatic SSL installation (SEC-221).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18460 CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows arbitrary code execution during account modification (SEC-220).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18459 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows file modification in the context of the root account because of incorrect HTTP authentication (SEC-424).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20888 CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows code execution in the context of the root account via a long DocumentRoot path (SEC-225).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18463 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via Encoding API calls (SEC-242).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18438 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows local users to disable the ClamAV daemon (SEC-409).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20873 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in the WHM "Create a New Account" interface (SEC-428).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20874 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows arbitrary file-write operations in the context of the root account during WHM Force Password Change (SEC-447).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20882 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 insecurely stores phpMyAdmin session files (SEC-418).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20886 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows attackers to read a user's crontab file during a short time interval upon a cPAddon upgrade (SEC-257).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18451 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows certain file-read operations via password file caching (SEC-425).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20889 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows code execution via Rails configuration files (SEC-259).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18452 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo and suspended accounts to use SSH port forwarding (SEC-247).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18443 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows certain file-chmod operations via /scripts/convert_roundcube_mysql2sqlite (SEC-255).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18450 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read root's crontab file during a short time interval upon a post-update task (SEC-352).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20943 CONFIRM</a>
	cPanel before 71.9980.37 allows stored			<a href="#">CVE-</a>



cpanel -- cpanel	XSS in the WHM cPAddons installation interface (SEC-398).	2019-08-01	not yet calculated	<a href="#">2018-20899 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS in via a WHM "Reset a DNS Zone" action (SEC-412).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20935 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows arbitrary file-chmod operations during legacy incremental backups (SEC-338).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20909 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read the SRS secret via exim.conf (SEC-308).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20936 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, Apache HTTP Server domlogs become temporarily world-readable during log processing (SEC-290).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18428 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows stored XSS in the YUM autorepair functionality (SEC-399).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20900 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to make API calls that bypass the cron feature restriction (SEC-427).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20904 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to make API calls that bypass the images feature restriction (SEC-430).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20906 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows .htaccess restrictions bypass when Htaccess Optimization is enabled (SEC-401).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20930 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 does not enforce the Mime::list_hotlinks API feature restriction (SEC-432).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20907 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows arbitrary file-read operations during pkgacct custom template handling (SEC-435).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20908 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows arbitrary file-read and file-unlink operations via WHM style uploads (SEC-378).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20924 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows code injection in the WHM cPAddons interface (SEC-394).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20896 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows local privilege escalation via the WHM Legacy Language File Upload interface (SEC-379).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20925 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows local privilege escalation via the WHM Locale XML Upload interface (SEC-380).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20926 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows jailshell escape because of incorrect crontab parsing (SEC-382).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20927 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via the cpaddons vendor interface (SEC-391).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20928 CONFIRM</a>
				<a href="#">CVE-</a>

cpanel -- cpanel	cPanel before 70.0.23 allows an open redirect via the /unprotected/redirect.html endpoint (SEC-392).	2019-08-01	not yet calculated	<a href="#">2018-20929 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, Apache HTTP Server SSL domain logs can persist on disk after an account termination (SEC-291).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18429 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, weak log-file permissions can occur after account modification (SEC-289).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18427 CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows SQL injection in bin/horde_update_usernames (SEC-71).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10839 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary code execution during locale duplication (SEC-72).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10840 MISC</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows arbitrary file-unlink operations via the cPAddons moderation system (SEC-395).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20897 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows e-mail injection during cPAddons moderation (SEC-396).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20898 CONFIRM</a>
cpanel -- cpanel	In cPanel before 71.9980.37, API tokens retain ACLs after those ACLs are removed from the corresponding accounts (SEC-393).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20895 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows certain file-write operations via the telnetcr script (SEC-356).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20947 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 does not validate database and dbuser names during renames (SEC-321).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20937 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows a user to discover contents of directories (that are not owned by that user) by leveraging backups (SEC-339).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20939 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read root's crontab file during a short time interval upon the enabling of backups (SEC-342).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20940 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows arbitrary file-read operations via restore adminbin (SEC-349).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20941 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read root's crontab file during a short time interval upon configuring crontab (SEC-351).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20942 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read a copy of httpd.conf that is created during a syntax test (SEC-353).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20944 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 makes web-site contents accessible to other local users via Git repositories (SEC-443).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20894 CONFIRM</a>
cpanel -- cpanel	bin/csvprocess in cPanel before 68.0.27 allows insecure file operations (SEC-354).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20945 CONFIRM</a>

cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read zone information because a world-readable archive is created by the archive_sync_zones script (SEC-355).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20946</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 exposes Apache HTTP Server logs after creation of certain domains (SEC-406).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20932</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in cPanel Backup Restoration (SEC-383).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20948</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows demo accounts to execute code via the Landing Page (SEC-405).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20931</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to make API calls that bypass the backup feature restriction (SEC-429).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20905</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows file-rename operations during account renames (SEC-442).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20893</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in WHM Apache Configuration Include Editor (SEC-385).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20949</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 does not enforce ownership during addpkgext and delpkgext WHM API calls (SEC-324).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20938</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 has Stored XSS via an WHM Edit DNS Zone action (SEC-410).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20933</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in the WHM listips interface (SEC-389).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20953</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 creates world-readable files during use of WHM Apache Includes Editor (SEC-388).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20952</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in WHM Spamd Startup Config (SEC-387).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20951</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self stored XSS in WHM Account Transfer (SEC-386).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20950</a> <a href="#">CONFIRM</a>
crypto++ -- crypto++	Crypto++ 8.3.0 and earlier contains a timing side channel in ECDSA signature generation. This allows a local or remote attacker, able to measure the duration of hundreds to thousands of signing operations, to compute the private key used. The issue occurs because scalar multiplication in ecp.cpp (prime field curves, small leakage) and algebra.cpp (binary field curves, large leakage) is not constant time and leaks the bit length of the scalar among other information.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14318</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_and_dwl-8610ap_ax_devices	An issue was discovered on D-Link 6600-AP, DWL-3600AP, and DWL-8610AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated Certificate and RSA Private Key extraction through an insecure	2019-08-01	not yet calculated	<a href="#">CVE-2019-14334</a> <a href="#">MISC</a> <a href="#">MISC</a>

	ssllcert-get.cgi HTTP command.			<a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated dump of all of the config files through a certain admin.cgi?action=insecure HTTP request.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14336</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a pre-authenticated denial of service attack against the access point via a long action parameter to admin.cgi.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14333</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is an ability to escape to a shell in the restricted command line interface, as demonstrated by the `bin/sh -c wget` sequence.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14337</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is use of weak ciphers for SSH such as diffie-hellman-group1-sha1.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14332</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a post-authentication admin.cgi?action=XSS vulnerability on the management interface.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14338</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dva-5592	The web interface of the D-Link DVA-5592 20180823 is vulnerable to XSS because HTML form parameters are directly reflected.	2019-08-02	not yet calculated	<a href="#">CVE-2019-6968</a> <a href="#">MISC</a>
d-link -- dva-5592	The web interface of the D-Link DVA-5592 20180823 is vulnerable to an authentication bypass that allows an unauthenticated user to have access to sensitive information such as the Wi-Fi password and the phone number (if VoIP is in use).	2019-08-02	not yet calculated	<a href="#">CVE-2019-6969</a> <a href="#">MISC</a>
das_q -- das_q	Das Q before 2019-08-02 allows web sites to execute arbitrary code on client machines, as demonstrated by a cross-origin /install request with an attacker-controlled releaseUrl, which triggers download and execution of code within a ZIP archive.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14551</a> <a href="#">MISC</a>
django -- django	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If django.utils.text.Truncator's chars() and words() methods were passed the html=True argument, they were extremely slow to evaluate certain inputs due to a catastrophic backtracking vulnerability in a regular expression. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which were thus vulnerable.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14232</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
django -- django	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If passed certain inputs, django.utils.encoding.uri_to_iri could lead to significant memory usage due to a recursion when repercent-encoding invalid UTF-8 octet sequences.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
	An issue was discovered in Django 1.11.x			

django -- django	before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. Due to the behaviour of the underlying HTMLParser, django.utils.html.strip_tags would be extremely slow to evaluate certain inputs containing large sequences of nested incomplete HTML entities.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14233</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
dnsmasq -- dnsmasq	Improper bounds checking in Dnsmasq before 2.76 allows an attacker controlled DNS server to send large DNS packets that result in a read operation beyond the buffer allocated for the packet, a different vulnerability than CVE-2017-14491.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14513</a> <a href="#">MISC</a>
docker -- docker	In Docker 19.03.x before 19.03.1 linked against the GNU C Library (aka glibc), code injection can occur when the nsswitch facility dynamically loads a library inside a chroot that contains the contents of the container.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14271</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
docker -- docker-credential-helpers	docker-credential-helpers before 0.6.3 has a double free in the List functions.	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020014</a> <a href="#">MISC</a> <a href="#">MISC</a>
dolibarr_foundation -- dolibarr_erp_and_crm	Dolibarr ERP/CRM 9.0.1 provides a module named website that provides for creation of public websites with a WYSIWYG editor. It was identified that the editor also allowed inclusion of dynamic code, which can lead to code execution on the host machine. An attacker has to check a setting on the same page, which specifies the inclusion of dynamic content. Thus, a lower privileged user of the application can execute code under the context and permissions of the underlying web server.	2019-07-29	not yet calculated	<a href="#">CVE-2019-11201</a> <a href="#">MISC</a>
dolibarr_foundation -- dolibarr_erp_and_crm	Dolibarr ERP/CRM 9.0.1 provides a web-based functionality that backs up the database content to a dump file. However, the application performs insufficient checks on the export parameters to mysqldump, which can lead to execution of arbitrary binaries on the server. (Malicious binaries can be uploaded by abusing other functionalities of the application.)	2019-07-29	not yet calculated	<a href="#">CVE-2019-11200</a> <a href="#">MISC</a>
dolibarr_foundation -- dolibarr_erp_and_crm	Dolibarr ERP/CRM 9.0.1 was affected by stored XSS within uploaded files. These vulnerabilities allowed the execution of a JavaScript payload each time any regular user or administrative user clicked on the malicious link hosted on the same domain. The vulnerabilities could be exploited by low privileged users to target administrators. The viewimage.php page did not perform any contextual output encoding and would display the content within the uploaded file with a user-requested MIME type.	2019-07-29	not yet calculated	<a href="#">CVE-2019-11199</a> <a href="#">MISC</a>
draytek -- draytek_routers	DrayTek routers before 2018-05-23 allow CSRF attacks to change DNS or DHCP settings, a related issue to CVE-2017-11649.	2019-07-31	not yet calculated	<a href="#">CVE-2018-20872</a> <a href="#">MISC</a>
	All builds of Eclipse OpenJ9 prior to 0.15 contain a bug where the loop versioner may fail to privatize a value that is pulled out of the loop by versioning - for example if there is a condition that is moved out of the loop that reads a field we may not privatize the value of that field in the			<a href="#">CVE-</a>



eclipse -- openj9	modified copy of the loop allowing the test to see one value of the field and subsequently the loop to see a modified field value without retesting the condition moved out of the loop. This can lead to a variety of different issues but read out of array bounds is one major consequence of these problems.	2019-07-30	not yet calculated	<a href="#">2019-11775</a> <a href="#">CONFIRM</a>
edx -- edx-platform	edx-platform before 2016-06-06 allows CSRF.	2019-07-29	not yet calculated	<a href="#">CVE-2016-10766</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
edx -- edx-platform	edx-platform before 2018-07-18 allows XSS via a response to a Chemical Equation advanced problem.	2019-07-30	not yet calculated	<a href="#">CVE-2018-20859</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
edx -- edx-platform	edx-platform before 2017-08-03 allows attackers to trigger password-reset e-mail messages in which the reset link has an attacker-controlled domain name.	2019-07-30	not yet calculated	<a href="#">CVE-2017-18380</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
edx -- edx-platform	edx-platform before 2016-06-10 allows account activation with a spoofed e-mail address.	2019-07-29	not yet calculated	<a href="#">CVE-2016-10765</a> <a href="#">CONFIRM</a>
edx -- open_edx	The installation process in Open edX before 2017-01-10 exposes a MongoDB instance to external connections with default credentials.	2019-07-30	not yet calculated	<a href="#">CVE-2017-18381</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- apm	A TLS certificate validation flaw was found in Elastic APM agent for Ruby versions before 2.9.0. When specifying a trusted server CA certificate via the 'server_ca_cert' setting, the Ruby agent would not properly verify the certificate returned by the APM server. This could result in a man in the middle style attack against the Ruby agent.	2019-07-30	not yet calculated	<a href="#">CVE-2019-7615</a> <a href="#">MISC</a>
elastic -- elasticsearch	A race condition flaw was found in the response headers Elasticsearch versions before 7.2.1 and 6.8.2 returns to a request. On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.	2019-07-30	not yet calculated	<a href="#">CVE-2019-7614</a> <a href="#">MISC</a>
elastic -- kibana	Kibana versions before 6.8.2 and 7.2.1 contain a server side request forgery (SSRF) flaw in the graphite integration for Timelion visualizer. An attacker with administrative Kibana access could set the timelion:graphite.url configuration option to an arbitrary URL. This could possibly lead to an attacker accessing external URL resources as the Kibana process on the host system.	2019-07-30	not yet calculated	<a href="#">CVE-2019-7616</a> <a href="#">MISC</a>
elm327 -- obd2_bluetooth_device	A clone version of an ELM327 OBD2 Bluetooth device has a hardcoded PIN, leading to arbitrary commands to an OBD-II bus of a vehicle, as demonstrated by turning off the vehicle's lights.	2019-07-31	not yet calculated	<a href="#">CVE-2019-12797</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	SubTypeValidator.java in FasterXML jackson-databind before 2.9.9.2 mishandles default typing when ehcache is	2019-07-29	not yet calculated	<a href="#">CVE-2019-14379</a>

	used, leading to remote code execution.			<a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9.2. This occurs when Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the logback jar in the classpath.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14439</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
foreman -- foreman-tasks	An authentication bypass vulnerability was discovered in foreman-tasks before 0.15.7. Previously, commit tasks were searched through find_resource, which performed authorization checks. After the change to Foreman, an unauthenticated user can view the details of a task through the web UI or API, if they can discover or guess the UUID of the task.	2019-07-31	not yet calculated	<a href="#">CVE-2019-10198</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
freetype -- freetype	In FreeType before 2.6.1, a buffer over-read occurs in type1/t1parse.c on function T1_Get_Private_Dict where there is no check that the new values of cur and limit are sensible before going to Again.	2019-07-30	not yet calculated	<a href="#">CVE-2015-9290</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- evolution-ews	It was discovered evolution-ews before 3.31.3 does not check the validity of SSL certificates. An attacker could abuse this flaw to get confidential information by tricking the user into connecting to a fake server without the user noticing the difference.	2019-08-01	not yet calculated	<a href="#">CVE-2019-3890</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
glibc -- glibc	GnuCOBOL 2.2 has a buffer overflow in cb_evaluate_expr in cobc/field.c via crafted COBOL source code.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14486</a> <a href="#">MISC</a>
glibc -- glibc	GnuCOBOL 2.2 has a stack-based buffer overflow in cb_encode_program_id in cobc/typeck.c via crafted COBOL source code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14541</a> <a href="#">MISC</a>
glibc -- glibc	GnuCOBOL 2.2 has a heap-based buffer overflow in read_literal in cobc/scanner.l via crafted COBOL source code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14528</a> <a href="#">MISC</a>
glibc -- glibc	GnuCOBOL 2.2 has a buffer overflow in cb_push_op in cobc/field.c via crafted COBOL source code.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14468</a> <a href="#">MISC</a>
gnu -- binutils	apply_relocations in readelf.c in GNU Binutils 2.32 contains an integer overflow that allows attackers to trigger a write access violation (in byte_put_little_endian function in elfcomm.c) via an ELF file, as demonstrated by readelf.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14444</a> <a href="#">MISC</a>
gogs -- gogs	routes/api/v1/api.go in Gogs 0.11.86 lacks permission checks for routes: deploy keys, collaborators, and hooks.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14544</a> <a href="#">MISC</a>
happypoint -- happypoint_mobile_app	When processing Deeplink scheme, Happypoint mobile app 6.3.19 and earlier versions doesn't check Deeplink URL correctly. This could lead to javascript code execution, url redirection, sensitive information disclosure. An attacker can exploit this issue by enticing an unsuspecting user to open a specific malicious URL.	2019-08-01	not yet calculated	<a href="#">CVE-2019-9140</a> <a href="#">CONFIRM</a>
hasura -- graphql_engine	graphql-engine (aka Hasura GraphQL Engine) before 1.0.0-beta.3 mishandles the audience check while verifying JWT.	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020015</a> <a href="#">MISC</a>

hewlett_packard_enterprise -- hp2910al-48g_switches	A potential security vulnerability has been identified in HP2910al-48G version W.15.14.0016. The attack exploits an xss injection by setting the attack vector in one of the switch persistent configuration fields (management URL, location, contact). But admin privileges are required to configure these fields thereby reducing the likelihood of exploit. HPE Aruba has provided firmware updates to resolve the vulnerability in HP 2910-48G al Switch. Please update to W.15.14.0017.	2019-08-01	not yet calculated	<a href="#">CVE-2019-5401</a> <a href="#">CONFIRM</a>
humhub -- humhub	HumHub Social Network Kit Enterprise v1.3.13 allows remote attackers to find the user accounts existing on any Social Network Kits (including self-hosted ones) by brute-forcing the username after the /u/ initial URI substring, aka Response Discrepancy Information Exposure.	2019-07-29	not yet calculated	<a href="#">CVE-2019-12743</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- i2_intelligent_analysis_platform	IBM i2 Intelligent Analysis Platform 9.0.0 through 9.1.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 157007.	2019-07-30	not yet calculated	<a href="#">CVE-2019-4062</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3, 1.1.3.1, and 1.1.3.2 could allow an unauthorized local user to create unique catalog names that could cause a denial of service. IBM X-Force ID: 160296.	2019-08-02	not yet calculated	<a href="#">CVE-2019-4275</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- spectrum_protect_for_enterprise_resource_planning	IBM Spectrum Protect for Enterprise Resource Planning 7.1 and 8.1, if tracing is activated, the IBM Spectrum Protect node password may be displayed in plain text in the ERP trace file. IBM X-Force ID: 154280.	2019-08-02	not yet calculated	<a href="#">CVE-2018-1987</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
imgix -- imgix	Imgix through 2019-06-19 allows remote attackers to cause a denial of service (resource consumption) by manipulating a small JPEG file to specify dimensions of 64250x64250 pixels, which is mishandled during an attempt to load the 'whole image' into memory.	2019-07-29	not yet calculated	<a href="#">CVE-2019-13655</a> <a href="#">MISC</a>
jolokia -- jolokia	A flaw was found in Jolokia versions from 1.2 to before 1.6.1. Affected versions are vulnerable to a system-wide CSRF. This holds true for properly configured instances with strict checking for origin and referrer headers. This could result in a Remote Code Execution attack.	2019-08-01	not yet calculated	<a href="#">CVE-2018-10899</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
libav -- libav	An issue was discovered in Libav 12.3. An access violation allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv. This is related to ff_mpa_synth_filter_float in avcodec/mpegaudioldsp_template.c.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14441</a> <a href="#">MISC</a>
libav -- libav	In mpc8_read_header in libavformat/mpc8.c in Libav 12.3, an input file can result in an avio_seek infinite loop and hang, with 100% CPU consumption. Attackers could leverage this vulnerability to cause a denial of service via a crafted file.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14442</a> <a href="#">MISC</a>
liblouis -- l louis	A vulnerability was found in l louis, versions 2.5.x before 2.5.4. A stack-based buffer overflow was found in findTable() in l louis. An attacker could create a malicious file that would cause applications that use liblouis (such as	2019-08-02	not yet calculated	<a href="#">CVE-2014-8184</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	Orca) to crash, or potentially execute arbitrary code when opened.			
libopenmpt -- libopenmpt	J2B in libopenmpt before 0.4.2 allows an assertion failure during file parsing with debug STLs.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14383</a> <a href="#">MISC</a>
libopenmpt -- libopenmpt	l bopenmpt before 0.3.11 allows a crash with certain malformed custom tunings in MPTM files.	2019-07-30	not yet calculated	<a href="#">CVE-2018-20861</a> <a href="#">MISC</a>
libopenmpt -- libopenmpt	DSM in libopenmpt before 0.4.2 allows an assertion failure during file parsing with debug STLs.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14382</a> <a href="#">MISC</a>
libopenmpt -- libopenmpt	l bopenmpt before 0.4.3 allows a crash due to a NULL pointer dereference when doing a portamento from an OPL instrument to an empty instrument note map slot.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14381</a> <a href="#">CONFIRM</a>
libvirtd -- libvirtd	It was discovered that libvirtd before versions 4.10.1 and 5.4.1 would permit read-only clients to use the virDomainSaveImageGetXMLDesc() API, specifying an arbitrary path which would be accessed with the permissions of the l bvirtd process. An attacker with access to the l bvirtd socket could use this to probe the existence of arbitrary files, cause denial of service or cause l bvirtd to execute arbitrary programs.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10161</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
libvirtd -- libvirtd	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit read-only clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10166</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
libvirt -- libvirt	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() l bvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, l bvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing l bvirtd to execute a crafted executable with its own privileges.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10168</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
libvirt -- libvirt	The virConnectGetDomainCapabilities() l bvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing l bvirtd to execute a crafted executable with its own privileges.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10167</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an ioctl was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw	2019-07-30	not yet calculated	<a href="#">CVE-2019-10142</a> <a href="#">CONFIRM</a>

	to crash the system, corrupt memory, or create other adverse security affects.			
linux -- linux_kernel	A flaw was found in the Linux kernel's NFS implementation, all versions 3.x and all versions 4.x up to 4.20. An attacker, who is able to mount an exported NFS filesystem, is able to trigger a null pointer dereference by using an invalid NFS sequence. This can panic the machine and deny access to the NFS server. Any outstanding disk writes to the NFS server will be lost.	2019-07-30	not yet calculated	<a href="#">CVE-2018-16871</a> <a href="#">CONFIRM</a>
magento -- magento	A file upload filter bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with admin privileges to edit configuration keys to remove file extension filters, potentially resulting in the malicious upload and execution of malicious files on the server.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7912</a> <a href="#">CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 due to insufficient authorizations checks. This can be abused by a user with admin privileges to add users to company accounts or modify existing user details.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7872</a> <a href="#">CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can result in unintended deletion of user roles.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7874</a> <a href="#">CONFIRM</a>
magento -- magento	An access control bypass vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An unauthenticated user can bypass access controls via REST API calls to assign themselves to an arbitrary company, thereby gaining read access to potentially confidential information.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7950</a> <a href="#">CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can lead to unintended data deletion from customer pages.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7851</a> <a href="#">CONFIRM</a>
magento -- magento	A denial-of-service vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. Under certain conditions, an unauthenticated attacker could force the Magento store's full page cache to serve a 404 page to customers.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7915</a> <a href="#">CONFIRM</a>
magento -- magento	An information disclosure vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to create email templates could leak sensitive data via a malicious email template.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7888</a> <a href="#">CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to access shipment settings can execute arbitrary code via server-side request forgery.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7892</a> <a href="#">CONFIRM</a>
	An Insecure Direct Object Reference (IDOR) vulnerability exists in the order			



magento -- magento	processing workflow of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can lead to unauthorized access to order details.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7890 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to layouts can execute arbitrary code through a combination of product import, crafted csv file and XML layout update.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7896 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to layouts can execute arbitrary code through a crafted XML layout update.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7895 CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can cause unwanted items to be added to a shopper's cart due to an insufficiently robust anti-CSRF token implementation.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7857 CONFIRM</a>
magento -- magento	A cryptographic flaw in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could be abused by an unauthenticated user to discover an invariant used in gift card generation.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7855 CONFIRM</a>
magento -- magento	A path disclosure vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. Requests for a specific file path could result in a redirect to the URL of the Magento admin panel, disclosing its location to potentially unauthorized parties.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7852 CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can lead to unauthorized disclosure of company credit history details.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7854 CONFIRM</a>
magento -- magento	A path traversal vulnerability in the WYSIWYG editor for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could result in unauthorized access to uploaded images due to insufficient access control.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7859 CONFIRM</a>
magento -- magento	A server-side request forgery (SSRF) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by authenticated user with admin privileges to manipulate shipment settings to execute arbitrary code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7923 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to email templates can execute arbitrary code by previewing a malicious template.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7903 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to create or edit a product	2019-08-02	not yet calculated	<a href="#">CVE-2019-7942 CONFIRM</a>

	can execute arbitrary code via malicious XML layout updates.			
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to edit product content pages to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7927 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify node attributes to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7926 CONFIRM</a>
magento -- magento	An information leakage vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. A SOAP web service endpoint does not properly enforce parameters related to access control. This could be abused to leak customer information via crafted SOAP requests.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7951 CONFIRM</a>
magento -- magento	Insufficient enforcement of user access controls in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could enable a low-privileged user to make unauthorized environment configuration changes.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7904 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify content block titles to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7936 CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an administrator with limited privileges to delete the downloadable products folder.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7925 CONFIRM</a>
magento -- magento	A reflected cross-site scripting vulnerability exists on the customer cart checkout page of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by sending a victim a crafted URL that results in malicious javascript execution in the victim's browser.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7939 CONFIRM</a>
magento -- magento	An information leakage vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges may be able to view metadata of a trusted device used by another administrator via a crafted http request.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7929 CONFIRM</a>
magento -- magento	A denial-of-service (DoS) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. By abusing insufficient brute-forcing defenses in the token exchange protocol, an unauthenticated attacker could disrupt transactions between the Magento merchant and PayPal.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7928 CONFIRM</a>
	A file upload restriction bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2			

magento -- magento	prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to the import feature can make modifications to a configuration file, resulting in potentially unauthorized removal of file upload restrictions. This can result in arbitrary code execution when a malicious file is then uploaded and executed on the system.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7930 CONFIRM</a>
magento -- magento	A cryptographic flaw in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9 and Magento 2.3 prior to 2.3.2 resulted in storage of sensitive information with an algorithm that is insufficiently resistant to brute force attacks.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7858 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to store product attributes to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7937 CONFIRM</a>
magento -- magento	A cryptographically weak pseudo-random number generator is used in multiple security relevant contexts in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7860 CONFIRM</a>
magento -- magento	A security bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 that could be abused to execute arbitrary PHP code. An authenticated user can bypass security protections that prevent arbitrary PHP script upload via form data injection.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7871 CONFIRM</a>
magento -- magento	Insufficient server-side validation of user input could allow an attacker to bypass file upload restrictions in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7861 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to edit Product information via the TinyMCE editor.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7866 CONFIRM</a>
magento -- magento	A cryptographic flaw exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. A weak cryptographic mechanism is used to generate the initialization vector in multiple security relevant contexts.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7886 CONFIRM</a>
magento -- magento	Insufficient input validation in the config builder of the Elastic search module could lead to remote code execution in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This vulnerability could be abused by an authenticated user with the ability to configure the catalog search.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7885 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to marketing email templates to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7880 CONFIRM</a>
	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9,			<a href="#">CVE-</a>

magento -- magento	Magento 2.3 prior to 2.3.2. An authenticated user with privileges to manage orders can inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">2019-7877 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the product catalog form of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to the product catalog to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7921 CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can result in unintended deletion of the store design schedule.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7873 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to manipulate layouts can insert a malicious payload into the layout.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7876 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with permissions to manage customer groups.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7869 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with permissions to manage tax rules.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7868 CONFIRM</a>
magento -- magento	A server-side request forgery (SSRF) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with admin privileges to manipulate shipment methods to execute arbitrary code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7913 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to manage orders and order status.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7867 CONFIRM</a>
magento -- magento	A reflected cross-site scripting vulnerability exists in the Product widget chooser functionality in the admin panel for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7862 CONFIRM</a>
magento -- magento	A cross-site request forgery (CSRF) vulnerability exists in the checkout cart item of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited at the time of editing or configuration.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7865 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to the tax notifications configuration in the Magento admin panel.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7853 CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability exists in the RSS feeds of Magento 2.1 prior to 2.1.18, Magento 2.2	2019-08-	not yet	<a href="#">CVE-2019-7864</a>

	prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can lead to unauthorized access to order details.	02	calculated	<a href="#">CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify product information.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7908 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to products and categories.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7863 CONFIRM</a>
magento -- magento_and_magento_commerce	A defense-in-depth check was added to mitigate inadequate session validation handling by 3rd party checkout modules. This impacts Magento 1.x prior to 1.9.4.2, Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9 and Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7849 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to customer configurations to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7897 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the WYSIWYG editor of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to the editor can inject malicious SWF files.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7882 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to email templates.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7909 CONFIRM</a>
magento -- multiple_products	A server-side request forgery (SSRF) vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to the admin panel to manipulate system configuration and execute arbitrary code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7911 CONFIRM</a>
magento -- multiple_products	A remote code execution vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to create sitemaps can execute arbitrary PHP code by creating a malicious sitemap file.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7932 CONFIRM</a>
magento -- multiple_products	A cross-site scripting mitigation bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3	2019-08-	not yet	<a href="#">CVE-2019-7881</a>



	prior to 2.3.2. This could be exploited by an authenticated user to escalate privileges (admin vs. admin XSS attack).	02	calculated	<a href="#">CONFIRM</a>
magento -- multiple_products	Names of disabled downloadable products could be disclosed due to inadequate validation of user input in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7899 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to edit newsletter templates to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7934 CONFIRM</a>
magento -- multiple_products	Samples of disabled downloadable products are accessible in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 due to inadequate validation of user input.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7898 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to modify currency symbols can inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7945 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify content page titles to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7935 CONFIRM</a>
magento -- multiple_products	A cross-site request forgery vulnerability exists in the GiftCardAccount removal feature for Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7947 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify catalog price rules to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7938 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify store currency options to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7940 CONFIRM</a>
	An injection vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento			

magento -- multiple_products	Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with marketing manipulation privileges can invoke methods that alter data of the underlying model followed by corresponding database modifications.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7889 CONFIRM</a>
magento -- multiple_products	A reflected cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 when the feature that adds a secret key to the Admin URL is disabled.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7887 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to newsletter templates.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7875 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the product comments field of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to the Return Product comments field can inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7944 CONFIRM</a>
matrixssl -- matrixssl	In MatrixSSL 3.8.3 Open through 4.2.1 Open, the DTLS server mishandles incoming network messages leading to a heap-based buffer overflow of up to 256 bytes and possible Remote Code Execution in parseSSLHandshake in sslDecode.c. During processing of a crafted packet, the server mishandles the fragment length value provided in the DTLS message.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14431 MISC</a>
mi kytracker -- milkytracker	ModuleEditor::convertInstrument in tracker/ModuleEditor.cpp in Mi kyTracker 1.02.00 has a heap-based buffer overflow.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14497 MISC</a>
mi kytracker -- milkytracker	LoaderXM::load in LoaderXM.cpp in milkyplay in Mi kyTracker 1.02.00 has a stack-based buffer overflow.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14496 MISC</a>
mi kytracker -- milkytracker	XMFile::read in XMFile.cpp in mi kyplay in MilkyTracker 1.02.00 has a heap-based buffer overflow.	2019-07-31	not yet calculated	<a href="#">CVE-2019-14464 MISC</a>
misskey -- misskey	Misskey before 10.102.4 allows h jacking a user's token.	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020010 MISC</a>
netapp -- data_ontap_7-mode	Data ONTAP operating in 7-Mode versions prior to 8.2.5P3 may disclose sensitive LDAP account information to unauthenticated remote attackers.	2019-08-02	not yet calculated	<a href="#">CVE-2019-5501 CONFIRM</a>
netapp -- data_ontap_7-mode	Data ONTAP operating in 7-Mode versions prior to 8.2.5P3 are susceptible to a vulnerability which discloses information to an unauthenticated attacker. A successful attack requires that multiple non-default options be enabled.	2019-08-02	not yet calculated	<a href="#">CVE-2019-5493 CONFIRM</a>
	A stack-based buffer overflow in the upnpd			

netgear -- n600_wifi_dual_band_router	binary running on NETGEAR WNDR3400v3 routers with firmware version 1.0.1.18_1.0.63 allows an attacker to remotely execute arbitrary code via a crafted UPnP SSDP packet.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14363</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Bypass lock protection in the Nextcloud Android app prior to version 3.6.2 causes leaking of thumbnails when requesting the Android content provider although the lock protection was not solved.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5452</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Bypassing lock protection exists in Nextcloud Android app 3.6.0 when creating a multi-account and aborting the process.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5455</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	SQL Injection in the Nextcloud Android app prior to version 3.0.0 allows to destroy a local cache when a harmful query is executed requiring to resetup the account.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5454</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Bypass lock protection in the Nextcloud Android app prior to version 3.3.0 allowed access to files when being prompted for the lock protection and switching to the Nextcloud file provider.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5453</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Improper sanitization of HTML in directory names in the Nextcloud Android app prior to version 3.7.0 allowed to style the directory name in the header bar when using basic HTML.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5450</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Bypass lock protection in the Nextcloud Android app prior to version 3.6.1 allows accessing the files when repeatedly opening and closing the app in a very short time.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5451</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A missing check in the Nextcloud Server prior to version 15.0.1 causes leaking of calendar event names when adding or modifying confidential or private events.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5449</a> <a href="#">MISC</a>
nfdump -- nfdump	nfdump 1.6.17 and earlier is affected by an integer overflow in the function Process_ipfix_template_withdraw in ipfix.c that can be abused in order to crash the process remotely (denial of service).	2019-07-31	not yet calculated	<a href="#">CVE-2019-14459</a> <a href="#">MISC</a> <a href="#">MISC</a>
one_identity -- cloud_access_manager	One Identity Cloud Access Manager 8.1.3 does not use HTTP Strict Transport Security (HSTS), which may allow man-in-the-middle (MITM) attacks. This issue is fixed in version 8.1.4.	2019-07-29	not yet calculated	<a href="#">CVE-2019-13498</a> <a href="#">CONFIRM</a>
openbravo -- openbravo_erp	Openbravo ERP before 3.0PR19Q1.3 is affected by Directory Traversal. This vulnerability could allow remote authenticated attackers to replace a file on the server via the getAttachmentDirectoryForNewAttachment inpKey value.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14362</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read in the function cv::predictOrdered<cv::HaarEvaluator> in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14491</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An issue was discovered in OpenCV before 4.1.1. There is a NULL pointer dereference in the function cv::XMLParser::parse at modules/core/src/persistence.cpp.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14493</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read/write in the function HaarEvaluator::OptFeature::calc in	2019-08-01	not yet calculated	<a href="#">CVE-2019-14492</a> <a href="#">MISC</a>

	modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.			<a href="#">MISC</a> <a href="#">MISC</a>
openemr -- openemr	OpenEMR before 5.0.2 allows SQL Injection in interface/forms/eye_mag/save.php.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14529</a> <a href="#">MISC</a>
opengear -- console_server	Opengear console server firmware releases prior to 4.5.0 have a stored XSS vulnerability related to serial port logging. If a malicious user of an external system (connected to a serial port on an Opengear console server) sends crafted text to a serial port (that has logging enabled), the text will be replayed when the logs are viewed. Exploiting this vulnerability requires access to the serial port and/or console server.	2019-07-31	not yet calculated	<a href="#">CVE-2019-14456</a> <a href="#">MISC</a>
openssl -- openssl	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, 'usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).	2019-07-30	not yet calculated	<a href="#">CVE-2019-1552</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
openstack -- openstack-ironic-inspector	A vulnerability was found in openstack-ironic-inspector all versions excluding 5.0.2, 6.0.3, 7.2.4, 8.0.3 and 8.2.1. A SQL-injection vulnerability was found in openstack-ironic-inspector's node_cache.find_node(). This function makes a SQL query using unfiltered data from a server reporting inspection results (by a POST to the /v1/continue endpoint). Because the API is unauthenticated, the flaw could be exploited by an attacker with access to the network on which ironic-inspector is listening. Because of how ironic-inspector uses the query results, it is unlikely that data could be obtained. However, the attacker could pass malicious data and create a denial of service.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10141</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

oxid -- oxid_eshop	OXID eShop 6.0.x before 6.0.5 and 6.1.x before 6.1.4 allows SQL Injection via a crafted URL, leading to full access by an attacker. This includes all shopping cart options, customer data, and the database. No interaction between the attacker and the victim is necessary.	2019-07-30	not yet calculated	<a href="#">CVE-2019-13026</a> <a href="#">CONFIRM</a>
pandao -- editor.md	pandao Editor.md 1.5.0 allows XSS via the <code>Javas&amp;#99;ript: string</code> .	2019-08-01	not yet calculated	<a href="#">CVE-2019-14517</a> <a href="#">MISC</a>
pandao -- editor.md	pandao Editor.md 1.5.0 allows XSS via an attribute of an ABBR or SUP element.	2019-08-03	not yet calculated	<a href="#">CVE-2019-14653</a> <a href="#">MISC</a>
pdfresurrect -- pdfresurrect	PDFResurrect 0.15 has a buffer overflow via a crafted PDF file because data associated with startxref and %%EOF is mishandled.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14267</a> <a href="#">MISC</a> <a href="#">MISC</a>
pixman -- pixman	An integer overflow issue has been reported in the <code>general_composite_rect()</code> function in pixman prior to version 0.32.8. An attacker could exploit this issue to cause an application using pixman to crash or, potentially, execute arbitrary code.	2019-07-31	not yet calculated	<a href="#">CVE-2015-5297</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
planon -- planon	Planon before Live Build 41 has XSS.	2019-07-29	not yet calculated	<a href="#">CVE-2018-18570</a> <a href="#">MISC</a>
podman -- podman	A path traversal vulnerability has been discovered in podman before version 1.4.0 in the way it handles symlinks inside containers. An attacker who has compromised an existing container can cause arbitrary files on the host filesystem to be read/written when an administrator tries to copy a file from/to the container.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10152</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
polycom -- multiple_products	A vulnerability in the web-based management interface of VVX, Trio, SoundStructure, SoundPoint, and SoundStation phones running Polycom UC Software, if exploited, could allow an authenticated, remote attacker with admin privileges to cause a denial of service (DoS) condition or execute arbitrary code.	2019-07-29	not yet calculated	<a href="#">CVE-2019-12948</a> <a href="#">CONFIRM</a>
polycom -- obihai_obi1022_voip_phone	On the Polycom Obihai Obi1022 VoIP phone with firmware 5.1.11, a command injection (missing input validation) issue in the NTP server IP address field for the "Time Service Settings web" interface allows an authenticated remote attacker in the same network to trigger OS commands via shell commands in a POST request.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14259</a> <a href="#">MISC</a>
poppler -- poppler	An issue was discovered in Poppler through 0.78.0. There is a divide-by-zero error in the function <code>SplashOutputDev::tilingPatternFill</code> at <code>SplashOutputDev.cc</code> .	2019-08-01	not yet calculated	<a href="#">CVE-2019-14494</a> <a href="#">MISC</a> <a href="#">MISC</a>
postgresql -- postgresql	A vulnerability was found in PostgreSQL versions 11.x up to excluding 11.3, 10.x up to excluding 10.8, 9.6.x up to, excluding 9.6.13, 9.5.x up to, excluding 9.5.17. PostgreSQL maintains column statistics for tables. Certain statistics, such as histograms and lists of most common values, contain values taken from the column. PostgreSQL does not evaluate row security policies before consulting	2019-07-30	not yet calculated	<a href="#">CVE-2019-10130</a>



	those statistics during query planning; an attacker can exploit this to read the most common values of certain columns. Affected columns are those for which the attacker has SELECT privilege and for which, in an ordinary query, row-level security prunes the set of rows visible to the attacker.			<a href="#">CONFIRM</a> <a href="#">MISC</a>
powerdns -- authoritative_server	A Vulnerability has been found in PowerDNS Authoritative Server before versions 4.1.9, 4.0.8 allowing a remote, authorized master server to cause a high CPU load or even prevent any further updates to any slave zone by sending a large number of NOTIFY messages. Note that only servers configured as slaves are affected by this issue.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10163</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
powerdns -- authoritative_server	A vulnerability has been found in PowerDNS Authoritative Server before versions 4.1.10, 4.0.8 allowing an authorized user to cause the server to exit by inserting a crafted record in a MASTER type zone under their control. The issue is due to the fact that the Authoritative Server will exit when it runs into a parsing error while looking up the NS/A/AAAA records it is about to use for an outgoing notify.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10162</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
printer-on -- printer-on_central_print_services	An issue was discovered in PrinterOn Central Print Services (CPS) through 4.1.4. A user without valid credentials can bypass the authentication process, obtaining a valid session cookie with guest/pseudo-guest level privileges. This cookie can then be further used to perform other attacks.	2019-07-29	not yet calculated	<a href="#">CVE-2018-17213</a> <a href="#">MISC</a>
printer-on -- printer-on_central_print_services	An issue was discovered in PrinterOn Central Print Services (CPS) through 4.1.4. An unauthenticated attacker can view details about the printers associated with CPS via a crafted HTTP GET request.	2019-07-29	not yet calculated	<a href="#">CVE-2018-17211</a> <a href="#">MISC</a>
rancher -- rancher	An issue was discovered that affects the following versions of Rancher: v2.0.0 through v2.0.13, v2.1.0 through v2.1.8, and v2.2.0 through 2.2.1. When Rancher starts for the first time, it creates a default admin user with a well-known password. After initial setup, the Rancher administrator may choose to delete this default admin user. If Rancher is restarted, the default admin user will be recreated with the well-known default password. An attacker could exploit this by logging in with the default admin credentials. This can be mitigated by deactivating the default admin user rather than completing deleting them.	2019-07-30	not yet calculated	<a href="#">CVE-2019-11202</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openshift_container_platform	A flaw was found in OpenShift Container Platform, versions 3.11 and later, in which the CSRF tokens used in the cluster console component were found to remain static during a user's session. An attacker with the ability to observe the value of this token would be able to re-use the token to perform a CSRF attack.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10176</a> <a href="#">CONFIRM</a>
red_hat -- atomic-openshift	A vulnerability exists in the garbage collection mechanism of atomic-openshift. An attacker able to spoof the UUID of a valid object from another namespace is able to delete children of those objects. Versions 3.6, 3.7, 3.8, 3.9, 3.10, 3.11 and 4.1 are	2019-08-01	not yet calculated	<a href="#">CVE-2019-3884</a> <a href="#">CONFIRM</a>

	affected.			
red_hat -- enterprise_linux	It was found that the fix for CVE-2018-14648 in 389-ds-base, versions 1.4.0.x before 1.4.0.17, was incorrectly applied in RHEL 7.5. An attacker would still be able to provoke excessive CPU consumption leading to a denial of service.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10171</a> CONFIRM
red_hat -- openshift_container_platform	OpenShift Container Platform before version 4.1.3 writes OAuth tokens in plaintext to the audit logs for the Kubernetes API server and OpenShift API server. A user with sufficient privileges could recover OAuth tokens from these audit logs and use them to access other resources.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10165</a> CONFIRM CONFIRM CONFIRM
red_hat -- openstack_platform	A flaw was discovered in the python-novajoin plugin, all versions up to, excluding 1.1.1, for Red Hat OpenStack Platform. The novajoin API lacked sufficient access control, allowing any keystone authenticated user to generate FreeIPA tokens.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10138</a> CONFIRM MISC
red_hat -- satellite	It was found that foreman, versions 1.x.x before 1.15.6, in Satellite 6 did not properly enforce access controls on certain resources. An attacker with access to the API and knowledge of the resource name can access resources in other organizations.	2019-08-01	not yet calculated	<a href="#">CVE-2014-8183</a> CONFIRM
samba -- heimdal_kdc	A flaw was found in samba's Heimdal KDC implementation, versions 4.8.x up to, excluding 4.8.12, 4.9.x up to, excluding 4.9.8 and 4.10.x up to, excluding 4.10.3, when used in AD DC mode. A man in the middle attacker could use this flaw to intercept the request to the KDC and replace the user name (principal) in the request with any desired user name (principal) that exists in the KDC effectively obtaining a ticket for that principal.	2019-07-31	not yet calculated	<a href="#">CVE-2018-16860</a> CONFIRM MISC
sas -- sas_drug_development	SAS Drug Development (SDD) before 32DRG02 mishandles logout actions, which allows a user (who was previously logged in) to access resources by pressing a back or forward button in a web browser.	2019-07-31	not yet calculated	<a href="#">CVE-2007-6763</a> MISC
schism_tracker -- schism_tracker	fmt_mtm_load_song in fmt/mtm.c in Schism Tracker 20190722 has a heap-based buffer overflow.	2019-07-31	not yet calculated	<a href="#">CVE-2019-14465</a> MISC
schism_tracker -- schism_tracker	An issue was discovered in Schism Tracker through 20190722. There is a heap-based buffer overflow via a large number of song patterns in fmt_mtm_load_song in fmt/mtm.c, a different vulnerability than CVE-2019-14465.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14524</a> MISC
schism_tracker -- schism_tracker	An issue was discovered in Schism Tracker through 20190722. There is an integer underflow via a large plen in fmt_okt_load_song in the Amiga Oktalyzer parser in fmt/okt.c.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14523</a> MISC
sdl2_image -- sdl2_image	An exploitable code execution vulnerability exists in the XPM image rendering function of SDL2_image 2.0.4. A specially crafted XPM image can cause an integer overflow in the colorhash function, allocating too small of a buffer. This buffer can then be written out of bounds, resulting in a heap overflow, ultimately ending in code execution. An attacker can display a	2019-07-31	not yet calculated	<a href="#">CVE-2019-5060</a> MISC

	<p>specialy crafted image to trigger this vulnerability.</p>			
siemens -- siprotec_5_devices	<p>A vulnerability has been identified in Ethernet plug-in communication modules for SIPROTEC 5 devices with CPU variants CP200 (All versions), SIPROTEC 5 devices with CPU variants CP300 (All versions). An unauthenticated attacker with network access to the device could potentially insert arbitrary code which is executed before firmware verification in the device.</p>	2019-08-02	not yet calculated	<a href="#">CVE-2019-10938</a> <a href="#">MISC</a>
sigil_ebook -- sigil	<p>Sigil before 0.9.16 is vulnerable to a directory traversal, allowing attackers to write arbitrary files via a ../ (dot dot slash) in a ZIP archive entry that is mishandled during extraction.</p>	2019-07-30	not yet calculated	<a href="#">CVE-2019-14452</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
sleuthkit -- sleuthkit	<p>An issue was discovered in The Sleuth Kit (TSK) 4.6.6. There is an off-by-one overwrite due to an underflow on tools/hashtools/hfind.cpp while using a bogus hash table.</p>	2019-08-02	not yet calculated	<a href="#">CVE-2019-14532</a> <a href="#">MISC</a>
sleuthkit -- sleuthkit	<p>An issue was discovered in The Sleuth Kit (TSK) 4.6.6. There is an out of bounds read on iso9660 while parsing System Use Sharing Protocol data in fs/iso9660.c.</p>	2019-08-02	not yet calculated	<a href="#">CVE-2019-14531</a> <a href="#">MISC</a>
smokedetector -- smokedetector	<p>SmokeDetector intentionally does automatic deployments of updated copies of SmokeDetector without server operator authority.</p>	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020011</a> <a href="#">MISC</a>
softether_vpn -- softethervpn	<p>See.sys through 4.25 in the SoftEther VPN Server allows a user to specify any kernel address to which arbitrary bytes are written.</p>	2019-07-29	not yet calculated	<a href="#">CVE-2019-11868</a> <a href="#">MISC</a> <a href="#">MISC</a>
sonos -- zoneplayer	<p>ZInsVX.dll ActiveX Control 2018.02 and earlier in Zoneplayer contains a vulnerability that could allow remote attackers to execute arbitrary files by setting the arguments to the ActiveX method. This can be leveraged for remote code execution.</p>	2019-08-02	not yet calculated	<a href="#">CVE-2019-9141</a> <a href="#">CONFIRM</a>
ssdp_responder -- ssdp_responder	<p>SSDP Responder 1.x through 1.5 mishandles incoming network messages, leading to a stack-based buffer overflow by 1 byte. This results in a crash of the server, but only when strict stack checking is enabled. This is caused by an off-by-one error in ssdp_recv in ssdpd.c.</p>	2019-07-28	not yet calculated	<a href="#">CVE-2019-14323</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	<p>Symantec Endpoint Protection, prior to 14.2 RU1 &amp; 12.1 RU6 MP10 and Symantec Endpoint Protection Small Business Edition, prior to 12.1 RU6 MP10c (12.1.7491.7002), may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.</p>	2019-07-31	not yet calculated	<a href="#">CVE-2019-12750</a> <a href="#">MISC</a>
terracotta -- quartz_scheduler	<p>initDocumentParser in xml/XMLSchedulingDataProcessor.java in Terracotta Quartz Scheduler through 2.3.0 allows XXE attacks via a job description.</p>	2019-07-26	not yet calculated	<a href="#">CVE-2019-13990</a> <a href="#">MISC</a>

the_pallets_project -- werkzeug	In Pallets Werkzeug before 0.15.5, SharedDataMiddleware mishandles drive names (such as C:) in Windows pathnames.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14322</a> <a href="#">MISC</a>
unifi -- network_controller	SMTP MITM refers to a malicious actor setting up an SMTP proxy server between the UniFi Controller version <= 5.10.21 and their actual SMTP server to record their SMTP credentials for malicious use later.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5456</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
univa -- grid_engine	In Univa Grid Engine before 8.6.3, when configured for Docker jobs and execd spooling on root_squash, weak file permissions ("other" write access) occur in certain cases (GE-6890).	2019-07-30	not yet calculated	<a href="#">CVE-2018-20871</a> <a href="#">MISC</a>
veritas -- veritas_resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. When uploading an application bundle, a directory traversal vulnerability allows a VRP user with sufficient privileges to overwrite any file in the VRP virtual machine. A malicious VRP user could use this to replace existing files to take control of the VRP virtual machine.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14418</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
vlc -- media_player	Double Free in VLC versions <= 3.0.6 leads to a crash.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5460</a> <a href="#">MISC</a>
vlc -- media_player	An Integer underflow in VLC Media Player versions < 3.0.7 leads to an out-of-band read.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5459</a> <a href="#">MISC</a>
wallacepos -- wallacepos	Unrestricted upload of file with dangerous type in WallacePOS 1.4.3 allows a remote, authenticated attacker to execute arbitrary code by uploading a malicious PHP file.	2019-07-31	not yet calculated	<a href="#">CVE-2019-3960</a> <a href="#">MISC</a>
windu -- windu_cms	Windu CMS 2.2 allows CSRF via admin/users/?mn=admin.message.error to add an admin account.	2019-08-01	not yet calculated	<a href="#">CVE-2013-7473</a> <a href="#">MISC</a>
windu -- windu_cms	Windu CMS 2.2 allows XSS via the name parameter to admin/content/edit or admin/content/add, or the username parameter to admin/users.	2019-08-01	not yet calculated	<a href="#">CVE-2013-7474</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Fastest Cache plugin through 0.8.9.5 for WordPress allows wpFastestCache.php and inc/cache.php Directory Traversal.	2019-07-30	not yet calculated	<a href="#">CVE-2019-13635</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The Adenion Blog2Social plugin through 5.5.0 for WordPress allows SQL Injection.	2019-08-01	not yet calculated	<a href="#">CVE-2019-13572</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	A SQL injection vulnerability exists in the Vsourz Digital Advanced CF7 DB plugin through 1.6.1 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system.	2019-07-29	not yet calculated	<a href="#">CVE-2019-13571</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Simple Membership plugin before 3.8.5 for WordPress has CSRF affecting the Bulk Operation section.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An exploitable denial of service vulnerability exists in the object lookup			

yara -- yara	functionality of Yara 3.8.1. A specially crafted binary file can cause a negative value to be read to satisfy an assert, resulting in Denial of Service. An attacker can create a malicious binary to trigger this vulnerability.	2019-07-31	not yet calculated	<a href="#">CVE-2019-5020</a> <a href="#">MISC</a>
yarn -- yarn	Yarn before 1.17.3 is vulnerable to Missing Encryption of Sensitive Data due to HTTP URLs in lockfile causing unencrypted authentication data to be sent over the network.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5448</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zurmo -- zurmo	Zurmo 3.2.7-2 has XSS via the app/index.php/zurmo/default PATH_INFO.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14472</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to tmcginnis@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870





**From:** [US-CERT](#)  
**To:** [wqutarte@ci.sunnyvale.ca.us](mailto:wqutarte@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of July 29, 2019  
**Date:** Monday, August 05, 2019 2:07 55 PM



National Cyber Awareness System:

## [Vulnerability Summary for the Week of July 29, 2019](#)

08/05/2019 06:36 AM EDT

Original release date: August 5, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the NIST [NVD](#). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
10web -- photo_gallery	A SQL injection vulnerability exists in the 10Web Photo Gallery plugin before 1.5.31 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via filemanager/model.php.	2019-07-30	<a href="#">10.0</a>	<a href="#">CVE-2019-14313</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. On the /cbs/system/ShowAdvanced.do "File Explorer" screen, it is possible to change the directory in the JavaScript code. If changed to (for example) "C:" then one can browse the whole server.	2019-07-26	<a href="#">7.8</a>	<a href="#">CVE-2019-10265</a> <a href="#">MISC</a>
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. When sending an out-of-bounds XML document to a URL, it is possible to read the file structure and even the content of files without authentication.	2019-07-26	<a href="#">7.8</a>	<a href="#">CVE-2019-10266</a> <a href="#">MISC</a> <a href="#">MISC</a>
ahsay -- cloud_backup_suite	An insecure file upload and code execution issue was discovered in Ahsay Cloud Backup Suite 8.1.0.50. It is possible to upload a file into any directory of the server. One can insert a JSP shell into the web server's directory and execute it. This leads to full access to the system, as the configured user (e.g., Administrator).	2019-07-26	<a href="#">9.0</a>	<a href="#">CVE-2019-10267</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 76.0.8 allows remote attackers to execute arbitrary code via mailing-list attachments (SEC-452).	2019-07-30	<a href="#">7.5</a>	<a href="#">CVE-2018-20863</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 allows arbitrary code execution in the context of the root account via dnssec adminbin (SEC-465).	2019-07-30	<a href="#">7.2</a>	<a href="#">CVE-2018-20869</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows SQL injection during database backups (SEC-420).	2019-08-01	<a href="#">7.5</a>	<a href="#">CVE-2018-20887</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows local users to escalate to root access because of userdata cache misparsing (SEC-479).	2019-07-30	<a href="#">7.2</a>	<a href="#">CVE-2019-14400</a> <a href="#">CONFIRM</a>
datagrid_project -- datagrid	The datagrid gem 1.0.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party.	2019-07-26	<a href="#">7.5</a>	<a href="#">CVE-2019-14281</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet due to a net_process_received_packet integer underflow during an nc_input_packet call.	2019-07-31	<a href="#">7.5</a>	<a href="#">CVE-2019-14192</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered in Das U-Boot through 2019.07.			<a href="#">CVE-2019-</a>

denx -- u-boot	There is an unbounded memcpy with an unvalidated length at nfs_readlink_reply, in the "if" block after calculating the new path length.	2019-07-31	7.5	<a href="#">14193</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv2 case.	2019-07-31	7.5	<a href="#">CVE-2019-14194</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with unvalidated length at nfs_readlink_reply in the "else" block after calculating the new path length.	2019-07-31	7.5	<a href="#">CVE-2019-14195</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_lookup_reply.	2019-07-31	7.5	<a href="#">CVE-2019-14196</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy with a failed length check at nfs_read_reply when calling store_block in the NFSv3 case.	2019-07-31	7.5	<a href="#">CVE-2019-14198</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is an unbounded memcpy when parsing a UDP packet due to a net_process_received_packet integer underflow during an *udp_packet_handler call.	2019-07-31	7.5	<a href="#">CVE-2019-14199</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: rpc_lookup_reply.	2019-07-31	7.5	<a href="#">CVE-2019-14200</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_lookup_reply.	2019-07-31	7.5	<a href="#">CVE-2019-14201</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_readlink_reply.	2019-07-31	7.5	<a href="#">CVE-2019-14202</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_mount_reply.	2019-07-31	7.5	<a href="#">CVE-2019-14203</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a stack-based buffer overflow in this nfs_handler reply helper function: nfs_umountall_reply.	2019-07-31	7.5	<a href="#">CVE-2019-14204</a> <a href="#">MISC</a> <a href="#">MISC</a>
discourse -- discourse	Discourse before v2.4.0.beta2 lacks a confirmation screen when logging in via an email link.	2019-07-29	7.5	<a href="#">CVE-2019-1020018</a> <a href="#">MISC</a> <a href="#">MISC</a>
libmodbus -- libmodbus	An issue was discovered in libmodbus before 3.0.7 and 3.1.x before 3.1.5. There is an out-of-bounds read for the MODBUS_FC_WRITE_MULTIPLE_COILS case, aka VD-1302.	2019-07-31	7.5	<a href="#">CVE-2019-14462</a> <a href="#">MISC</a> <a href="#">MISC</a>
libmodbus -- libmodbus	An issue was discovered in libmodbus before 3.0.7 and 3.1.x before 3.1.5. There is an out-of-bounds read for the MODBUS_FC_WRITE_MULTIPLE_REGISTERS case, aka VD-1301.	2019-07-31	7.5	<a href="#">CVE-2019-14463</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 2.6.20, there is an off-by-one bug in net/netlabel/netlabel_cipso_v4.c where it is possible to overflow the doi_def->tags[] array.	2019-07-27	7.5	<a href="#">CVE-2007-6762</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 2.6.34, a range check issue in drivers/gpu/drm/radeon/atombios.c could cause an off by one (buffer overflow) problem.	2019-07-27	7.5	<a href="#">CVE-2010-5331</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 2.6.37, an out of bounds array access happened in drivers/net/mlx4/port.c. When searching for a free entry in either mlx4_register_vlan() or	2019-07-27	7.5	<a href="#">CVE-2010-5332</a> <a href="#">MISC</a>

	mlx4_register_mac(), and there is no free entry, the loop terminates without updating the local variable free thus causing out of array bounds access.			<a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 3.1, an off by one in the drivers/target/loopback/tcm_loop.c tcm_loop_make_naa_tpg() function could result in at least memory corruption.	2019-07-27	<a href="#">7.5</a>	<a href="#">CVE-2011-5327</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 3.4, a buffer overflow occurs in drivers/net/wireless/iwlwifi/iwl-agn-sta.c, which will cause at least memory corruption.	2019-07-27	<a href="#">7.5</a>	<a href="#">CVE-2012-6712</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 4.1.4, a buffer overflow occurs when checking userspace params in drivers/media/dvb-frontends/cx24116.c. The maximum size for a DiSEqC command is 6, according to the userspace API. However, the code allows larger values such as 23.	2019-07-27	<a href="#">7.5</a>	<a href="#">CVE-2015-9289</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 4.9.6, there is an off by one in the drivers/mtd/spi-nor/cadence-quadspi.c cqspi_setup_flash() function. There are CQSPI_MAX_CHIPSELECT elements in the ->f_pdata array so the ">" should be ">=" instead.	2019-07-27	<a href="#">7.5</a>	<a href="#">CVE-2016-10764</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 4.14, an out of boundary access happened in drivers/nvme/target/fc.c.	2019-07-27	<a href="#">7.5</a>	<a href="#">CVE-2017-18379</a> <a href="#">MISC</a> <a href="#">MISC</a>
simple_captcha2_project -- simple_captcha2	The simple_captcha2 gem 0.2.3 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party.	2019-07-26	<a href="#">7.5</a>	<a href="#">CVE-2019-14282</a> <a href="#">MISC</a> <a href="#">MISC</a>
veritas -- resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. An arbitrary command execution vulnerability allows a malicious VRP user to execute commands with root privilege within the VRP virtual machine, related to resiliency plans and custom script functionality.	2019-07-29	<a href="#">9.0</a>	<a href="#">CVE-2019-14416</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
veritas -- resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. An arbitrary command execution vulnerability allows a malicious VRP user to execute commands with root privilege within the VRP virtual machine, related to DNS functionality.	2019-07-29	<a href="#">9.0</a>	<a href="#">CVE-2019-14417</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. When creating a trial account, it is possible to inject XSS in the Alias field, allowing the attacker to retrieve the admin's cookie and take over the account.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-10263</a> <a href="#">MISC</a>
ahsay -- cloud_backup_suite	An issue was discovered in Ahsay Cloud Backup Suite before 8.1.1.50. With a valid administrator account, the "Move / Import / Export Users" screen has an Import Users option. This option accepts a ZIP archive containing a users.xml file that can trigger XXE.	2019-07-26	<a href="#">6.5</a>	<a href="#">CVE-2019-10264</a> <a href="#">MISC</a>
ash-aio_project -- ash-aio	ASH-AIO before 2.0.0.3 allows an open redirect.	2019-07-29	<a href="#">5.8</a>	<a href="#">CVE-2019-1020016</a> <a href="#">MISC</a>
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.840, File and Directory Information Exposure in filemanager allows attackers to enumerate users and check for active users of the application by reading /tmp/login.log.	2019-07-26	<a href="#">4.0</a>	<a href="#">CVE-2019-13385</a> <a href="#">MISC</a> <a href="#">MISC</a>
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, a hidden action=9 feature in filemanager2.php allows attackers to execute a shell command, i.e., obtain a	2019-07-26	<a href="#">6.5</a>	<a href="#">CVE-2019-13386</a> <a href="#">MISC</a>

	reverse shell with user privilege.			<a href="#">MISC</a>
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, Reflected XSS in filemanager2.php (parameter fm_current_dir) allows attackers to steal a cookie or session, or redirect to a phishing website.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-13387</a> <a href="#">MISC</a> <a href="#">MISC</a>
central_dogma_project -- central_dogma	Cross-site scripting vulnerability in Central Dogma 0.17.0 to 0.40.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-6002</a> <a href="#">JVN</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 76.0.8 allows a persistent Virtual FTP accounts after removal of its associated domain (SEC-454).	2019-07-30	<a href="#">6.4</a>	<a href="#">CVE-2018-20864</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has Self XSS in the WHM Additional Backup Destination field (SEC-459).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20865</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has Stored XSS in the WHM "Reset a DNS Zone" feature (SEC-461).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20866</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has an open redirect when resetting connections (SEC-462).	2019-07-30	<a href="#">5.8</a>	<a href="#">CVE-2018-20867</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 76.0.8 has Stored XSS in the WHM MultiPHP Manager interface (SEC-464).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20868</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows demo accounts to execute arbitrary code via the Fileman::viewfile API (SEC-444).	2019-08-01	<a href="#">6.5</a>	<a href="#">CVE-2018-20879</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows FTP access during account suspension (SEC-449).	2019-08-01	<a href="#">4.0</a>	<a href="#">CVE-2018-20883</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows Apache HTTP Server configuration injection because of DocumentRoot variable interpolation (SEC-416).	2019-08-01	<a href="#">5.0</a>	<a href="#">CVE-2018-20885</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows Remote-Stored XSS in WHM Save Theme Interface (SEC-400).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20901</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows self XSS in the WHM Backup Configuration interface (SEC-421).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20903</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows self XSS in the WHM cPAddons showsecurity Interface (SEC-357).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20910</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows code execution because "." is in @INC during a Perl syntax check of cpaddonsup (SEC-359).	2019-08-01	<a href="#">6.5</a>	<a href="#">CVE-2018-20911</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows demo accounts to execute code via awstats (SEC-362).	2019-08-01	<a href="#">6.5</a>	<a href="#">CVE-2018-20912</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 70.0.23, OpenID providers can inject arbitrary data into cPanel session files (SEC-368).	2019-08-01	<a href="#">4.9</a>	<a href="#">CVE-2018-20914</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS in WHM DNS Cluster (SEC-372).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20918</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Create Account action (SEC-373).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20919</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Edit DNS Zone action (SEC-374).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20920</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM "Delete a DNS Zone" action (SEC-375).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20921</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM DNS Cleanup action (SEC-376).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20922</a> <a href="#">CONFIRM</a>

cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Synchronize DNS Records action (SEC-377).	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20923</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 82.0.2 has Self XSS in the cPanel and webmail master templates (SEC-506).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14387</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 allows unauthenticated file creation because Exim log parsing is mishandled (SEC-507).	2019-07-30	<a href="#">5.0</a>	<a href="#">CVE-2019-14388</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 80.0.22 allows remote code execution by a demo account because of incorrect URI dispatching (SEC-501).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14392</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 allows local code execution in the context of a different cPanel account because of insecure cpphp execution (SEC-486).	2019-07-30	<a href="#">4.6</a>	<a href="#">CVE-2019-14393</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 allows demo accounts to modify arbitrary files via the extractfile API1 call (SEC-496).	2019-07-30	<a href="#">5.0</a>	<a href="#">CVE-2019-14397</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 allows demo accounts to execute arbitrary code via ajax_makertext_syntax_util.pl (SEC-498).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14398</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The SSL certificate-storage feature in cPanel before 78.0.18 allows unsafe file operations in the context of the root account (SEC-477).	2019-07-30	<a href="#">6.1</a>	<a href="#">CVE-2019-14399</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows code execution via an addforward API1 call (SEC-480).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14401</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 offers an open mail relay because of incorrect domain-redirect routing (SEC-483).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14403</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows certain file-read operations in the context of the root account via the Exim virtual_user_spam router (SEC-484).	2019-07-30	<a href="#">4.9</a>	<a href="#">CVE-2019-14404</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 allows demo accounts to execute code via securitypolicy.cg (SEC-487).	2019-07-30	<a href="#">6.5</a>	<a href="#">CVE-2019-14405</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 has stored XSS in the BoxTrapper Queue Listing (SEC-493).	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14406</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 reveals internal data to OpenID providers (SEC-415).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-14407</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 allows a demo account to link with an OpenID provider (SEC-460).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-14408</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 does not properly restrict demo accounts from writing to files via the DCV UAPI (SEC-473).	2019-07-30	<a href="#">5.0</a>	<a href="#">CVE-2019-14411</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 allows certain file-write operations as shared users during connection resets (SEC-476).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-14413</a> <a href="#">CONFIRM</a>
craftcms -- craft_cms	In some circumstances, Craft 2 before 2.7.10 and 3 before 3.2.6 wasn't stripping EXIF data from user-uploaded images when it was configured to do so, potentially exposing personal/geolocation data to the public.	2019-07-26	<a href="#">5.0</a>	<a href="#">CVE-2019-14280</a> <a href="#">MISC</a> <a href="#">MISC</a>
custom_simple_rss_project -- custom_simple_rss	A CSRF vulnerability in Settings form in the Custom Simple Rss plugin 2.0.6 for WordPress allows attackers to change the plugin settings.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14327</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	A crafted self-referential DOS partition table will cause all Das U-Boot versions through 2019.07-rc4 to infinitely recurse, causing the stack to grow infinitely and eventually either crash or overwrite other data.	2019-07-29	<a href="#">6.4</a>	<a href="#">CVE-2019-13103</a> <a href="#">MISC</a> <a href="#">MISC</a>
denx -- u-boot	An issue was discovered in Das U-Boot through 2019.07. There is a read of out-of-bounds data at nfs_read_reply.	2019-07-31	<a href="#">6.4</a>	<a href="#">CVE-2019-14197</a> <a href="#">MISC</a> <a href="#">MISC</a>



discourse -- discourse	Discourse before v2.4.0.beta2 lacks a confirmation screen when logging in via a user-api OTP.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020017</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	An issue was discovered in EspoCRM before 5.6.6. There is stored XSS due to lack of filtration of user-supplied data in Create Task. A malicious attacker can modify the parameter name to contain JavaScript code.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14329</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	An issue was discovered in EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create Case. A malicious attacker can modify the firstName and lastName to contain JavaScript code.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14330</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	An issue was discovered in EspoCRM before 5.6.6. Stored XSS exists due to lack of filtration of user-supplied data in Create User. A malicious attacker can modify the firstName and lastName to contain JavaScript code.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14331</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
espocrm -- espocrm	EspoCRM version 5.6.4 is vulnerable to stored XSS due to lack of filtration of user-supplied data in the api/v1/Document functionality for storing documents in the account tab. An attacker can upload a crafted file that contains JavaScript code in its name. This code will be executed when a user opens a page of any profile with this.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14349</a> <a href="#">MISC</a>
espocrm -- espocrm	EspoCRM 5.6.4 is vulnerable to stored XSS due to lack of filtration of user-supplied data in the Knowledge base. A malicious attacker can inject JavaScript code in the body parameter during api/v1/KnowledgeBaseArticle knowledge-base record creation.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14350</a> <a href="#">MISC</a>
espocrm -- espocrm	EspoCRM 5.6.4 is vulnerable to user password hash enumeration. A malicious authenticated attacker can brute-force a user password hash by 1 symbol at a time using specially crafted api/v1/User?filterList filters.	2019-07-28	<a href="#">4.0</a>	<a href="#">CVE-2019-14351</a> <a href="#">MISC</a>
exiv2 -- exiv2	Exiv2 0.27.99.0 has a heap-based buffer over-read in Exiv2::RaflImage::readMetadata() in rafimage.cpp.	2019-07-28	<a href="#">6.8</a>	<a href="#">CVE-2019-14368</a> <a href="#">MISC</a>
exiv2 -- exiv2	Exiv2::PngImage::readMetadata() in pngimage.cpp in Exiv2 0.27.99.0 allows attackers to cause a denial of service (heap-based buffer over-read) via a crafted image file.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14369</a> <a href="#">MISC</a>
exiv2 -- exiv2	In Exiv2 0.27.99.0, there is an out-of-bounds read in Exiv2::MrwlImage::readMetadata() in mrwlimage.cpp. It could result in denial of service.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14370</a> <a href="#">MISC</a>
flif -- flif	An issue was discovered in image_save_png in image/image-png.cpp in Free Lossless Image Format (FLIF) 0.3. Attackers can trigger a heap-based buffer over-read in libpng via a crafted flif file.	2019-07-28	<a href="#">6.8</a>	<a href="#">CVE-2019-14373</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an Integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "one byte per line" case.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14288</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an integer overflow in the function JBIG2Bitmap::combine at JBIG2Stream.cc for the "multiple bytes per line" case.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14289</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 2.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14290</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA==6 case 3.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14291</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6 case 1.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14292</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-</a>

glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is an out of bounds read in the function GfxPatchMeshShading::parse at GfxState.cc for typeA!=6 case 2.	2019-07-27	4.3	<a href="#">14293</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	An issue was discovered in Xpdf 4.01.01. There is a use-after-free in the function JPXStream::fillReadBuf at JPXStream.cc, due to an out of bounds read.	2019-07-27	4.3	<a href="#">CVE-2019-14294</a> <a href="#">MISC</a> <a href="#">MISC</a>
google -- kubernetes_engine	Jenkins Google Kubernetes Engine Plugin 0.6.2 and earlier created a temporary file containing a temporary access token in the project workspace, where it could be accessed by users with Job/Read permission.	2019-07-31	4.0	<a href="#">CVE-2019-10365</a> <a href="#">MLIST</a> <a href="#">MISC</a>
ibm -- daeja_viewone	IBM Daeja ViewONE Professional, Standard & Virtual 5.0.5 and 5.0.6 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 163620.	2019-07-30	5.5	<a href="#">CVE-2019-4456</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- storediq	IBM StoreIQ 7.6.0.0. through 7.6.0.18 could allow an authenticated user to obtain sensitive information that a privileged user should only be allowed to view. IBM X-Force ID: 158696.	2019-07-31	4.0	<a href="#">CVE-2019-4163</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- storediq	IBM StoreIQ 7.6.0.0. through 7.6.0.18 could allow a remote attacker to cause a denial of service attack using repeated requests to the server. IBM X-Force ID: 158698.	2019-07-31	5.0	<a href="#">CVE-2019-4165</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
icegram -- email_subscribers_&_newsletters	An XSS vulnerability in the "Email Subscribers & Newsletters" plugin 4.1.6 for WordPress allows an attacker to inject malicious JavaScript code through a publicly available subscription form using the esfp_x_name wp-admin/admin-ajax.php POST parameter.	2019-07-28	4.3	<a href="#">CVE-2019-14364</a> <a href="#">MISC</a> <a href="#">MISC</a>
inveniosoftware -- invenio-app	invenio-app before 1.1.1 allows host header injection.	2019-07-29	5.8	<a href="#">CVE-2019-1020006</a> <a href="#">CONFIRM</a>
inveniosoftware -- invenio-previewer	invenio-previewer before 1.0.0a12 allows XSS.	2019-07-29	4.3	<a href="#">CVE-2019-1020019</a> <a href="#">MISC</a>
jenkins -- configuration_as_code	Missing permission checks in Jenkins Configuration as Code Plugin 1.24 and earlier in various HTTP endpoints allowed users with Overall/Read access to access the generated schema and documentation for this plugin containing detailed information about installed plugins.	2019-07-31	4.0	<a href="#">CVE-2019-10344</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.24 and earlier did not escape values resulting in variable interpolation during configuration import when exporting, allowing attackers with permission to change Jenkins system configuration to obtain the values of environment variables.	2019-07-31	5.5	<a href="#">CVE-2019-10362</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.24 and earlier did not reliably identify sensitive values expected to be exported in their encrypted form.	2019-07-31	4.0	<a href="#">CVE-2019-10363</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- m2release	A cross-site request forgery vulnerability in Jenkins Maven Release Plugin 0.14.0 and earlier in the M2ReleaseAction#doSubmit method allowed attackers to perform releases with attacker-specified options.	2019-07-31	6.8	<a href="#">CVE-2019-10359</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- maven	Jenkins Maven Integration Plugin 3.3 and earlier did not apply build log decorators to module builds, potentially revealing sensitive build variables in the build log.	2019-07-31	4.0	<a href="#">CVE-2019-10358</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- pipeline:shared_groovy_libraries	A missing permission check in Jenkins Pipeline: Shared Groovy Libraries Plugin 2.14 and earlier allowed users with Overall/Read access to obtain limited information about the content of SCM repositories referenced by global libraries.	2019-07-31	4.0	<a href="#">CVE-2019-10357</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- script_security	A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.61 and earlier related to the handling of type casts allowed attackers to execute arbitrary code in sandboxed scripts.	2019-07-31	6.5	<a href="#">CVE-2019-10355</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- script_security	A sandbox bypass vulnerability in Jenkins Script Security Plugin 1.61 and earlier related to the handling of method pointer expressions allowed attackers to execute arbitrary	2019-07-31	6.5	<a href="#">CVE-2019-10356</a> <a href="#">MLIST</a>

	code in sandboxed scripts.			<a href="#">MISC</a>
jenkins -- skytap_cloud_ci	Jenkins Skytap Cloud CI Plugin 2.06 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system.	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10366</a> <a href="#">MLIST</a> <a href="#">MISC</a>
kolide -- fleet	Fleet before 2.1.2 allows exposure of SMTP credentials.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020009</a> <a href="#">MISC</a>
libav -- libav	An issue was discovered in L baw 12.3. There is an infinite loop in the function mov_probe in the file libavformat/mov.c, related to offset and tag.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14371</a> <a href="#">MISC</a>
libav -- libav	In L baw 12.3, there is an infinite loop in the function wv_read_block_header() in the file wvdec.c.	2019-07-28	<a href="#">4.3</a>	<a href="#">CVE-2019-14372</a> <a href="#">MISC</a>
libav -- libav	An issue was discovered in L baw 12.3. Division by zero in range_decode_culshift in l bawcodec/apedec.c allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14443</a> <a href="#">MISC</a>
libsdl -- sdl2_image	An exploitable code execution vulnerability exists in the PCX image-rendering functionality of SDL2_image 2.0.4. A specially crafted PCX image can cause a heap overflow, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-5057</a> <a href="#">MISC</a>
libsdl -- sdl2_image	An exploitable code execution vulnerability exists in the XCF image rendering functionality of SDL2_image 2.0.4. A specially crafted XCF image can cause a heap overflow, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-5058</a> <a href="#">MISC</a>
libsdl -- sdl2_image	An exploitable code execution vulnerability exists in the XPM image rendering functionality of SDL2_image 2.0.4. A specially crafted XPM image can cause an integer overflow, allocating too small of a buffer. This buffer can then be written out of bounds resulting in a heap overflow, ultimately ending in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-5059</a> <a href="#">MISC</a>
libslirp_project -- l bslirp	ip_reass in ip_input.c in libslirp 4.0.0 has a heap-based buffer overflow via a large packet because it mishandles a case involving the first fragment.	2019-07-29	<a href="#">6.5</a>	<a href="#">CVE-2019-14378</a> <a href="#">MLIST</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.20. drivers/phy/mscc/phy-ocelot-serdes.c has an off-by-one error with a resultant ctrl->phys out-of-bounds read.	2019-07-26	<a href="#">4.6</a>	<a href="#">CVE-2018-20854</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue() use-after-free because a certain error case is mishandled.	2019-07-26	<a href="#">4.6</a>	<a href="#">CVE-2018-20856</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.2.3, set_geometry in drivers/block/floppy.c does not validate the sect and head fields, as demonstrated by an integer overflow and out-of-bounds read. It can be triggered by an unprivileged local user when a floppy disk has been inserted. NOTE: QEMU creates the floppy device by default.	2019-07-26	<a href="#">4.6</a>	<a href="#">CVE-2019-14283</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mcpp_project -- mcpp	MCP 2.7.2 has a heap-based buffer overflow in the do_msg() function in support.c.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-14274</a> <a href="#">MISC</a>
misp -- misp	In app/webroot/js/event-graph.js in MISP 2.4.111, a stored XSS vulnerability exists in the event-graph view when a user toggles the event graph view. A malicious MISP event must be crafted in order to trigger the vulnerability.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14286</a> <a href="#">MISC</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. A sesskey (CSRF) token was not being utilised by the XML loading/unloading admin tool.	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-10186</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. Users with permission to delete entries from a glossary were able to delete entries from other glossaries they did not	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10187</a> <a href="#">CONFIRM</a>

	have direct access to.			<a href="#">MISC</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. Teachers in a quiz group could modify group overrides for other groups in the same quiz.	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10188</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
moodle -- moodle	A flaw was found in moodle before versions 3.7.1, 3.6.5, 3.5.7. Teachers in an assignment group could modify group overrides for other groups in the same assignment.	2019-07-31	<a href="#">4.0</a>	<a href="#">CVE-2019-10189</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
nats -- nats_server	An integer overflow in NATS Server 2.0.0 allows a remote attacker to crash the server by sending a crafted request.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-13126</a> <a href="#">MISC</a> <a href="#">MISC</a>
open.edx -- edx-platform	edx-platform before 2015-07-20 allows code execution by privileged users because the course import endpoint mishandles .tar.gz files.	2019-07-29	<a href="#">6.5</a>	<a href="#">CVE-2015-5601</a> <a href="#">CONFIRM</a>
open.edx -- edx-platform	edx-platform before 2015-09-17 allows XSS via a team name.	2019-07-29	<a href="#">4.3</a>	<a href="#">CVE-2015-6960</a> <a href="#">CONFIRM</a>
openmpt -- libopenmpt	libopenmpt before 0.3.13 allows a crash with malformed MED files.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20860</a> <a href="#">MISC</a>
openmpt -- libopenmpt	libopenmpt before 0.4.5 allows a crash during playback due to an out-of-bounds read in XM and MT2 files.	2019-07-30	<a href="#">4.3</a>	<a href="#">CVE-2019-14380</a> <a href="#">MISC</a>
parseplatform -- parse-server	parse-server before 3.4.1 allows DoS after any POST to a volatile class.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020012</a> <a href="#">MISC</a>
parseplatform -- parse-server	parse-server before 3.6.0 allows account enumeration.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020013</a> <a href="#">MISC</a>
postgresql -- postgresql	A vulnerability was found in postgresql versions 11.x prior to 11.3. Using a purpose-crafted insert to a partitioned table, an attacker can read arbitrary bytes of server memory. In the default configuration, any user can create a partitioned table suitable for this attack. (Exploit prerequisites are the same as for CVE-2018-1052).	2019-07-30	<a href="#">4.0</a>	<a href="#">CVE-2019-10129</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
pterodactyl -- panel	Pterodactyl before 0.7.14 with 2FA allows credential sniffing.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020002</a> <a href="#">CONFIRM</a>
stacktable.js_project -- stacktable.js	stacktable.js before 1.0.4 allows XSS.	2019-07-29	<a href="#">4.3</a>	<a href="#">CVE-2019-1020008</a> <a href="#">MISC</a>
sunhater -- kcfinder	A cross-site scripting (XSS) vulnerability in upload.php in SunHater KCFinder 3.20-test1, 3.20-test2, 3.12, and earlier allows remote attackers to inject arbitrary web script or HTML via the CKEditorFuncNum parameter.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14315</a> <a href="#">MISC</a>
testlink -- testlink	TestLink 1.9.19 has XSS via the error.php message parameter.	2019-08-01	<a href="#">4.3</a>	<a href="#">CVE-2019-14471</a> <a href="#">MISC</a>
tridactyl_project -- tridactyl	Tridactyl before 1.16.0 allows fake key events.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020004</a> <a href="#">MISC</a>
unity -- web_player	The Unity Web Player plugin before 4.6.6f2 and 5.x before 5.0.3f2 allows attackers to read messages or access online services via a victim's credentials	2019-07-29	<a href="#">4.0</a>	<a href="#">CVE-2015-9288</a> <a href="#">CONFIRM</a>
upx_project -- upx	An Integer overflow in the getElfSections function in p_vmlnx.cpp in UPX 3.95 allows remote attackers to cause a denial of service (crash) via a skewed offset larger than the size of the PE section in a UPX packed executable, which triggers an allocation of excessive memory.	2019-07-27	<a href="#">4.3</a>	<a href="#">CVE-2019-14295</a> <a href="#">MISC</a>
upx_project -- upx	canUnpack in p_vmlnx.cpp in UPX 3.95 allows remote attackers to cause a denial of service (SEGV or buffer overflow, and application crash) or possibly have unspecified other impact via a crafted UPX packed file.	2019-07-27	<a href="#">6.8</a>	<a href="#">CVE-2019-14296</a> <a href="#">MISC</a>
wallaceit -- wallacepos	Cross-site request forgery in WallacePOS 1.4.3 allows a remote attacker to perform sensitive application actions by	2019-07-31	<a href="#">6.8</a>	<a href="#">CVE-2019-3959</a>

	tricking legitimate users into clicking a crafted link.			<a href="#">MISC</a>
wikindx_project -- wikindx	A cross-site scripting (XSS) vulnerability in getPagingStart() in core/lists/PAGING.php in WIKINDX through 5.8.1 allows remote attackers to inject arbitrary web script or HTML via the PagingStart parameter.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-13588</a> <a href="#">CONFIRM</a>
wpfastestcache -- wp_fastest_cache	The WP Fastest Cache plugin through 0.8.9.0 for WordPress allows remote attackers to delete arbitrary files because wp_postratings_clear_fastest_cache and rm_folder_recursively in wpFastestCache.php mishandle ../ in an HTTP Referer header.	2019-07-29	<a href="#">5.8</a>	<a href="#">CVE-2019-6726</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
xfig_project -- fig2dev	Xfig fig2dev 3.2.7a has a stack-based buffer overflow in the calc_arrow function in bound.c.	2019-07-26	<a href="#">4.3</a>	<a href="#">CVE-2019-14275</a> <a href="#">MISC</a>
yardoc -- yard	yard before 0.9.20 allows path traversal.	2019-07-29	<a href="#">5.0</a>	<a href="#">CVE-2019-1020001</a> <a href="#">MISC</a>
zendesk -- samlr	Zendesk Samlr before 2.6.2 allows an XML nodes comment attack such as a name_id node with user@example.com followed by <!-->. and then the attacker's domain name.	2019-07-26	<a href="#">5.0</a>	<a href="#">CVE-2018-20857</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cpanel -- cpanel	cPanel before 76.0.8 unsafely performs PostgreSQL password changes (SEC-366).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2018-20862</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The WebDAV transport feature in cPanel before 76.0.8 enables debug logging (SEC-467).	2019-07-30	<a href="#">2.1</a>	<a href="#">CVE-2018-20870</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in the WHM Security Questions interface (SEC-433).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20875</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in the Site Software Moderation interface (SEC-434).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20876</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in WHM Style Upload interface (SEC-437).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20877</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows stored XSS in WHM "File and Directory Restoration" interface (SEC-441).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20878</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 mishandles account suspension because of an invalid email_accounts.json file (SEC-445).	2019-08-01	<a href="#">2.1</a>	<a href="#">CVE-2018-20880</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self stored XSS on the Security Questions login page (SEC-446).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20881</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows stored XSS in the WHM File Restoration interface (SEC-367).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20884</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to read root's crontab file by leveraging ClamAV installation (SEC-408).	2019-08-01	<a href="#">2.1</a>	<a href="#">CVE-2018-20902</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows attackers to read the root accessshash via the WHM /cgi/trustclustermaster.cgi (SEC-364).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20913</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via a WHM Edit DNS Zone action (SEC-369).	2019-08-01	<a href="#">3.5</a>	<a href="#">CVE-2018-20915</a> <a href="#">CONFIRM</a>
	cPanel before 70.0.23 allows Stored XSS via a WHM Edit MX			<a href="#">CVE-2018-</a>



cpanel -- cpanel	Entry (SEC-370).	2019-08-01	3.5	<a href="#">20916 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows any user to disable Solr (SEC-371).	2019-08-01	2.1	<a href="#">CVE-2018-20917 CONFIRM</a>
cpanel -- cpanel	cPanel before 82.0.2 has stored XSS in the WHM Tomcat Manager interface (SEC-504).	2019-07-30	3.5	<a href="#">CVE-2019-14386 MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 allows local users to discover the MySQL root password (SEC-510).	2019-07-30	2.1	<a href="#">CVE-2019-14389 MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 has stored XSS in the WHM Modify Account interface (SEC-512).	2019-07-30	3.5	<a href="#">CVE-2019-14390 MISC</a>
cpanel -- cpanel	cPanel before 82.0.2 does not properly enforce Reseller package creation ACLs (SEC-514).	2019-07-30	2.1	<a href="#">CVE-2019-14391 MISC</a>
cpanel -- cpanel	cPanel before 80.0.5 allows unsafe file operations in the context of the root account via the fetch_ssl_certificates_for_fqdns API (SEC-489).	2019-07-30	2.1	<a href="#">CVE-2019-14394 CONFIRM</a>
cpanel -- cpanel	cPanel before 80.0.5 uses world-readable permissions for the Queueproc log (SEC-494).	2019-07-30	2.1	<a href="#">CVE-2019-14395 CONFIRM</a>
cpanel -- cpanel	API Analytics adminbin in cPanel before 80.0.5 allows spoofed insertions of log data (SEC-495).	2019-07-30	2.1	<a href="#">CVE-2019-14396 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.18 unsafely determines terminal capabilities by using infocmp (SEC-481).	2019-07-30	2.1	<a href="#">CVE-2019-14402 CONFIRM</a>
cpanel -- cpanel	cPanel before 78.0.2 allows arbitrary file-read operations via Passenger adminbin (SEC-466).	2019-07-30	2.1	<a href="#">CVE-2019-14409 CONFIRM</a>
cpanel -- cpanel	Makertext in cPanel before 78.0.2 allows format-string injection in the Email store_filter UAPI (SEC-472).	2019-07-30	2.1	<a href="#">CVE-2019-14410 CONFIRM</a>
cpanel -- cpanel	Makertext in cPanel before 78.0.2 allows format-string injection in the DCV check_domains_via_dns UAPI (SEC-474).	2019-07-30	2.1	<a href="#">CVE-2019-14412 CONFIRM</a>
cpanel -- cpanel	In cPanel before 78.0.2, a Userdata cache temporary file can conflict with domains (SEC-478).	2019-07-30	2.1	<a href="#">CVE-2019-14414 CONFIRM</a>
dependencytrack -- dependency-track	Dependency-Track before 3.5.1 allows XSS.	2019-07-29	3.5	<a href="#">CVE-2019-1020007 CONFIRM</a>
http-file-server_project -- http-file-server	Cross-site scripting (XSS) vulnerability in http-file-server (all versions) allows an attacker with access to the server file system to execute arbitrary JavaScript code in victim's browser.	2019-07-30	3.5	<a href="#">CVE-2019-5458 MISC</a>
ibm -- websphere_application_server	IBM WebSphere Application Server - Liberty Admin Center could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could send a specially-crafted HTTP request to hijack the victim's click actions or launch other client-side browser attacks. IBM X-Force ID: 160513.	2019-07-30	3.5	<a href="#">CVE-2019-4285 XF CONFIRM</a>
inveniosoftware -- invenio-communities	invenio-communities before 1.0.0a20 allows XSS.	2019-07-29	3.5	<a href="#">CVE-2019-1020005 MISC</a>
inveniosoftware -- invenio-records	invenio-records before 1.2.2 allows XSS.	2019-07-29	3.5	<a href="#">CVE-2019-1020003 MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.24 and earlier did not properly apply masking to values expected to be hidden when logging the configuration being applied.	2019-07-31	2.1	<a href="#">CVE-2019-10343 MLIST MISC</a>
jenkins -- configuration_as_code	Jenkins Configuration as Code Plugin 1.20 and earlier did not treat the proxy password as a secret to be masked when	2019-07-31	2.1	<a href="#">CVE-2019-10345 MLIST</a>

	logging or encrypted for export.			<a href="#">MISC</a>
jenkins -- ec2	Jenkins Amazon EC2 Plugin 1.43 and earlier wrote the beginning of private keys to the Jenkins system log.	2019-07-31	<a href="#">2.1</a>	<a href="#">CVE-2019-10364</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- m2_release	A stored cross site scripting vulnerability in Jenkins Maven Release Plugin 0.14.0 and earlier allowed attackers to inject arbitrary HTML and JavaScript in the plugin-provided web pages in Jenkins.	2019-07-31	<a href="#">3.5</a>	<a href="#">CVE-2019-10360</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- m2release	Jenkins Maven Release Plugin 0.14.0 and earlier stored credentials unencrypted on the Jenkins master where they could be viewed by users with access to the master file system.	2019-07-31	<a href="#">2.1</a>	<a href="#">CVE-2019-10361</a> <a href="#">MLIST</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in the Linux kernel before 4.18.7. In create_qp_common in drivers/infiniband/hw/mlx5/qp.c, mlx5_b_create_qp_resp was never initialized, resulting in a leak of stack memory to userspace.	2019-07-26	<a href="#">2.1</a>	<a href="#">CVE-2018-20855</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.2.3, drivers/block/floppy.c allows a denial of service by setup_format_params division-by-zero. Two consecutive ioctl's can trigger the bug: the first one should set the drive geometry with .sect and .rate values that make F_SECT_PER_TRACK be zero. Next, the floppy format operation should be called. It can be triggered by an unprivileged local user even when a floppy disk has not been inserted. NOTE: QEMU creates the floppy device by default.	2019-07-26	<a href="#">2.1</a>	<a href="#">CVE-2019-14284</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
microsoft -- outlook	A spoofing vulnerability exists in the way Microsoft Outlook for Android software parses specifically crafted email messages, aka 'Outlook for Android Spoofing Vulnerability'.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2019-1105</a> <a href="#">N/A</a>
min-http-server_project -- min-http-server	Cross-site scripting (XSS) vulnerability in min-http-server (all versions) allows an attacker with access to the server file system to execute arbitrary JavaScript code in victim's browser.	2019-07-30	<a href="#">3.5</a>	<a href="#">CVE-2019-5457</a> <a href="#">MISC</a>
open.edx -- edx-platform	edx-platform before 2015-08-17 allows XSS in the Studio listing of courses.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2015-6253</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
veeam -- one_reporter	Veeam ONE Reporter 9.5.0.3201 allows XSS via the Add/Edit Widget with a crafted Caption field to setDashboardWidget in CommonDataHandlerReadOnly.ashx.	2019-07-27	<a href="#">3.5</a>	<a href="#">CVE-2019-14297</a> <a href="#">MISC</a>
veeam -- one_reporter	Veeam ONE Reporter 9.5.0.3201 allows XSS via a crafted Description(config) field to addDashboard or editDashboard in CommonDataHandlerReadOnly.ashx.	2019-07-27	<a href="#">3.5</a>	<a href="#">CVE-2019-14298</a> <a href="#">MISC</a>
veritas -- resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. A persistent cross-site scripting (XSS) vulnerability allows a malicious VRP user to inject malicious script into another user's browser, related to resiliency plans functionality. A victim must open a resiliency plan that an attacker has access to.	2019-07-29	<a href="#">3.5</a>	<a href="#">CVE-2019-14415</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
wallaceit -- wallacepos	Insufficient output sanitization in WallacePOS 1.4.3 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks via a crafted sales transaction.	2019-07-31	<a href="#">3.5</a>	<a href="#">CVE-2019-3958</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3proxy -- 3proxy	webadmin.c in 3proxy before 0.8.13 has an out-of-bounds write in the admin interface.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14495</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	It was found that icedtea-web though 1.7.2			<a href="#">CVE-</a>

adoptopenjdk -- icedtea-web	and 1.8.2 did not properly sanitize paths from <jar/> elements in JNLP files. An attacker could trick a victim into running a specially crafted application and use this flaw to upload arbitrary files to arbitrary locations in the context of the user.	2019-07-31	not yet calculated	<a href="#">2019-10182</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
adoptopenjdk -- icedtea-web	It was found that icedtea-web up to and including 1.7.2 and 1.8.2 was vulnerable to a zip-slip attack during auto-extraction of a JAR file. An attacker could use this flaw to write files to arbitrary locations. This could also be used to replace the main running application and, possibly, break out of the sandbox.	2019-07-31	not yet calculated	<a href="#">CVE-2019-10185</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
adoptopenjdk -- icedtea-web	It was found that in icedtea-web up to and including 1.7.2 and 1.8.2 executable code could be injected in a JAR file without compromising the signature verification. An attacker could use this flaw to inject code in a trusted JAR. The code would be executed inside the sandbox.	2019-07-31	not yet calculated	<a href="#">CVE-2019-10181</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
advantech -- webaccess_hmi_designer	In Advantech WebAccess HMI Designer Version 2.1.9.23 and prior, processing specially crafted MCR files lacking proper validation of user supplied data may cause the system to write outside the intended buffer area, allowing remote code execution.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10961</a> <a href="#">MISC</a>
alcatel-lucent_enterprise -- 8008_cloud_edition_deskphone_voip_phone	On the Alcatel-Lucent Enterprise (ALE) 8008 Cloud Edition Deskphone VoIP phone with firmware 1.50.13, a command injection (missing input validation) issue in the password change field for the Change Password interface allows an authenticated remote attacker in the same network to trigger OS commands via shell commands in a POST request.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14260</a> <a href="#">MISC</a>
alcatel -- linkzone_mw40-v-v1.0_mw40_02.00_02_devices	The web interface of Alcatel LINKZONE MW40-V-V1.0 MW40_LU_02.00_02 devices is vulnerable to an authentication bypass that allows an unauthenticated user to have access to the web interface without knowing the administrator's password.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7163</a> <a href="#">MISC</a>
amcrest -- ip2m-841b_ip_camera	The Amcrest IP2M-841B IP camera firmware version V2.520.AC00.18.R does not require authentication to access the HTTP endpoint /videotalk. An unauthenticated, remote person can connect to this endpoint and listen to the audio the camera is capturing.	2019-07-29	not yet calculated	<a href="#">CVE-2019-3948</a> <a href="#">MISC</a> <a href="#">MISC</a>
ansible -- ansible	A flaw was discovered in the way Ansible templating was implemented in versions before 2.6.18, 2.7.12 and 2.8.2, causing the possibility of information disclosure through unexpected variable substitution. By taking advantage of unintended variable substitution the content of any variable may be disclosed.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10156</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
apache -- activemq_client	It was found that the Apache ActiveMQ client before 5.15.5 exposed a remote shutdown command in the ActiveMQConnection class. An attacker logged into a compromised broker could use this flaw to achieve denial of service on a connected client.	2019-08-01	not yet calculated	<a href="#">CVE-2015-7559</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
	In Apache Solr, the DataImportHandler, an optional but popular module to pull in data from databases and other sources, has a feature in which the whole DIH			

apache -- solr	configuration can come from a request's "dataConfig" parameter. The debug mode of the DIH admin screen uses this to allow convenient debugging / development of a DIH config. Since a DIH config can contain scripts, this parameter is a security risk. Starting with version 8.2.0 of Solr, use of this parameter requires setting the Java System property "enable.dih.dataConfigParam" to true.	2019-08-01	not yet calculated	<a href="#">CVE-2019-0193</a> <a href="#">CONFIRM</a>
apache -- tika	A carefully crafted or corrupt zip file can cause an OOM in Apache Tika's RecursiveParserWrapper in versions 1.7-1.21. Users should upgrade to 1.22 or later.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10088</a> <a href="#">CONFIRM</a>
apache -- tika	In Apache Tika 1.19 to 1.21, a carefully crafted 2003ml or 2006ml file could consume all available SAXParsers in the pool and lead to very long hangs. Apache Tika users should upgrade to 1.22 or later.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10093</a> <a href="#">CONFIRM</a>
apache -- tika	A carefully crafted package/compressed file that, when unzipped/uncompressed yields the same file (a quine), causes a StackOverflowError in Apache Tika's RecursiveParserWrapper in versions 1.7-1.21. Apache Tika users should upgrade to 1.22 or later.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10094</a> <a href="#">CONFIRM</a>
apache -- vcl	Apache VCL versions 2.1 through 2.5 do not properly validate cookie input when determining what node (if any) was previously selected in the privilege tree. The cookie data is then used in an SQL statement. This allows for an SQL injection attack. Access to this portion of a VCL system requires admin level rights. Other layers of security seem to protect against malicious attack. However, all VCL systems running versions earlier than 2.5.1 should be upgraded or patched. This vulnerability was found and reported to the Apache VCL project by ADLab of Venustech.	2019-07-29	not yet calculated	<a href="#">CVE-2018-11772</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apache -- vcl	Apache VCL versions 2.1 through 2.5 do not properly validate form input when processing a submitted block allocation. The form data is then used as an argument to the php built in function strtotime. This allows for an attack against the underlying implementation of that function. The implementation of strtotime at the time the issue was discovered appeared to be resistant to a malicious attack. However, all VCL systems running versions earlier than 2.5.1 should be upgraded or patched. This vulnerability was found and reported to the Apache VCL project by ADLab of Venustech.	2019-07-29	not yet calculated	<a href="#">CVE-2018-11773</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
apache -- vcl	Apache VCL versions 2.1 through 2.5 do not properly validate form input when adding and removing VMs to and from hosts. The form data is then used in SQL statements. This allows for an SQL injection attack. Access to this portion of a VCL system requires admin level rights. Other layers of security seem to protect against malicious attack. However, all VCL systems running versions earlier than 2.5.1 should be upgraded or patched. This vulnerability was found and reported to the Apache VCL project by ADLab of Venustech.	2019-07-29	not yet calculated	<a href="#">CVE-2018-11774</a> <a href="#">MLIST</a> <a href="#">MLIST</a>

avaya -- aura_conferencing	A Cross-Site Scripting (XSS) vulnerability in the Web UI of Avaya Aura Conferencing may allow code execution and potentially disclose sensitive information. Affected versions of Avaya Aura Conferencing include all 8.x versions prior to 8.0 SP14 (8.0.14). Prior versions not listed were not evaluated.	2019-07-31	not yet calculated	<a href="#">CVE-2019-7000</a> <a href="#">CONFIRM</a>
bitdefender -- multiple_products	An issue was discovered in Bitdefender products for Windows (Bitdefender Endpoint Security Tool versions prior to 6.6.8.115; and Bitdefender Antivirus Plus, Bitdefender Internet Security, and Bitdefender Total Security versions prior to 23.0.24.120) that can lead to local code injection. A local attacker with administrator privileges can create a malicious DLL file in %SystemRoot%\System32\ that will be executed with local user privileges.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14242</a> <a href="#">CONFIRM</a>
cisco -- nexus_9000_series_aci_mode_switch_software	A vulnerability in the Link Layer Discovery Protocol (LLDP) subsystem of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an adjacent, unauthenticated attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges. The vulnerability is due to improper input validation of certain type, length, value (TLV) fields of the LLDP frame header. An attacker could exploit this vulnerability by sending a crafted LLDP packet to the targeted device. A successful exploit may lead to a buffer overflow condition that could either cause a DoS condition or allow the attacker to execute arbitrary code with root privileges. Note: This vulnerability cannot be exploited by transit traffic through the device; the crafted packet must be targeted to a directly connected interface. This vulnerability affects Cisco Nexus 9000 Series Fabric Switches in ACI mode if they are running a Cisco Nexus 9000 Series ACI Mode Switch Software release prior to 13.2(7f) or any 14.x release.	2019-07-31	not yet calculated	<a href="#">CVE-2019-1901</a> <a href="#">CISCO</a>
clmg -- clmg	Clmg through 2.6.7 has a heap-based buffer overflow in _load_bmp in Clmg.h because of erroneous memory allocation for a malformed BMP image.	2019-07-31	not yet calculated	<a href="#">CVE-2019-13568</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
clusterlabs -- fence-agents	A flaw was discovered in fence-agents, prior to version 4.3.4, where using non-ASCII characters in a guest VM's comment or other fields would cause fence_rhevm to exit with an exception. In cluster environments, this could lead to preventing automated recovery or otherwise denying service to clusters of which that VM is a member.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10153</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows arbitrary file-read operations for Webmail accounts via Branding APIs (SEC-120).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10815</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 11.52.0.13 does not prevent arbitrary file-read operations via get_information_for_applications (CPANEL-1221).	2019-08-01	not yet calculated	<a href="#">CVE-2015-9291</a> <a href="#">MISC</a>
	cPanel before 55.9999.141 allows arbitrary code execution in the context of the root	2019-08-	not yet	<a href="#">CVE-2016-</a>



cpanel -- cpanel	account because of MakeText interpolation (SEC-89).	01	calculated	<a href="#">10823 MISC</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows Webmail accounts to execute arbitrary code through forwarders (SEC-121).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10816 MISC</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows SQL Injection via the ModSecurity TailWatch log file (SEC-123).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10817 MISC</a>
cpanel -- cpanel	cPanel before 57.9999.54 incorrectly sets log-file permissions in dnsadmin-startup and spamd-startup (SEC-124).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10818 MISC</a>
cpanel -- cpanel	In cPanel before 57.9999.54, user log files become world-readable when rotated by cpanellogd (SEC-125).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10819 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows daemons to access their controlling TTYS (SEC-31).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10820 MISC</a>
cpanel -- cpanel	In cPanel before 55.9999.141, Scripts/addpop reveals a command-line password in a process list (SEC-75).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10821 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows ACL bypass for AppConfig applications via magic_revision (SEC-100).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10830 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows a POP/IMAP cPHulk bypass via account name munging (SEC-107).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10835 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows unauthenticated arbitrary code execution via DNS NS entry poisoning (SEC-90).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10824 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows attackers to bypass a Security Policy by faking static documents (SEC-92).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10825 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows attackers to bypass Two Factor Authentication via DNS clustering requests (SEC-93).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10826 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows self stored XSS in WHM Edit System Mail Preferences (SEC-96).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10827 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows arbitrary code execution because of an unsafe @INC path (SEC-97).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10828 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows arbitrary file-read operations because of a multipart form processing error (SEC-99).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10829 MISC</a>
cpanel -- cpanel	cPanel before 66.0.2 allows resellers to read other accounts' domain log files (SEC-288).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18426 CONFIRM</a>
cpanel -- cpanel	cPanel before 55.9999.141 does not perform as two-factor authentication check when possessing another account (SEC-101).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10831 MISC</a>
	cPanel before 57.9999.54 allows demo-			<a href="#">CVE-</a>

cpanel -- cpanel	mode escape via show_template.stor (SEC-119).	2019-08-01	not yet calculated	<a href="#">2016-10814 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows subaccounts to discover sensitive data through comet feeds (SEC-29).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10856 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows self XSS in X3 Reseller Branding Images (SEC-88).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10822 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows stored XSS in the WHM Feature Manager interface (SEC-86).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10853 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-overwrite operations in scripts/check_system_storable (SEC-78).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10845 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-chown and file-chmod operations during Roundcube database conversions (SEC-79).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10846 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-read and file-write operations via scripts/fixmailboxpath (SEC-80).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10847 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-overwrite operations in scripts/quotacheck (SEC-81).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10848 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary code execution via scripts/syncpaddonswithsqlhost (SEC-83).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10850 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary code execution because of an unsafe @INC path (SEC-46).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10837 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows self XSS in the WHM PHP Configuration editor interface (SEC-84).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10851 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 lacks ACL enforcement in the AppConfig subsystem (SEC-85).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10852 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows self XSS in the X3 Entropy Banner interface (SEC-87).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10854 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 allows jailed accounts to restore files that are outside of the jail (SEC-310).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18384 CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows unauthenticated arbitrary code execution via cpsrvd (SEC-91).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10855 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 mishandles username-based blocking for PRE requests in cPHulkd (SEC-104).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10833 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows unauthenticated arbitrary code execution via DNS NS entry poisoning (SEC-64).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10858 MISC</a>
				<a href="#">CVE-</a>

cpanel -- cpanel	cPanel before 11.54.0.0 allows unauthorized password changes via Webmail API commands (SEC-65).	2019-08-01	not yet calculated	<a href="#">2016-10859 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows unauthorized zone modification via the WHM API (SEC-66).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10860 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 allows use of an unreserved e-mail address in DNS zone SOA records (SEC-306).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18382 CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary file-read operations via the bin/fmq script (SEC-70).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10838 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows arbitrary file-read operations during authentication with caldav (SEC-108).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10836 MISC</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows FTP cPHulk bypass via account name munging (SEC-102).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10832 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary code execution via Maketext injection in PostgresAdmin (SEC-313).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18386 CONFIRM</a>
cpanel -- cpanel	cPanel before 55.9999.141 allows account-suspension bypass via ftp (SEC-105).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10834 MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 can perform unsafe file operations because Jailshell does not set the umask (SEC-315).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18388 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, domain log files become readable after log processing (SEC-273).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18423 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, the Apache HTTP Server configuration file is changed to world-readable when rebuilt (SEC-274).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18424 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, the cpdavd_error_log file can be created with weak permissions (SEC-280).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18425 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows user accounts to be partially created with invalid username formats (SEC-334).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18401 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary file-read operations because of the backup .htaccess modification logic (SEC-345).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18405 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows attackers to read root's crontab file during a short time interval upon enabling or disabling sqloptimizer (SEC-332).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18399 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows collisions because PostgreSQL databases can be assigned to multiple accounts (SEC-325).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18392 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary code execution via Maketext injection in a Reseller style upload (SEC-314).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18387 CONFIRM</a>

cpanel -- cpanel	cPanel before 68.0.15 allows string format injection in dovecot-xaps-plugin (SEC-318).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18389</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows demo accounts to create databases and users (SEC-271).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18421</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	DnsUtils in cPanel before 68.0.15 allows zone creation for hostname and account subdomains (SEC-331).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18398</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows code execution in the context of the root account because of weak permissions on incremental backups (SEC-322).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18390</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows attackers to read backup files because they are world-readable during a short time interval (SEC-323).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18391</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 57.9999.54 allows self XSS during ftp account creation under addon domains (SEC-118).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10813</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 does not have a sufficient list of reserved usernames (SEC-327).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18394</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 does not preserve permissions for local backup transport (SEC-330).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18397</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows arbitrary file-read operations via Exim vdomainaliases (SEC-329).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18396</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 does not block a username of postmaster, which might allow reception of private e-mail (SEC-326).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18393</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 does not block a username of ssl (SEC-328).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18395</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, EasyApache 4 conversion sets weak domlog ownership and permissions (SEC-272).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18422</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons processing (SEC-269).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18420</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 writes home-directory backups to an incorrect location (SEC-309).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18383</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows stored XSS in WHM MySQL Password Change interfaces (SEC-282).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18408</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.0 allows a bypass of the e-mail sending limit (SEC-60).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10857</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 68.0.15 allows unprivileged users to access restricted directories during account restores (SEC-311).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18385</a> <a href="#">CONFIRM</a>

cpanel -- cpanel	In cPanel before 67.9999.103, the backup system overwrites root's home directory when a mount disappears (SEC-299).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18413</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows stored XSS during a cpaddons moderated upgrade (SEC-336).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18402</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows code execution in the context of the nobody account via Mailman archives (SEC-337).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18403</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows domain data to be deleted for domains with the .lock TLD (SEC-341).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18404</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows code execution in the context of shared users via JSON-API (SEC-76).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10843</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows SQL injection during eximstats processing (SEC-276).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18406</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 does not enforce SSL hostname verification for the support-agreement download (SEC-279).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18407</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 67.9999.103, the backup interface could return a backup archive with all MySQL databases (SEC-283).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18409</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons uninstallation (SEC-266).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18419</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 67.9999.103, a user account's backup archive could contain all MySQL databases on the server (SEC-284).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18410</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The "addon domain conversion" feature in cPanel before 67.9999.103 can copy all MySQL databases to the new account (SEC-285).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18411</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows Apache HTTP Server log files to become world-readable because of mishandling on an account rename (SEC-296).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18412</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows an open redirect in /unprotected/redirect.html (SEC-300).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18414</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.15 allows local root code execution via cpdavd (SEC-333).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18400</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows code execution in the context of the mailman account because of incorrect environment-variable filtering (SEC-302).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18415</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 67.9999.103 allows arbitrary file-overwrite operations during a Roundcube SQLite schema update (SEC-303).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18416</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons installation (SEC-263).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18417</a> <a href="#">CONFIRM</a>



cpanel -- cpanel	cPanel before 66.0.2 allows stored XSS during WHM cPAddons file operations (SEC-265).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18418</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The chcpass script in cPanel before 11.54.0.4 reveals a password hash (SEC-77).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10844</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows certain file-chmod operations in scripts/secureit (SEC-82).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10849</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows certain file-read operations in bin/setup_global_spam_filter.pl (SEC-74).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10842</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to redirect web traffic (SEC-245).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18441</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows code execution by webmail and demo accounts via a store_filter API call (SEC-236).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18433</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows code execution in the context of the root account via a SET_VHOST_LANG_PACKAGE multilang adminbin call (SEC-237).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18434</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via the BoxTrapper API (SEC-238).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18435</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to read files via a Fileman::getfileactions API2 call (SEC-239).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18436</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows a Webmail account to execute code via forwarders (SEC-240).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18437</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via an ImageManager_dimensions API call (SEC-243).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18439</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows certain file-rename operations in the context of the root account via scripts/convert_roundcube_mysql2sqlite (SEC-254).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18449</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo users to execute traceroute via api2 (SEC-244).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18440</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute Cpanel::SPFUI API commands (SEC-246).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18442</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 66.0.1 does not reliably perform suspend/unsuspend operations on accounts (CPANEL-13941).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18431</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows arbitrary file-read operations during File Restoration (SEC-436).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20891</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute SSH API commands	2019-08-	not yet	<a href="#">CVE-2017-</a>

	(SEC-248).	02	calculated	<a href="#">18444</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 does not enforce demo restrictions for SSL API calls (SEC-249).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18445</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows file-read and file-write operations for demo accounts via the SourceIPCheck API (SEC-250).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18446</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via the ClamScanner_getsocket API (SEC-251).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18447</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows certain file-read operations via a Serverinfo_manpage API call (SEC-252).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18448</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows arbitrary zone file modifications during record edits (SEC-426).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20890</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	The bin/mkxhostspasswd script in cPanel before 11.54.0.4 discloses password hashes (SEC-73).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10841</a> <a href="#">MISC</a>
cpanel -- cpanel	cPanel before 74.0.0 allows arbitrary zone file modifications because of incorrect CAA record handling (SEC-439).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20892</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 64.0.21, Horde MySQL to SQLite conversion can leak a database password (SEC-234).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18432</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, user and group ownership may be incorrectly set when using reassign_post_terminate_cruft (SEC-294).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18430</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 does not prevent e-mail account suspensions from being applied to unowned accounts (SEC-411).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20934</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows does not preserve security policy questions across an account rename (SEC-223).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18461</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	In cPanel before 62.0.17, addon domain conversion did not require a package for resellers (SEC-208).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18455</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows self XSS in the WHM cPAddons showsecurity interface (SEC-217).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18456</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows arbitrary file-read operations via WHM /styled/ URLs (SEC-218).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18457</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows file overwrite when renaming an account (SEC-219).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18458</a> <a href="#">CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.24 allows stored XSS in the WHM cPAddons install interface (SEC-262).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18454</a> <a href="#">CONFIRM</a>
	cPanel before 64.0.21 does not preserve	2019-08-	not yet	<a href="#">CVE-2017-</a>

cpanel -- cpanel	supplemental groups across account renames (SEC-260).	02	calculated	<a href="#">18453 CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows arbitrary code execution during automatic SSL installation (SEC-221).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18460 CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows arbitrary code execution during account modification (SEC-220).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18459 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows file modification in the context of the root account because of incorrect HTTP authentication (SEC-424).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20888 CONFIRM</a>
cpanel -- cpanel	cPanel before 62.0.17 allows code execution in the context of the root account via a long DocumentRoot path (SEC-225).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18463 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo accounts to execute code via Encoding API calls (SEC-242).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18438 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows local users to disable the ClamAV daemon (SEC-409).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20873 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows self XSS in the WHM "Create a New Account" interface (SEC-428).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20874 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.8 allows arbitrary file-write operations in the context of the root account during WHM Force Password Change (SEC-447).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20882 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 insecurely stores phpMyAdmin session files (SEC-418).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20886 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows attackers to read a user's crontab file during a short time interval upon a cPAddon upgrade (SEC-257).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18451 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows certain file-read operations via password file caching (SEC-425).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20889 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows code execution via Rails configuration files (SEC-259).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18452 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows demo and suspended accounts to use SSH port forwarding (SEC-247).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18443 CONFIRM</a>
cpanel -- cpanel	cPanel before 64.0.21 allows certain file-chmod operations via /scripts/convert_roundcube_mysql2sqlite (SEC-255).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18450 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read root's crontab file during a short time interval upon a post-update task (SEC-352).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20943 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows stored XSS in the WHM cPAddons installation interface (SEC-398).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20899 CONFIRM</a>
	cPanel before 70.0.23 allows stored XSS			<a href="#">CVE-</a>

cpanel -- cpanel	in via a WHM "Reset a DNS Zone" action (SEC-412).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20935 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows arbitrary file-chmod operations during legacy incremental backups (SEC-338).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20909 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read the SRS secret via exim.conf (SEC-308).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20936 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, Apache HTTP Server domlogs become temporarily world-readable during log processing (SEC-290).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18428 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows stored XSS in the YUM autorepair functionality (SEC-399).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20900 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to make API calls that bypass the cron feature restriction (SEC-427).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20904 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to make API calls that bypass the images feature restriction (SEC-430).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20906 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows .htaccess restrictions bypass when Htaccess Optimization is enabled (SEC-401).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20930 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 does not enforce the Mime::list_hotlinks API feature restriction (SEC-432).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20907 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows arbitrary file-read operations during pkgacct custom template handling (SEC-435).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20908 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows arbitrary file-read and file-unlink operations via WHM style uploads (SEC-378).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20924 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows code injection in the WHM cPAddons interface (SEC-394).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20896 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows local privilege escalation via the WHM Legacy Language File Upload interface (SEC-379).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20925 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows local privilege escalation via the WHM Locale XML Upload interface (SEC-380).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20926 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows jailshell escape because of incorrect crontab parsing (SEC-382).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20927 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows stored XSS via the cpaddons vendor interface (SEC-391).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20928 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows an open redirect via the /unprotected/redirect.html endpoint (SEC-392).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20929 CONFIRM</a>
	In cPanel before 66.0.2, Apache HTTP			<a href="#">CVE-</a>

cpanel -- cpanel	Server SSL domain logs can persist on disk after an account termination (SEC-291).	2019-08-02	not yet calculated	<a href="#">2017-18429 CONFIRM</a>
cpanel -- cpanel	In cPanel before 66.0.2, weak log-file permissions can occur after account modification (SEC-289).	2019-08-02	not yet calculated	<a href="#">CVE-2017-18427 CONFIRM</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows SQL injection in bin/horde_update_usernames (SEC-71).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10839 MISC</a>
cpanel -- cpanel	cPanel before 11.54.0.4 allows arbitrary code execution during locale duplication (SEC-72).	2019-08-01	not yet calculated	<a href="#">CVE-2016-10840 MISC</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows arbitrary file-unlink operations via the cPAddons moderation system (SEC-395).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20897 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows e-mail injection during cPAddons moderation (SEC-396).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20898 CONFIRM</a>
cpanel -- cpanel	In cPanel before 71.9980.37, API tokens retain ACLs after those ACLs are removed from the corresponding accounts (SEC-393).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20895 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows certain file-write operations via the telnetcr script (SEC-356).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20947 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 does not validate database and dbuser names during renames (SEC-321).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20937 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows a user to discover contents of directories (that are not owned by that user) by leveraging backups (SEC-339).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20939 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read root's crontab file during a short time interval upon the enabling of backups (SEC-342).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20940 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows arbitrary file-read operations via restore adminbin (SEC-349).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20941 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read root's crontab file during a short time interval upon configuring crontab (SEC-351).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20942 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read a copy of httpd.conf that is created during a syntax test (SEC-353).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20944 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 makes web-site contents accessible to other local users via Git repositories (SEC-443).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20894 CONFIRM</a>
cpanel -- cpanel	bin/csvprocess in cPanel before 68.0.27 allows insecure file operations (SEC-354).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20945 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows attackers to read zone information because a world-readable archive is created by the archive_sync_zones script (SEC-355).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20946 CONFIRM</a>
				<a href="#">CVE-</a>



cpanel -- cpanel	cPanel before 70.0.23 exposes Apache HTTP Server logs after creation of certain domains (SEC-406).	2019-08-01	not yet calculated	<a href="#">2018-20932 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in cPanel Backup Restoration (SEC-383).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20948 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 allows demo accounts to execute code via the Landing Page (SEC-405).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20931 CONFIRM</a>
cpanel -- cpanel	cPanel before 71.9980.37 allows attackers to make API calls that bypass the backup feature restriction (SEC-429).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20905 CONFIRM</a>
cpanel -- cpanel	cPanel before 74.0.0 allows file-rename operations during account renames (SEC-442).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20893 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in WHM Apache Configuration Include Editor (SEC-385).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20949 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 does not enforce ownership during addpkgext and delpkgext WHM API calls (SEC-324).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20938 CONFIRM</a>
cpanel -- cpanel	cPanel before 70.0.23 has Stored XSS via an WHM Edit DNS Zone action (SEC-410).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20933 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in the WHM listips interface (SEC-389).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20953 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 creates world-readable files during use of WHM Apache Includes Editor (SEC-388).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20952 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self XSS in WHM Spamd Startup Config (SEC-387).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20951 CONFIRM</a>
cpanel -- cpanel	cPanel before 68.0.27 allows self stored XSS in WHM Account Transfer (SEC-386).	2019-08-01	not yet calculated	<a href="#">CVE-2018-20950 CONFIRM</a>
crypto++ -- crypto++	Crypto++ 8.3.0 and earlier contains a timing side channel in ECDSA signature generation. This allows a local or remote attacker, able to measure the duration of hundreds to thousands of signing operations, to compute the private key used. The issue occurs because scalar multiplication in ecp.cpp (prime field curves, small leakage) and algebra.cpp (binary field curves, large leakage) is not constant time and leaks the bit length of the scalar among other information.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14318 MISC MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_and_dwl-8610ap_ax_devices	An issue was discovered on D-Link 6600-AP, DWL-3600AP, and DWL-8610AP Ax 4.2.0.14 21/03/2019 devices. There is post-authenticated Certificate and RSA Private Key extraction through an insecure sslcert-get.cgi HTTP command.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14334 MISC MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is post-	2019-08-	not yet	<a href="#">CVE-2019-14336</a>

	authenticated dump of all of the config files through a certain admin.cgi?action=insecure HTTP request.	01	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a pre-authenticated denial of service attack against the access point via a long action parameter to admin.cgi.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14333</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is an ability to escape to a shell in the restricted command line interface, as demonstrated by the '/bin/sh -c wget' sequence.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14337</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is use of weak ciphers for SSH such as diffie-hellman-group1-sha1.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14332</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- 6600-ap_and_dwl_3600ap_ax_devices	An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/2019 devices. There is a post-authentication admin.cgi?action=XSS vulnerability on the management interface.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14338</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dva-5592	The web interface of the D-Link DVA-5592 20180823 is vulnerable to XSS because HTML form parameters are directly reflected.	2019-08-02	not yet calculated	<a href="#">CVE-2019-6968</a> <a href="#">MISC</a>
d-link -- dva-5592	The web interface of the D-Link DVA-5592 20180823 is vulnerable to an authentication bypass that allows an unauthenticated user to have access to sensitive information such as the Wi-Fi password and the phone number (if VoIP is in use).	2019-08-02	not yet calculated	<a href="#">CVE-2019-6969</a> <a href="#">MISC</a>
das_q -- das_q	Das Q before 2019-08-02 allows web sites to execute arbitrary code on client machines, as demonstrated by a cross-origin /install request with an attacker-controlled releaseUrl, which triggers download and execution of code within a ZIP archive.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14551</a> <a href="#">MISC</a>
django -- django	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If django.utils.text.Truncator's chars() and words() methods were passed the html=True argument, they were extremely slow to evaluate certain inputs due to a catastrophic backtracking vulnerability in a regular expression. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which were thus vulnerable.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14232</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
django -- django	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. If passed certain inputs, django.utils.encoding.uri_to_iri could lead to significant memory usage due to a recursion when percent-encoding invalid UTF-8 octet sequences.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14235</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
django -- django	An issue was discovered in Django 1.11.x before 1.11.23, 2.1.x before 2.1.11, and 2.2.x before 2.2.4. Due to the behaviour of the underlying HTMLParser, django.utils.html.strip_tags would be	2019-08-02	not yet calculated	<a href="#">CVE-2019-14233</a> <a href="#">MISC</a>

	extremely slow to evaluate certain inputs containing large sequences of nested incomplete HTML entities.			<a href="#">MISC</a> <a href="#">CONFIRM</a>
dnsmasq -- dnsmasq	Improper bounds checking in Dnsmasq before 2.76 allows an attacker controlled DNS server to send large DNS packets that result in a read operation beyond the buffer allocated for the packet, a different vulnerability than CVE-2017-14491.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14513</a> <a href="#">MISC</a>
docker -- docker	In Docker 19.03.x before 19.03.1 linked against the GNU C Library (aka glibc), code injection can occur when the nsswitch facility dynamically loads a library inside a chroot that contains the contents of the container.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14271</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
docker -- docker-credential-helpers	docker-credential-helpers before 0.6.3 has a double free in the List functions.	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020014</a> <a href="#">MISC</a> <a href="#">MISC</a>
dolibarr_foundation -- dolibarr_erp_and_crm	Dolibarr ERP/CRM 9.0.1 provides a module named website that provides for creation of public websites with a WYSIWYG editor. It was identified that the editor also allowed inclusion of dynamic code, which can lead to code execution on the host machine. An attacker has to check a setting on the same page, which specifies the inclusion of dynamic content. Thus, a lower privileged user of the application can execute code under the context and permissions of the underlying web server.	2019-07-29	not yet calculated	<a href="#">CVE-2019-11201</a> <a href="#">MISC</a>
dolibarr_foundation -- dolibarr_erp_and_crm	Dolibarr ERP/CRM 9.0.1 provides a web-based functionality that backs up the database content to a dump file. However, the application performs insufficient checks on the export parameters to mysqldump, which can lead to execution of arbitrary binaries on the server. (Malicious binaries can be uploaded by abusing other functionalities of the application.)	2019-07-29	not yet calculated	<a href="#">CVE-2019-11200</a> <a href="#">MISC</a>
dolibarr_foundation -- dolibarr_erp_and_crm	Dolibarr ERP/CRM 9.0.1 was affected by stored XSS within uploaded files. These vulnerabilities allowed the execution of a JavaScript payload each time any regular user or administrative user clicked on the malicious link hosted on the same domain. The vulnerabilities could be exploited by low privileged users to target administrators. The viewimage.php page did not perform any contextual output encoding and would display the content within the uploaded file with a user-requested MIME type.	2019-07-29	not yet calculated	<a href="#">CVE-2019-11199</a> <a href="#">MISC</a>
draytek -- draytek_routers	DrayTek routers before 2018-05-23 allow CSRF attacks to change DNS or DHCP settings, a related issue to CVE-2017-11649.	2019-07-31	not yet calculated	<a href="#">CVE-2018-20872</a> <a href="#">MISC</a>
eclipse -- openj9	All builds of Eclipse OpenJ9 prior to 0.15 contain a bug where the loop versioner may fail to privatize a value that is pulled out of the loop by versioning - for example if there is a condition that is moved out of the loop that reads a field we may not privatize the value of that field in the modified copy of the loop allowing the test to see one value of the field and subsequently the loop to see a modified field value without retesting the condition	2019-07-30	not yet calculated	<a href="#">CVE-2019-11775</a> <a href="#">CONFIRM</a>

	moved out of the loop. This can lead to a variety of different issues but read out of array bounds is one major consequence of these problems.			
edx -- edx-platform	edx-platform before 2016-06-06 allows CSRF.	2019-07-29	not yet calculated	<a href="#">CVE-2016-10766</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
edx -- edx-platform	edx-platform before 2018-07-18 allows XSS via a response to a Chemical Equation advanced problem.	2019-07-30	not yet calculated	<a href="#">CVE-2018-20859</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
edx -- edx-platform	edx-platform before 2017-08-03 allows attackers to trigger password-reset e-mail messages in which the reset link has an attacker-controlled domain name.	2019-07-30	not yet calculated	<a href="#">CVE-2017-18380</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
edx -- edx-platform	edx-platform before 2016-06-10 allows account activation with a spoofed e-mail address.	2019-07-29	not yet calculated	<a href="#">CVE-2016-10765</a> <a href="#">CONFIRM</a>
edx -- open_edx	The installation process in Open edX before 2017-01-10 exposes a MongoDB instance to external connections with default credentials.	2019-07-30	not yet calculated	<a href="#">CVE-2017-18381</a> <a href="#">MISC</a> <a href="#">MISC</a>
elastic -- apm	A TLS certificate validation flaw was found in Elastic APM agent for Ruby versions before 2.9.0. When specifying a trusted server CA certificate via the 'server_ca_cert' setting, the Ruby agent would not properly verify the certificate returned by the APM server. This could result in a man in the middle style attack against the Ruby agent.	2019-07-30	not yet calculated	<a href="#">CVE-2019-7615</a> <a href="#">MISC</a>
elastic -- elasticsearch	A race condition flaw was found in the response headers Elasticsearch versions before 7.2.1 and 6.8.2 returns to a request. On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.	2019-07-30	not yet calculated	<a href="#">CVE-2019-7614</a> <a href="#">MISC</a>
elastic -- kibana	Kibana versions before 6.8.2 and 7.2.1 contain a server side request forgery (SSRF) flaw in the graphite integration for Timelion visualizer. An attacker with administrative Kibana access could set the timelion:graphite.url configuration option to an arbitrary URL. This could possibly lead to an attacker accessing external URL resources as the Kibana process on the host system.	2019-07-30	not yet calculated	<a href="#">CVE-2019-7616</a> <a href="#">MISC</a>
elm327 -- obd2_bluetooth_device	A clone version of an ELM327 OBD2 Bluetooth device has a hardcoded PIN, leading to arbitrary commands to an OBD-II bus of a vehicle, as demonstrated by turning off the vehicle's lights.	2019-07-31	not yet calculated	<a href="#">CVE-2019-12797</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	SubTypeValidator.java in FasterXML jackson-databind before 2.9.9.2 mishandles default typing when ehcache is used, leading to remote code execution.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14379</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9.2. This occurs when			<a href="#">CVE-2019-</a>

fasterxml -- jackson-databind	Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the logback jar in the classpath.	2019-07-30	not yet calculated	<a href="#">14439 MISC MISC MISC</a>
foreman -- foreman-tasks	An authentication bypass vulnerability was discovered in foreman-tasks before 0.15.7. Previously, commit tasks were searched through find_resource, which performed authorization checks. After the change to Foreman, an unauthenticated user can view the details of a task through the web UI or API, if they can discover or guess the UUID of the task.	2019-07-31	not yet calculated	<a href="#">CVE-2019-10198 CONFIRM MISC</a>
freetype -- freetype	In FreeType before 2.6.1, a buffer over-read occurs in type1/t1parse.c on function T1_Get_Private_Dict where there is no check that the new values of cur and limit are sensible before going to Again.	2019-07-30	not yet calculated	<a href="#">CVE-2015-9290 MISC MISC</a>
gnome -- evolution-ews	It was discovered evolution-ews before 3.31.3 does not check the validity of SSL certificates. An attacker could abuse this flaw to get confidential information by tricking the user into connecting to a fake server without the user noticing the difference.	2019-08-01	not yet calculated	<a href="#">CVE-2019-3890 CONFIRM CONFIRM</a>
glibc -- glibc	GnuCOBOL 2.2 has a buffer overflow in cb_evaluate_expr in cobc/field.c via crafted COBOL source code.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14486 MISC</a>
glibc -- glibc	GnuCOBOL 2.2 has a stack-based buffer overflow in cb_encode_program_id in cobc/typeck.c via crafted COBOL source code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14541 MISC</a>
glibc -- glibc	GnuCOBOL 2.2 has a heap-based buffer overflow in read_literal in cobc/scanner.l via crafted COBOL source code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14528 MISC</a>
glibc -- glibc	GnuCOBOL 2.2 has a buffer overflow in cb_push_op in cobc/field.c via crafted COBOL source code.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14468 MISC</a>
gnu -- binutils	apply_relocations in readelf.c in GNU Binutils 2.32 contains an integer overflow that allows attackers to trigger a write access violation (in byte_put_little_endian function in elfcomm.c) via an ELF file, as demonstrated by readelf.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14444 MISC</a>
gogs -- gogs	routes/api/v1/api.go in Gogs 0.11.86 lacks permission checks for routes: deploy keys, collaborators, and hooks.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14544 MISC</a>
happypoint -- happypoint_mobile_app	When processing Deeplink scheme, Happypoint mobile app 6.3.19 and earlier versions doesn't check Deeplink URL correctly. This could lead to javascript code execution, url redirection, sensitive information disclosure. An attacker can exploit this issue by enticing an unsuspecting user to open a specific malicious URL.	2019-08-01	not yet calculated	<a href="#">CVE-2019-9140 CONFIRM</a>
hasura -- graphql_engine	graphql-engine (aka Hasura GraphQL Engine) before 1.0.0-beta.3 mishandles the audience check while verifying JWT.	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020015 MISC</a>
	A potential security vulnerability has been identified in HP2910al-48G version W.15.14.0016. The attack exploits an xss injection by setting the attack vector in one of the switch persistent configuration fields			



hewlett_packard_enterprise -- hp2910al-48g_switches	(management URL, location, contact). But admin privileges are required to configure these fields thereby reducing the likelihood of exploit. HPE Aruba has provided firmware updates to resolve the vulnerability in HP 2910-48G al Switch. Please update to W.15.14.0017.	2019-08-01	not yet calculated	<a href="#">CVE-2019-5401</a> <a href="#">CONFIRM</a>
humhub -- humhub	HumHub Social Network Kit Enterprise v1.3.13 allows remote attackers to find the user accounts existing on any Social Network Kits (including self-hosted ones) by brute-forcing the username after the /u/ initial URI substring, aka Response Discrepancy Information Exposure.	2019-07-29	not yet calculated	<a href="#">CVE-2019-12743</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- i2_intelligent_analysis_platform	IBM i2 Intelligent Analysis Platform 9.0.0 through 9.1.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 157007.	2019-07-30	not yet calculated	<a href="#">CVE-2019-4062</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3, 1.1.3.1, and 1.1.3.2 could allow an unauthorized local user to create unique catalog names that could cause a denial of service. IBM X-Force ID: 160296.	2019-08-02	not yet calculated	<a href="#">CVE-2019-4275</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- spectrum_protect_for_enterprise_resource_planning	IBM Spectrum Protect for Enterprise Resource Planning 7.1 and 8.1, if tracing is activated, the IBM Spectrum Protect node password may be displayed in plain text in the ERP trace file. IBM X-Force ID: 154280.	2019-08-02	not yet calculated	<a href="#">CVE-2018-1987</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
imgix -- imgix	Imgix through 2019-06-19 allows remote attackers to cause a denial of service (resource consumption) by manipulating a small JPEG file to specify dimensions of 64250x64250 pixels, which is mishandled during an attempt to load the 'whole image' into memory.	2019-07-29	not yet calculated	<a href="#">CVE-2019-13655</a> <a href="#">MISC</a>
jolokia -- jolokia	A flaw was found in Jolokia versions from 1.2 to before 1.6.1. Affected versions are vulnerable to a system-wide CSRF. This holds true for properly configured instances with strict checking for origin and referrer headers. This could result in a Remote Code Execution attack.	2019-08-01	not yet calculated	<a href="#">CVE-2018-10899</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
libav -- libav	An issue was discovered in Libav 12.3. An access violation allows remote attackers to cause a denial of service (application crash), as demonstrated by avconv. This is related to ff_mpa_synth_filter_float in avcodec/mpegauddiodsp_template.c.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14441</a> <a href="#">MISC</a>
libav -- libav	In mpc8_read_header in libavformat/mpc8.c in Libav 12.3, an input file can result in an avio_seek infinite loop and hang, with 100% CPU consumption. Attackers could leverage this vulnerability to cause a denial of service via a crafted file.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14442</a> <a href="#">MISC</a>
liblouis -- liblouis	A vulnerability was found in liblouis, versions 2.5.x before 2.5.4. A stack-based buffer overflow was found in findTable() in liblouis. An attacker could create a malicious file that would cause applications that use liblouis (such as Orca) to crash, or potentially execute arbitrary code when opened.	2019-08-02	not yet calculated	<a href="#">CVE-2014-8184</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
libopenmpt -- libopenmpt	J2B in libopenmpt before 0.4.2 allows an assertion failure during file parsing with	2019-07-	not yet	<a href="#">CVE-2019-</a>

	debug STLs.	30	calculated	<a href="#">14383 MISC</a>
libopenmpt -- libopenmpt	libopenmpt before 0.3.11 allows a crash with certain malformed custom tunings in MPTM files.	2019-07-30	not yet calculated	<a href="#">CVE-2018-20861 MISC</a>
libopenmpt -- libopenmpt	DSM in libopenmpt before 0.4.2 allows an assertion failure during file parsing with debug STLs.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14382 MISC</a>
libopenmpt -- libopenmpt	libopenmpt before 0.4.3 allows a crash due to a NULL pointer dereference when doing a portamento from an OPL instrument to an empty instrument note map slot.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14381 CONFIRM</a>
libvirt -- libvirt	It was discovered that libvirt before versions 4.10.1 and 5.4.1 would permit read-only clients to use the virDomainSaveImageGetXMLDesc() API, specifying an arbitrary path which would be accessed with the permissions of the libvirt process. An attacker with access to the libvirt socket could use this to probe the existence of arbitrary files, cause denial of service or cause libvirt to execute arbitrary programs.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10161 CONFIRM CONFIRM CONFIRM</a>
libvirt -- libvirt	It was discovered that libvirt, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirt would execute an arbitrary program when the domain was resumed.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10166 CONFIRM CONFIRM</a>
libvirt -- libvirt	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirt to execute a crafted executable with its own privileges.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10168 CONFIRM CONFIRM</a>
libvirt -- libvirt	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirt to execute a crafted executable with its own privileges.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10167 CONFIRM CONFIRM</a>
linux -- linux_kernel	A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an ioctl was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw to crash the system, corrupt memory, or create other adverse security affects.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10142 CONFIRM</a>
	A flaw was found in the Linux kernel's NFS implementation, all versions 3.x and all			

linux -- linux_kernel	versions 4.x up to 4.20. An attacker, who is able to mount an exported NFS filesystem, is able to trigger a null pointer dereference by using an invalid NFS sequence. This can panic the machine and deny access to the NFS server. Any outstanding disk writes to the NFS server will be lost.	2019-07-30	not yet calculated	<a href="#">CVE-2018-16871 CONFIRM</a>
magento -- magento	A file upload filter bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with admin privileges to edit configuration keys to remove file extension filters, potentially resulting in the malicious upload and execution of malicious files on the server.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7912 CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 due to insufficient authorizations checks. This can be abused by a user with admin privileges to add users to company accounts or modify existing user details.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7872 CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can result in unintended deletion of user roles.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7874 CONFIRM</a>
magento -- magento	An access control bypass vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An unauthenticated user can bypass access controls via REST API calls to assign themselves to an arbitrary company, thereby gaining read access to potentially confidential information.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7950 CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can lead to unintended data deletion from customer pages.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7851 CONFIRM</a>
magento -- magento	A denial-of-service vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. Under certain conditions, an unauthenticated attacker could force the Magento store's full page cache to serve a 404 page to customers.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7915 CONFIRM</a>
magento -- magento	An information disclosure vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to create email templates could leak sensitive data via a malicious email template.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7888 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to access shipment settings can execute arbitrary code via server-side request forgery.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7892 CONFIRM</a>
magento -- magento	An Insecure Direct Object Reference (IDOR) vulnerability exists in the order processing workflow of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can lead to unauthorized access to order details.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7890 CONFIRM</a>

magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to layouts can execute arbitrary code through a combination of product import, crafted csv file and XML layout update.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7896 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to layouts can execute arbitrary code through a crafted XML layout update.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7895 CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can cause unwanted items to be added to a shopper's cart due to an insufficiently robust anti-CSRF token implementation.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7857 CONFIRM</a>
magento -- magento	A cryptographic flaw in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could be abused by an unauthenticated user to discover an invariant used in gift card generation.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7855 CONFIRM</a>
magento -- magento	A path disclosure vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. Requests for a specific file path could result in a redirect to the URL of the Magento admin panel, disclosing its location to potentially unauthorized parties.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7852 CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 can lead to unauthorized disclosure of company credit history details.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7854 CONFIRM</a>
magento -- magento	A path traversal vulnerability in the WYSIWYG editor for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could result in unauthorized access to uploaded images due to insufficient access control.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7859 CONFIRM</a>
magento -- magento	A server-side request forgery (SSRF) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by authenticated user with admin privileges to manipulate shipment settings to execute arbitrary code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7923 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to email templates can execute arbitrary code by previewing a malicious template.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7903 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to create or edit a product can execute arbitrary code via malicious XML layout updates.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7942 CONFIRM</a>
	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9,			<a href="#">CVE-</a>

magento -- magento	Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to edit product content pages to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">2019-7927 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify node attributes to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7926 CONFIRM</a>
magento -- magento	An information leakage vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. A SOAP web service endpoint does not properly enforce parameters related to access control. This could be abused to leak customer information via crafted SOAP requests.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7951 CONFIRM</a>
magento -- magento	Insufficient enforcement of user access controls in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 could enable a low-privileged user to make unauthorized environment configuration changes.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7904 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify content block titles to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7936 CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an administrator with limited privileges to delete the downloadable products folder.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7925 CONFIRM</a>
magento -- magento	A reflected cross-site scripting vulnerability exists on the customer cart checkout page of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by sending a victim a crafted URL that results in malicious javascript execution in the victim's browser.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7939 CONFIRM</a>
magento -- magento	An information leakage vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges may be able to view metadata of a trusted device used by another administrator via a crafted http request.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7929 CONFIRM</a>
magento -- magento	A denial-of-service (DoS) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. By abusing insufficient brute-forcing defenses in the token exchange protocol, an unauthenticated attacker could disrupt transactions between the Magento merchant and PayPal.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7928 CONFIRM</a>
magento -- magento	A file upload restriction bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with administrator privileges to the import feature can make modifications to a configuration file, resulting in potentially unauthorized	2019-08-02	not yet calculated	<a href="#">CVE-2019-7930 CONFIRM</a>



	removal of file upload restrictions. This can result in arbitrary code execution when a malicious file is then uploaded and executed on the system.			
magento -- magento	A cryptographic flaw in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9 and Magento 2.3 prior to 2.3.2 resulted in storage of sensitive information with an algorithm that is insufficiently resistant to brute force attacks.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7858 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to store product attributes to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7937 CONFIRM</a>
magento -- magento	A cryptographically weak pseudo-random number generator is used in multiple security relevant contexts in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7860 CONFIRM</a>
magento -- magento	A security bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 that could be abused to execute arbitrary PHP code. An authenticated user can bypass security protections that prevent arbitrary PHP script upload via form data injection.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7871 CONFIRM</a>
magento -- magento	Insufficient server-side validation of user input could allow an attacker to bypass file upload restrictions in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7861 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to edit Product information via the TinyMCE editor.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7866 CONFIRM</a>
magento -- magento	A cryptographic flaw exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. A weak cryptographic mechanism is used to generate the initialization vector in multiple security relevant contexts.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7886 CONFIRM</a>
magento -- magento	Insufficient input validation in the config builder of the Elastic search module could lead to remote code execution in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This vulnerability could be abused by an authenticated user with the ability to configure the catalog search.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7885 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to marketing email templates to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7880 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to manage orders can inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7877 CONFIRM</a>
	A stored cross-site scripting vulnerability			

magento -- magento	exists in the product catalog form of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to the product catalog to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7921 CONFIRM</a>
magento -- magento	A cross-site request forgery vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can result in unintended deletion of the store design schedule.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7873 CONFIRM</a>
magento -- magento	A remote code execution vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to manipulate layouts can insert a malicious payload into the layout.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7876 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with permissions to manage customer groups.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7869 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with permissions to manage tax rules.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7868 CONFIRM</a>
magento -- magento	A server-side request forgery (SSRF) vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with admin privileges to manipulate shipment methods to execute arbitrary code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7913 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to manage orders and order status.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7867 CONFIRM</a>
magento -- magento	A reflected cross-site scripting vulnerability exists in the Product widget chooser functionality in the admin panel for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7862 CONFIRM</a>
magento -- magento	A cross-site request forgery (CSRF) vulnerability exists in the checkout cart item of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited at the time of editing or configuration.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7865 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to the tax notifications configuration in the Magento admin panel.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7853 CONFIRM</a>
magento -- magento	An insecure direct object reference (IDOR) vulnerability exists in the RSS feeds of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can lead to unauthorized access to order details.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7864 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel of Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9,	2019-08-	not yet	<a href="#">CVE-</a>

	Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify product information.	02	calculated	<a href="#">2019-7908 CONFIRM</a>
magento -- magento	A stored cross-site scripting vulnerability exists in the admin panel for Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to products and categories.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7863 CONFIRM</a>
magento -- magento_and_magento_commerce	A defense-in-depth check was added to mitigate inadequate session validation handling by 3rd party checkout modules. This impacts Magento 1.x prior to 1.9.4.2, Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9 and Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7849 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to customer configurations to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7897 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the WYSIWYG editor of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to the editor can inject malicious SWF files.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7882 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to email templates.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7909 CONFIRM</a>
magento -- multiple_products	A server-side request forgery (SSRF) vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This can be exploited by an authenticated user with access to the admin panel to manipulate system configuration and execute arbitrary code.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7911 CONFIRM</a>
magento -- multiple_products	A remote code execution vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with admin privileges to create sitemaps can execute arbitrary PHP code by creating a malicious sitemap file.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7932 CONFIRM</a>
magento -- multiple_products	A cross-site scripting mitigation bypass exists in Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user to escalate privileges (admin vs. admin XSS attack).	2019-08-02	not yet calculated	<a href="#">CVE-2019-7881 CONFIRM</a>
	Names of disabled downloadable products could be disclosed due to inadequate validation of user input in Magento Open			<a href="#">CVE-</a>

magento -- multiple_products	Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7899 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to edit newsletter templates to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7934 CONFIRM</a>
magento -- multiple_products	Samples of disabled downloadable products are accessible in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 due to inadequate validation of user input.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7898 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to modify currency symbols can inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7945 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify content page titles to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7935 CONFIRM</a>
magento -- multiple_products	A cross-site request forgery vulnerability exists in the GiftCardAccount removal feature for Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7947 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify catalog price rules to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7938 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to modify store currency options to inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7940 CONFIRM</a>
magento -- multiple_products	An injection vulnerability exists in Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with marketing manipulation privileges can invoke methods that alter data of the underlying	2019-08-02	not yet calculated	<a href="#">CVE-2019-7889 CONFIRM</a>

	model followed by corresponding database modifications.			
magento -- multiple_products	A reflected cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2 when the feature that adds a secret key to the Admin URL is disabled.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7887 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the admin panel of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. This could be exploited by an authenticated user with privileges to newsletter templates.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7875 CONFIRM</a>
magento -- multiple_products	A stored cross-site scripting vulnerability exists in the product comments field of Magento Open Source prior to 1.9.4.2, and Magento Commerce prior to 1.14.4.2, Magento 2.1 prior to 2.1.18, Magento 2.2 prior to 2.2.9, Magento 2.3 prior to 2.3.2. An authenticated user with privileges to the Return Product comments field can inject malicious javascript.	2019-08-02	not yet calculated	<a href="#">CVE-2019-7944 CONFIRM</a>
matrixssl -- matrixssl	In MatrixSSL 3.8.3 Open through 4.2.1 Open, the DTLS server mishandles incoming network messages leading to a heap-based buffer overflow of up to 256 bytes and possible Remote Code Execution in parseSSLHandshake in sslDecode.c. During processing of a crafted packet, the server mishandles the fragment length value provided in the DTLS message.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14431 MISC</a>
mi kytracker -- milkytracker	ModuleEditor::convertInstrument in tracker/ModuleEditor.cpp in Mi kyTracker 1.02.00 has a heap-based buffer overflow.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14497 MISC</a>
mi kytracker -- milkytracker	LoaderXM::load in LoaderXM.cpp in milkyplay in Mi kyTracker 1.02.00 has a stack-based buffer overflow.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14496 MISC</a>
mi kytracker -- milkytracker	XMFile::read in XMFile.cpp in mi kyplay in MilkyTracker 1.02.00 has a heap-based buffer overflow.	2019-07-31	not yet calculated	<a href="#">CVE-2019-14464 MISC</a>
misskey -- misskey	Misskey before 10.102.4 allows h jacking a user's token.	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020010 MISC</a>
netapp -- data_ontap_7-mode	Data ONTAP operating in 7-Mode versions prior to 8.2.5P3 may disclose sensitive LDAP account information to unauthenticated remote attackers.	2019-08-02	not yet calculated	<a href="#">CVE-2019-5501 CONFIRM</a>
netapp -- data_ontap_7-mode	Data ONTAP operating in 7-Mode versions prior to 8.2.5P3 are susceptible to a vulnerability which discloses information to an unauthenticated attacker. A successful attack requires that multiple non-default options be enabled.	2019-08-02	not yet calculated	<a href="#">CVE-2019-5493 CONFIRM</a>
netgear -- n600_wifi_dual_band_router	A stack-based buffer overflow in the upnpd binary running on NETGEAR WNDR3400v3 routers with firmware version 1.0.1.18_1.0.63 allows an attacker to remotely execute arbitrary code via a crafted UPnP SSDP packet.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14363 MISC</a>



nextcloud -- nextcloud_android_application	Bypass lock protection in the Nextcloud Android app prior to version 3.6.2 causes leaking of thumbnails when requesting the Android content provider although the lock protection was not solved.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5452</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Bypassing lock protection exists in Nextcloud Android app 3.6.0 when creating a multi-account and aborting the process.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5455</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	SQL Injection in the Nextcloud Android app prior to version 3.0.0 allows to destroy a local cache when a harmful query is executed requiring to resetup the account.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5454</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Bypass lock protection in the Nextcloud Android app prior to version 3.3.0 allowed access to files when being prompted for the lock protection and switching to the Nextcloud file provider.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5453</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Improper sanitization of HTML in directory names in the Nextcloud Android app prior to version 3.7.0 allowed to style the directory name in the header bar when using basic HTML.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5450</a> <a href="#">MISC</a>
nextcloud -- nextcloud_android_application	Bypass lock protection in the Nextcloud Android app prior to version 3.6.1 allows accessing the files when repeatedly opening and closing the app in a very short time.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5451</a> <a href="#">MISC</a>
nextcloud -- nextcloud_server	A missing check in the Nextcloud Server prior to version 15.0.1 causes leaking of calendar event names when adding or modifying confidential or private events.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5449</a> <a href="#">MISC</a>
nfdump -- nfdump	nfdump 1.6.17 and earlier is affected by an integer overflow in the function Process_ipfix_template_withdraw in ipfix.c that can be abused in order to crash the process remotely (denial of service).	2019-07-31	not yet calculated	<a href="#">CVE-2019-14459</a> <a href="#">MISC</a> <a href="#">MISC</a>
one_identity -- cloud_access_manager	One Identity Cloud Access Manager 8.1.3 does not use HTTP Strict Transport Security (HSTS), which may allow man-in-the-middle (MITM) attacks. This issue is fixed in version 8.1.4.	2019-07-29	not yet calculated	<a href="#">CVE-2019-13498</a> <a href="#">CONFIRM</a>
openbravo -- openbravo_erp	Openbravo ERP before 3.0PR19Q1.3 is affected by Directory Traversal. This vulnerability could allow remote authenticated attackers to replace a file on the server via the getAttachmentDirectoryForNewAttachment inpKey value.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14362</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read in the function cv::predictOrdered<cv::HaarEvaluator> in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14491</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An issue was discovered in OpenCV before 4.1.1. There is a NULL pointer dereference in the function cv::XMLParser::parse at modules/core/src/persistence.cpp.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14493</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencv -- opencv	An issue was discovered in OpenCV before 3.4.7 and 4.x before 4.1.1. There is an out of bounds read/write in the function HaarEvaluator::OptFeature::calc in modules/objdetect/src/cascadedetect.hpp, which leads to denial of service.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14492</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
openemr -- openemr	OpenEMR before 5.0.2 allows SQL Injection in interface/forms/eye_mag/save.php.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14529</a>

				<a href="#">MISC</a>
opengear -- console_server	Opengear console server firmware releases prior to 4.5.0 have a stored XSS vulnerability related to serial port logging. If a malicious user of an external system (connected to a serial port on an Opengear console server) sends crafted text to a serial port (that has logging enabled), the text will be replayed when the logs are viewed. Exploiting this vulnerability requires access to the serial port and/or console server.	2019-07-31	not yet calculated	<a href="#">CVE-2019-14456</a> <a href="#">MISC</a>
openssl -- openssl	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, 'usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).	2019-07-30	not yet calculated	<a href="#">CVE-2019-1552</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
openstack -- openstack-ironic-inspector	A vulnerability was found in openstack-ironic-inspector all versions excluding 5.0.2, 6.0.3, 7.2.4, 8.0.3 and 8.2.1. A SQL-injection vulnerability was found in openstack-ironic-inspector's node_cache.find_node(). This function makes a SQL query using unfiltered data from a server reporting inspection results (by a POST to the /v1/continue endpoint). Because the API is unauthenticated, the flaw could be exploited by an attacker with access to the network on which ironic-inspector is listening. Because of how ironic-inspector uses the query results, it is unlikely that data could be obtained. However, the attacker could pass malicious data and create a denial of service.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10141</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
oxid -- oxid_eshop	OXID eShop 6.0.x before 6.0.5 and 6.1.x before 6.1.4 allows SQL Injection via a crafted URL, leading to full access by an attacker. This includes all shopping cart options, customer data, and the database.	2019-07-30	not yet calculated	<a href="#">CVE-2019-13026</a>

	No interaction between the attacker and the victim is necessary.			<a href="#">CONFIRM</a>
pandao -- editor.md	pandao Editor.md 1.5.0 allows XSS via the <code>JavaScript: string</code> .	2019-08-01	not yet calculated	<a href="#">CVE-2019-14517</a> <a href="#">MISC</a>
pandao -- editor.md	pandao Editor.md 1.5.0 allows XSS via an attribute of an ABBR or SUP element.	2019-08-03	not yet calculated	<a href="#">CVE-2019-14653</a> <a href="#">MISC</a>
pdfresurrect -- pdfresurrect	PDFResurrect 0.15 has a buffer overflow via a crafted PDF file because data associated with startxref and %%EOF is mishandled.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14267</a> <a href="#">MISC</a> <a href="#">MISC</a>
pixmap -- pixmap	An integer overflow issue has been reported in the <code>general_composite_rect()</code> function in pixmap prior to version 0.32.8. An attacker could exploit this issue to cause an application using pixmap to crash or, potentially, execute arbitrary code.	2019-07-31	not yet calculated	<a href="#">CVE-2015-5297</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
planon -- planon	Planon before Live Build 41 has XSS.	2019-07-29	not yet calculated	<a href="#">CVE-2018-18570</a> <a href="#">MISC</a>
podman -- podman	A path traversal vulnerability has been discovered in podman before version 1.4.0 in the way it handles symlinks inside containers. An attacker who has compromised an existing container can cause arbitrary files on the host filesystem to be read/written when an administrator tries to copy a file from/to the container.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10152</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
polycom -- multiple_products	A vulnerability in the web-based management interface of VVX, Trio, SoundStructure, SoundPoint, and SoundStation phones running Polycom UC Software, if exploited, could allow an authenticated, remote attacker with admin privileges to cause a denial of service (DoS) condition or execute arbitrary code.	2019-07-29	not yet calculated	<a href="#">CVE-2019-12948</a> <a href="#">CONFIRM</a>
polycom -- obihai_obi1022_voip_phone	On the Polycom Obihai Obi1022 VoIP phone with firmware 5.1.11, a command injection (missing input validation) issue in the NTP server IP address field for the "Time Service Settings web" interface allows an authenticated remote attacker in the same network to trigger OS commands via shell commands in a POST request.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14259</a> <a href="#">MISC</a>
poppler -- poppler	An issue was discovered in Poppler through 0.78.0. There is a divide-by-zero error in the function <code>SplashOutputDev::tilingPatternFill</code> at <code>SplashOutputDev.cc</code> .	2019-08-01	not yet calculated	<a href="#">CVE-2019-14494</a> <a href="#">MISC</a> <a href="#">MISC</a>
postgresql -- postgresql	A vulnerability was found in PostgreSQL versions 11.x up to excluding 11.3, 10.x up to excluding 10.8, 9.6.x up to, excluding 9.6.13, 9.5.x up to, excluding 9.5.17. PostgreSQL maintains column statistics for tables. Certain statistics, such as histograms and lists of most common values, contain values taken from the column. PostgreSQL does not evaluate row security policies before consulting those statistics during query planning; an attacker can exploit this to read the most common values of certain columns. Affected columns are those for which the	2019-07-30	not yet calculated	<a href="#">CVE-2019-10130</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

	attacker has SELECT privilege and for which, in an ordinary query, row-level security prunes the set of rows visible to the attacker.			
powerdns -- authoritative_server	A Vulnerability has been found in PowerDNS Authoritative Server before versions 4.1.9, 4.0.8 allowing a remote, authorized master server to cause a high CPU load or even prevent any further updates to any slave zone by sending a large number of NOTIFY messages. Note that only servers configured as slaves are affected by this issue.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10163</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
powerdns -- authoritative_server	A vulnerability has been found in PowerDNS Authoritative Server before versions 4.1.10, 4.0.8 allowing an authorized user to cause the server to exit by inserting a crafted record in a MASTER type zone under their control. The issue is due to the fact that the Authoritative Server will exit when it runs into a parsing error while looking up the NS/A/AAAA records it is about to use for an outgoing notify.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10162</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
printeron -- printeron_central_print_services	An issue was discovered in PrinterOn Central Print Services (CPS) through 4.1.4. A user without valid credentials can bypass the authentication process, obtaining a valid session cookie with guest/pseudo-guest level privileges. This cookie can then be further used to perform other attacks.	2019-07-29	not yet calculated	<a href="#">CVE-2018-17213</a> <a href="#">MISC</a>
printeron -- printeron_central_print_services	An issue was discovered in PrinterOn Central Print Services (CPS) through 4.1.4. An unauthenticated attacker can view details about the printers associated with CPS via a crafted HTTP GET request.	2019-07-29	not yet calculated	<a href="#">CVE-2018-17211</a> <a href="#">MISC</a>
rancher -- rancher	An issue was discovered that affects the following versions of Rancher: v2.0.0 through v2.0.13, v2.1.0 through v2.1.8, and v2.2.0 through 2.2.1. When Rancher starts for the first time, it creates a default admin user with a well-known password. After initial setup, the Rancher administrator may choose to delete this default admin user. If Rancher is restarted, the default admin user will be recreated with the well-known default password. An attacker could exploit this by logging in with the default admin credentials. This can be mitigated by deactivating the default admin user rather than completing deleting them.	2019-07-30	not yet calculated	<a href="#">CVE-2019-11202</a> <a href="#">MISC</a> <a href="#">MISC</a>
red_hat -- openshift_container_platform	A flaw was found in OpenShift Container Platform, versions 3.11 and later, in which the CSRF tokens used in the cluster console component were found to remain static during a user's session. An attacker with the ability to observe the value of this token would be able to re-use the token to perform a CSRF attack.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10176</a> <a href="#">CONFIRM</a>
red_hat -- atomic-openshift	A vulnerability exists in the garbage collection mechanism of atomic-openshift. An attacker able spoof the UUID of a valid object from another namespace is able to delete children of those objects. Versions 3.6, 3.7, 3.8, 3.9, 3.10, 3.11 and 4.1 are affected.	2019-08-01	not yet calculated	<a href="#">CVE-2019-3884</a> <a href="#">CONFIRM</a>
red_hat -- enterprise_linux	It was found that the fix for CVE-2018-14648 in 389-ds-base, versions 1.4.0.x before 1.4.0.17, was incorrectly applied in RHEL 7.5. An attacker would still be able	2019-08-02	not yet calculated	<a href="#">CVE-2019-10171</a>

	to provoke excessive CPU consumption leading to a denial of service.			<a href="#">CONFIRM</a>
red_hat -- openshift_container_platform	OpenShift Container Platform before version 4.1.3 writes OAuth tokens in plaintext to the audit logs for the Kubernetes API server and OpenShift API server. A user with sufficient privileges could recover OAuth tokens from these audit logs and use them to access other resources.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10165</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
red_hat -- openstack_platform	A flaw was discovered in the python-novajoin plugin, all versions up to, excluding 1.1.1, for Red Hat OpenStack Platform. The novajoin API lacked sufficient access control, allowing any keystone authenticated user to generate FreeIPA tokens.	2019-07-30	not yet calculated	<a href="#">CVE-2019-10138</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
red_hat -- satellite	It was found that foreman, versions 1.x.x before 1.15.6, in Satellite 6 did not properly enforce access controls on certain resources. An attacker with access to the API and knowledge of the resource name can access resources in other organizations.	2019-08-01	not yet calculated	<a href="#">CVE-2014-8183</a> <a href="#">CONFIRM</a>
samba -- heimdal_kdc	A flaw was found in samba's Heimdal KDC implementation, versions 4.8.x up to, excluding 4.8.12, 4.9.x up to, excluding 4.9.8 and 4.10.x up to, excluding 4.10.3, when used in AD DC mode. A man in the middle attacker could use this flaw to intercept the request to the KDC and replace the user name (principal) in the request with any desired user name (principal) that exists in the KDC effectively obtaining a ticket for that principal.	2019-07-31	not yet calculated	<a href="#">CVE-2018-16860</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
sas -- sas_drug_development	SAS Drug Development (SDD) before 32DRG02 mishandles logout actions, which allows a user (who was previously logged in) to access resources by pressing a back or forward button in a web browser.	2019-07-31	not yet calculated	<a href="#">CVE-2007-6763</a> <a href="#">MISC</a>
schism_tracker -- schism_tracker	fmt_mtm_load_song in fmt/mtm.c in Schism Tracker 20190722 has a heap-based buffer overflow.	2019-07-31	not yet calculated	<a href="#">CVE-2019-14465</a> <a href="#">MISC</a>
schism_tracker -- schism_tracker	An issue was discovered in Schism Tracker through 20190722. There is a heap-based buffer overflow via a large number of song patterns in fmt_mtm_load_song in fmt/mtm.c, a different vulnerability than CVE-2019-14465.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14524</a> <a href="#">MISC</a>
schism_tracker -- schism_tracker	An issue was discovered in Schism Tracker through 20190722. There is an integer underflow via a large plen in fmt_okt_load_song in the Amiga Oktalyzer parser in fmt/okt.c.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14523</a> <a href="#">MISC</a>
sdl2_image -- sdl2_image	An exploitable code execution vulnerability exists in the XPM image rendering function of SDL2_image 2.0.4. A specially crafted XPM image can cause an integer overflow in the colorhash function, allocating too small of a buffer. This buffer can then be written out of bounds, resulting in a heap overflow, ultimately ending in code execution. An attacker can display a specially crafted image to trigger this vulnerability.	2019-07-31	not yet calculated	<a href="#">CVE-2019-5060</a> <a href="#">MISC</a>
	A vulnerability has been identified in Ethernet plug-in communication modules for SIPROTEC 5 devices with CPU			



siemens -- siprotec_5_devices	variants CP200 (All versions), SIPROTEC 5 devices with CPU variants CP300 (All versions). An unauthenticated attacker with network access to the device could potentially insert arbitrary code which is executed before firmware verification in the device.	2019-08-02	not yet calculated	<a href="#">CVE-2019-10938</a> <a href="#">MISC</a>
sigil_ebook -- sigil	Sigil before 0.9.16 is vulnerable to a directory traversal, allowing attackers to write arbitrary files via a ../ (dot dot slash) in a ZIP archive entry that is mishandled during extraction.	2019-07-30	not yet calculated	<a href="#">CVE-2019-14452</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
sleuthkit -- sleuthkit	An issue was discovered in The Sleuth Kit (TSK) 4.6.6. There is an off-by-one overwrite due to an underflow on tools/hashtools/hfind.cpp while using a bogus hash table.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14532</a> <a href="#">MISC</a>
sleuthkit -- sleuthkit	An issue was discovered in The Sleuth Kit (TSK) 4.6.6. There is an out of bounds read on iso9660 while parsing System Use Sharing Protocol data in fs/iso9660.c.	2019-08-02	not yet calculated	<a href="#">CVE-2019-14531</a> <a href="#">MISC</a>
smokedetector -- smokedetector	SmokeDetector intentionally does automatic deployments of updated copies of SmokeDetector without server operator authority.	2019-07-29	not yet calculated	<a href="#">CVE-2019-1020011</a> <a href="#">MISC</a>
softether_vpn -- softethervpn	See.sys through 4.25 in the SoftEther VPN Server allows a user to specify any kernel address to which arbitrary bytes are written.	2019-07-29	not yet calculated	<a href="#">CVE-2019-11868</a> <a href="#">MISC</a> <a href="#">MISC</a>
sonos -- zoneplayer	ZInsVX.dll ActiveX Control 2018.02 and earlier in Zoneplayer contains a vulnerability that could allow remote attackers to execute arbitrary files by setting the arguments to the ActiveX method. This can be leveraged for remote code execution.	2019-08-02	not yet calculated	<a href="#">CVE-2019-9141</a> <a href="#">CONFIRM</a>
ssdp_responder -- ssdp_responder	SSDP Responder 1.x through 1.5 mishandles incoming network messages, leading to a stack-based buffer overflow by 1 byte. This results in a crash of the server, but only when strict stack checking is enabled. This is caused by an off-by-one error in ssdp_recv in ssdpd.c.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14323</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- endpoint_protection_and_endpoint_protection_small_business_edition	Symantec Endpoint Protection, prior to 14.2 RU1 & 12.1 RU6 MP10 and Symantec Endpoint Protection Small Business Edition, prior to 12.1 RU6 MP10c (12.1.7491.7002), may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2019-07-31	not yet calculated	<a href="#">CVE-2019-12750</a> <a href="#">MISC</a>
terracotta -- quartz_scheduler	initDocumentParser in xml/XMLSchedulingDataProcessor.java in Terracotta Quartz Scheduler through 2.3.0 allows XXE attacks via a job description.	2019-07-26	not yet calculated	<a href="#">CVE-2019-13990</a> <a href="#">MISC</a>
the_pallets_project -- werkzeug	In Pallets Werkzeug before 0.15.5, SharedDataMiddleware mishandles drive names (such as C:) in Windows pathnames.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14322</a> <a href="#">MISC</a>
	SMTP MITM refers to a malicious actor			<a href="#">CVE-</a>

unifi -- network_controller	setting up an SMTP proxy server between the UniFi Controller version <= 5.10.21 and their actual SMTP server to record their SMTP credentials for malicious use later.	2019-07-30	not yet calculated	<a href="#">2019-5456 CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
univa -- grid_engine	In Univa Grid Engine before 8.6.3, when configured for Docker jobs and execd spooling on root_squash, weak file permissions ("other" write access) occur in certain cases (GE-6890).	2019-07-30	not yet calculated	<a href="#">CVE-2018-20871 MISC</a>
veritas -- veritas_resiliency_platform	An issue was discovered in Veritas Resiliency Platform (VRP) before 3.4 HF1. When uploading an application bundle, a directory traversal vulnerability allows a VRP user with sufficient privileges to overwrite any file in the VRP virtual machine. A malicious VRP user could use this to replace existing files to take control of the VRP virtual machine.	2019-07-29	not yet calculated	<a href="#">CVE-2019-14418 MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
vlc -- media_player	Double Free in VLC versions <= 3.0.6 leads to a crash.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5460 MISC</a>
vlc -- media_player	An Integer underflow in VLC Media Player versions < 3.0.7 leads to an out-of-band read.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5459 MISC</a>
wallacepos -- wallacepos	Unrestricted upload of file with dangerous type in WallacePOS 1.4.3 allows a remote, authenticated attacker to execute arbitrary code by uploading a malicious PHP file.	2019-07-31	not yet calculated	<a href="#">CVE-2019-3960 MISC</a>
windu -- windu_cms	Windu CMS 2.2 allows CSRF via admin/users/?mn=admin.message.error to add an admin account.	2019-08-01	not yet calculated	<a href="#">CVE-2013-7473 MISC</a>
windu -- windu_cms	Windu CMS 2.2 allows XSS via the name parameter to admin/content/edit or admin/content/add, or the username parameter to admin/users.	2019-08-01	not yet calculated	<a href="#">CVE-2013-7474 MISC</a>
wordpress -- wordpress	The WP Fastest Cache plugin through 0.8.9.5 for WordPress allows wpFastestCache.php and inc/cache.php Directory Traversal.	2019-07-30	not yet calculated	<a href="#">CVE-2019-13635 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The Adenion Blog2Social plugin through 5.5.0 for WordPress allows SQL Injection.	2019-08-01	not yet calculated	<a href="#">CVE-2019-13572 MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	A SQL injection vulnerability exists in the Vsourz Digital Advanced CF7 DB plugin through 1.6.1 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system.	2019-07-29	not yet calculated	<a href="#">CVE-2019-13571 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Simple Membership plugin before 3.8.5 for WordPress has CSRF affecting the Bulk Operation section.	2019-07-28	not yet calculated	<a href="#">CVE-2019-14328 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
yara -- yara	An exploitable denial of service vulnerability exists in the object lookup functionality of Yara 3.8.1. A specially crafted binary file can cause a negative value to be read to satisfy an assert, resulting in Denial of Service. An attacker can create a malicious binary to trigger this	2019-07-31	not yet calculated	<a href="#">CVE-2019-5020 MISC</a>

	vulnerability.			
yarn -- yarn	Yarn before 1.17.3 is vulnerable to Missing Encryption of Sensitive Data due to HTTP URLs in lockfile causing unencrypted authentication data to be sent over the network.	2019-07-30	not yet calculated	<a href="#">CVE-2019-5448</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
zurmo -- zurmo	Zurmo 3.2.7-2 has XSS via the app/index.php/zurmo/default PATH_INFO.	2019-08-01	not yet calculated	<a href="#">CVE-2019-14472</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

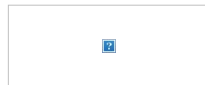
[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) 245 Murray Lane SW Bldg 410 Washington, DC 20598 (888) 282-0870



From: [US-CERT](mailto:US-CERT@summyvale.ca.gov)  
To: [US-CERT](mailto:US-CERT@summyvale.ca.gov)  
Subject: Vulnerability Summary for the Week of July 15 2019  
Date: Monday, July 22, 2019 2:36:14 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## Vulnerability Summary for the Week of July 15 2019

07/22/2019 06:30 AM EDT

Original release date: July 22, 2019

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have a Command injection vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user.	2019-07-18	7.5	<a href="#">CVE-2019-7850</a> MISC
archivesunleashed -- graphpass	borg-reducer c6d5240 is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Output parameter within the executable.	2019-07-15	7.5	<a href="#">CVE-2019-1010044</a> MISC
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.836, a cwpsrv-xxx cookie allows a normal user to craft and upload a session file to the /tmp directory, and use it to become the root user.	2019-07-16	8.5	<a href="#">CVE-2019-13359</a> MISC MISC
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.836, remote attackers can bypass authentication in the login process by leveraging knowledge of a valid username.	2019-07-16	7.5	<a href="#">CVE-2019-13360</a> MISC MISC
fanucamerica -- robotics_virtual_robot_controller	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 has a Buffer Overflow via a forged HTTP request.	2019-07-17	7.5	<a href="#">CVE-2019-13585</a> MISC BUGTRAQ
foliovision -- fv_flowplayer_video_player	A SQL injection vulnerability exists in the FolioVision FV Flowplayer Video Player plugin before 7.3.19.727 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system.	2019-07-17	10.0	<a href="#">CVE-2019-13573</a> MISC CONFIRM CONFIRM
gdnssd -- gdnssd	The set_ipv4() function in zscan_rfc1035.rl in gdnssd 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv4 address in zone data.	2019-07-18	7.5	<a href="#">CVE-2019-13951</a> MISC
gdnssd -- gdnssd	The set_ipv6() function in zscan_rfc1035.rl in gdnssd before 2.4.3 and 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv6 address in zone data.	2019-07-18	7.5	<a href="#">CVE-2019-13952</a> MISC
getvera -- vera_edge_firmware	LuaUPnP in Vera Edge Home Controller 1.7.4452 allows remote unauthenticated users to execute arbitrary OS commands via the code parameter to /port_3480/data_request because the "No unsafe lua allowed" code block is skipped.	2019-07-14	10.0	<a href="#">CVE-2019-13598</a> MISC
gnu -- glibc	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard.	2019-07-15	7.5	<a href="#">CVE-2019-1010022</a> MISC
layerbb -- layerbb	LayerBB 1.1.3 allows admin/general.php arbitrary file upload because the custom_logo filename suffix is not restricted, and .php may be used.	2019-07-19	7.5	<a href="#">CVE-2019-13973</a> MISC
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Boundary crossing. The impact is: Memory corruption of the TEE itself. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	7.5	<a href="#">CVE-2019-1010293</a> MISC
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Memory corruption and disclosure of memory content. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	7.5	<a href="#">CVE-2019-1010295</a> MISC
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Code execution in context of TEE core (kernel). The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	10.0	<a href="#">CVE-2019-1010296</a> MISC
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Execution of code in TEE core (kernel) context. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	10.0	<a href="#">CVE-2019-1010297</a> MISC
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Code execution in the context of TEE core (kernel). The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	10.0	<a href="#">CVE-2019-1010298</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1004, CVE-2019-1056, CVE-2019-1059.	2019-07-15	7.6	<a href="#">CVE-2019-1001</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1092, CVE-2019-1103, CVE-2019-1106, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1062</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1103, CVE-2019-1106, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1092</a> MISC
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1106, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1103</a> N/A
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1103, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1106</a> N/A
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1103, CVE-2019-1106.	2019-07-15	7.6	<a href="#">CVE-2019-1107</a> N/A
microsoft -- edge	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'.	2019-07-15	7.6	<a href="#">CVE-2019-1104</a> N/A
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1111.	2019-07-15	9.3	<a href="#">CVE-2019-1110</a> N/A
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1110.	2019-07-15	9.3	<a href="#">CVE-2019-1111</a> N/A
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1001, CVE-2019-1056, CVE-2019-1059.	2019-07-15	7.6	<a href="#">CVE-2019-1004</a> MISC
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1001, CVE-2019-1004, CVE-2019-1059.	2019-07-15	7.6	<a href="#">CVE-2019-1056</a> MISC
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1001, CVE-2019-1004, CVE-2019-1056.	2019-07-15	7.6	<a href="#">CVE-2019-1059</a> MISC
microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	2019-07-15	7.6	<a href="#">CVE-2019-1063</a> MISC
microsoft -- team_foundation_server	A remote code execution vulnerability exists when Azure DevOps Server and Team Foundation Server (TFS) improperly handle user input, aka 'Azure DevOps Server and Team Foundation Server Remote Code Execution Vulnerability'.	2019-07-15	7.5	<a href="#">CVE-2019-1072</a> MISC

microsoft -- windows_10	A remote code execution vulnerability exists in Remote Desktop Services - formerly known as Terminal Services - when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.	2019-07-15	8.5	<a href="#">CVE-2019-0887</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-0999</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1067</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in Microsoft Windows where a certain DLL, with Local Service privilege, is vulnerable to race planting a customized DLL. An attacker who successfully exploited this vulnerability could potentially elevate privilege to SYSTEM. The update addresses this vulnerability by requiring SYSTEM privileges for a certain DLL, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1074.	2019-07-15	7.2	<a href="#">CVE-2019-1082</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in rpcss.dll when the RPC service Activation Kernel improperly handles an RPC request. To exploit this vulnerability, a low level authenticated attacker could run a specially crafted application. The security update addresses this vulnerability by correcting how rpcss.dll handles these requests., aka 'Windows RPCSS Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1089</a> MISC MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the way that the dnssrvr.dll handles objects in memory, aka 'Windows dnssrvr.dll Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1090</a> MISC
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.	2019-07-15	9.3	<a href="#">CVE-2019-1102</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1117</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1118</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1119</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1120</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1121</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1122</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1123</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1124</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1127</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1128</a> N/A
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1130.	2019-07-15	7.2	<a href="#">CVE-2019-1129</a> N/A
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1129.	2019-07-15	7.2	<a href="#">CVE-2019-1130</a> N/A
microsoft -- windows_7	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1132</a> N/A
microsoft -- windows_server_2012	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP failover server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'.	2019-07-15	7.5	<a href="#">CVE-2019-0785</a> MISC
onosproject -- onos	In ONOS 1.15.0, apps/yang/web/src/main/java/org/onosproject/yang/web/YangWebResource.java mishandles backquote characters within strings that can be used in a shell command.	2019-07-16	10.0	<a href="#">CVE-2019-13624</a> MISC
rapid7 -- insight_agent	Rapid7 Insight Agent, version 2.6.3 and prior, suffers from a local privilege escalation due to an uncontrolled DLL search path. Specifically, when Insight Agent 2.6.3 and prior starts, the Python interpreter attempts to load python3.dll at "C:\DLLs\python3.dll," which normally is writable by locally authenticated users. Because of this, a malicious local user could use Insight Agent's startup conditions to elevate to SYSTEM privileges. This issue was fixed in Rapid7 Insight Agent 2.6.4.	2019-07-12	7.2	<a href="#">CVE-2019-5629</a> MISC FULLDISC MISC CONFIRM BUGTRAQ
realization -- concerto_critical_chain_planner	Realization Concerto Critical Chain Planner (aka CCPM) 5.10.8071 has SQL Injection in at least in the taskupd/taskdetails.aspx webpage via the projectname parameter.	2019-07-12	7.5	<a href="#">CVE-2019-13027</a> MISC
saltstack -- salt_2018	SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql_user_chpass function from the MySQL module for Salt (https://github.com/saltstack/salt/blob/develop/salt/modules/mysql.py#L1462). The attack vector is: specially crafted password string. The fixed version is: 2018.3.4.	2019-07-18	7.5	<a href="#">CVE-2019-1010259</a> MISC MISC MISC
schneider-electric -- proclima	A CWE-94: Code Injection vulnerability exists in ProClima (all versions prior to version 8.0.0) which could allow an unauthenticated, remote attacker to execute arbitrary code on the targeted system in all versions of ProClima prior to version 8.0.0.	2019-07-15	10.0	<a href="#">CVE-2019-6823</a> MISC
schneider-electric -- proclima	A CWE-119: Buffer Errors vulnerability exists in ProClima (all versions prior to version 8.0.0) which allows an unauthenticated, remote attacker to execute arbitrary code on the targeted system in all versions of ProClima prior to version 8.0.0.	2019-07-15	10.0	<a href="#">CVE-2019-6824</a> MISC
sertek -- xpare	An issue was discovered in Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could access the backend database via SQL injection.	2019-07-17	10.0	<a href="#">CVE-2019-13447</a> MISC
videolan -- vlc_media_player	VideoLAN VLC media player 3.0.7.1 has a heap-based buffer over-read in mkv::demux_sys_t::FreeUnused() in modules/demux/mkv/demux.cpp when called from mkv::Open in modules/demux/mkv/mkv.cpp.	2019-07-16	7.5	<a href="#">CVE-2019-13615</a> MISC
wpeverest -- everest_forms	A SQL injection vulnerability exists in WPEverest Everest Forms plugin for WordPress through 1.4.9. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via includes/evf-entry-functions.php	2019-07-18	7.5	<a href="#">CVE-2019-13575</a> CONFIRM MISC MISC MISC MISC
zohocorp -- manageengine_admanager_plus	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System.	2019-07-17	8.5	<a href="#">CVE-2019-12876</a> BID MISC

[Back to top](#)



## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Insufficient input validation vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7843</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Improper error handling vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7846</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Improper Restriction of XML External Entity Reference (XXE) vulnerability. Successful exploitation could lead to Arbitrary read access to the file system in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7847</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Inadequate access control vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7848</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Information Exposure Through an Error Message vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7941</a> MISC
adobe -- dreamweaver	Adobe Dreamweaver direct download installer versions 19.0 and below, 18.0 and below have an Insecure Library Loading (DLL hijacking) vulnerability. Successful exploitation could lead to Privilege Escalation in the context of the current user.	2019-07-18	6.8	<a href="#">CVE-2019-7956</a> MISC
adobe -- experience_manager	Adobe Experience Manager version 6.4 and earlier have a Cross-Site Request Forgery vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user.	2019-07-18	4.3	<a href="#">CVE-2019-7953</a> MISC
adobe -- experience_manager	Adobe Experience Manager version 6.4 and earlier have a Reflected Cross-site Scripting vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user.	2019-07-18	5.8	<a href="#">CVE-2019-7955</a> MISC
altn -- mdaemon_webmail	MDaemon Webmail (formerly WorldClient) has CSRF.	2019-07-19	6.8	<a href="#">CVE-2018-17792</a> MISC MISC
apache -- roller	A Reflected Cross-site Scripting (XSS) vulnerability exists in Apache Roller. Roller's Math Comment Authenticator did not properly sanitize user input and could be exploited to perform Reflected Cross Site Scripting (XSS). The mitigation for this vulnerability is to upgrade to the latest version of Roller, which is now Roller 5.2.3.	2019-07-15	4.3	<a href="#">CVE-2019-0234</a> CONFIRM
automatic -- camptix_event_ticketing	The CampTix Event Ticketing plugin before 1.5 for WordPress allows CSV injection when the export tool is used.	2019-07-18	5.1	<a href="#">CVE-2016-10762</a> MISC MISC
axiosys -- bento4	In Bento4 1.5.1-627, AP4_DataBuffer::SetDataSize does not handle reallocation failures, leading to a memory copy into a NULL pointer. This is different from CVE-2018-20186.	2019-07-18	4.3	<a href="#">CVE-2019-13959</a> MISC
blackberry -- qnx_software_development_platform	An information disclosure vulnerability leading to a potential local escalation of privilege in the procs service (the /proc filesystem) of BlackBerry QNX Software Development Platform version(s) 6.5.0 SP1 and earlier could allow an attacker to potentially gain unauthorized access to a chosen process address space.	2019-07-12	4.6	<a href="#">CVE-2019-8998</a> MISC
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, the Login process allows attackers to check whether a username is valid by reading the HTTP response.	2019-07-16	5.0	<a href="#">CVE-2019-13383</a> MISC MISC
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.838 to 0.9.8.846, remote attackers can bypass authentication in the login process by leveraging the knowledge of a valid username. The attacker must defeat an encoding that is not equivalent to base64, and thus this is different from CVE-2019-13360.	2019-07-16	6.5	<a href="#">CVE-2019-13605</a> MISC MISC MISC
cmsmadesimple -- bable:multilingual_site	Babel: Multilingual site Babel All is affected by: Open Redirection. The impact is: Redirection to any URL, which is supplied to redirect.php in a "newurl" parameter. The component is: redirect.php. The attack vector is: The victim must open a link created by an attacker. Attacker may use any legitimate site using Babel to redirect user to a URL of his/her choosing.	2019-07-16	5.8	<a href="#">CVE-2019-1010290</a> MISC MISC
deepsoft -- weblibrarian	Deepwoods Software WebLibrarian 3.5.2 and earlier is affected by: SQL Injection. The impact is: Exposing the entire database. The component is: Function "AllBarCodes" (defined at database_code.php line 1018) is vulnerable to a boolean-based blind sql injection. This function call can be triggered by any user logged-in with at least Volunteer role or manage_circulation capabilities. PoC : /wordpress/wp-admin/admin.php?page=weblib-circulation-desk&orderby=title&order=DESC.	2019-07-15	4.0	<a href="#">CVE-2019-1010034</a> MISC
digium -- asterisk	Buffer overflow in res_pjsip_messaging in Digium Asterisk versions 13.21-cert3, 13.27.0, 15.7.2, 16.4.0 and earlier allows remote authenticated users to crash Asterisk by sending a specially crafted SIP MESSAGE message.	2019-07-12	4.0	<a href="#">CVE-2019-12827</a> CONFIRM CONFIRM
dolibarr -- dolibarr	Dolibarr 6.0.4 is affected by: Cross Site Scripting (XSS). The impact is: Cookie stealing. The component is: htdocs/product/stats/card.php. The attack vector is: Victim must click a specially crafted link sent by the attacker.	2019-07-14	4.3	<a href="#">CVE-2019-1010016</a> MISC
dolibarr -- dolibarr	Dolibarr 7.0.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: allow malicious html to change user password, disable users and disable password encryption. The component is: Function User password change, user disable and password encryption. The attack vector is: admin access malicious urls.	2019-07-18	6.8	<a href="#">CVE-2019-1010054</a> MISC
domainmod -- domainmod	domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change admin password. The component is: http://127.0.0.1/settings/password/ http://127.0.0.1/admin/users/add.php http://127.0.0.1/admin/users/edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page.	2019-07-18	6.8	<a href="#">CVE-2019-1010094</a> MISC
domainmod -- domainmod	domainmod(https://domainmod.org/) domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can add the administrator account. The component is: http://127.0.0.1/admin/users/add.php. The attack vector is: After the administrator logged in, open the html page.	2019-07-18	6.8	<a href="#">CVE-2019-1010095</a> MISC
domainmod -- domainmod	domainmod(https://domainmod.org/) domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change the read-only user to admin. The component is: http://127.0.0.1/admin/users/edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page.	2019-07-18	6.8	<a href="#">CVE-2019-1010096</a> MISC
eclipse -- openj9	AIX builds of Eclipse OpenJ9 before 0.15.0 contain unused RPATHs which may facilitate code injection and privilege elevation by local users.	2019-07-17	4.6	<a href="#">CVE-2019-11771</a> CONFIRM
fanucamerica -- robotics_virtual_robot_controller	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 allows Directory Traversal via a forged HTTP request.	2019-07-17	5.0	<a href="#">CVE-2019-13584</a> MISC BUGTRAQ
flatcore -- flatcore	A CSRF vulnerability was found in flatCore before 1.5, leading to the upload of arbitrary .php files via acp/core/files.upload-script.php.	2019-07-18	6.8	<a href="#">CVE-2019-13961</a> MISC MISC
gitea -- gitea	Gitea 1.7.0 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attacker is able to have victim execute arbitrary JS in browser. The component is: go-get URL generation - PR to fix: https://github.com/go-gitea/gitea/pull/5905. The attack vector is: victim must open a specifically crafted URL. The fixed version is: 1.7.1 and later.	2019-07-18	4.3	<a href="#">CVE-2019-1010261</a> MISC
gnome -- evince	Evince 3.26.0 is affected by buffer overflow. The impact is: DOS / Possible code execution. The component is: backend/tiff/tiff-document.c. The attack vector is: Victim must open a crafted PDF file. The issue occurs because of an incorrect integer overflow protection mechanism in tiff_document_render and tiff_document_get_thumbnail.	2019-07-14	6.8	<a href="#">CVE-2019-1010006</a> MISC MISC
gnu -- glibc	GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run lld on it. ldd execute code.	2019-07-15	6.8	<a href="#">CVE-2019-1010023</a> BID MISC
gnu -- glibc	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc.	2019-07-15	5.0	<a href="#">CVE-2019-1010024</a> BID MISC
gnu -- glibc	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc.	2019-07-15	5.0	<a href="#">CVE-2019-1010025</a> MISC
gpac -- gpac	In GPAC before 0.8.0, isomedia/isom_read.c in libgpac.a has a heap-based buffer over-read, as demonstrated by a crash in gf_m2ts_sync in media_tools/mpegs.c.	2019-07-16	5.0	<a href="#">CVE-2019-13618</a> MISC MISC
hexoeditor_project -- hexoeditor	HexoEditor v1.1.8-beta is affected by: XSS to code execution.	2019-07-14	4.3	<a href="#">CVE-2019-1010005</a> MISC

				MISC
h2labs -- learning_locker	In HT2 Labs Learning Locker 3.15.1, it's possible to inject malicious HTML and JavaScript code into the DOM of the website via the PATH_INFO to the dashboards/ URI.	2019-07-16	4.3	<a href="#">CVE-2019-12834</a> MISC
http-file-server_project -- http-file-server	A path traversal vulnerability in <= v0.2.6 of http-file-server npm module allows attackers to list files in arbitrary folders.	2019-07-15	5.0	<a href="#">CVE-2019-5447</a> MISC
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3, 1.1.3.1, and 1.1.3.2 is missing function level access control that could allow a user to delete authorized resources. IBM X-Force ID: 159033.	2019-07-17	4.0	<a href="#">CVE-2019-4194</a> CONFIRM XF
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 162887.	2019-07-17	5.0	<a href="#">CVE-2019-4430</a> XF CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155345.	2019-07-17	4.3	<a href="#">CVE-2018-2021</a> XF CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 155346.	2019-07-17	5.0	<a href="#">CVE-2018-2022</a> XF CONFIRM
jenkins -- jenkins	CSRF tokens in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier did not expire, thereby allowing attackers able to obtain them to bypass CSRF protection.	2019-07-17	5.1	<a href="#">CVE-2019-10353</a> MLIST MISC
jhead_project -- jhead	jhead 3.03 is affected by: Buffer Overflow. The impact is: Denial of service. The component is: gpsinfo.c Line 151 ProcessGpsInfo(). The attack vector is: Open a specially crafted JPEG file.	2019-07-15	4.3	<a href="#">CVE-2019-1010301</a> MISC
jhead_project -- jhead	jhead 3.03 is affected by: Incorrect Access Control. The impact is: Denial of service. The component is: iptc.c Line 122 show_IPTC(). The attack vector is: the victim must open a specially crafted JPEG file.	2019-07-15	4.3	<a href="#">CVE-2019-1010302</a> MISC
knot-resolver -- knot_resolver	A vulnerability was discovered in DNS resolver component of knot resolver through version 3.2.0 before 4.1.0 which allows remote attackers to bypass DNSSEC validation for non-existence answer. NXDOMAIN answer would get passed through to the client even if its DNSSEC validation failed, instead of sending a SERVFAIL packet. Caching is not affected by this particular bug but see CVE-2019-10191.	2019-07-16	5.0	<a href="#">CVE-2019-10190</a> CONFIRM FEDORA FEDORA CONFIRM
layerbb -- layerbb	LayerBB 1.1.3 allows XSS via the application/commands/new.php pm_title variable, a related issue to CVE-2019-17997.	2019-07-19	4.3	<a href="#">CVE-2019-13972</a> MISC
layerbb -- layerbb	LayerBB 1.1.3 allows conversations.php/cmd/new CSRF.	2019-07-19	6.8	<a href="#">CVE-2019-13974</a> MISC
libnmap -- libnmap	libnmap < v0.6.3 is affected by: XML Injection. The impact is: Denial of service (DoS) by consuming resources. The component is: XML Parsing. The attack vector is: Specially crafted XML payload.	2019-07-14	5.0	<a href="#">CVE-2019-1010017</a> MISC
libsdsl -- libsdsl	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in BlitNtoN in video/SDL_blit_N.c when called from SDL_SoftBlit in video/SDL_blit.c.	2019-07-16	6.8	<a href="#">CVE-2019-13616</a> MISC
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Rounding error. The impact is: Potentially leaking code and/or data from previous Trusted Application. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	5.0	<a href="#">CVE-2019-1010294</a> MISC
lodash -- lodash	lodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler. The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11.	2019-07-17	4.0	<a href="#">CVE-2019-1010266</a> MISC CONFIRM MISC
metinfo -- metinfo	Metinfo 6.x allows SQL Injection via the id parameter in an admin/index.php?n=ui_set&m=admin&c=index&a=doget_text_content&table=lang&field=1 request.	2019-07-19	6.5	<a href="#">CVE-2019-13969</a> MISC
microsoft -- .net_framework	An authentication bypass vulnerability exists in Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allowing signing of SAML tokens with arbitrary symmetric keys, aka 'WCF/WIF SAML Token Authentication Bypass Vulnerability'.	2019-07-15	5.0	<a href="#">CVE-2019-1006</a> MISC
microsoft -- .net_framework	A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests, aka '.NET Denial of Service Vulnerability'.	2019-07-15	5.0	<a href="#">CVE-2019-1083</a> MISC
microsoft -- .net_framework	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka '.NET Framework Remote Code Execution Vulnerability'.	2019-07-15	6.8	<a href="#">CVE-2019-1113</a> N/A
microsoft -- asp.net_core	A spoofing vulnerability exists in ASP.NET Core that could lead to an open redirect, aka 'ASP.NET Core Spoofing Vulnerability'.	2019-07-15	5.8	<a href="#">CVE-2019-1075</a> MISC
microsoft -- azure_automation	An elevation of privilege vulnerability exists in Azure Automation 'RunAs account' runbooks for users with contributor role, aka 'Azure Automation Elevation of Privilege Vulnerability'.	2019-07-15	4.0	<a href="#">CVE-2019-0962</a> MISC
microsoft -- exchange_server	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'.	2019-07-15	5.1	<a href="#">CVE-2019-1136</a> N/A
microsoft -- office	A spoofing vulnerability exists when Microsoft Office Javascript does not check the validity of the web page making a request to Office documents. An attacker who successfully exploited this vulnerability could read or write information in Office documents. The security update addresses the vulnerability by correcting the way that Microsoft Office Javascript verifies trusted web pages., aka 'Microsoft Office Spoofing Vulnerability'.	2019-07-15	6.4	<a href="#">CVE-2019-1109</a> N/A
microsoft -- office	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'.	2019-07-15	4.3	<a href="#">CVE-2019-1112</a> N/A
microsoft -- sql_server	A remote code execution vulnerability exists in Microsoft SQL Server when it incorrectly handles processing of internal functions, aka 'Microsoft SQL Server Remote Code Execution Vulnerability'.	2019-07-15	6.5	<a href="#">CVE-2019-1068</a> MISC
microsoft -- visual_studio	An information disclosure vulnerability exists when Visual Studio improperly parses XML input in certain settings files, aka 'Visual Studio Information Disclosure Vulnerability'.	2019-07-15	4.3	<a href="#">CVE-2019-1079</a> MISC
microsoft -- visual_studio_2017	An elevation of privilege vulnerability exists when the Visual Studio updater service improperly handles file permissions, aka 'Visual Studio Elevation of Privilege Vulnerability'.	2019-07-15	6.6	<a href="#">CVE-2019-1077</a> MISC
microsoft -- windows_10	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'.	2019-07-15	4.6	<a href="#">CVE-2019-0880</a> MISC
microsoft -- windows_10	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'.	2019-07-15	5.5	<a href="#">CVE-2019-0966</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.	2019-07-15	6.9	<a href="#">CVE-2019-1037</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the way that the wlanSvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'.	2019-07-15	4.6	<a href="#">CVE-2019-1085</a> MISC
microsoft -- windows_10	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1087, CVE-2019-1088.	2019-07-15	4.6	<a href="#">CVE-2019-1086</a> MISC
microsoft -- windows_10	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1086, CVE-2019-1088.	2019-07-15	4.6	<a href="#">CVE-2019-1087</a> MISC
microsoft -- windows_10	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1086, CVE-2019-1087.	2019-07-15	4.6	<a href="#">CVE-2019-1088</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1094</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1095</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows RDP client improperly discloses the contents of its memory, aka 'Remote Desktop Protocol Client Information Disclosure Vulnerability'.	2019-07-15	4.0	<a href="#">CVE-2019-1108</a> N/A
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1098</a> N/A
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1099</a> N/A
	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique			<a href="#">CVE-2019-1100</a>

microsoft -- windows_7	from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	N/A
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability". This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1101</a> N/A
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability". This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101.	2019-07-15	4.3	<a href="#">CVE-2019-1116</a> N/A
microsoft -- windows_server_2012	A denial of service vulnerability exists in Windows DNS Server when it fails to properly handle DNS queries, aka "Windows DNS Server Denial of Service Vulnerability".	2019-07-15	5.0	<a href="#">CVE-2019-0811</a> MISC
microstrategy -- microstrategy_web	In MicroStrategy Web before 10.4.6, there is stored XSS in metric due to insufficient input validation.	2019-07-17	4.3	<a href="#">CVE-2019-12475</a> MISC
mirumee -- saleor	In Mirumee Saleor 2.7.0 (fixed in 2.8.0), CSRF protection middleware was accidentally disabled, which allowed attackers to send a POST request without a valid CSRF token and be accepted by the server.	2019-07-14	6.8	<a href="#">CVE-2019-13594</a> MISC
moinejf -- abcm2ps	moinejf abcm2ps 8.13.20 is affected by: Incorrect Access Control. The impact is: Allows attackers to cause a denial of service attack via a crafted file. The component is: front.c, function txt_add. The fixed version is: after commit commit 08ae5f7656d065e86075f3d53fda89765845eae.	2019-07-18	4.3	<a href="#">CVE-2019-1010069</a> MISC MISC
myt_project -- myt	In MyT 1.5.1, the User[username] parameter has XSS.	2019-07-17	4.3	<a href="#">CVE-2019-13346</a> EXPLOIT-DB
netfilter -- iptables	A buffer overflow in iptables-restore in netfilter iptables 1.8.2 allows an attacker to (at least) crash the program or potentially gain code execution via a specially crafted iptables-save file. This is related to add_param_to_argv in xshared.c.	2019-07-12	4.3	<a href="#">CVE-2019-11360</a> MISC CONFIRM
nginx -- njs	njs through 0.3.3, used in NGINX, has a heap-based buffer over-read in nxt_vsprintf in nxt/nxt_vsprintf.c during error handling, as demonstrated by an njs_regex_literal call that leads to an njs_parser_lexer_error call and then an njs_parser_scope_error call.	2019-07-16	4.3	<a href="#">CVE-2019-13617</a> MISC MISC
nsa -- ghidra	In NSA Ghidra through 9.0.4, path traversal can occur in RestoreTask.java (from the package ghidra.app.plugin.core.archive) via an archive with an executable file that has an initial ./ in its filename. This allows attackers to overwrite arbitrary files in scenarios where an intermediate analysis result is archived for sharing with other persons. To achieve arbitrary code execution, one approach is to overwrite some critical Ghidra modules, e.g., the decompile module.	2019-07-16	6.8	<a href="#">CVE-2019-13623</a> MISC MISC
ovidentia -- ovidentia	Ovidentia 8.4.3 has SQL Injection via the id parameter in an index.php?tg=delegat&idx=mem request.	2019-07-19	6.5	<a href="#">CVE-2019-13978</a> MISC
paloaltonetworks -- pan-os	Information disclosure in PAN-OS 7.1.23 and earlier, PAN-OS 8.0.18 and earlier, PAN-OS 8.1.8-h4 and earlier, and PAN-OS 9.0.2 and earlier may allow for an authenticated user with read-only privileges to extract the API key of the device and/or the username/password from the XML API (in PAN-OS) and possibly escalate privileges granted to them.	2019-07-16	6.5	<a href="#">CVE-2019-1575</a> BID CONFIRM
paloaltonetworks -- pan-os	Command injection in PAN-OS 9.0.2 and earlier may allow an authenticated attacker to gain access to a remote shell in PAN-OS, and potentially run with the escalated user's permissions.	2019-07-16	6.5	<a href="#">CVE-2019-1576</a> CONFIRM
python -- python	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.	2019-07-13	5.0	<a href="#">CVE-2018-20852</a> MISC MISC
rust-lang -- rust	The Rust Programming Language Standard Library 1.18.0 and later is affected by: CWE-200: Information Exposure. The impact is: Contents of uninitialized memory could be printed to string or to log file. The component is: Debug trait implementation for std::collections::VecDeque::Iter. The attack vector is: The program needs to invoke debug printing for iterator over an empty VecDeque. The fixed version is: 1.30.0, nightly versions after commit b85e4cc8fadaabd41da5b9645c08c68b8f89908d.	2019-07-15	5.0	<a href="#">CVE-2019-1010299</a> MISC MISC
schneider-electric -- interactive_graphical_scada_system	A CWE-787: Out-of-bounds Write vulnerability exists in Interactive Graphical SCADA System (IGSS), Version 14 and prior, which could cause a software crash when data in the mdb database is manipulated.	2019-07-15	6.8	<a href="#">CVE-2019-6827</a> MISC
schneider-electric -- proclima	A CWE-427: Uncontrolled Search Path Element vulnerability exists in ProClima (all versions prior to version 8.0.0) which could allow a malicious DLL file, with the same name of any resident DLLs inside the software installation, to execute arbitrary code in all versions of ProClima prior to version 8.0.0.	2019-07-15	6.8	<a href="#">CVE-2019-6825</a> MISC
schneider-electric -- zelio_soft_2	A Use After Free: CWE-416 vulnerability exists in Zelio Soft 2, V5.2 and earlier, which could cause remote code execution when opening a specially crafted Zelio Soft 2 project file.	2019-07-15	6.8	<a href="#">CVE-2019-6822</a> MISC
school_college_portal_with_erp_script_project -- school_college_portal_with_erp_script	phpscriptsml.com School College Portal with ERP Script 2.6.1 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attack administrators and teachers, students and more. The component is: /pro-school/index.php?student/message/send_reply/. The attack vector is: <img src=x onerror=alert(document.domain) />.	2019-07-15	4.3	<a href="#">CVE-2019-1010028</a> MISC
sertek -- xpare	An issue was discovered in Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could exploit the vulnerable function in order to prepare an XSS payload to send to the product's clients.	2019-07-17	4.3	<a href="#">CVE-2019-13448</a> MISC
solarwinds -- network_performance_monitor	SolarWinds Network Performance Monitor 12.3 allows SQL Injection via the /api/ActiveAlertsOnThisEntity/GetActiveAlerts TriggeringObjectEntityNames parameter.	2019-07-16	6.5	<a href="#">CVE-2018-13442</a> MISC
soundexchange -- sound_exchange	SoX - Sound eXchange 14.4.2 and earlier is affected by: Out-of-bounds Read. The impact is: Denial of Service. The component is: read_samples function at xa.c:219. The attack vector is: Victim must open specially crafted .xa file. NOTE: this may overlap CVE-2017-18189.	2019-07-14	4.3	<a href="#">CVE-2019-1010004</a> MISC MISC
syguestbook_a5_project -- syguestbook_a5	SyGuestBook A5 Version 1.2 has no CSRF protection mechanism, as demonstrated by CSRF for an index.php?c=Administrator&a=update admin password change.	2019-07-18	6.8	<a href="#">CVE-2019-13949</a> MISC MISC
temenos -- cwx	Temenos CWX version 8.9 has an Broken Access Control vulnerability in the module /CWX/Employee/EmployeeEdit2.aspx, leading to the viewing of user information.	2019-07-17	5.0	<a href="#">CVE-2019-13403</a> MISC
videolan -- vlc_media_player	An Integer Underflow in MP4_EIA608_Convert() in modules/demux/mp4/mp4.c in VideoLAN VLC media player through 3.0.7.1 allows remote attackers to cause a denial of service (heap-based buffer overflow and crash) or possibly have unspecified other impact via a crafted .mp4 file.	2019-07-14	6.8	<a href="#">CVE-2019-13602</a> BID MISC MISC
wireshark -- wireshark	In Wireshark 3.0.0 to 3.0.2, 2.6.0 to 2.6.9, and 2.4.0 to 2.4.15, the ASN.1 BER dissector and related dissectors could crash. This was addressed in epan/asn1.c by properly restricting buffer increments.	2019-07-17	5.0	<a href="#">CVE-2019-13619</a> BID MISC MISC MISC
zammad -- zammad	Zammad GmbH Zammad 2.3.0 and earlier is affected by: Cross Site Scripting (XSS) - CWE-80. The impact is: Execute java script code on users browser. The component is: web app. The attack vector is: the victim must open a ticket. The fixed version is: 2.3.1, 2.2.2 and 2.1.3.	2019-07-16	4.3	<a href="#">CVE-2019-1010018</a> MISC MISC MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
automatic -- campitx_event_ticketing	The CampTix Event Ticketing plugin before 1.5 for WordPress allows XSS in the admin section via a ticket title or body.	2019-07-18	3.5	<a href="#">CVE-2016-10763</a> MISC MISC
firefly-iii -- firefly_iii	Firefly III before 4.7.17.1 is vulnerable to stored XSS due to lack of filtration of user-supplied data in a budget name. The JavaScript code is contained in a transaction, and is executed on the tags/show/\$tag_number\$ tag summary page.	2019-07-17	3.5	<a href="#">CVE-2019-13644</a> MISC MISC
firefly-iii -- firefly_iii	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user-supplied data in image file names. The JavaScript code is executed during attachments/edit/\$file_id\$ attachment editing.	2019-07-17	3.5	<a href="#">CVE-2019-13645</a> MISC MISC
firefly-iii -- firefly_iii	Firefly III before 4.7.17.3 is vulnerable to reflected XSS due to lack of filtration of user-supplied data in a search query.	2019-07-17	3.5	<a href="#">CVE-2019-13646</a> MISC MISC

firefly-iii -- firefly_iii	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user-supplied data in image file content. The JavaScript code is executed during attachments/view/\$file_id\$ attachment viewing.	2019-07-17	3.5	<a href="#">CVE-2019-13647</a> MISC MISC
glpi-project -- glpi	GLPI GLPI Product 9.3.1 is affected by: Cross Site Scripting (XSS). The impact is: All dropdown values are vulnerable to XSS leading to privilege escalation and executing js on admin. The component is: /glpi/ajax/getDropDownValue.php. The attack vector is: 1- User Create a ticket , 2- Admin opens another ticket and click on the "Link Tickets" feature, 3- a request to the endpoint fetches js and executes it.	2019-07-15	3.5	<a href="#">CVE-2019-1010307</a> MISC MISC
glpi-project -- glpi	GLPI GLPI Product 9.3.1 is affected by: Frame and Form tags Injection allowing admins to phish users by putting code in reminder description. The impact is: Admins can phish any user or group of users for credentials / credit cards. The component is: Tools > Reminder > Description .. Set the description to any iframe/form tags and apply. The attack vector is: The attacker puts a login form, the user fills it and clicks on submit .. the request is sent to the attacker domain saving the data. The fixed version is: 9.4.1.	2019-07-12	3.5	<a href="#">CVE-2019-1010310</a> MISC MISC
ibm -- campaign	IBM Campaign 9.1.0, 9.1.2, 10.1, and 11.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152857.	2019-07-17	3.5	<a href="#">CVE-2018-1921</a> XF CONFIRM
ibm -- radar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 could allow a local user to obtain sensitive information when exporting content that could aid an attacker in further attacks against the system. IBM X-Force ID: 156563.	2019-07-17	2.1	<a href="#">CVE-2019-4054</a> XF CONFIRM
ibm -- radar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159131.	2019-07-17	3.5	<a href="#">CVE-2019-4211</a> XF CONFIRM
microsoft -- exchange_server	A cross-site-scripting (XSS) vulnerability exists when Microsoft Exchange Server does not properly sanitize a specially crafted web request to an affected Exchange server, aka 'Microsoft Exchange Server Spoofing Vulnerability'.	2019-07-15	3.5	<a href="#">CVE-2019-1137</a> N/A
microsoft -- sharepoint_enterprise_server	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'.	2019-07-15	3.5	<a href="#">CVE-2019-1134</a> N/A
microsoft -- team_foundation_server	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting Vulnerability'.	2019-07-15	3.5	<a href="#">CVE-2019-1076</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1073.	2019-07-15	2.1	<a href="#">CVE-2019-1071</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071.	2019-07-15	2.1	<a href="#">CVE-2019-1073</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in Microsoft Windows where certain folders, with local service privilege, are vulnerable to symbolic link attack. An attacker who successfully exploited this vulnerability could potentially access unauthorized information. The update addresses this vulnerability by not allowing symbolic links in these scenarios., aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1082.	2019-07-15	2.1	<a href="#">CVE-2019-1074</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when Unistore.dll fails to properly handle objects in memory, aka 'Microsoft unistore.dll Information Disclosure Vulnerability'.	2019-07-15	2.1	<a href="#">CVE-2019-1091</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1097.	2019-07-15	2.1	<a href="#">CVE-2019-1093</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	2019-07-15	2.1	<a href="#">CVE-2019-1096</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1093.	2019-07-15	2.1	<a href="#">CVE-2019-1097</a> MISC
norton -- password_manager	Norton Password Manager, prior to 6.3.0.2082, may be susceptible to an address spoofing issue. This type of issue may allow an attacker to disguise their origin IP address in order to obfuscate the source of network traffic.	2019-07-16	1.7	<a href="#">CVE-2019-9700</a> CONFIRM
openenergymonitor -- emoncms	OpenEnergyMonitor Project Emoncms 9.8.8 is affected by: Cross Site Scripting (XSS). The impact is: Theoretically low, but might potentially enable persistent XSS (user could embed mal. code). The component is: Javascript code execution in "Name", "Location", "Bio" and "Starting Page" fields in the "My Account" page. File: Lib/listjs/list.js, line 67. The attack vector is: unknown, victim must open profile page if persistent was possible.	2019-07-14	3.5	<a href="#">CVE-2019-1010008</a> MISC
ovidentia -- ovidentia	index.php in Ovidentia 8.4.3 has XSS via tg=groups, tg=maildoms&idx=create&userid=0&bgrp=y, tg=delegat, tg=site&idx=create, tg=site&item=4, tg=admdir&idx=mdb&id=1, tg=notes&idx=Create, tg=admfqs&idx=Add, or tg=admoc&idx=addoc&item=.	2019-07-19	3.5	<a href="#">CVE-2019-13977</a> MISC
rdbrck -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	2.1	<a href="#">CVE-2019-12912</a> CONFIRM
rdbrck -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	2.1	<a href="#">CVE-2019-12913</a> CONFIRM
sitecore -- experience_platform	In Sitecore 9.0 rev 171002, Persistent XSS exists in the Media Library and File Manager. An authenticated unprivileged user can modify the uploaded file extension parameter to inject arbitrary JavaScript.	2019-07-17	3.5	<a href="#">CVE-2019-13493</a> MISC
syguestbook_a5_project -- syguestbook_a5	SyGuestBook A5 Version 1.2 allows stored XSS because the isValidData function in include/functions.php does not properly block XSS payloads, as demonstrated by a crafted use of the onerror attribute of an IMG element.	2019-07-18	3.5	<a href="#">CVE-2019-13948</a> MISC MISC
syguestbook_a5_project -- syguestbook_a5	index.php?c=admin&a=index in SyGuestBook A5 Version 1.2 has stored XSS via a reply to a comment.	2019-07-18	3.5	<a href="#">CVE-2019-13950</a> MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- bridge_cc	Adobe Bridge CC version 9.0.2 and earlier versions have an out of bound read vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	not yet calculated	<a href="#">CVE-2019-7963</a> MISC
adobe -- experience_manager	Adobe Experience Manager version 6.4 and earlier have a Stored Cross-site Scripting vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user.	2019-07-18	not yet calculated	<a href="#">CVE-2019-7954</a> MISC
akeo_consulting -- rufus	Akeo Consulting Rufus 3.0 and earlier is affected by: Insecure Permissions. The impact is: arbitrary code execution with escalation of privilege. The component is: Executable installer, portable executable (ALL executables available). The attack vector is: CWE-29, CWE-377, CWE-379.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010101</a> MISC
akeo_consulting -- rufus	Akeo Consulting Rufus 3.0 and earlier is affected by: DLL search order hijacking. The impact is: Arbitrary code execution WITH escalation of privilege. The component is: Executable installers, portable executables (ALL executables on the web site). The attack vector is: CAPEC-471, CWE-426, CWE-427.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010100</a> MISC
antword_project -- antword	n antSword before 2.1.0, self-XSS in the database configuration leads to code execution via modules/database/asp/index.js, modules/database/custom/index.js, modules/database/index.js, or modules/database/php/index.js.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13970</a> MISC MISC MISC
aquaverde -- aquarius_cms	Aquaverde GmbH Aquarius CMS prior to version 4.1.1 is affected by: Incorrect Access Control. The impact is: The access o the log file is not restricted. It contains sensitive information like passwords etc. The component is: log file. The attack vector is: open the file.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010308</a> MISC MISC
arduino -- arduino	Embedded systems based on Arduino before Rev3 allow remote attackers to send data to LEDs (directly connected to GPIO pins) via a laser, because of LED photosensitivity.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13991</a> MISC
audiocodes -- multiple_mediant_devices	An issue was discovered on AudioCodes Mediant 500L-MSBR, 500-MBSR, M800B-MSBR and 800C-MSBR devices with firmware versions F7.20A to F7.20A.251. An internal interface exposed to the link-local address 169.254.254.253 allows attackers in the local network to access multiple quagga VTYS. Attackers can authenticate with the default 1234 password hat cannot be changed, and can execute malicious and unauthorized actions.	2019-07-19	not yet calculated	<a href="#">CVE-2019-9229</a> MISC



audiocodes -- multiple_mediant_devices	An issue was discovered on AudioCodes Mediant 500L-MSBR, 500-MBSR, M800B-MSBR and 800C-MSBR devices with firmware versions F7.20A to F7.20A.253. A cross-site scripting (XSS) vulnerability in the search function of the management web interface allows remote attackers to inject arbitrary web script or HTML via the keyword parameter.	2019-07-18	not yet calculated	<a href="#">CVE-2019-8230</a> <a href="#">MISC</a>
audiocodes -- multiple_mediant_devices	An issue was discovered on AudioCodes Mediant 500L-MSBR, 500-MBSR, M800B-MSBR and 800C-MSBR devices with firmware versions before 7.20A.202.307. A Cross-Site Request Forgery (CSRF) vulnerability in the management web interface allows remote attackers to execute malicious and unauthorized actions, because CSRFProtection=1 is not a default and is not documented.	2019-07-18	not yet calculated	<a href="#">CVE-2019-8231</a> <a href="#">MISC</a>
avast -- antivirus	In Avast Antivirus before 19.4, a local administrator can trick the product into renaming arbitrary files by replacing the Logs\Update.log file with a symlink. The next time the product attempts to write to the log file, the target of the symlink is renamed. This defect can be exploited to rename a critical product file (e.g., AvastSvc.exe), causing the product to fail to start on the next system restart.	2019-07-18	not yet calculated	<a href="#">CVE-2019-11230</a> <a href="#">MISC</a>
b3log -- wide	b3log Wide before 1.6.0 allows three types of attacks to access arbitrary files. First, the attacker can write code in the editor, and compile and run it approximately three times to read an arbitrary file. Second, the attacker can create a symlink, and then place the symlink into a ZIP archive. An unzip operation leads to read access, and write access (depending on file permissions), to the symlink target. Third, the attacker can import a Git repository that contains a symlink, similarly leading to read and write access.	2019-07-18	not yet calculated	<a href="#">CVE-2019-13915</a> <a href="#">MISC</a>
bacnet -- stack_bacserv	BACnet Stack bacserv 0.9.1 and 0.8.5 is affected by: Buffer Overflow. The impact is: exploit was not explored. The component is: bacserv BVLC forwarded NPDU. bvlc_bdt_forward_npdu() calls bvlc_encode_forwarded_npdu() which copies the content from the request into a local in the bvlc_bdt_forward_npdu() stack frame and clobbers the canary. The attack vector is: A BACnet/IP device with BBMD enabled based on this library connected to IP network. The fixed version is: 0.8.6.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010073</a> <a href="#">MISC</a> <a href="#">MISC</a>
chinamobile -- plc_wireless_router_gpn2.4p21-c-cn	ChinaMobile GPN2.4P21-C-CN W2001EN-00 is affected by: Incorrect Access Control - Unauthenticated Remote Reboot. The impact is: PLC Wireless Router's are vulnerable to an unauthenticated remote reboot due. The component is: Reboot settings are available to unauthenticated users instead of only authenticated users. The attack vector is: Remote.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010136</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a>
cisco -- findit_network_manager_and_findit_network_probe_release	A vulnerability in the Cisco FindIT Network Management Software virtual machine (VM) images could allow an unauthenticated, local attacker who has access to the VM console to log in to the device with a static account that has root privileges. The vulnerability is due to the presence of an account with static credentials in the underlying Linux operating system. An attacker could exploit this vulnerability by logging in to the command line of the affected VM with the static account. A successful exploit could allow the attacker to log in with root-level privileges. This vulnerability affects only Cisco FindIT Network Manager and Cisco FindIT Network Probe Release 1.1.4 if these products are using Cisco-supplied VM images. No other releases or deployment models are known to be vulnerable.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1919</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the sponsor portal web interface for Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. At the time of publication, this vulnerability affected Cisco ISE running software releases 2.6.0 and prior.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1942</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. At the time of publication, this vulnerability affected Cisco ISE running software releases prior to 2.4.0 Patch 9 and 2.6.0.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1941</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- industrial_network_director	A vulnerability in the Web Services Management Agent (WSMA) feature of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data using an invalid X.509 certificate. The vulnerability is due to insufficient X.509 certificate validation when establishing a WSMA connection. An attacker could exploit this vulnerability by supplying a crafted X.509 certificate during the WSMA connection setup phase. A successful exploit could allow the attacker to conduct man-in-the-middle attacks to decrypt confidential information on WSMA connections to the affected software. At the time of publication, this vulnerability affected Cisco IND Software releases prior to 1.7.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1940</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- ios_access_points_software	A vulnerability in the 802.11r Fast Transition (FT) implementation for Cisco IOS Access Points (APs) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected interface. The vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1920</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_switches	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1943</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- small_business_spa500_series_ip_phones	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1923</a> <a href="#">MISC</a> <a href="#">CISCO</a>
cisco -- vision_dynamic_signage_director	A vulnerability in the REST API interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to bypass authentication on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to execute arbitrary actions through the REST API with administrative privileges on the affected system. The REST API is enabled by default and cannot be disabled.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1917</a> <a href="#">MISC</a> <a href="#">CISCO</a>
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 allow SQL Injection.	2019-07-16	not yet calculated	<a href="#">CVE-2019-12989</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 3 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12987</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 4 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12988</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 6 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12992</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 allow Directory Traversal.	2019-07-16	not yet calculated	<a href="#">CVE-2019-12990</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 5 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12991</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 2 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12986</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-12985</a>



citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 1 of 6).	2019-07-16	not yet calculated	BID MISC MISC
cjson -- cjson	DaveGamble/cJSON cJSON 1.7.8 is affected by: Improper Check for Unusual or Exceptional Conditions. The impact is: Null dereference, so attack can cause denial of service. The component is: cJSON_GetObjectItemCaseSensitive() function. The attack vector is: crafted json file. The fixed version is: 1.7.9 and later.	2019-07-19	not yet calculated	CVE-2019-0239 MISC MISC
cloud_foundry -- uua	Cloud Foundry UAA, versions prior to v73.4.0, does not set an X-FRAME-OPTIONS header on various endpoints. A remote user can perform clickjacking attacks on UAA's frontend sites.	2019-07-18	not yet calculated	CVE-2019-3734 CONFIRM
code42 -- code42_enterprise_and_crashplan_for_small_business	Code42 Enterprise and Crashplan for Small Business Client version 6.7 before 6.7.5, 6.8 before 6.8.8, and 6.9 before 6.9.4 allows eval injection. A proxy auto-configuration file, crafted by a lesser privileged user, may be used to execute arbitrary code at a higher privilege as the service user.	2019-07-19	not yet calculated	CVE-2019-11552 MISC CONFIRM
code42 -- code42_for_enterprise	Code42 for Enterprise through 6.8.4 has Incorrect Access Control.	2019-07-19	not yet calculated	CVE-2019-11553 CONFIRM
cohesity -- dataplatform	A man-in-the-middle vulnerability related to vCenter access was found in Cohesity DataPlatform version 5.x and 6.x prior to 6.1.1c. Cohesity clusters did not verify TLS certificates presented by vCenter. This vulnerability could expose Cohesity user credentials configured to access vCenter.	2019-07-12	not yet calculated	CVE-2019-11242 CONFIRM
computerlab -- maple_wbt_snmp_administrator	SnmpAdm.exe in MAPLE WBT SNMP Administrator v2.0.195.15 has an Unauthenticated Remote Buffer Overflow via a on string to the CE Remote feature listening on Port 987.	2019-07-17	not yet calculated	CVE-2019-13577 MISC MISC FULLDISC BUGTRAQ
dancer-plugin-simplecrud -- dancer-plugin-simplecrud	Dancer::Plugin::SimpleCRUD 1.14 and earlier is affected by: Incorrect Access Control. The impact is: Potential for unauthorised access to data. The component is: Incorrect calls to _ensure_auth() wrapper result in authentication-checking not being applied to al routes.	2019-07-17	not yet calculated	CVE-2019-1010084 MISC
dell_emc -- unity_and_unityvsa	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain a plain-text password storage vulnerability. A Unisphere user's (including the admin privilege user) password is stored in a plain text in Unity Data Collection bundle logs files for troubleshooting). A local authenticated attacker with access to the Data Collection bundle may use the exposed password to gain access with the privileges of the compromised user.	2019-07-18	not yet calculated	CVE-2019-3741 MISC
dell_emc -- unity_and_unityvsa	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain an improper authorization vulnerability in NAS Server quotas configuration. A remote authenticated Unisphere Operator could potentially exploit this vulnerability to edit quota configuration of other users.	2019-07-18	not yet calculated	CVE-2019-3734 MISC
dglgik_inc -- dglux_server	DGLogik Inc DGLux Server All Versions is affected by: Insecure Permissions. The impact is: Remote Execution, Credential Leaks. The component is: IoT API. The attack vector is: Any Accessible Server.	2019-07-14	not yet calculated	CVE-2019-1010009 MISC
discuz!ml -- discuz!ml	Discuz!ML 3.2 through 3.4 allows remote attackers to execute arbitrary PHP code via a modified language cookie, as demonstrated by changing 4gH4_0df5_language=en to 4gH4_0df5_language=en'.phpinfo('; (if the random prefix 4gH4_0df5_were used).	2019-07-18	not yet calculated	CVE-2019-13956 MISC
docker -- docker_ce_and_docker_ee	n Docker CE and EE before 18.09.8 (as well as Docker EE before 17.06.2-ee-23 and 18.x before 18.03.1-ee-10), Docker Engine in debug mode may sometimes add secrets to the debug log. This applies to a scenario where docker stack deploys run to redeploy a stack that includes (non external) secrets. It potentially applies to other API users of the stack API if they resend the secret.	2019-07-18	not yet calculated	CVE-2019-13509 MISC
dpic -- dpic	dpic 2019.06.20 has a Stack-based Buffer Overflow in the wfloat() function in main.c.	2019-07-19	not yet calculated	CVE-2019-13989 MISC
eclipse -- openj9	n Eclipse OpenJ9 prior to 0.15, the String.getBytes(int, int, byte[], int) method does not verify that the provided byte array is non-null nor that the provided index is in bounds when compiled by the JIT. This allows arbitrary writes to any 32-bit address or beyond the end of a byte array within Java code run under a SecurityManager.	2019-07-17	not yet calculated	CVE-2019-11772 CONFIRM
elcom -- elcom_cms	Elcom CMS before 10.7 has SQL Injection via EventSearchByState.aspx and EventSearchAdv.aspx.	2019-07-19	not yet calculated	CVE-2019-12946 MISC
epsocrm -- epsocrm	Stored XSS in EpoCRM before 5.6.4 allows remote attackers to execute malicious JavaScript and inject arbitrary source code into the target pages. The attack begins by storing a new stream message containing an XSS payload. The stored payload can then be triggered by clicking a malicious link on the Notifications page.	2019-07-17	not yet calculated	CVE-2019-13643 MISC MISC
facebook -- hhvm	Call to the script_enc() function in HHVM can lead to heap corruption by using specifically crafted parameters (N, r and p). This happens if the parameters are configurable by an attacker for instance by providing the output of script_enc() in a context where Hack/PHP code would attempt to verify it by re-running script_enc() with the same parameters. This could result in information disclosure, memory being overwritten or crashes of the HHVM process. This issue affects versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.7.0, 4.8.0, versions 3.30.5 and below, and all versions in the 4.0, 4.1, and 4.2 series.	2019-07-18	not yet calculated	CVE-2019-3570 CONFIRM CONFIRM
facebook -- whatsapp_desktop	An input validation issue affected WhatsApp Desktop versions prior to 0.3.3793 which allows malicious clients to send files o users that would be displayed with a wrong extension.	2019-07-16	not yet calculated	CVE-2019-3571 CONFIRM
fitbit -- multiple_products	On Fitbit activity-tracker devices, certain addresses never change. According to the popets-2019-0036.pdf document, this eads to "permanent trackability" and "considerable privacy concerns" without a user-accessible anonymization feature. The devices, such as Charge 2, transmit Bluetooth Low Energy (BLE) advertising packets with a TxAdd flag indicating random addresses, but the addresses remain constant. If devices come within BLE range at one or more locations where an adversary has set up passive sniffing, the adversary can determine whether the same device has entered one of these ocatons.	2019-07-15	not yet calculated	CVE-2014-10374 MISC MISC
gnome -- pango	Gnome Pango 1.42 and later is affected by: Buffer Overflow. The impact is: The heap based buffer overflow can be used to get code execution. The component is: function name: pango_log2vis_get_embedding_levels, assignment of nchars and he loop condition. The attack vector is: Bug can be used when application pass invalid utf-8 strings to functions like pango_itemize.	2019-07-19	not yet calculated	CVE-2019-1010238 MISC
gnu -- patch	n GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c.	2019-07-17	not yet calculated	CVE-2019-13636 MISC MLIST
h3c -- h3cloud	H3C H3Cloud OS all versions allows SQL injection via the ear/grid_event sidx parameter.	2019-07-19	not yet calculated	CVE-2019-12193 MISC
helm -- helm	helm Before 2.7.2 is affected by: CWE-295: Improper Certificate Validation. The impact is: Unauthorized clients could connect to the server because self-signed client certs were allowed. The component is: helm (many files updated, see https://github.com/helm/helm/pull/3152/files/1096813bf9a425e2aa4ac755b6c991b626dfab50). The attack vector is: A malicious client could connect to the server over the network. The fixed version is: 2.7.2.	2019-07-17	not yet calculated	CVE-2019-1010275 MISC MISC MISC
hid_digitalpersona -- u.are.u_4500_fingerprint_reader	An issue was discovered in the HID Global DigitalPersona (formerly Crossmatch) U.are.U 4500 Fingerprint Reader Windows Biometric Framework driver 5.0.0.5. It has a statically coded initialization vector to encrypt a user's fingerprint mage, resulting in weak encryption of that. This, in combination with retrieving an encrypted fingerprint image and encryption key (through another vulnerability), allows an attacker to obtain a user's fingerprint image.	2019-07-16	not yet calculated	CVE-2019-13603 MISC MISC MISC
hid_digitalpersona -- u.are.u_4500_fingerprint_reader	There is a short key vulnerability in HID Global DigitalPersona (formerly Crossmatch) U.are.U 4500 Fingerprint Reader v24. The key for obfuscating the fingerprint image is vulnerable to brute-force attacks. This allows an attacker to recover the key and decrypt that image using the key. Successful exploitation causes a sensitive biometric information leak.	2019-07-15	not yet calculated	CVE-2019-13604 MISC MISC MISC
hpe -- icewall_sso_agent_option_and_icewall_mfa	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module ) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and 6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP-UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7.	2019-07-19	not yet calculated	CVE-2019-11989 MISC
hpe -- icewall_sso_agent_option_and_icewall_mfa	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module ) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and 6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP-UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7.	2019-07-19	not yet calculated	CVE-2019-11990 MISC
huawei -- tony-al00b_smartphones	There is an information disclosure vulnerability on Secure Input of certain Huawei smartphones in Versions earlier than Tony-AL00B 9.1.0.216(C00E214R2P1). The Secure Input does not properly limit certain system privilege. An attacker tricks he user to install a malicious application and successful exploit could result in information disclosure.	2019-07-17	not yet calculated	CVE-2019-8222 MISC
				CVE-2018-



				MISC
logmein -- join.me	n LogMeIn join.me before 3.16.0.5505, an attacker could execute arbitrary commands on a targeted system. This vulnerability is due to unsafe search paths used by the application URI that is defined in Windows. An attacker could exploit his vulnerability by convincing a targeted user to follow a malicious link. Successful exploitation could cause the application to load libraries from the directory targeted by the URI link. The attacker could use this behavior to execute arbitrary commands on the system with the privileges of the targeted user if the attacker can place a crafted library in a directory that is accessible to the vulnerable system.	2019-07-17	not yet calculated	CVE-2019-13637 MISC
mailcleaner -- mailcleaner	MailCleaner before c888fbb6aa7c5f8400f637bcf1cbb844de46cd9 is affected by: Unauthenticated MySQL database password information disclosure. The impact is: MySQL database content disclosure (e.g. username, password). The component is: The API call in the function allowAction() in NewslettersController.php. The attack vector is: HTTP Get request. The fixed version is: c888fbb6aa7c5f8400f637bcf1cbb844de46cd9.	2019-07-18	not yet calculated	CVE-2019-1010246 MISC
mcafee -- agent	Privilege escalation vulnerability in McAfee Agent (MA) before 5.6.1 HF3, allows local administrator users to potentially disable some McAfee processes by manipulating the MA directory control and placing a carefully constructed file in the MA directory.	2019-07-18	not yet calculated	CVE-2019-3592 CONFIRM
mdaemon_technologies -- email_server	MDaemon Email Server 19 skips SpamAssassin checks by default for e-mail messages larger than 2 MB (and limits checks to 10 MB even with special configuration), which is arguably inconsistent with currently popular message sizes. This might interfere with risk management for malicious e-mail, if a customer deploys a server with sufficient resources to scan large messages.	2019-07-16	not yet calculated	CVE-2019-13612 MISC
microsoft -- active_directory_federation_services	A security feature bypass vulnerability exists in Active Directory Federation Services (ADFS) which could allow an attacker to bypass the extranet logout policy. To exploit this vulnerability, an attacker could run a specially crafted application, which would allow an attacker to launch a password brute-force attack or cause account lockouts in Active Directory. This security update corrects how ADFS handles external authentication requests., aka 'ADFS Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0975.	2019-07-15	not yet calculated	CVE-2019-11226 N/A
microsoft -- active_directory_federation_services	A security feature bypass vulnerability exists when Active Directory Federation Services (ADFS) improperly updates its list of banned IP addresses. To exploit this vulnerability, an attacker would have to convince a victim ADFS administrator to update the list of banned IP addresses. This security update corrects how ADFS updates its list of banned IP addresses., aka 'ADFS Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-1126.	2019-07-15	not yet calculated	CVE-2019-0975 MISC
microsoft -- exchange	An information disclosure vulnerability exists when Exchange allows creation of entities with Display Names having non-printable characters. An authenticated attacker could exploit this vulnerability by creating entities with invalid display names, which, when added to conversations, remain invisible. This security update addresses the issue by validating display names upon creation in Microsoft Exchange, and by rendering invalid display names correctly in Microsoft Outlook clients., aka 'Microsoft Exchange Information Disclosure Vulnerability'.	2019-07-15	not yet calculated	CVE-2019-1084 MISC
microsoft -- symcrypt	A denial of service vulnerability exists when SymCrypt improperly handles a specially crafted digital signature. An attacker could exploit the vulnerability by creating a specially crafted connection or message. The security update addresses the vulnerability by correcting the way SymCrypt handles digital signatures., aka 'SymCrypt Denial of Service Vulnerability'.	2019-07-15	not yet calculated	CVE-2019-08659 MISC
microsoft -- windows_defender_application_control	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'.	2019-07-19	not yet calculated	CVE-2019-1167 MISC
microstrategy -- microstrategy_web	n MicroStrategy Web before 10.1 patch 10, stored XSS is possible in the FLTB parameter due to missing input validation.	2019-07-19	not yet calculated	CVE-2019-12453 MISC
mongodb -- mongodb_enterprise_server	Improper handling of LDAP authentication in MongoDB Server versions 3.0.0 to 3.0.6 allows an unauthenticated client to gain unauthorized access.	2019-07-19	not yet calculated	CVE-2019-7882 CONFIRM
nasa -- cftsio	NASA CFITSIO prior to 3.43 is affected by: Buffer Overflow. The impact is: arbitrary code execution. The component is: over 40 source code files were changed. The attack vector is: remote unauthenticated attacker. The fixed version is: 3.43. NOTE: this CVE refers to the issues not covered by CVE-2018-3846, CVE-2018-3847, CVE-2018-3848, and CVE-2018-3849. One example is ftp_status in drvnet.c mishandling a long string beginning with a '4' character.	2019-07-16	not yet calculated	CVE-2019-1010060 MISC MISC MISC MISC
nfdump -- nfdump	nfdump 1.6.16 and earlier is affected by: Buffer Overflow. The impact is: The impact could range from a denial of service to local code execution. The component is: nfx.c:546, nfile_inline.c:83, minilzo.c (redistributed). The attack vector is: nfdump must read and process a specially crafted file. The fixed version is: after commit 9f0fe9563366f62a71d34c92229da3432ec5cfe.	2019-07-16	not yet calculated	CVE-2019-1010057 MISC
nsa -- ghidra	NSA Ghidra before 9.0.1 allows XXE when a project is opened or restored, or a tool is imported, as demonstrated by a project.prp file.	2019-07-16	not yet calculated	CVE-2019-13625 MISC MISC MISC
nvidia -- jetson_tx1	n NVIDIA Jetson TX1 L4T R32 version branch prior to R32.2. Tegra bootloader contains a vulnerability in nvboot in which the nvboot-cpu image is loaded without the load address first being validated, which may lead to code execution, denial of service, or escalation of privileges.	2019-07-19	not yet calculated	CVE-2019-5680 CONFIRM
oecms -- oecms	OECMS v4.3.R60321 and v4.3 later is affected by: Cross Site Request Forgery (CSRF). The impact is: The victim clicks on adding an administrator account. The component is: admincp.php. The attack vector is: network connectivity. The fixed version is: v4.3.	2019-07-18	not yet calculated	CVE-2019-1010112 MISC
open_information_security_foundation -- suricata	Open Information Security Foundation Suricata prior to version 4.1.3 is affected by: Denial of Service - TCP/HTTP detection bypass. The impact is: An attacker can evade a signature detection with a specially formed sequence of network packets. The component is: detect.c https://github.com/OISF/suricata/pull/3625/commits/d8634daf74c882356659adbb65fb142b738a186b). The attack vector is: An attacker can trigger the vulnerability by a specifically crafted network TCP session. The fixed version is: 4.1.3.	2019-07-18	not yet calculated	CVE-2019-1010279 MISC MISC MISC
open_information_security_foundation -- suricata	Open Information Security Foundation Suricata prior to version 4.1.2 is affected by: Denial of Service - DNS detection bypass. The impact is: An attacker can evade a signature detection with a specially formed network packet. The component is: app-layer-detect-proto.c, decode.c, decode-teredo.c and decode-ipv6.c https://github.com/OISF/suricata/pull/3590/commits/11f3659f64a4e42e90cb3c09fcef66894205aefe, https://github.com/OISF/suricata/pull/3590/commits/8357ef3f8ffcd99ef6571350724160de356158b). The attack vector is: An attacker can trigger the vulnerability by sending a specifically crafted network request. The fixed version is: 4.1.2.	2019-07-18	not yet calculated	CVE-2019-1010261 MISC MISC MISC
openmodelica -- omcompiler	OpenModelica OMCompiler is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: OPENMODELICAHOME parameter changeable via environment variable. The attack vector is: Changing an environment variable.	2019-07-15	not yet calculated	CVE-2019-1010038 CONFIRM
opera_software -- opera_mini_for_ios	The Opera Mini application through 16.0.14 for iOS has a UXSS vulnerability that can be triggered by performing navigation to a javascript: URL.	2019-07-18	not yet calculated	CVE-2019-13607 MISC
otcms -- otcms	OTCMS 3.81 allows XSS via the mode parameter in an apiRun.php?mudi=autoRun request.	2019-07-19	not yet calculated	CVE-2019-13971 MISC
pallets_project -- flask	The Pallets Project Flask before 1.0 is affected by: unexpected memory usage. The impact is: denial of service. The attack vector is: crafted encoded JSON data. The fixed version is: 1.	2019-07-17	not yet calculated	CVE-2019-010083 CONFIRM
palo_alto_networks -- pan-os	Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code.	2019-07-19	not yet calculated	CVE-2019-1579 BID MISC
perl_crypt-jwt -- perl_crypt-jwt	Perl Crypt::JWT prior to 0.023 is affected by: Incorrect Access Control. The impact is: allow attackers to bypass authentication by providing a token by crafting with hmac(). The component is: JWT.pm, line 614. The attack vector is: network connectivity. The fixed version is: after commit b98a59b42ded9f9e51b2560410106207c2152d6c.	2019-07-17	not yet calculated	CVE-2019-1010263 MISC MISC
pluckcms -- pluckcms	PluckCMS 4.7.4 and earlier is affected by: CWE-434 Unrestricted Upload of File with Dangerous Type. The impact is: get webshell. The component is: data/inc/images.php line36. The attack vector is: modify the MIME TYPE on HTTP request to upload a php file. The fixed version is: after commit 09f0ab871bf633973cfd9fc4fe59d4a912397cf8.	2019-07-16	not yet calculated	CVE-2019-1010062 MISC MISC
premium_software -- cleditor	Premium Software CLEditor 1.4.5 and earlier is affected by: Cross Site Scripting (XSS). The impact is: An attacker might be able to inject arbitrary html and script code into the web site. The component is: jQuery plug-in. The attack vector is: the victim must open a crafted href attribute of a link (A) element.	2019-07-19	not yet calculated	CVE-2019-1010113 MISC
printer_on -- printer_on_central_print_services	An issue was discovered in PrinterOn Central Print Services (CPS) through 4.1.4. The core components that create and launch a print job do not perform complete verification of the session cookie that is supplied to them. As a result, an attacker with guest/pseudo-guest level permissions can bypass the session checks (that would otherwise log out a low-privileged user) by calling the core print job components directly via crafted HTTP GET and POST requests.	2019-07-19	not yet calculated	CVE-2018-17210 MISC
proftpd -- proftpd	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information	2019-07-	not yet	CVE-2019-12815 MISC

	disclosure without authentication, a related issue to CVE-2015-3306.	19	calculated	MISC MISC
python_engineio -- python_engineio	An issue was discovered in python-engineio through 3.8.2. There is a Cross-Site WebSocket Hijacking (CSWSH) vulnerability that allows attackers to make WebSocket connections to a server by using a victim's credentials, because the Origin header is not restricted.	2019-07-15	not yet calculated	CVE-2019-13611 MISC
qbittorrent -- qbittorrent	n qBittorrent before 4.1.7, the function Application::runExternalProgram() located in app/application.cpp allows command njection via shell metacharacters in the torrent name parameter or current tracker parameter, as demonstrated by remote command execution via a crafted name within an RSS feed.	2019-07-17	not yet calculated	CVE-2019-13640 MISC
quake3e -- quake3e	Quake3e < 5ed740d is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Argument string creation.	2019-07-16	not yet calculated	CVE-2019-1010043 MISC
ranger_studios -- directus_7_api	n Directus 7 API before 2.2.1, uploading of PHP files is not blocked, leading to uploads/_/originals remote code execution.	2019-07-19	not yet calculated	CVE-2019-13979 MISC
ranger_studios -- directus_7_api	n Directus 7 API through 2.3.0, uploading of PHP files is blocked only when the Apache HTTP Server is used, leading to uploads/_/originals remote code execution with nginx.	2019-07-19	not yet calculated	CVE-2019-13980 MISC
ranger_studios -- directus_7_api	n Directus 7 API through 2.3.0, remote attackers can read image files via a direct request for a filename under the uploads/_/originals/ directory. This is related to a configuration option in which the file collection can be non-public, but this option does not apply to the thumbnailer.	2019-07-19	not yet calculated	CVE-2019-13981 MISC
ranger_studios -- directus_7_api	Directus 7 API before 2.2.2 has insufficient anti-automation, as demonstrated by lack of a CAPTCHA in core/Directus/Services/AuthService.php and endpoints/Auth.php.	2019-07-19	not yet calculated	CVE-2019-13983 MISC
ranger_studios -- directus_7_api	Directus 7 API before 2.3.0 does not validate uploaded files. Regardless of the file extension or MIME type, there is a direct link to each uploaded file, accessible by unauthenticated users, as demonstrated by the EICAR Anti-Virus Test File.	2019-07-19	not yet calculated	CVE-2019-13984 MISC
ranger_studios -- directus_7_api	nterfaces/markdown/input.vue in Directus 7 Application before 7.7.0 does not sanitize Markdown text before rendering a preview.	2019-07-19	not yet calculated	CVE-2019-13982 MISC
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	CVE-2019-8932 CONFIRM
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	CVE-2019-8931 CONFIRM
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	CVE-2019-12914 CONFIRM
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	CVE-2019-12911 CONFIRM
rubygems -- paranoid2_gem	The paranoid2 gem 1.1.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a hird party. The current version, without this backdoor, is 1.1.5.	2019-07-14	not yet calculated	CVE-2019-13589 BID MISC
sahi_pro -- sahi_pro	s_sprml/_s_/dyn/Player_setScriptFile in Sahi Pro 8.0.0 allows command execution. It allows one to run ".sah" scripts via Sahi Launcher. Also, one can create a new script with an editor. It is possible to execute commands on the server using the _execute() function.	2019-07-14	not yet calculated	CVE-2019-13597 MISC
saleor -- saleor	Saleor Issue was introduced by merge commit: e1b01bad0703afd08d297ed3f1f472248312cc9c. This commit was released as part of 2.0.0 release is affected by: Incorrect Access Control. The impact is: Important. The component is: ProductVariant type in GraphQL API. The attack vector is: Unauthenticated user can access the GraphQL API (which is by default publicly exposed under '/graphql/' URL) and fetch products data which may include admin-restricted shop's revenue data. The fixed version is: 2.3.1.	2019-07-15	not yet calculated	CVE-2019-1010304 MISC
scapy -- scapy	scapy 2.4.0 is affected by: Denial of Service. The impact is: infinite loop, resource consumption and program unresponsive. The component is: _RADIUSAttrPacketListField.getField(self..). The attack vector is: over the network or in a pcap. both work.	2019-07-19	not yet calculated	CVE-2019-1010142 MISC
schneider_electric -- modicon_m580_cpu-bmep582040_and_modicon_ethernet_module_bmenoc0301	A CWE-119 Buffer Errors vulnerability exists in Modicon M580 CPU - BMEP582040, all versions before V2.90, and Modicon Ethernet Module BMENOC0301, all versions before V2.16, which could cause denial of service on the FTP service of the controller or the Ethernet BMENOC module when it receives a FTP CWD command with a data length greater than 1020 bytes. A power cycle is then needed to reactivate the FTP service.	2019-07-15	not yet calculated	CVE-2018-6838 MISC
shenzhen -- jisiwei_i3_robot_vacuum_cleaner	A vulnerability was found in the app 2.0 of the Shenzhen Jisiwei i3 robot vacuum cleaner. Actions performed on the app such as changing a password, and personal information it communicates with the server, use unencrypted HTTP. As an example, while logging in through the app to a Jisiwei account, the login request is being sent in plaintext. The vulnerability exists in both the Android and iOS version of the app. An attacker could exploit this by using an MITM attack on the local network to obtain someone's login credentials, which gives them full access to the robot vacuum cleaner.	2019-07-19	not yet calculated	CVE-2019-12820 MISC
shenzhen -- jisiwei_i3_robot_vacuum_cleaner	A vulnerability was found in the app 2.0 of the Shenzhen Jisiwei i3 robot vacuum cleaner, while adding a device to the account using a QR-code. The QR-code follows an easily predictable pattern that depends only on the specific device ID of he robot vacuum cleaner. By generating a QR-code containing information about the device ID, it is possible to connect an arbitrary device and gain full access to it. The device ID has an initial "JSW" substring followed by a six digit number that depends on the specific device.	2019-07-19	not yet calculated	CVE-2019-12821 MISC
slanger -- slanger	Slanger 0.6.0 is affected by: Remote Code Execution (RCE). The impact is: A remote attacker can execute arbitrary commands by sending a crafted request to the server. The component is: Message handler & request validator. The attack vector is: Remote unauthenticated. The fixed version is: after commit 5267b455caeb2e055cccf0d2b6a22727c11f5c3.	2019-07-15	not yet calculated	CVE-2019-1010306 MISC
sleuthkit -- sleuthkit	The Sleuth Kit 4.6.0 and earlier is affected by: Integer Overflow. The impact is: Opening crafted disk image triggers crash in sk/fs/hfs_dent.c:237. The component is: Overflow in fls tool used on HFS image. Bug is in tsk/fs/hfs.c file in function hfs_cat_traverse() in lines: 952, 1062. The attack vector is: Victim must open a crafted HFS filesystem image.	2019-07-18	not yet calculated	CVE-2019-1010065 MISC
snapview -- mikogo	The Windows versions of Snapview Mikogo, versions before 5.10.2 are affected by insecure implementations which allow ocal attackers to escalate privileges.	2019-07-12	not yet calculated	CVE-2019-12731 MISC
sourceforge -- timesheet_next_gen	Timesheet Next Gen 1.5.3 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Allows an attacker to execute arbitrary HTML and JavaScript code via a "redirect" parameter. The component is: Web login form: login.php, lines 40 and 54. The attack vector is: reflected XSS, victim may click the malicious url.	2019-07-17	not yet calculated	CVE-2019-1010287 MISC
sox -- sox	An issue was discovered in libsox.a in Sox 14.4.2. In sox-fmt.h (startread function), there is an integer overflow on the result of integer addition (wraparound to 0) fed into the lxx_callocc macro that wraps malloc. When a NULL pointer is returned, it is used without a prior check that it is a valid pointer, leading to a NULL pointer dereference on lxx_readbuf in formats_i.c.	2019-07-14	not yet calculated	CVE-2019-13590 MISC
synetics_gmbh -- i-doit	Synetics GmbH I-doit 1.12 and earlier is affected by: SQL Injection. The impact is: Unauthenticated mysql database access. The component is: Web login form. The attack vector is: An attacker can exploit the vulnerability by sending a malicious HTTP POST request. The fixed version is: 1.12.1.	2019-07-18	not yet calculated	CVE-2019-1010248 MISC
tenable -- comodo_antivirus	Comodo Antivirus versions 12.0.0.6810 and below are vulnerable to Denial of Service affecting CmdAgent.exe via an unprotected section object "<GUID>_CisSharedMemBuff". This section object is exposed by CmdAgent and contains a SharedMemoryDictionary object, which allows a low privileged process to modify the object data causing CmdAgent.exe to crash.	2019-07-17	not yet calculated	CVE-2019-3972 MISC
tenable -- comodo_antivirus	Comodo Antivirus versions 11.0.0.6582 and below are vulnerable to Denial of Service affecting CmdGuard.sys via its filter port "cmdServicePort". A low privileged process can crash CmdVirth.exe to decrease the port's connection count followed by process hollowing a CmdVirth.exe instance with malicious code to obtain a handle to "cmdServicePort". Once this occurs, a specially crafted message can be sent to "cmdServicePort" using "FilterSendMessage" API. This can trigger an out-of-bounds write if lpOutBuffer parameter in FilterSendMessage API is near the end of specified buffer bounds. The crash occurs when the driver performs a memset operation which uses a size beyond the size of buffer specified, causing kernel crash.	2019-07-17	not yet calculated	CVE-2019-3973 MISC
	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Local Privilege Escalation due to CmdAgent's handling of			CVE-2019-

tenable -- comodo_antivirus	COM clients. A local process can bypass the signature check enforced by CmdAgent via process hollowing which can then allow the process to invoke sensitive COM methods in CmdAgent such as writing to the registry with SYSTEM privileges.	2019-07-17	not yet calculated	<a href="#">3969 MISC</a>
tenable -- comodo_antivirus	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to a local Denial of Service affecting CmdVrth.exe via its LPC port "cmdvrtLPCServerPort". A low privileged local process can connect to this port and send an LPC_DATAGRAM, which triggers an Access Violation due to hardcoded NULLs used for Source parameter in a memcopy operation that is called for his handler. This results in CmdVrth.exe and its child svchost.exe instances to terminate.	2019-07-17	not yet calculated	<a href="#">CVE-2019-3971 MISC</a>
tenable -- comodo_antivirus	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Arbitrary File Write due to Cavwp.exe handling of Comodo's Antivirus database. Cavwp.exe loads Comodo antivirus definition database in unsecured global section objects, allowing a local low privileged process to modify this data directly and change virus signatures.	2019-07-17	not yet calculated	<a href="#">CVE-2019-3970 MISC</a>
tinymce -- tinymce	inymce 4.7.11, 4.7.12 is affected by: CWE-79: Improper Neutralization of Input During Web Page Generation. The impact is: JavaScript code execution. The component is: Media element. The attack vector is: The victim must paste malicious content to media element's embed tab.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010091 MISC</a>
tp-link -- archer_c1200	CMD_SET_CONFIG_COUNTRY in the TP-Link Device Debug protocol in TP-Link Archer C1200 1.0.0 Build 20180502 rel.45702 and earlier is prone to a stack-based buffer overflow, which allows a remote attacker to achieve code execution or denial of service by sending a crafted payload to the listening server.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13614 MISC</a>
tp-link -- wireless_router_archer_router	CMD_FTEST_CONFIG in the TP-Link Device Debug protocol in TP-Link Wireless Router Archer Router version 1.0.0 Build 20180502 rel.45702 (EU) and earlier is prone to a stack-based buffer overflow, which allows a remote attacker to achieve code execution or denial of service by sending a crafted payload to the listening server.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13613 MISC</a>
ulaunchelf_project -- ulaunchelf	uLaunchELF < commit 170827a is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Loader program (loader.c) overly trusts the arguments provided via command line.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010039 MISC</a>
univention -- univention_corporate_server	Univention Corporate Server univention-directory-notifier 12.0.1-3 and earlier is affected by: CWE-213: Intentional Information Exposure. The impact is: Loss of Confidentiality. The component is: function data_on_connection() in src/callback.c. The attack vector is: network connectivity. The fixed version is: 12.0.1-4 and later.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010283 MISC</a>
videolan -- vlc_media_player	avc_CopyPicture in modules/codecs/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height.	2019-07-18	not yet calculated	<a href="#">CVE-2019-13962 MISC MISC</a>
wordpress -- wordpress	TechyTalk Quick Chat WordPress Plugin All up to the latest is affected by: SQL Injection. The impact is: Access to the database. The component is: like_escape is used in Quick-chat.php line 399. The attack vector is: Crafted ajax request.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010104 MISC</a>
wordpress -- wordpress	A SQL injection vulnerability exists in the Icegram Email Subscribers & Newsletters plugin through 4.1.7 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13569 MISC</a>
wordpress -- wordpress	An issue was discovered in the wp-code-highlightjs plugin through 0.6.2 for WordPress. wp-admin/options-general.php?page=wp-code-highlight-js allows CSRF, as demonstrated by an XSS payload in the hljs_additional_css parameter.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12934 MISC MISC</a>
zeek -- zeek	n Zeek Network Security Monitor (formerly known as Bro) before 2.6.2, a NULL pointer dereference in the Kerberos (aka KRB) protocol parser leads to DoS because a case-type index is mishandled.	2019-07-17	not yet calculated	<a href="#">CVE-2019-12175 CONFIRM</a>
zeroshell -- zeroshell	Zeroshell 3.9.0 is prone to a remote command execution vulnerability. Specifically, this issue occurs because the web application mishandles a few HTTP parameters. An unauthenticated attacker can exploit this issue by injecting OS commands inside the vulnerable parameters.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12725 MISC MISC</a>
zipios_project -- zipios	Zipios before 0.1.7 does not properly handle certain malformed zip archives and can go into an infinite loop, causing a denial of service. This is related to zipheadio.h:readUInt32() and zipfile.cpp:Zipfile::Zipfile().	2019-07-17	not yet calculated	<a href="#">CVE-2019-13453 BID MISC CONFIRM</a>
zmartzone -- iam_auth_openidc	ZmartZone IAM mod_auth_openidc 2.3.10.1 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Redirecting the user to a phishing page or interacting with the application on behalf of the user. The component is: File: src/mod_auth_openidc.c, Line: 3109. The fixed version is: 2.3.10.2.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010247 MISC MISC MISC</a>
zzcms -- zzmcms	zzcms zzmcms 8.3 and earlier is affected by: File Delete to getshell. The impact is: getshell. The component is: user/ppsave.php.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010151 MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [us-cert.gov](#). If you need help or have questions, please send an email to [help@us-cert.gov](mailto:help@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add [US-CERT@nccss.us-cert.gov](mailto:US-CERT@nccss.us-cert.gov) to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)





From: [US-CERT](mailto:US-CERT@cissummyside.ca.us)  
To: [uscert@cissummyside.ca.us](mailto:uscert@cissummyside.ca.us)  
Subject: Vulnerability Summary for the Week of July 15 2019  
Date: Monday, July 22, 2019 2:32:44 PM

92

National Cyber Awareness System:

## Vulnerability Summary for the Week of July 15, 2019

07/22/2019 06 30 AM EDT

Original release date: July 22, 2019

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have a Command injection vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user.	2019-07-18	7.5	<a href="#">CVE-2019-7850</a> <a href="#">MISC</a>
archivesunleashed -- graphpass	borg-reducer c6d5240 is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Output parameter within the executable.	2019-07-15	7.5	<a href="#">CVE-2019-1010044</a> <a href="#">MISC</a>
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.836, a cwpsrv-xxx cookie allows a normal user to craft and upload a session file to the /tmp directory, and use it to become the root user.	2019-07-16	8.5	<a href="#">CVE-2019-13359</a> <a href="#">MISC</a> <a href="#">MISC</a>
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.836, remote attackers can bypass authentication in the login process by leveraging knowledge of a valid username.	2019-07-16	7.5	<a href="#">CVE-2019-13360</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fanucamerica -- robotics_virtual_robot_controller	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 has a Buffer Overflow via a forged HTTP request.	2019-07-17	7.5	<a href="#">CVE-2019-13585</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
foliovision -- fv_flowplayer_video_player	A SQL injection vulnerability exists in the FolioVision FV Flowplayer Video Player plugin before 7.3.19.727 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system.	2019-07-17	10.0	<a href="#">CVE-2019-13573</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gdnsd -- gdnsd	The set_ipv4() function in zscan_rfc1035.rl in gdnsd 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv4 address in zone data.	2019-07-18	7.5	<a href="#">CVE-2019-13951</a> <a href="#">MISC</a>
gdnsd -- gdnsd	The set_ipv6() function in zscan_rfc1035.rl in gdnsd before 2.4.3 and 3.x before 3.2.1 has a stack-based buffer overflow via a long and malformed IPv6 address in zone data.	2019-07-18	7.5	<a href="#">CVE-2019-13952</a> <a href="#">MISC</a>
getvera -- vera_edge_firmware	LuaUPnP in Vera Edge Home Controller 1.7.4452 allows remote unauthenticated users to execute arbitrary OS commands via the code parameter to /port_3480/data_request because the "No unsafe lua allowed" code block is skipped.	2019-07-14	10.0	<a href="#">CVE-2019-13598</a> <a href="#">MISC</a>
gnu -- glibc	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard.	2019-07-15	7.5	<a href="#">CVE-2019-1010022</a> <a href="#">MISC</a>
layerbb -- layerbb	LayerBB 1.1.3 allows admin/general.php arbitrary file upload because the custom_logo filename suffix is not restricted, and .php may be used.	2019-07-19	7.5	<a href="#">CVE-2019-13973</a> <a href="#">MISC</a>
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Boundary crossing. The impact is: Memory corruption of the TEE itself. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	7.5	<a href="#">CVE-2019-1010293</a> <a href="#">MISC</a>
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Memory corruption and disclosure of memory content. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	7.5	<a href="#">CVE-2019-1010295</a> <a href="#">MISC</a>
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Code execution in context of TEE core (kernel). The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	10.0	<a href="#">CVE-2019-1010296</a> <a href="#">MISC</a>
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Execution of code in TEE core (kernel) context. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	10.0	<a href="#">CVE-2019-1010297</a> <a href="#">MISC</a>
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Code execution in the context of TEE core (kernel). The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	10.0	<a href="#">CVE-2019-1010298</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1004, CVE-2019-1056, CVE-2019-1059.	2019-07-15	7.6	<a href="#">CVE-2019-1001</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1092, CVE-2019-1103, CVE-2019-1106, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1062</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1103, CVE-2019-1106, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1092</a> <a href="#">MISC</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1106, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1103</a> <a href="#">N/A</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1103, CVE-2019-1107.	2019-07-15	7.6	<a href="#">CVE-2019-1106</a> <a href="#">N/A</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1062, CVE-2019-1092, CVE-2019-1103, CVE-2019-1106.	2019-07-15	7.6	<a href="#">CVE-2019-1107</a> <a href="#">N/A</a>
microsoft -- edge	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'.	2019-07-15	7.6	<a href="#">CVE-2019-1104</a> <a href="#">N/A</a>
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1111.	2019-07-15	9.3	<a href="#">CVE-2019-1110</a> <a href="#">N/A</a>
microsoft -- excel	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1110.	2019-07-15	9.3	<a href="#">CVE-2019-1111</a> <a href="#">N/A</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1001, CVE-2019-1056, CVE-2019-1059.	2019-07-15	7.6	<a href="#">CVE-2019-1004</a> <a href="#">MISC</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1001, CVE-2019-1004, CVE-2019-1059.	2019-07-15	7.6	<a href="#">CVE-2019-1056</a> <a href="#">MISC</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1001, CVE-2019-1004, CVE-2019-1056.	2019-07-15	7.6	<a href="#">CVE-2019-1059</a> <a href="#">MISC</a>
microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	2019-07-15	7.6	<a href="#">CVE-2019-1063</a> <a href="#">MISC</a>
microsoft -- team_foundation_server	A remote code execution vulnerability exists when Azure DevOps Server and Team Foundation Server (TFS) improperly handle user input, aka 'Azure DevOps Server and Team Foundation Server Remote Code Execution Vulnerability'.	2019-07-15	7.5	<a href="#">CVE-2019-1072</a> <a href="#">MISC</a>
microsoft -- windows_10	A remote code execution vulnerability exists in Remote Desktop Services - formerly known as Terminal Services - when an authenticated attacker abuses clipboard redirection, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.	2019-07-15	8.5	<a href="#">CVE-2019-0887</a> <a href="#">MISC</a>

microsoft -- windows_10	An elevation of privilege vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-0999</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1067</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in Microsoft Windows where a certain DLL, with Local Service privilege, is vulnerable to race planting a customized DLL. An attacker who successfully exploited this vulnerability could potentially elevate privilege to SYSTEM. The update addresses this vulnerability by requiring SYSTEM privileges for a certain DLL., aka 'Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1074.	2019-07-15	7.2	<a href="#">CVE-2019-1082</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in rpcss.dll when the RPC service Activation Kernel improperly handles an RPC request. To exploit this vulnerability, a low level authenticated attacker could run a specially crafted application. The security update addresses this vulnerability by correcting how rpcss.dll handles these requests., aka 'Windows RPCSS Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1089</a> MISC MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the way that the dnssrvr.dll handles objects in memory, aka 'Windows dnssrvr.dll Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1090</a> MISC
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'.	2019-07-15	9.3	<a href="#">CVE-2019-1102</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1117</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1118</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1119</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1120</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1121</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1122</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1123</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1124</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1127</a> N/A
microsoft -- windows_10	A remote code execution vulnerability exists in the way that DirectWrite handles objects in memory, aka 'DirectWrite Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1117, CVE-2019-1118, CVE-2019-1119, CVE-2019-1120, CVE-2019-1121, CVE-2019-1122, CVE-2019-1123, CVE-2019-1124, CVE-2019-1127, CVE-2019-1128.	2019-07-15	9.3	<a href="#">CVE-2019-1128</a> N/A
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1130.	2019-07-15	7.2	<a href="#">CVE-2019-1129</a> N/A
microsoft -- windows_10	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1129.	2019-07-15	7.2	<a href="#">CVE-2019-1130</a> N/A
microsoft -- windows_7	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'.	2019-07-15	7.2	<a href="#">CVE-2019-1132</a> N/A
microsoft -- windows_server_2012	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP failover server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'.	2019-07-15	7.5	<a href="#">CVE-2019-0785</a> MISC
onosproject -- onos	In ONOS 1.15.0, apps/yang/web/src/main/java/org/onosproject/yang/web/YangWebResource.java mishandles backquote characters within strings that can be used in a shell command.	2019-07-16	10.0	<a href="#">CVE-2019-13624</a> MISC
rapid7 -- insight_agent	Rapid7 Insight Agent, version 2.6.3 and prior, suffers from a local privilege escalation due to an uncontrolled DLL search path. Specifically, when Insight Agent 2.6.3 and prior starts, the Python interpreter attempts to load python3.dll at "C:\DLLs\python3.dll," which normally is writable by locally authenticated users. Because of this, a malicious local user could use Insight Agent's startup conditions to elevate to SYSTEM privileges. This issue was fixed in Rapid7 Insight Agent 2.6.4.	2019-07-12	7.2	<a href="#">CVE-2019-5629</a> MISC FULLDISC MISC CONFIRM BUGTRAQ
realization -- concerto_critical_chain_planner	Realization Concerto Critical Chain Planner (aka CCPM) 5.10.8071 has SQL Injection in at least in the taskupdt/taskdetails.aspx webpage via the projectname parameter.	2019-07-12	7.5	<a href="#">CVE-2019-13027</a> MISC
saltstack -- salt_2018	SaltStack Salt 2018.3, 2019.2 is affected by: SQL Injection. The impact is: An attacker could escalate privileges on MySQL server deployed by cloud provider. It leads to RCE. The component is: The mysql.user_chpass function from the MySQL module for Salt (https://github.com/saltstack/salt/blob/develop/salt/modules/mysql.py#L1462). The attack vector is: specially crafted password string. The fixed version is: 2018.3.4.	2019-07-18	7.5	<a href="#">CVE-2019-1010259</a> MISC MISC MISC
schneider-electric -- proclima	A CWE-94: Code Injection vulnerability exists in ProClima (all versions prior to version 8.0.0) which could allow an unauthenticated, remote attacker to execute arbitrary code on the targeted system in all versions of ProClima prior to version 8.0.0.	2019-07-15	10.0	<a href="#">CVE-2019-6823</a> MISC
schneider-electric -- proclima	A CWE-119: Buffer Errors vulnerability exists in ProClima (all versions prior to version 8.0.0) which allows an unauthenticated, remote attacker to execute arbitrary code on the targeted system in all versions of ProClima prior to version 8.0.0.	2019-07-15	10.0	<a href="#">CVE-2019-6824</a> MISC
sertek -- xpare	An issue was discovered in Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could access the backend database via SQL injection.	2019-07-17	10.0	<a href="#">CVE-2019-13447</a> MISC
videolan -- vlc_media_player	VideoLAN VLC media player 3.0.7.1 has a heap-based buffer over-read in mkv::demux_sys_t::FreeUnused() in modules/demux/mkv/demux.cpp when called from mkv::Open in modules/demux/mkv/mkv.cpp.	2019-07-16	7.5	<a href="#">CVE-2019-13615</a> MISC
wpeverest -- everest_forms	A SQL injection vulnerability exists in WPEverest Everest Forms plugin for WordPress through 1.4.9. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system via includes/evf-entry-functions.php	2019-07-18	7.5	<a href="#">CVE-2019-13575</a> CONFIRM MISC MISC MISC
zohocorp -- manageengine_admanager_plus	Zoho ManageEngine ADManager Plus 6.6.5, ADSelfService Plus 5.7, and DesktopCentral 10.0.380 have Insecure Permissions, leading to Privilege Escalation from low level privileges to System.	2019-07-17	8.5	<a href="#">CVE-2019-12876</a> BID MISC

[Back to top](#)

## Medium Vulnerabilities

Primary	Description	Published	CVSS	Source & Patch Info
---------	-------------	-----------	------	---------------------

Vendor -- Product			Score	
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Insufficient input validation vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7843</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Improper error handling vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7846</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Improper Restriction of XML External Entity Reference (XXE) vulnerability. Successful exploitation could lead to Arbitrary read access to the file system in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7847</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Inadequate access control vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7848</a> MISC
adobe -- campaign	Adobe Campaign Classic version 18.10.5-8984 and earlier versions have an Information Exposure Through an Error Message vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	5.0	<a href="#">CVE-2019-7941</a> MISC
adobe -- dreamweaver	Adobe Dreamweaver direct download installer versions 19.0 and below, 18.0 and below have an Insecure Library Loading (DLL hijacking) vulnerability. Successful exploitation could lead to Privilege Escalation in the context of the current user.	2019-07-18	6.8	<a href="#">CVE-2019-7956</a> MISC
adobe -- experience_manager	Adobe Experience Manager version 6.4 and earlier have a Cross-Site Request Forgery vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user.	2019-07-18	4.3	<a href="#">CVE-2019-7953</a> MISC
adobe -- experience_manager	Adobe Experience Manager version 6.4 and earlier have a Reflected Cross-site Scripting vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user.	2019-07-18	5.8	<a href="#">CVE-2019-7955</a> MISC
altn -- mdaemon_webmail	MDaemon Webmail (formerly WorldClient) has CSRF.	2019-07-19	6.8	<a href="#">CVE-2018-17792</a> MISC MISC
apache -- roller	A Reflected Cross-site Scripting (XSS) vulnerability exists in Apache Roller. Roller's Math Comment Authenticator did not properly sanitize user input and could be exploited to perform Reflected Cross Site Scripting (XSS). The mitigation for this vulnerability is to upgrade to the latest version of Roller, which is now Roller 5.2.3.	2019-07-15	4.3	<a href="#">CVE-2019-0234</a> CONFIRM
automatic -- camptix_event_ticketing	The CampTix Event Ticketing plugin before 1.5 for WordPress allows CSV injection when the export tool is used.	2019-07-18	5.1	<a href="#">CVE-2016-10762</a> MISC MISC
axiosys -- bento4	In Bento4 1.5.1-627, AP4_DataBuffer::SetDataSize does not handle reallocation failures, leading to a memory copy into a NULL pointer. This is different from CVE-2018-20186.	2019-07-18	4.3	<a href="#">CVE-2019-13959</a> MISC
blackberry -- qnx_software_development_platform	An information disclosure vulnerability leading to a potential local escalation of privilege in the procs service (the /proc filesystem) of BlackBerry QNX Software Development Platform version(s) 6.5.0 SP1 and earlier could allow an attacker to potentially gain unauthorized access to a chosen process address space.	2019-07-12	4.6	<a href="#">CVE-2019-8998</a> MISC
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.846, the Login process allows attackers to check whether a username is valid by reading the HTTP response.	2019-07-16	5.0	<a href="#">CVE-2019-13383</a> MISC MISC
centos-webpanel -- centos_web_panel	In CentOS-WebPanel.com (aka CWP) CentOS Web Panel 0.9.8.838 to 0.9.8.846, remote attackers can bypass authentication in the login process by leveraging the knowledge of a valid username. The attacker must defeat an encoding that is not equivalent to base64, and thus this is different from CVE-2019-13360.	2019-07-16	6.5	<a href="#">CVE-2019-13605</a> MISC MISC MISC
crmsmadesimple -- bable:multilingual_site	Babel: Multilingual site Babel All is affected by: Open Redirection. The impact is: Redirection to any URL, which is supplied to redirect.php in a "newurl" parameter. The component is: redirect.php. The attack vector is: The victim must open a link created by an attacker. Attacker may use any legitimate site using Babel to redirect user to a URL of his/her choosing.	2019-07-16	5.8	<a href="#">CVE-2019-1010290</a> MISC MISC
deepsoft -- weblibrarian	Deepwoods Software WebLibrarian 3.5.2 and earlier is affected by: SQL Injection. The impact is: Exposing the entire database. The component is: Function "AllBarCodes" (defined at database_code.php line 1018) is vulnerable to a boolean-based blind sql injection. This function call can be triggered by any user logged-in with at least Volunteer role or manage_circulation capabilities. PoC : /wordpress/wp-admin/admin.php?page=weblib-circulation-desk&orderby=title&order=DESC.	2019-07-15	4.0	<a href="#">CVE-2019-1010034</a> MISC
digium -- asterisk	Buffer overflow in res_pjsip_messaging in Digium Asterisk versions 13.21-cert3, 13.27.0, 15.7.2, 16.4.0 and earlier allows remote authenticated users to crash Asterisk by sending a specially crafted SIP MESSAGE message.	2019-07-12	4.0	<a href="#">CVE-2019-12827</a> CONFIRM CONFIRM
dolbarr -- dolbarr	Dolbarr 6.0.4 is affected by: Cross Site Scripting (XSS). The impact is: Cookie stealing. The component is: htdocs/product/stats/card.php. The attack vector is: Victim must click a specially crafted link sent by the attacker.	2019-07-14	4.3	<a href="#">CVE-2019-1010016</a> MISC
dolbarr -- dolbarr	Dolbarr 7.0.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: allow malicious html to change user password, disable users and disable password encryption. The component is: Function User password change, user disable and password encryption. The attack vector is: admin access malicious urls.	2019-07-18	6.8	<a href="#">CVE-2019-1010054</a> MISC
domainmod -- domainmod	domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change admin password. The component is: http://127.0.0.1/settings/password/ http://127.0.0.1/admin/users/add.php http://127.0.0.1/admin/users/edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page.	2019-07-18	6.8	<a href="#">CVE-2019-1010094</a> MISC
domainmod -- domainmod	domainmod(https://domainmod.org/) domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can add the administrator account. The component is: http://127.0.0.1/admin/users/add.php. The attack vector is: After the administrator logged in, open the html page.	2019-07-18	6.8	<a href="#">CVE-2019-1010095</a> MISC
domainmod -- domainmod	domainmod(https://domainmod.org/) domainmod v4.10.0 is affected by: Cross Site Request Forgery (CSRF). The impact is: There is a CSRF vulnerability that can change the read-only user to admin. The component is: http://127.0.0.1/admin/users/edit.php?uid=2. The attack vector is: After the administrator logged in, open the html page.	2019-07-18	6.8	<a href="#">CVE-2019-1010096</a> MISC
eclipse -- openj9	AIX builds of Eclipse OpenJ9 before 0.15.0 contain unused RPATHs which may facilitate code injection and privilege elevation by local users.	2019-07-17	4.6	<a href="#">CVE-2019-11771</a> CONFIRM
fanucamerica -- robotics_virtual_robot_controller	The remote admin webserver on FANUC Robotics Virtual Robot Controller 8.23 allows Directory Traversal via a forged HTTP request.	2019-07-17	5.0	<a href="#">CVE-2019-13584</a> MISC BUGTRAQ
flatcore -- flatcore	A CSRF vulnerability was found in flatCore before 1.5, leading to the upload of arbitrary .php files via acp/core/files.upload-script.php.	2019-07-18	6.8	<a href="#">CVE-2019-13961</a> MISC MISC
gitea -- gitea	Gitea 1.7.0 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attacker is able to have victim execute arbitrary JS in browser. The component is: go-get URL generation - PR to fix: https://github.com/go-gitea/gitea/pull/5905. The attack vector is: victim must open a specifically crafted URL. The fixed version is: 1.7.1 and later.	2019-07-18	4.3	<a href="#">CVE-2019-1010261</a> MISC
gnome -- evince	Evince 3.26.0 is affected by buffer overflow. The impact is: DOS / Possible code execution. The component is: backend/tiff/tiff-document.c. The attack vector is: Victim must open a crafted PDF file. The issue occurs because of an incorrect integer overflow protection mechanism in tiff_document_render and tiff_document_get_thumbnail.	2019-07-14	6.8	<a href="#">CVE-2019-1010006</a> MISC MISC
gnu -- glibc	GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code.	2019-07-15	6.8	<a href="#">CVE-2019-1010023</a> BID MISC
gnu -- glibc	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc.	2019-07-15	5.0	<a href="#">CVE-2019-1010024</a> BID MISC
gnu -- glibc	GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc.	2019-07-15	5.0	<a href="#">CVE-2019-1010025</a> MISC
gpac -- gpac	In GPAC before 0.8.0, isomedia/isom_read.c in libgpac.a has a heap-based buffer over-read, as demonstrated by a crash in gf_m2ts_sync in media_tools/mpegts.c.	2019-07-16	5.0	<a href="#">CVE-2019-13618</a> MISC MISC
hexoeditor_project -- hexoeditor	HexoEditor v1.1.8-beta is affected by: XSS to code execution.	2019-07-14	4.3	<a href="#">CVE-2019-1010005</a> MISC MISC
ht2labs -- learning_locker	In HT2 Labs Learning Locker 3.15.1, it's possible to inject malicious HTML and JavaScript code into the DOM of the website via the PATH_INFO to the dashboards/ URI.	2019-07-16	4.3	<a href="#">CVE-2019-12834</a> MISC

http-file-server_project -- http-file-server	A path traversal vulnerability in <= v0.2.6 of http-file-server npm module allows attackers to list files in arbitrary folders.	2019-07-15	5.0	<a href="#">CVE-2019-5447</a> MISC
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3, 1.1.3.1, and 1.1.3.2 is missing function level access control that could allow a user to delete authorized resources. IBM X-Force ID: 159033.	2019-07-17	4.0	<a href="#">CVE-2019-4194</a> CONFIRM XF
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.6 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (../) to view arbitrary files on the system. IBM X-Force ID: 162887.	2019-07-17	5.0	<a href="#">CVE-2019-4430</a> XF CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155345.	2019-07-17	4.3	<a href="#">CVE-2018-2021</a> XF CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 155346.	2019-07-17	5.0	<a href="#">CVE-2018-2022</a> XF CONFIRM
jenkins -- jenkins	CSRF tokens in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier did not expire, thereby allowing attackers able to obtain them to bypass CSRF protection.	2019-07-17	5.1	<a href="#">CVE-2019-10353</a> MLIST MISC
jhead_project -- jhead	jhead 3.03 is affected by: Buffer Overflow. The impact is: Denial of service. The component is: gpsinfo.c Line 151 ProcessGpsInfo(). The attack vector is: Open a specially crafted JPEG file.	2019-07-15	4.3	<a href="#">CVE-2019-1010301</a> MISC
jhead_project -- jhead	jhead 3.03 is affected by: Incorrect Access Control. The impact is: Denial of service. The component is: iptc.c Line 122 show_IPTC(). The attack vector is: the victim must open a specially crafted JPEG file.	2019-07-15	4.3	<a href="#">CVE-2019-1010302</a> MISC
knot-resolver -- knot_resolver	A vulnerability was discovered in DNS resolver component of knot resolver through version 3.2.0 before 4.1.0 which allows remote attackers to bypass DNSSEC validation for non-existence answer. NXDOMAIN answer would get passed through to the client even if its DNSSEC validation failed, instead of sending a SERVFAIL packet. Caching is not affected by this particular bug but see CVE-2019-10191.	2019-07-16	5.0	<a href="#">CVE-2019-10190</a> CONFIRM FEDORA FEDORA CONFIRM
layerbb -- layerbb	LayerBB 1.1.3 allows XSS via the application/commands/new.php pm_title variable, a related issue to CVE-2019-17997.	2019-07-19	4.3	<a href="#">CVE-2019-13972</a> MISC
layerbb -- layerbb	LayerBB 1.1.3 allows conversations.php/cmd/new CSRF.	2019-07-19	6.8	<a href="#">CVE-2019-13974</a> MISC
libnmap -- libnmap	libnmap < v0.6.3 is affected by: XML Injection. The impact is: Denial of service (DoS) by consuming resources. The component is: XML Parsing. The attack vector is: Specially crafted XML payload.	2019-07-14	5.0	<a href="#">CVE-2019-1010017</a> MISC
libsdl -- libsdl	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in BlitNtoN in video/SDL_blit_N.c when called from SDL_SoftBlit in video/SDL_blit.c.	2019-07-16	6.8	<a href="#">CVE-2019-13616</a> MISC
linaro -- op-tee	Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Rounding error. The impact is: Potentially leaking code and/or data from previous Trusted Application. The component is: optee_os. The fixed version is: 3.4.0 and later.	2019-07-15	5.0	<a href="#">CVE-2019-1010294</a> MISC
iodash -- iodash	iodash prior to 4.17.11 is affected by: CWE-400: Uncontrolled Resource Consumption. The impact is: Denial of service. The component is: Date handler. The attack vector is: Attacker provides very long strings, which the library attempts to match using a regular expression. The fixed version is: 4.17.11.	2019-07-17	4.0	<a href="#">CVE-2019-1010266</a> MISC CONFIRM MISC
metinfo -- metinfo	Metinfo 6.x allows SQL Injection via the id parameter in an admin/index.php?n=ui_set&m=admin&c=index&a=doget_text_content&table=lang&field=1 request.	2019-07-19	6.5	<a href="#">CVE-2019-13969</a> MISC
microsoft -- .net_framework	An authentication bypass vulnerability exists in Windows Communication Foundation (WCF) and Windows Identity Foundation (WIF), allowing signing of SAML tokens with arbitrary symmetric keys, aka 'WCF/WIF SAML Token Authentication Bypass Vulnerability'.	2019-07-15	5.0	<a href="#">CVE-2019-1006</a> MISC
microsoft -- .net_framework	A denial of service vulnerability exists when Microsoft Common Object Runtime Library improperly handles web requests, aka '.NET Denial of Service Vulnerability'.	2019-07-15	5.0	<a href="#">CVE-2019-1083</a> MISC
microsoft -- .net_framework	A remote code execution vulnerability exists in .NET software when the software fails to check the source markup of a file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka '.NET Framework Remote Code Execution Vulnerability'.	2019-07-15	6.8	<a href="#">CVE-2019-1113</a> N/A
microsoft -- asp.net_core	A spoofing vulnerability exists in ASP.NET Core that could lead to an open redirect, aka 'ASP.NET Core Spoofing Vulnerability'.	2019-07-15	5.8	<a href="#">CVE-2019-1075</a> MISC
microsoft -- azure_automation	An elevation of privilege vulnerability exists in Azure Automation "RunAs account" runbooks for users with contributor role, aka 'Azure Automation Elevation of Privilege Vulnerability'.	2019-07-15	4.0	<a href="#">CVE-2019-0962</a> MISC
microsoft -- exchange_server	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'.	2019-07-15	5.1	<a href="#">CVE-2019-1136</a> N/A
microsoft -- office	A spoofing vulnerability exists when Microsoft Office Javascript does not check the validity of the web page making a request to Office documents. An attacker who successfully exploited this vulnerability could read or write information in Office documents. The security update addresses the vulnerability by correcting the way that Microsoft Office Javascript verifies trusted web pages., aka 'Microsoft Office Spoofing Vulnerability'.	2019-07-15	6.4	<a href="#">CVE-2019-1109</a> N/A
microsoft -- office	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'.	2019-07-15	4.3	<a href="#">CVE-2019-1112</a> N/A
microsoft -- sql_server	A remote code execution vulnerability exists in Microsoft SQL Server when it incorrectly handles processing of internal functions, aka 'Microsoft SQL Server Remote Code Execution Vulnerability'.	2019-07-15	6.5	<a href="#">CVE-2019-1068</a> MISC
microsoft -- visual_studio	An information disclosure vulnerability exists when Visual Studio improperly parses XML input in certain settings files, aka 'Visual Studio Information Disclosure Vulnerability'.	2019-07-15	4.3	<a href="#">CVE-2019-1079</a> MISC
microsoft -- visual_studio_2017	An elevation of privilege vulnerability exists when the Visual Studio updater service improperly handles file permissions, aka 'Visual Studio Elevation of Privilege Vulnerability'.	2019-07-15	6.6	<a href="#">CVE-2019-1077</a> MISC
microsoft -- windows_10	A local elevation of privilege vulnerability exists in how splwow64.exe handles certain calls, aka 'Microsoft splwow64 Elevation of Privilege Vulnerability'.	2019-07-15	4.6	<a href="#">CVE-2019-0880</a> MISC
microsoft -- windows_10	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'.	2019-07-15	5.5	<a href="#">CVE-2019-0966</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the way Windows Error Reporting (WER) handles files, aka 'Windows Error Reporting Elevation of Privilege Vulnerability'.	2019-07-15	6.9	<a href="#">CVE-2019-1037</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in the way that the wlanvc.dll handles objects in memory, aka 'Windows WLAN Service Elevation of Privilege Vulnerability'.	2019-07-15	4.6	<a href="#">CVE-2019-1085</a> MISC
microsoft -- windows_10	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1087, CVE-2019-1088.	2019-07-15	4.6	<a href="#">CVE-2019-1086</a> MISC
microsoft -- windows_10	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1086, CVE-2019-1088.	2019-07-15	4.6	<a href="#">CVE-2019-1087</a> MISC
microsoft -- windows_10	An elevation of privilege exists in Windows Audio Service, aka 'Windows Audio Service Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1086, CVE-2019-1087.	2019-07-15	4.6	<a href="#">CVE-2019-1088</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1094</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1095</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows RDP client improperly discloses the contents of its memory, aka 'Remote Desktop Protocol Client Information Disclosure Vulnerability'.	2019-07-15	4.0	<a href="#">CVE-2019-1108</a> N/A
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1098</a> N/A
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1100, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1099</a> N/A
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1101, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1100</a> N/A
	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the			



microsoft -- windows_7	contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1116.	2019-07-15	4.3	<a href="#">CVE-2019-1101</a> <a href="#">N/A</a>
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1094, CVE-2019-1095, CVE-2019-1098, CVE-2019-1099, CVE-2019-1100, CVE-2019-1101.	2019-07-15	4.3	<a href="#">CVE-2019-1116</a> <a href="#">N/A</a>
microsoft -- windows_server_2012	A denial of service vulnerability exists in Windows DNS Server when it fails to properly handle DNS queries, aka 'Windows DNS Server Denial of Service Vulnerability'.	2019-07-15	5.0	<a href="#">CVE-2019-0811</a> <a href="#">MISC</a>
microstrategy -- microstrategy_web	In MicroStrategy Web before 10.4.6, there is stored XSS in metric due to insufficient input validation.	2019-07-17	4.3	<a href="#">CVE-2019-12475</a> <a href="#">MISC</a>
mirumee -- saleor	In Mirumee Saleor 2.7.0 (fixed in 2.8.0), CSRF protection middleware was accidentally disabled, which allowed attackers to send a POST request without a valid CSRF token and be accepted by the server.	2019-07-14	6.8	<a href="#">CVE-2019-13594</a> <a href="#">MISC</a>
moinejf -- abcm2ps	moinejf abcm2ps 8.13.20 is affected by: Incorrect Access Control. The impact is: Allows attackers to cause a denial of service attack via a crafted file. The component is: front.c, function txt_add. The fixed version is: after commit commit 08aef597656d065e860753d53fda89765845eae.	2019-07-18	4.3	<a href="#">CVE-2019-1010069</a> <a href="#">MISC</a> <a href="#">MISC</a>
myt_project -- myt	In MyT 1.5.1, the User[username] parameter has XSS.	2019-07-17	4.3	<a href="#">CVE-2019-13346</a> <a href="#">EXPLOIT-DB</a>
netfilter -- iptables	A buffer overflow in iptables-restore in netfilter iptables 1.8.2 allows an attacker to (at least) crash the program or potentially gain code execution via a specially crafted iptables-save file. This is related to add_param_to_argv in xshared.c.	2019-07-12	4.3	<a href="#">CVE-2019-11360</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
nginx -- njs	njs through 0.3.3, used in NGINX, has a heap-based buffer over-read in nxt_vsprintf in ntxt/nxt_sprintf.c during error handling, as demonstrated by an njs_regex literal call that leads to an njs_parser_lexer_error call and then an njs_parser_scope_error call.	2019-07-16	4.3	<a href="#">CVE-2019-13617</a> <a href="#">MISC</a> <a href="#">MISC</a>
nsa -- ghidra	In NSA Ghidra through 9.0.4, path traversal can occur in RestoreTask.java (from the package ghidra.app.plugin.core.archive) via an archive with an executable file that has an initial ./ in its filename. This allows attackers to overwrite arbitrary files in scenarios where an intermediate analysis result is archived for sharing with other persons. To achieve arbitrary code execution, one approach is to overwrite some critical Ghidra modules, e.g., the decompile module.	2019-07-16	6.8	<a href="#">CVE-2019-13623</a> <a href="#">MISC</a> <a href="#">MISC</a>
ovidentia -- ovidentia	Ovidentia 8.4.3 has SQL injection via the id parameter in an index.php?tg=delegat&idx=mem request.	2019-07-19	6.5	<a href="#">CVE-2019-13978</a> <a href="#">MISC</a>
paloaltonetworks -- pan-os	Information disclosure in PAN-OS 7.1.23 and earlier, PAN-OS 8.0.18 and earlier, PAN-OS 8.1.8-h4 and earlier, and PAN-OS 9.0.2 and earlier may allow for an authenticated user with read-only privileges to extract the API key of the device and/or the username/password from the XML API (in PAN-OS) and possibly escalate privileges granted to them.	2019-07-16	6.5	<a href="#">CVE-2019-1575</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
paloaltonetworks -- pan-os	Command injection in PAN-OS 9.0.2 and earlier may allow an authenticated attacker to gain access to a remote shell in PAN-OS, and potentially run with the escalated user's permissions.	2019-07-16	6.5	<a href="#">CVE-2019-1576</a> <a href="#">CONFIRM</a>
python -- python	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.	2019-07-13	5.0	<a href="#">CVE-2018-20852</a> <a href="#">MISC</a> <a href="#">MISC</a>
rust-lang -- rust	The Rust Programming Language Standard Library 1.18.0 and later is affected by: CWE-200: Information Exposure. The impact is: Contents of uninitialized memory could be printed to string or to log file. The component is: Debug trait implementation for std::collections::Vec, deque::Iter. The attack vector is: The program needs to invoke debug printing for iterator over an empty VecDeque. The fixed version is: 1.30.0, nightly versions after commit b85e4cc8fdaab41da5b59645c08c68b8f9908d.	2019-07-15	5.0	<a href="#">CVE-2019-1010299</a> <a href="#">MISC</a> <a href="#">MISC</a>
schneider-electric -- interactive_graphical_scada_system	A CWE-787: Out-of-bounds Write vulnerability exists in Interactive Graphical SCADA System (IGSS), Version 14 and prior, which could cause a software crash when data in the mdb database is manipulated.	2019-07-15	6.8	<a href="#">CVE-2019-6827</a> <a href="#">MISC</a>
schneider-electric -- proclima	A CWE-427: Uncontrolled Search Path Element vulnerability exists in ProClima (all versions prior to version 8.0.0) which could allow a malicious DLL file, with the same name of any resident DLLs inside the software installation, to execute arbitrary code in all versions of ProClima prior to version 8.0.0.	2019-07-15	6.8	<a href="#">CVE-2019-6825</a> <a href="#">MISC</a>
schneider-electric -- zelio_soft_2	A Use After Free: CWE-416 vulnerability exists in Zelio Soft 2, V5.2 and earlier, which could cause remote code execution when opening a specially crafted Zelio Soft 2 project file.	2019-07-15	6.8	<a href="#">CVE-2019-6822</a> <a href="#">MISC</a>
school_college_portal_with_erp_script_project -- school_college_portal_with_erp_script	phpscripts.small School College Portal with ERP Script 2.6.1 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Attack administrators and teachers, students and more. The component is: /pro-school/index.php?student/message/send_reply/. The attack vector is: <img src=x onerror=alert(document.domain) />.	2019-07-15	4.3	<a href="#">CVE-2019-1010028</a> <a href="#">MISC</a>
sertek -- xpare	An issue was discovered in Sertek Xpare 3.67. The login form does not sanitize input data. Because of this, a malicious agent could exploit the vulnerable function in order to prepare an XSS payload to send to the product's clients.	2019-07-17	4.3	<a href="#">CVE-2019-13448</a> <a href="#">MISC</a>
solarwinds -- network_performance_monitor	SolarWinds Network Performance Monitor 12.3 allows SQL Injection via the /api/ActiveAlertsOnThisEntity/GetActiveAlerts TriggeringObjectEntityNames parameter.	2019-07-16	6.5	<a href="#">CVE-2018-13442</a> <a href="#">MISC</a>
soundexchange -- sound_exchange	SoX - Sound eXchange 14.4.2 and earlier is affected by: Out-of-bounds Read. The impact is: Denial of Service. The component is: read_samples function at xa.c:219. The attack vector is: Victim must open specially crafted .xa file. NOTE: this may overlap CVE-2017-18189.	2019-07-14	4.3	<a href="#">CVE-2019-1010004</a> <a href="#">MISC</a> <a href="#">MISC</a>
syguestbook_a5_project -- syguestbook_a5	SyGuestBook A5 Version 1.2 has no CSRF protection mechanism, as demonstrated by CSRF for an index.php?c=Administrator&a=update admin password change.	2019-07-18	6.8	<a href="#">CVE-2019-13949</a> <a href="#">MISC</a> <a href="#">MISC</a>
temenos -- cwx	Temenos CWX version 8.9 has an Broken Access Control vulnerability in the module /CWX/Employee/EmployeeEdit2.aspx, leading to the viewing of user information.	2019-07-17	5.0	<a href="#">CVE-2019-13403</a> <a href="#">MISC</a>
videolan -- vlc_media_player	An Integer Underflow in MP4_EIA608_Convert() in modules/demux/mp4/mp4.c in VideoLAN VLC media player through 3.0.7.1 allows remote attackers to cause a denial of service (heap-based buffer overflow and crash) or possibly have unspecified other impact via a crafted .mp4 file.	2019-07-14	6.8	<a href="#">CVE-2019-13602</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
wireshark -- wireshark	In Wireshark 3.0.0 to 3.0.2, 2.6.0 to 2.6.9, and 2.4.0 to 2.4.15, the ASN.1 BER dissector and related dissectors could crash. This was addressed in epan/asn1.c by properly restricting buffer increments.	2019-07-17	5.0	<a href="#">CVE-2019-13619</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zammad -- zammad	Zammad GmbH Zammad 2.3.0 and earlier is affected by: Cross Site Scripting (XSS) - CWE-80. The impact is: Execute javascript code on users browser. The component is: web app. The attack vector is: the victim must open a ticket. The fixed version is: 2.3.1, 2.2.2 and 2.1.3.	2019-07-16	4.3	<a href="#">CVE-2019-1010018</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
automatic -- campitx_event_ticketing	The CampTix Event Ticketing plugin before 1.5 for WordPress allows XSS in the admin section via a ticket title or body.	2019-07-18	3.5	<a href="#">CVE-2016-10763</a> <a href="#">MISC</a> <a href="#">MISC</a>
firefly-iii -- firefly_iii	Firefly III before 4.7.17.1 is vulnerable to stored XSS due to lack of filtration of user-supplied data in a budget name. The JavaScript code is contained in a transaction, and is executed on the tags/show/\$tag_number\$ tag summary page.	2019-07-17	3.5	<a href="#">CVE-2019-13644</a> <a href="#">MISC</a> <a href="#">MISC</a>
firefly-iii -- firefly_iii	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user-supplied data in image file names. The JavaScript code is executed during attachments/edit/\$file_id\$ attachment editing.	2019-07-17	3.5	<a href="#">CVE-2019-13645</a> <a href="#">MISC</a> <a href="#">MISC</a>
firefly-iii -- firefly_iii	Firefly III before 4.7.17.3 is vulnerable to reflected XSS due to lack of filtration of user-supplied data in a search query.	2019-07-17	3.5	<a href="#">CVE-2019-13646</a> <a href="#">MISC</a> <a href="#">MISC</a>
firefly-iii -- firefly_iii	Firefly III before 4.7.17.3 is vulnerable to stored XSS due to lack of filtration of user-supplied data in image file content. The JavaScript code is executed during attachments/view/\$file_id\$ attachment viewing.	2019-07-17	3.5	<a href="#">CVE-2019-13647</a> <a href="#">MISC</a> <a href="#">MISC</a>



glpi-project -- glpi	GLPI GLPI Product 9.3.1 is affected by: Cross Site Scripting (XSS). The impact is: All dropdown values are vulnerable to XSS leading to privilege escalation and executing js on admin. The component is: /glpi/ajax/getDropDownValue.php. The attack vector is: 1- User Create a ticket , 2- Admin opens another ticket and click on the "Link Tickets" feature, 3- a request to the endpoint fetches js and executes it.	2019-07-15	3.5	<a href="#">CVE-2019-1010307</a> MISC MISC
glpi-project -- glpi	GLPI GLPI Product 9.3.1 is affected by: Frame and Form tags Injection allowing admins to phish users by putting code in reminder description. The impact is: Admins can phish any user or group of users for credentials / credit cards. The component is: Tools > Reminder > Description .. Set the description to any iframe/form tags and apply. The attack vector is: The attacker puts a login form, the user fills it and clicks on submit .. the request is sent to the attacker domain saving the data. The fixed version is: 9.4.1.	2019-07-12	3.5	<a href="#">CVE-2019-1010310</a> MISC MISC
ibm -- campaign	IBM Campaign 9.1.0, 9.1.2, 10.1, and 11.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152857.	2019-07-17	3.5	<a href="#">CVE-2018-1921</a> XF CONFIRM
ibm -- radar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 could allow a local user to obtain sensitive information when exporting content that could aid an attacker in further attacks against the system. IBM X-Force ID: 156563.	2019-07-17	2.1	<a href="#">CVE-2019-4054</a> XF CONFIRM
ibm -- radar_security_information_and_event_manager	IBM QRadar SIEM 7.2 and 7.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159131.	2019-07-17	3.5	<a href="#">CVE-2019-4211</a> XF CONFIRM
microsoft -- exchange_server	A cross-site-scripting (XSS) vulnerability exists when Microsoft Exchange Server does not properly sanitize a specially crafted web request to an affected Exchange server, aka 'Microsoft Exchange Server Spoofing Vulnerability'.	2019-07-15	3.5	<a href="#">CVE-2019-1137</a> N/A
microsoft -- sharepoint_enterprise_server	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'.	2019-07-15	3.5	<a href="#">CVE-2019-1134</a> N/A
microsoft -- team_foundation_server	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting Vulnerability'.	2019-07-15	3.5	<a href="#">CVE-2019-1076</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1073.	2019-07-15	2.1	<a href="#">CVE-2019-1071</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071.	2019-07-15	2.1	<a href="#">CVE-2019-1073</a> MISC
microsoft -- windows_10	An elevation of privilege vulnerability exists in Microsoft Windows where certain folders, with local service privilege, are vulnerable to symbolic link attack. An attacker who successfully exploited this vulnerability could potentially access unauthorized information. The update addresses this vulnerability by not allowing symbolic links in these scenarios, aka Microsoft Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-1082.	2019-07-15	2.1	<a href="#">CVE-2019-1074</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when Unistore.dll fails to properly handle objects in memory, aka 'Microsoft unistore.dll Information Disclosure Vulnerability'.	2019-07-15	2.1	<a href="#">CVE-2019-1091</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1097.	2019-07-15	2.1	<a href="#">CVE-2019-1093</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	2019-07-15	2.1	<a href="#">CVE-2019-1096</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory, aka 'DirectWrite Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1093.	2019-07-15	2.1	<a href="#">CVE-2019-1097</a> MISC
norton -- password_manager	Norton Password Manager, prior to 6.3.0.2082, may be susceptible to an address spoofing issue. This type of issue may allow an attacker to disguise their origin IP address in order to obfuscate the source of network traffic.	2019-07-16	1.7	<a href="#">CVE-2019-9700</a> CONFIRM
openenergymonitor -- emoncms	OpenEnergyMonitor Project Emoncms 9.8.8 is affected by: Cross Site Scripting (XSS). The impact is: Theoretically low, but might potentially enable persistent XSS (user could embed mal. code). The component is: Javascript code execution in "Name", "Location", "Bio" and "Starting Page" fields in the "My Account" page. File: Lib/!stjs/list.js, line 67. The attack vector is: unknown, victim must open profile page if persistent was possible.	2019-07-14	3.5	<a href="#">CVE-2019-1010008</a> MISC
ovidentia -- ovidentia	index.php in Ovidentia 8.4.3 has XSS via tg=groups, tg=maildoms&idx=create&userid=0&bgrp=y, tg=delegat, tg=site&idx=create, tg=site&item=4, tg=admdir&idx=mbd&id=1, tg=notes&idx=Create, tg=admfqs&idx=Add, or tg=admoc&idx=addoc&item=.	2019-07-19	3.5	<a href="#">CVE-2019-13977</a> MISC
rdbrck -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	2.1	<a href="#">CVE-2019-12912</a> CONFIRM
rdbrck -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	2.1	<a href="#">CVE-2019-12913</a> CONFIRM
sitecore -- experience_platform	In Sitecore 9.0 rev 171002, Persistent XSS exists in the Media Library and File Manager. An authenticated unprivileged user can modify the uploaded file extension parameter to inject arbitrary JavaScript.	2019-07-17	3.5	<a href="#">CVE-2019-13493</a> MISC
syguestbook_a5_project -- syguestbook_a5	SyGuestBook A5 Version 1.2 allows stored XSS because the isValidData function in include/functions.php does not properly block XSS payloads, as demonstrated by a crafted use of the onerror attribute of an IMG element.	2019-07-18	3.5	<a href="#">CVE-2019-13948</a> MISC MISC
syguestbook_a5_project -- syguestbook_a5	index.php?c=admin&a=index in SyGuestBook A5 Version 1.2 has stored XSS via a reply to a comment.	2019-07-18	3.5	<a href="#">CVE-2019-13950</a> MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- bridge_cc	Adobe Bridge CC version 9.0.2 and earlier versions have an out of bound read vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.	2019-07-18	not yet calculated	<a href="#">CVE-2019-7963</a> MISC
adobe -- experience_manager	Adobe Experience Manager version 6.4 and earlier have a Stored Cross-site Scripting vulnerability. Successful exploitation could lead to Sensitive Information disclosure in the context of the current user.	2019-07-18	not yet calculated	<a href="#">CVE-2019-7954</a> MISC
akeo_consulting -- rufus	Akeo Consulting Rufus 3.0 and earlier is affected by: Insecure Permissions. The impact is: arbitrary code execution with escalation of privilege. The component is: Executable installer, portable executable (ALL executables available). The attack vector is: CWE-29, CWE-377, CWE-379.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010101</a> MISC
akeo_consulting -- rufus	Akeo Consulting Rufus 3.0 and earlier is affected by: DLL search order hijacking. The impact is: Arbitrary code execution WITH escalation of privilege. The component is: Executable installers, portable executables (ALL executables on the web site). The attack vector is: CAPEC-471, CWE-426, CWE-427.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010100</a> MISC
antword_project -- antword	n antSword before 2.1.0, self-XSS in the database configuration leads to code execution via modules/database/asp/index.js, modules/database/custom/index.js, modules/database/index.js, or modules/database/php/index.js.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13970</a> MISC MISC MISC
aquaverde -- aquarius_cms	Aquaverde GmbH Aquarius CMS prior to version 4.1.1 is affected by: Incorrect Access Control. The impact is: The access o the log file is not restricted. It contains sensitive information like passwords etc. The component is: log file. The attack vector is: open the file.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010308</a> MISC MISC
arduino -- arduino	Embedded systems based on Arduino before Rev3 allow remote attackers to send data to LEDs (directly connected to GPIO pins) via a laser, because of LED photosensitivity.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13991</a> MISC
audiocodes -- multiple_mediant_devices	An issue was discovered on AudioCodes Mediant 500L-MSBR, 500-MBSR, M800B-MSBR and 800C-MSBR devices with firmware versions F7.20A to F7.20A.251. An internal interface exposed to the link-local address 169.254.254.253 allows attackers in the local network to access multiple quagga VTYS. Attackers can authenticate with the default 1234 password hat cannot be changed, and can execute malicious and unauthorized actions.	2019-07-19	not yet calculated	<a href="#">CVE-2019-9229</a> MISC
audiocodes -- multiple_mediant_devices	An issue was discovered on AudioCodes Mediant 500L-MSBR, 500-MBSR, M800B-MSBR and 800C-MSBR devices with firmware versions F7.20A to F7.20A.253. A cross-site scripting (XSS) vulnerability in the search function of the management web interface allows remote attackers to inject arbitrary web script or HTML via the keyword parameter.	2019-07-18	not yet calculated	<a href="#">CVE-2019-9230</a> MISC

audiocodes -- multiple_mediant_devices	An issue was discovered on AudioCodes Mediant 500L-MSBR, 500-MBSR, M800B-MSBR and 800C-MSBR devices with firmware versions before 7.20A.202.307. A Cross-Site Request Forgery (CSRF) vulnerability in the management web interface allows remote attackers to execute malicious and unauthorized actions, because CSRFProtection=1 is not a default and is not documented.	2019-07-18	not yet calculated	<a href="#">CVE-2019-3231</a> MISC
avast -- antivirus	n Avast Antivirus before 19.4, a local administrator can trick the product into renaming arbitrary files by replacing the Logs/Update.log file with a symlink. The next time the product attempts to write to the log file, the target of the symlink is renamed. This defect can be exploited to rename a critical product file (e.g., AvastSvc.exe), causing the product to fail to start on the next system restart.	2019-07-18	not yet calculated	<a href="#">CVE-2019-11230</a> MISC
b3log -- wide	b3log Wide before 1.6.0 allows three types of attacks to access arbitrary files. First, the attacker can write code in the editor, and compile and run it approximately three times to read an arbitrary file. Second, the attacker can create a symlink, and then place the symlink into a ZIP archive. An unzip operation leads to read access, and write access (depending on file permissions), to the symlink target. Third, the attacker can import a Git repository that contains a symlink, similarly leading to read and write access.	2019-07-18	not yet calculated	<a href="#">CVE-2019-13915</a> MISC
bacnet -- stack_bacserv	BACnet Stack bacserv 0.9.1 and 0.8.5 is affected by: Buffer Overflow. The impact is: exploit was not explored. The component is: bacserv BVLC forwarded NPDU. bvlc_bdt_forward_n pdu() calls bvlc_encode_forwarded_n pdu() which copies the content from the request into a local in the bvlc_bdt_forward_n pdu() stack frame and clobbers the canary. The attack vector is: A BACnet/IP device with BBMD enabled based on this library connected to IP network. The fixed version is: 0.8.6.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010073</a> MISC
chinamobile -- plc_wireless_router_gpn2.4p21-c-cn	ChinaMobile GPN2.4P21-C-CN W2001EN-00 is affected by: Incorrect Access Control - Unauthenticated Remote Reboot. The impact is: PLC Wireless Router's are vulnerable to an unauthenticated remote reboot due. The component is: Reboot settings are available to unauthenticated users instead of only authenticated users. The attack vector is: Remote.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010136</a> EXPLOIT-DB MISC
cisco -- findit_network_manager_and_findit_network_probe_release	A vulnerability in the Cisco FindIT Network Management Software virtual machine (VM) images could allow an unauthenticated, local attacker who has access to the VM console to log in to the device with a static account that has root privileges. The vulnerability is due to the presence of an account with static credentials in the underlying Linux operating system. An attacker could exploit this vulnerability by logging in to the command line of the affected VM with the static account. A successful exploit could allow the attacker to log in with root-level privileges. This vulnerability affects only Cisco FindIT Network Manager and Cisco FindIT Network Probe Release 1.1.4 if these products are using Cisco-supplied VM images. No other releases or deployment models are known to be vulnerable.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1919</a> BID CISCO
cisco -- identity_services_engine	A vulnerability in the sponsor portal web interface for Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. At the time of publication, this vulnerability affected Cisco ISE running software releases 2.6.0 and prior.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1942</a> BID CISCO
cisco -- identity_services_engine	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. At the time of publication, this vulnerability affected Cisco ISE running software releases prior to 2.4.0 Patch 9 and 2.6.0.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1941</a> BID CISCO
cisco -- industrial_network_director	A vulnerability in the Web Services Management Agent (WSMA) feature of Cisco Industrial Network Director (IND) could allow an unauthenticated, remote attacker to gain unauthorized read access to sensitive data using an invalid X.509 certificate. The vulnerability is due to insufficient X.509 certificate validation when establishing a WSMA connection. An attacker could exploit this vulnerability by supplying a crafted X.509 certificate during the WSMA connection setup phase. A successful exploit could allow the attacker to conduct man-in-the-middle attacks to decrypt confidential information on WSMA connections to the affected software. At the time of publication, this vulnerability affected Cisco IND Software releases prior to 1.7.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1940</a> BID CISCO
cisco -- ios_access_points_software	A vulnerability in the 802.11r Fast Transition (FT) implementation for Cisco IOS Access Points (APs) Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected interface. The vulnerability is due to a lack of complete error handling condition for client authentication requests sent to a targeted interface configured for FT. An attacker could exploit this vulnerability by sending crafted authentication request traffic to the targeted interface, causing the device to restart unexpectedly.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1920</a> CISCO
cisco -- small_business_200_and_300_and_500_series_switches	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Switches software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. The vulnerability is due to improper input validation of the parameters of an HTTP request. An attacker could exploit this vulnerability by intercepting a user's HTTP request and modifying it into a request that causes the web interface to redirect the user to a specific malicious URL. This type of vulnerability is known as an open redirect attack and is used in phishing attacks that get users to unknowingly visit malicious sites.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1943</a> BID CISCO
cisco -- small_business_spa500_series_ip_phones	A vulnerability in Cisco Small Business SPA500 Series IP Phones could allow a physically proximate attacker to execute arbitrary commands on the device. The vulnerability is due to improper input validation in the device configuration interface. An attacker could exploit this vulnerability by accessing the configuration interface, which may require a password, and then accessing the device's physical interface and inserting a USB storage device. A successful exploit could allow the attacker to execute arbitrary commands on the device in an elevated security context. At the time of publication, this vulnerability affected Cisco Small Business SPA500 Series IP Phones firmware releases 7.6.2SR5 and prior.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1923</a> BID CISCO
cisco -- vision_dynamic_signage_director	A vulnerability in the REST API interface of Cisco Vision Dynamic Signage Director could allow an unauthenticated, remote attacker to bypass authentication on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to execute arbitrary actions through the REST API with administrative privileges on the affected system. The REST API is enabled by default and cannot be disabled.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1917</a> BID CISCO
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 allow SQL Injection.	2019-07-16	not yet calculated	<a href="#">CVE-2019-12989</a> MISC BID MISC MISC
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 3 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12987</a> BID MISC MISC
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 4 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12988</a> BID MISC MISC
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 6 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12992</a> BID MISC MISC
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 allow Directory Traversal.	2019-07-16	not yet calculated	<a href="#">CVE-2019-12990</a> BID MISC MISC
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 5 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12991</a> MISC BID MISC MISC
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 2 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12986</a> BID MISC MISC
citrix -- sd-wan_and_netscaler_sd-wan	Citrix SD-WAN 10.2.x before 10.2.3 and NetScaler SD-WAN 10.0.x before 10.0.8 have Improper Input Validation (issue 1 of 6).	2019-07-16	not yet calculated	<a href="#">CVE-2019-12985</a> BID MISC MISC

cjson -- cjson	DaveGamble/cJSON cJSON 1.7.8 is affected by: Improper Check for Unusual or Exceptional Conditions. The impact is: Null dereference, so attack can cause denial of service. The component is: cJSON_GetObjectItemCaseSensitive() function. The attack vector is: crafted json file. The fixed version is: 1.7.9 and later.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010239</a> MISC
cloud_foundry -- uua	Cloud Foundry UAA, versions prior to v73.4.0, does not set an X-FRAME-OPTIONS header on various endpoints. A remote user can perform clickjacking attacks on UAA's frontend sites.	2019-07-18	not yet calculated	<a href="#">CVE-2019-8794</a> CONFIRM
code42 -- code42_enterprise_and_crashplan_for_small_business	Code42 Enterprise and Crashplan for Small Business Client version 6.7 before 6.7.5, 6.8 before 6.8.8, and 6.9 before 6.9.4 allows eval injection. A proxy auto-configuration file, crafted by a lesser privileged user, may be used to execute arbitrary code at a higher privilege as the service user.	2019-07-19	not yet calculated	<a href="#">CVE-2019-11552</a> MISC CONFIRM
code42 -- code42_for_enterprise	Code42 for Enterprise through 6.8.4 has Incorrect Access Control.	2019-07-19	not yet calculated	<a href="#">CVE-2019-11553</a> CONFIRM
cohesity -- dataplatform	A man-in-the-middle vulnerability related to vCenter access was found in Cohesity DataPlatform version 5.x and 6.x prior to 6.1.1c. Cohesity clusters did not verify TLS certificates presented by vCenter. This vulnerability could expose Cohesity user credentials configured to access vCenter.	2019-07-12	not yet calculated	<a href="#">CVE-2019-11242</a> CONFIRM
computerlab -- maple_wbt_snmp_administrator	SnmpAdm.exe in MAPLE WBT SNMP Administrator v2.0.195.15 has an Unauthenticated Remote Buffer Overflow via a ong string to the CE Remote feature listening on Port 987.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13577</a> MISC MISC FULLDISC BUGTRAQ
dancer-plugin-simplecrud -- dancer-plugin-simplecrud	Dancer::Plugin::SimpleCRUD 1.14 and earlier is affected by: Incorrect Access Control. The impact is: Potential for unauthorised access to data. The component is: Incorrect calls to _ensure_auth() wrapper result in authentication-checking not being applied to al routes.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010084</a> MISC
dell_emc -- unity_and_unityvsa	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain a plain-text password storage vulnerability. A Unisphere user's (including the admin privilege user) password is stored in a plain text in Unity Data Collection bundle logs files for troubleshooting). A local authenticated attacker with access to the Data Collection bundle may use the exposed password to gain access with the privileges of the compromised user.	2019-07-18	not yet calculated	<a href="#">CVE-2019-3741</a> MISC
dell_emc -- unity_and_unityvsa	Dell EMC Unity and UnityVSA versions prior to 5.0.0.0.5.116 contain an improper authorization vulnerability in NAS Server quotas configuration. A remote authenticated Unisphere Operator could potentially exploit this vulnerability to edit quota configuration of other users.	2019-07-18	not yet calculated	<a href="#">CVE-2019-3734</a> MISC
dglogik_inc -- dglux_server	DGLogik Inc DGLux Server All Versions is affected by: Insecure Permissions. The impact is: Remote Execution, Credential Leaks. The component is: IoT API. The attack vector is: Any Accessible Server.	2019-07-14	not yet calculated	<a href="#">CVE-2019-1010009</a> MISC
discuzml -- discuzml	Discuz!ML 3.2 through 3.4 allows remote attackers to execute arbitrary PHP code via a modified language cookie, as demonstrated by changing 4gH4_OdF5_language=en to 4gH4_OdF5_language=en'.phpinfo('; (if the random prefix 4gH4_OdF5_were used).	2019-07-18	not yet calculated	<a href="#">CVE-2019-13956</a> MISC
docker -- docker_ce_and_docker_ee	n Docker CE and EE before 18.09.8 (as well as Docker EE before 17.06.2-ee-23 and 18.x before 18.03.1-ee-10), Docker Engine in debug mode may sometimes add secrets to the debug log. This applies to a scenario where docker stack deploy s run to redeploy a stack that includes (non external) secrets. It potentially applies to other API users of the stack API if hey resend the secret.	2019-07-18	not yet calculated	<a href="#">CVE-2019-13509</a> MISC
dpic -- dpic	dpic 2019.06.20 has a Stack-based Buffer Overflow in the wfloat() function in main.c.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13989</a> MISC
eclipse -- openj9	n Eclipse OpenJ9 prior to 0.15, the String.getBytes(int, int, byte[], int) method does not verify that the provided byte array is non-null nor that the provided index is in bounds when compiled by the JIT. This allows arbitrary writes to any 32-bit address or beyond the end of a byte array within Java code run under a SecurityManager.	2019-07-17	not yet calculated	<a href="#">CVE-2019-11772</a> CONFIRM
elcom -- elcom_cms	Elcom CMS before 10.7 has SQL Injection via EventSearchByState.aspx and EventSearchAdv.aspx.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12946</a> MISC
epsocrm -- epsocrm	Stored XSS in EspoCRM before 5.6.4 allows remote attackers to execute malicious JavaScript and inject arbitrary source code into the target pages. The attack begins by storing a new stream message containing an XSS payload. The stored payload can then be triggered by clicking a malicious link on the Notifications page.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13643</a> MISC MISC
facebook -- hhvm	Call to the script_enc() function in HHVM can lead to heap corruption by using specifically crafted parameters (N, r and p). This happens if the parameters are configurable by an attacker for instance by providing the output of script_enc() in a context where Hack/PHP code would attempt to verify it by re-running script_enc() with the same parameters. This could result in information disclosure, memory being overwritten or crashes of the HHVM process. This issue affects versions 4.3.0, 4.4.0, 4.5.0, 4.6.0, 4.7.0, 4.8.0, versions 3.30.5 and below, and all versions in the 4.0, 4.1, and 4.2 series.	2019-07-18	not yet calculated	<a href="#">CVE-2019-3570</a> CONFIRM CONFIRM
facebook -- whatsapp_desktop	An input validation issue affected WhatsApp Desktop versions prior to 0.3.3793 which allows malicious clients to send files o users that would be displayed with a wrong extension.	2019-07-16	not yet calculated	<a href="#">CVE-2019-3571</a> CONFIRM
fitbit -- multiple_products	On Fitbit activity-tracker devices, certain addresses never change. According to the popets-2019-0036.pdf document, this leads to "permanent trackability" and "considerable privacy concerns" without a user-accessible anonymization feature. The devices, such as Charge 2, transmit Bluetooth Low Energy (BLE) advertising packets with a TxAdd flag indicating random addresses, but the addresses remain constant. If devices come within BLE range at one or more locations where an adversary has set up passive sniffing, the adversary can determine whether the same device has entered one of these oations.	2019-07-15	not yet calculated	<a href="#">CVE-2014-10374</a> MISC MISC
gnome -- pango	Gnome Pango 1.42 and later is affected by: Buffer Overflow. The impact is: The heap based buffer overflow can be used to get code execution. The component is: function name: pango_log2vis_get_embedding_levels, assignment of nchars and he loop condition. The attack vector is: Bug can be used when application pass invalid utf-8 strings to functions like pango_itemize.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010238</a> MISC
gnu -- patch	n GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13636</a> MISC MLIST
h3c -- h3cloud	H3C H3Cloud OS all versions allows SQL injection via the ear/grid_event sidx parameter.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12193</a> MISC
helm -- helm	helm Before 2.7.2 is affected by: CWE-295: Improper Certificate Validation. The impact is: Unauthorized clients could connect to the server because self-signed client certs were allowed. The component is: helm (many files updated, see https://github.com/helm/helm/pull/3152/files/1096813bf9a425e2aa4ac755b6c991b626dfab50). The attack vector is: A malicious client could connect to the server over the network. The fixed version is: 2.7.2.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010275</a> MISC MISC MISC
hid_digitalpersona -- u.are.u_4500_fingerprint_reader	An issue was discovered in the HID Global DigitalPersona (formerly Crossmatch) U.are.U 4500 Fingerprint Reader Windows Biometric Framework driver 5.0.0.5. It has a statically coded initialization vector to encrypt a user's fingerprint mage, resulting in weak encryption of that. This, in combination with retrieving an encrypted fingerprint image and encryption key (through another vulnerability), allows an attacker to obtain a user's fingerprint image.	2019-07-16	not yet calculated	<a href="#">CVE-2019-13603</a> MISC MISC MISC
hid_digitalpersona -- u.are.u_4500_fingerprint_reader	There is a short key vulnerability in HID Global DigitalPersona (formerly Crossmatch) U.are.U 4500 Fingerprint Reader v24. The key for obfuscating the fingerprint image is vulnerable to brute-force attacks. This allows an attacker to recover the key and decrypt that image using the key. Successful exploitation causes a sensitive biometric information leak.	2019-07-15	not yet calculated	<a href="#">CVE-2019-13604</a> MISC MISC MISC
hpe -- icewall_sso_agent_option_and_icewall_mfa	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module ) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and 6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP-UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7.	2019-07-19	not yet calculated	<a href="#">CVE-2019-11989</a> MISC
hpe -- icewall_sso_agent_option_and_icewall_mfa	A security vulnerability in HPE IceWall SSO Agent Option and IceWall MFA (Agent module ) could be exploited remotely to cause a denial of service. The versions and platforms of Agent Option modules that are impacted are as follows: 10.0 for Apache 2.2 on RHEL 5 and 6, 10.0 for Apache 2.4 on RHEL 7, 10.0 for Apache 2.4 on HP-UX 11i v3, 10.0 for IIS on Windows, 11.0 for Apache 2.4 on RHEL 7, MFA Proxy 4.0 (Agent module only) for Apache 2.4 on RHEL 7.	2019-07-19	not yet calculated	<a href="#">CVE-2019-11990</a> MISC
huawei -- tony-al00b_smartphones	There is an information disclosure vulnerability on Secure Input of certain Huawei smartphones in Versions earlier than Tony-AL00B 9.1.0.216(C00E214R2P1). The Secure Input does not properly limit certain system privilege. An attacker tricks he user to install a malicious application and successful exploit could result in information disclosure.	2019-07-17	not yet calculated	<a href="#">CVE-2019-5222</a> MISC
hyland -- perceptive_content_server	A Denial of Service vulnerability in the ImageNow Server service in Hyland Perceptive Content Server before 7.1.5 allows an attacker to crash the service via a TCP connection.	2019-07-16	not yet calculated	<a href="#">CVE-2018-19629</a> MISC
				<a href="#">CVE-2019-</a>

jenkins -- jenkins	A path traversal vulnerability in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier in core/src/main/java/hudson/model/FileParameterValue.java allowed attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build.	2019-07-17	not yet calculated	<a href="#">10352 MLIST BID MISC MISC</a>
jenkins -- jenkins	A vulnerability in the Stapler web framework used in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier allowed attackers to access view fragments directly, bypassing permission checks and possibly obtain sensitive information.	2019-07-17	not yet calculated	<a href="#">CVE-2019-10354 MLIST MISC</a>
jenkins -- jenkins	Jenkins Credentials Binding Plugin Jenkins 1.17 is affected by: CWE-257: Storing Passwords in a Recoverable Format. The impact is: Authenticated users can recover credentials. The component is: config-variables.jelly line #30 passwordVariable). The attack vector is: Attacker creates and executes a Jenkins job.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010241 MISC</a>
johnson_controls -- exacqvision_server	ExacqVision Server's services 'exacqVisionServer', 'dvrdhpcserver' and 'mdnsresponder' have an unquoted service path. If an authenticated user is able to insert code in their system root path it potentially can be executed during the application startup. This could allow the authenticated user to elevate privileges on the system. This issue affects: Exacq Technologies, Inc. exacqVision Server 9.6; 9.8. This issue does not affect: Exacq Technologies, Inc. exacqVision Server version 9.4 and prior versions; 19.03. It is not known whether this issue affects: Exacq Technologies, Inc. exacqVision Server versions prior to 8.4.	2019-07-19	not yet calculated	<a href="#">CVE-2019-7590 BID MISC CONFIRM MISC MISC</a>
kaspersky -- multiple_products	Information Disclosure in Kaspersky Anti-Virus, Kaspersky Internet Security, Kaspersky Total Security versions up to 2019 could potentially disclose unique Product ID by forcing victim to visit a specially crafted webpage (for example, via clicking phishing link). Vulnerability has CVSS v3.0 base score 2.6	2019-07-18	not yet calculated	<a href="#">CVE-2019-8286 BID CONFIRM</a>
knot_resolver -- knot_resolver	A vulnerability was discovered in DNS resolver of knot resolver before version 4.1.0 which allows remote attackers to downgrade DNSSEC-secure domains to DNSSEC-insecure state, opening possibility of domain hijack using attacks against insecure DNS protocol.	2019-07-16	not yet calculated	<a href="#">CVE-2019-10191 CONFIRM FEDORA FEDORA CONFIRM</a>
ladon -- ladon	Ladon since 0.6.1 (since ebef0aae48af78c159b6fce81bc6f5e7e0ddb059) is affected by: XML External Entity (XXE). The impact is: Information Disclosure, reading files and reaching internal network endpoints. The component is: SOAP request handlers. For instance: https://bitbucket.org/jakobsg/ladon/src/42944fc012a3a48214791c120ee5619434505067/src/ladon/interfaces/soap.py#lines-688. The attack vector is: Send a specially crafted SOAP call.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010268 MISC MISC</a>
lawrence_livermore_national_laboratory -- msr-safe	Lawrence Livermore National Laboratory msr-safe v1.1.0 is affected by: Incorrect Access Control. The impact is: An attacker could modify model specific registers. The component is: ioctl handling. The attack vector is: An attacker could exploit a bug in ioctl interface whitelisting checking, in order to write to model specific registers, normally a function reserved for the root user. The fixed version is: v1.2.0.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010066 MISC MISC</a>
lenovoemc -- nas_products	A vulnerability in various versions of Iomega and LenovoEMC NAS products could allow an unauthenticated user to access files on NAS shares via the API.	2019-07-16	not yet calculated	<a href="#">CVE-2019-8160 CONFIRM</a>
libiec61850 -- libiec61850	mz-automation libiec61850 1.3.2 1.3.1 1.3.0 is affected by: Buffer Overflow. The impact is: Software crash. The component is: server_example_complex_array. The attack vector is: Send a specific MMS protocol packet.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010300 MISC</a>
libmspack -- libmspack	libmspack 0.9.1alpha is affected by: Buffer Overflow. The impact is: Information Disclosure. The component is: function chmd_read_headers() in libmspack/file/libmspack/mspack/chmd.c. The attack vector is: the victim must open a specially crafted chm file. The fixed version is: after commit 2f084136cfe0d05ebf5703f3e83cd955234bd.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010305 MISC MISC UBUNTU</a>
libreoffice -- libreoffice	LibreOffice has a feature where documents can specify that pre-installed scripts can be executed on various document events such as mouse-over, etc. LibreOffice is typically also bundled with LibreLogo, a programmable turtle vector graphics script, which can be manipulated into executing arbitrary python commands. By using the document event feature to trigger LibreLogo to execute python contained within a document a malicious document could be constructed which would execute arbitrary python commands silently without warning. In the fixed versions, LibreLogo cannot be called from a document event handler. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5.	2019-07-17	not yet calculated	<a href="#">CVE-2019-9848 FEDORA UBUNTU CONFIRM</a>
libreoffice -- libreoffice	LibreOffice has a 'stealth mode' in which only documents from locations deemed 'trusted' are allowed to retrieve remote resources. This mode is not the default mode, but can be enabled by users who want to disable LibreOffice's ability to include remote resources within a document. A flaw existed where bullet graphics were omitted from this protection prior to version 6.2.5. This issue affects: Document Foundation LibreOffice versions prior to 6.2.5.	2019-07-17	not yet calculated	<a href="#">CVE-2019-9849 FEDORA UBUNTU CONFIRM</a>
libSDL -- libSDL	SDL (Simple DirectMedia Layer) 2.x through 2.0.9 has a heap-based buffer over-read in Fill_IMA_ADPCM_block, caused by an integer overflow in IMA_ADPCM_decode() in audio/SDL_wave.c.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13626 MISC</a>
libssh2 -- libssh2	n libssh2 before 1.9.0, kex_method_diffie_hellman_group_exchange_sha256_key_exchange in kex.c has an integer overflow that could lead to an out-of-bounds read in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server. This is related to an _libssh2_check_length mistake, and is different from the various issues fixed in 1.8.1, such as CVE-2019-3855.	2019-07-16	not yet calculated	<a href="#">CVE-2019-13115 MISC MISC MISC MISC</a>
linario -- op-tee	Linario/OP-TEE Prior to version v3.4.0 is affected by: Boundary checks. The impact is: This could lead to corruption of any memory which the TA can access. The component is: optee_os. The fixed version is: v3.4.0.	2019-07-16	not yet calculated	<a href="#">CVE-2019-1010292 MISC</a>
linksys -- wifi_extender_products	Unsanitized user input in the web interface for Linksys WIFI extender products (RE6400 and RE6300 through 1.2.04.022) allows for remote command execution. An attacker can access system OS configurations and commands that are not intended for use beyond the web UI.	2019-07-17	not yet calculated	<a href="#">CVE-2019-11535 CONFIRM</a>
linux -- linux_kernel	In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13272 MISC CONFIRM CONFIRM MISC MISC FEDORA DEBIAN</a>
linux_foundation -- onos	The Linux Foundation ONOS 2.0.0 and earlier is affected by: Poor Input-validation. The impact is: A network administrator or attacker can install unintended flow rules in the switch by mistake. The component is: createFlow() and createFlows() functions in FlowWebResource.java (RESTful service). The attack vector is: network management and connectivity.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010250 MISC MISC</a>
linux_foundation -- onos	The Linux Foundation ONOS 2.0.0 and earlier is affected by: Poor Input-validation. The impact is: A network administrator or attacker can install unintended flow rules in the switch by mistake. The component is: applyFlowRules() and apply() functions in FlowRuleManager.java. The attack vector is: network management and connectivity.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010252 MISC MISC</a>
linux_foundation -- onos	The Linux Foundation ONOS 2.0.0 and earlier is affected by: Integer Overflow. The impact is: A network administrator (or attacker) can install unintended flow rules in the switch by mistake. The component is: createFlow() and createFlows() functions in FlowWebResource.java (RESTful service). The attack vector is: network management and connectivity.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010249 MISC MISC</a>
linux_foundation -- onos_sdn_controller	The Linux Foundation ONOS SDN Controller 1.15 and earlier versions is affected by: Improper Input Validation. The impact is: A remote attacker can execute arbitrary commands on the controller. The component is: apps/yang/src/main/java/org/onosproject/yang/impl/YangLiveCompilerManager.java. The attack vector is: network connectivity. The fixed version is: 1.15.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010245 MISC MISC</a>
linux -- linux_kernel	In the Linux kernel through 5.2.1 on the powerpc platform, when hardware transactional memory is disabled, a local user can cause a denial of service (TM Bad Thing exception and system crash) via a sigreturn() system call that sends a crafted signal frame. This affects arch/powerpc/kernel/signal_32.c and arch/powerpc/kernel/signal_64.c.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13648 MISC</a>
linux -- linux_kernel	In parse_hid_report_descriptor in drivers/input/tablet/gtco.c in the Linux kernel through 5.2.1, a malicious USB device can send an HID report that triggers an out-of-bounds write during generation of debugging messages.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13631 BID MISC</a>
	In LogMeIn join.me before 3.16.0.5505, an attacker could execute arbitrary commands on a targeted system. This vulnerability is due to unsafe search paths used by the application URI that is defined in Windows. An attacker could exploit his vulnerability by convincing a targeted user to follow a malicious link. Successful exploitation could cause the application	2019-07-	not yet	<a href="#">CVE-2019-</a>



logmein -- join.me	o load libraries from the directory targeted by the URI link. The attacker could use this behavior to execute arbitrary commands on the system with the privileges of the targeted user if the attacker can place a crafted library in a directory that is accessible to the vulnerable system.	17	calculated	<a href="#">CVE-2019-13637</a> MISC
mailcleaner -- mailcleaner	MailCleaner before c889fbb6aaa7c5f8400f637bcf1cbb844de46cd9 is affected by: Unauthenticated MySQL database password information disclosure. The impact is: MySQL database content disclosure (e.g. username, password). The component is: The API call in the function allowAction() in NewsletterController.php. The attack vector is: HTTP GET request. The fixed version is: c889fbb6aaa7c5f8400f637bcf1cbb844de46cd9.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010246</a> MISC
mcafee -- agent	Privilege escalation vulnerability in McAfee Agent (MA) before 5.6.1 HF3, allows local administrator users to potentially disable some McAfee processes by manipulating the MA directory control and placing a carefully constructed file in the MA directory.	2019-07-18	not yet calculated	<a href="#">CVE-2019-3592</a> CONFIRM
mdaemon_technologies -- email_server	MDaemon Email Server 19 skips SpamAssassin checks by default for e-mail messages larger than 2 MB (and limits checks to 10 MB even with special configuration), which is arguably inconsistent with currently popular message sizes. This might interfere with risk management for malicious e-mail, if a customer deploys a server with sufficient resources to scan large messages.	2019-07-16	not yet calculated	<a href="#">CVE-2019-13612</a> MISC
microsoft -- active_directory_federation_services	A security feature bypass vulnerability exists in Active Directory Federation Services (ADFS) which could allow an attacker to bypass the extranet lockout policy. To exploit this vulnerability, an attacker could run a specially crafted application, which would allow an attacker to launch a password brute-force attack or cause account lockouts in Active Directory. This security update corrects how ADFS handles external authentication requests., aka 'ADFS Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0975.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1126</a> N/A
microsoft -- active_directory_federation_services	A security feature bypass vulnerability exists when Active Directory Federation Services (ADFS) improperly updates its list of banned IP addresses. To exploit this vulnerability, an attacker would have to convince a victim ADFS administrator to update the list of banned IP addresses. This security update corrects how ADFS updates its list of banned IP addresses., aka 'ADFS Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-1126.	2019-07-15	not yet calculated	<a href="#">CVE-2019-0975</a> MISC
microsoft -- exchange	An information disclosure vulnerability exists when Exchange allows creation of entities with Display Names having non-printable characters. An authenticated attacker could exploit this vulnerability by creating entities with invalid display names, which, when added to conversations, remain invisible. This security update addresses the issue by validating display names upon creation in Microsoft Exchange, and by rendering invalid display names correctly in Microsoft Outlook clients., aka 'Microsoft Exchange Information Disclosure Vulnerability'.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1084</a> MISC
microsoft -- symcrypt	A denial of service vulnerability exists when SymCrypt improperly handles a specially crafted digital signature. An attacker could exploit the vulnerability by creating a specially crafted connection or message. The security update addresses the vulnerability by correcting the way SymCrypt handles digital signatures., aka 'SymCrypt Denial of Service Vulnerability'.	2019-07-15	not yet calculated	<a href="#">CVE-2019-0865</a> MISC
microsoft -- windows_defender_application_control	A security feature bypass vulnerability exists in Windows Defender Application Control (WDAC) which could allow an attacker to bypass WDAC enforcement, aka 'Windows Defender Application Control Security Feature Bypass Vulnerability'.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1167</a> MISC
microstrategy -- microstrategy_web	n MicroStrategy Web before 10.1 patch 10, stored XSS is possible in the FLTB parameter due to missing input validation.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12453</a> MISC
mongodb -- mongodb_enterprise_server	mproper handling of LDAP authentication in MongoDB Server versions 3.0.0 to 3.0.6 allows an unauthenticated client to gain unauthorized access.	2019-07-19	not yet calculated	<a href="#">CVE-2019-7882</a> CONFIRM
nasa -- cftsio	NASA CFITSIO prior to 3.43 is affected by: Buffer Overflow. The impact is: arbitrary code execution. The component is: over 40 source code files were changed. The attack vector is: remote unauthenticated attacker. The fixed version is: 3.43. NOTE: this CVE refers to the issues not covered by CVE-2018-3846, CVE-2018-3847, CVE-2018-3848, and CVE-2018-3849. One example is ftp_status in drvnet.c mishandling a long string beginning with a '4' character.	2019-07-16	not yet calculated	<a href="#">CVE-2019-1010060</a> MISC <a href="#">CVE-2019-1010060</a> MISC <a href="#">CVE-2019-1010060</a> MISC
nfdump -- nfdump	nfdump 1.6.16 and earlier is affected by: Buffer Overflow. The impact is: The impact could range from a denial of service to local code execution. The component is: nfx.c:546, nfile_inline.c:83, minilzo.c (redistributed). The attack vector is: nfdump must read and process a specially crafted file. The fixed version is: after commit 9f0fe9563366f62a71d34c92229da3432ec5f0e.	2019-07-16	not yet calculated	<a href="#">CVE-2019-1010057</a> MISC
nsa -- ghidra	NSA Ghidra before 9.0.1 allows XXE when a project is opened or restored, or a tool is imported, as demonstrated by a project.prp file.	2019-07-16	not yet calculated	<a href="#">CVE-2019-13625</a> MISC <a href="#">CVE-2019-13625</a> MISC
nvidia -- jetson_tx1	n NVIDIA Jetson TX1 L4T R32 version branch prior to R32.2, Tegra bootloader contains a vulnerability in nvboot in which the nvboot-cpu image is loaded without the load address first being validated, which may lead to code execution, denial of service, or escalation of privileges.	2019-07-19	not yet calculated	<a href="#">CVE-2019-5680</a> CONFIRM
oecms -- oecms	OECMS v4.3.R60321 and v4.3 later is affected by: Cross Site Request Forgery (CSRF). The impact is: The victim clicks on adding an administrator account. The component is: admincp.php. The attack vector is: network connectivity. The fixed version is: v4.3.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010112</a> MISC
open_information_security_foundation -- suricata	Open Information Security Foundation Suricata prior to version 4.1.3 is affected by: Denial of Service - TCP/HTTP detection bypass. The impact is: An attacker can evade a signature detection with a specially formed sequence of network packets. The component is: detect.c. https://github.com/OISF/suricata/pull/3625/commits/d9634daf74c882356659addb65fb142b738a196b. The attack vector is: An attacker can trigger the vulnerability by a specifically crafted network TCP session. The fixed version is: 4.1.3.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010279</a> MISC <a href="#">CVE-2019-1010279</a> MISC
open_information_security_foundation -- suricata	Open Information Security Foundation Suricata prior to version 4.1.2 is affected by: Denial of Service - DNS detection bypass. The impact is: An attacker can evade a signature detection with a specially formed network packet. The component is: app-layer-detect-prot.c, decode.c, decode-teredo.c and decode-ipv6.c. https://github.com/OISF/suricata/pull/3590/commits/11f659f64a4e42e90cb3c09fcef66894205aefe. https://github.com/OISF/suricata/pull/3590/commits/8357ef3f8f7cd99ef6571350724160de356158b. The attack vector is: An attacker can trigger the vulnerability by sending a specifically crafted network request. The fixed version is: 4.1.2.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010251</a> MISC <a href="#">CVE-2019-1010251</a> MISC
openmodelica -- omcompiler	OpenModelica OMCompiler is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: OPENMODELICAHOME parameter changeable via environment variable. The attack vector is: Changing an environment variable.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010038</a> CONFIRM
opera_software -- opera_mini_for_ios	The Opera Mini application through 16.0.14 for iOS has a UXSS vulnerability that can be triggered by performing navigation to a javascript: URL.	2019-07-18	not yet calculated	<a href="#">CVE-2019-13607</a> MISC
otcms -- otcms	OTCMS 3.81 allows XSS via the mode parameter in an apiRun.php?mod=autoRun request.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13971</a> MISC
pallets_project -- flask	The Pallets Project Flask before 1.0 is affected by: unexpected memory usage. The impact is: denial of service. The attack vector is: crafted encoded JSON data. The fixed version is: 1.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010083</a> CONFIRM
palo_alto_networks -- pan-os	Remote Code Execution in PAN-OS 7.1.18 and earlier, PAN-OS 8.0.11 and earlier, and PAN-OS 8.1.2 and earlier with GlobalProtect Portal or GlobalProtect Gateway Interface enabled may allow an unauthenticated remote attacker to execute arbitrary code.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1579</a> BID MISC
perl_crypt-jwt -- perl_crypt-jwt	Perl Crypt::JWT prior to 0.023 is affected by: Incorrect Access Control. The impact is: allow attackers to bypass authentication by providing a token by crafting with hmac(). The component is: JWT.pm, line 614. The attack vector is: network connectivity. The fixed version is: after commit b98a59b42ded9f9e51b2560410106207c2152d6c.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010263</a> MISC
pluckcms -- pluckcms	PluckCMS 4.7.4 and earlier is affected by: CVE-434 Unrestricted Upload of File with Dangerous Type. The impact is: get webshell. The component is: data/inc/images.php line36. The attack vector is: modify the MIME TYPE on HTTP request to upload a php file. The fixed version is: after commit 09f0ab671bf633973cd9f4fe59d4a912397cf8.	2019-07-16	not yet calculated	<a href="#">CVE-2019-1010062</a> MISC
premium_software -- cleditor	Premium Software CLEditor 1.4.5 and earlier is affected by: Cross Site Scripting (XSS). The impact is: An attacker might be able to inject arbitrary html and script code into the web site. The component is: JQuery plug-in. The attack vector is: the victim must open a crafted href attribute of a link (A) element.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010113</a> MISC
printeron -- printeron_central_print_services	An issue was discovered in PrinterOn Central Print Services (CPS) through 4.1.4. The core components that create and launch a print job do not perform complete verification of the session cookie that is supplied to them. As a result, an attacker with guest/pseudo-guest level permissions can bypass the session checks (that would otherwise logout a low-privileged user) by calling the core print job components directly via crafted HTTP GET and POST requests.	2019-07-19	not yet calculated	<a href="#">CVE-2019-17210</a> MISC
proftpd -- proftpd	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12815</a> MISC <a href="#">CVE-2019-12815</a> MISC
	An issue was discovered in python-engineio through 3.8.2. There is a Cross-Site WebSocket Hijacking (CSWSH)	2019-07-	not yet	<a href="#">CVE-2019-</a>



python_engineio -- python_engineio	vulnerability that allows attackers to make WebSocket connections to a server by using a victim's credentials, because the Origin header is not restricted.	15	calculated	<a href="#">13611 MISC</a>
qbittorrent -- qbittorrent	n qBittorrent before 4.1.7, the function Application::runExternalProgram() located in app/application.cpp allows command njection via shell metacharacters in the torrent name parameter or current tracker parameter, as demonstrated by remote command execution via a crafted name within an RSS feed.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13640 MISC</a>
quake3e -- quake3e	Quake3e < 5ed740d is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Argument string creation.	2019-07-16	not yet calculated	<a href="#">CVE-2019-1010043 MISC</a>
ranger_studios -- directus_7_api	n Directus 7 API before 2.2.1, uploading of PHP files is not blocked, leading to uploads/_originals remote code execution.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13979 MISC MISC</a>
ranger_studios -- directus_7_api	n Directus 7 API through 2.3.0, uploading of PHP files is blocked only when the Apache HTTP Server is used, leading to uploads/_originals remote code execution with nginx.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13980 MISC</a>
ranger_studios -- directus_7_api	n Directus 7 API through 2.3.0, remote attackers can read image files via a direct request for a filename under the uploads/_originals/ directory. This is related to a configuration option in which the file collection can be non-public, but this option does not apply to the thumbnailer.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13981 MISC MISC</a>
ranger_studios -- directus_7_api	Directus 7 API before 2.2.2 has insufficient anti-automation, as demonstrated by lack of a CAPTCHA in core/Directus/Services/AuthService.php and endpoints/Auth.php.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13983 MISC MISC</a>
ranger_studios -- directus_7_api	Directus 7 API before 2.3.0 does not validate uploaded files. Regardless of the file extension or MIME type, there is a direct link to each uploaded file, accessible by unauthenticated users, as demonstrated by the EICAR Anti-Virus Test File.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13984 MISC MISC</a>
ranger_studios -- directus_7_api	nterfaces/markdown/Input.vue in Directus 7 Application before 7.7.0 does not sanitize Markdown text before rendering a preview.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13982 MISC</a>
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	<a href="#">CVE-2019-8932 CONFIRM</a>
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract emails of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	<a href="#">CVE-2019-8931 CONFIRM</a>
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	<a href="#">CVE-2019-12914 CONFIRM</a>
redbrick -- shift	Redbrick Shift through 3.4.3 allows an attacker to extract authentication tokens of services (such as Gmail, Outlook, etc.) used in the application.	2019-07-17	not yet calculated	<a href="#">CVE-2019-12911 CONFIRM</a>
rubygems -- paranoid2_gem	The paranoid2 gem 1.1.6 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a hird party. The current version, without this backdoor, is 1.1.5.	2019-07-14	not yet calculated	<a href="#">CVE-2019-13589 BID MISC MISC</a>
sahi_pro -- sahi_pro	_s/_sprm/_s/_dyn/Player_setScriptFile in Sahi Pro 8.0.0 allows command execution. It allows one to run ".sah" scripts via Sahi Launcher. Also, one can create a new script with an editor. It is possible to execute commands on the server using the _execute() function.	2019-07-14	not yet calculated	<a href="#">CVE-2019-13597 MISC MISC</a>
saleor -- saleor	Saleor issue was introduced by merge commit: e1b01bad0703afd08d297ed3f1f472248312cc9c. This commit was released as part of 2.0.0 release is affected by: Incorrect Access Control. The impact is: Important. The component is: ProductVariant type in GraphQL API. The attack vector is: Unauthenticated user can access the GraphQL API (which is by default publicly exposed under '/graphql/' URL) and fetch products data which may include admin-restricted shop's revenue data. The fixed version is: 2.3.1.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010304 MISC</a>
scapy -- scapy	scapy 2.4.0 is affected by: Denial of Service. The impact is: infinite loop, resource consumption and program unresponsive. The component is: _RADIUSAttrPacketListField.getfield(self...). The attack vector is: over the network or in a pcap. both work.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010142 MISC MISC MISC</a>
schneider_electric -- modicon_m580_cpu-bmp582040_and_modicon_ethernet_module_bmenoc0301	A CWE-119 Buffer Errors vulnerability exists in Modicon M580 CPU - BMPE582040, all versions before V2.90, and Modicon Ethernet Module BMENOC0301, all versions before V2.16, which could cause denial of service on the FTP service of the controller or the Ethernet BMENOC module when it receives a FTP CWD command with a data length greater than 1020 bytes. A power cycle is then needed to reactivate the FTP service.	2019-07-15	not yet calculated	<a href="#">CVE-2018-7838 MISC</a>
shenzhen -- jisiwei_i3_robot_vacuum_cleaner	A vulnerability was found in the app 2.0 of the Shenzhen Jisiwei i3 robot vacuum cleaner. Actions performed on the app such as changing a password, and personal information it communicates with the server, use unencrypted HTTP. As an example, while logging in through the app to a Jisiwei account, the login request is being sent in cleartext. The vulnerability exists in both the Android and iOS version of the app. An attacker could exploit this by using an MITM attack on the local network to obtain someone's login credentials, which gives them full access to the robot vacuum cleaner.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12820 MISC</a>
shenzhen -- jisiwei_i3_robot_vacuum_cleaner	A vulnerability was found in the app 2.0 of the Shenzhen Jisiwei i3 robot vacuum cleaner, while adding a device to the account using a QR-code. The QR-code follows an easily predictable pattern that depends only on the specific device ID of he robot vacuum cleaner. By generating a QR-code containing information about the device ID, it is possible to connect an arbitrary device and gain full access to it. The device ID has an initial "JSW" substring followed by a six digit number that depends on the specific device.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12821 MISC</a>
slanger -- slanger	Slanger 0.6.0 is affected by: Remote Code Execution (RCE). The impact is: A remote attacker can execute arbitrary commands by sending a crafted request to the server. The component is: Message handler & request validator. The attack vector is: Remote unauthenticated. The fixed version is: after commit 5267b455caeb2e055cccf0d2b6a22727c111f5c3.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010306 MISC</a>
slleuthkit -- sleuthkit	The Sleuth Kit 4.6.0 and earlier is affected by: Integer Overflow. The impact is: Opening crafted disk image triggers crash in sk/fs/hfs_dent.c:237. The component is: Overflow in fls tool used on HFS image. Bug is in tsk/fs/hfs.c file in function hfs_cat_traverse() in lines: 952, 1062. The attack vector is: Victim must open a crafted HFS filesystem image.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010065 MISC MISC</a>
snapview -- mikogo	The Windows versions of Snapview Mikogo, versions before 5.10.2 are affected by insecure implementations which allow ocal attackers to escalate privileges.	2019-07-12	not yet calculated	<a href="#">CVE-2019-12731 MISC</a>
sourceforge -- timesheet_next_gen	Timesheet Next Gen 1.5.3 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Allows an attacker to execute arbitrary HTML and JavaScript code via a "redirect" parameter. The component is: Web login form: login.php, lines 40 and 54. The attack vector is: reflected XSS, victim may click the malicious url.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010287 MISC MISC</a>
sox -- sox	An issue was discovered in libsox.a in SoX 14.4.2. In sox-fmt.h (startread function), there is an integer overflow on the result of integer addition (wraparound to 0) fed into the lsx_callo macro that wraps malloc. When a NULL pointer is returned, it is used without a prior check that it is a valid pointer, leading to a NULL pointer dereference on lsx_readbuf in formats_i.c.	2019-07-14	not yet calculated	<a href="#">CVE-2019-13590 MISC</a>
synetics_gmbh -- i-doit	Synetics GmbH I-doit 1.12 and earlier is affected by: SQL Injection. The impact is: Unauthenticated mysql database access. The component is: Web login form. The attack vector is: An attacker can exploit the vulnerability by sending a malicious HTTP POST request. The fixed version is: 1.12.1.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010248 MISC</a>
tenable -- comodo_antivirus	Comodo Antivirus versions 12.0.0.6810 and below are vulnerable to Denial of Service affecting CmdAgent.exe via an unprotected section object "<GUID> C:\SharedMemBuff". This section object is exposed by CmdAgent and contains a SharedMemoryDictionary object, which allows a low privileged process to modify the object data causing CmdAgent.exe to crash.	2019-07-17	not yet calculated	<a href="#">CVE-2019-3972 MISC</a>
tenable -- comodo_antivirus	Comodo Antivirus versions 11.0.0.6582 and below are vulnerable to Denial of Service affecting CmdGuard.sys via its filter port "cmdServicePort". A low privileged process can crash CmdVirt.exe to decrease the port's connection count followed by process hollowing a CmdVirt.exe instance with malicious code to obtain a handle to "cmdServicePort". Once this occurs, a specially crafted message can be sent to "cmdServicePort" using "FilterSendMessage" API. This can trigger an out-of-bounds write if lpOutBuffer parameter in FilterSendMessage API is near the end of specified buffer bounds. The crash occurs when the driver performs a memset operation which uses a size beyond the size of buffer specified, causing kernel crash.	2019-07-17	not yet calculated	<a href="#">CVE-2019-3973 MISC</a>
tenable -- comodo_antivirus	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Local Privilege Escalation due to CmdAgent's handling of COM clients. A local process can bypass the signature check enforced by CmdAgent via process hollowing which can then allow the process to invoke sensitive COM methods in CmdAgent such as writing to the registry with SYSTEM privileges.	2019-07-17	not yet calculated	<a href="#">CVE-2019-3969 MISC</a>
	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to a local Denial of Service affecting CmdVirt.exe via its LPC			<a href="#">CVE-2019-</a>

tenable -- comodo_antivirus	port "cmdvrtLPCServerPort". A low privileged local process can connect to this port and send an LPC_DATAGRAM, which triggers an Access Violation due to hardcoded NULLs used for Source parameter in a memcpy operation that is called for this handler. This results in CmdVirt.exe and its child svchost.exe instances to terminate.	2019-07-17	not yet calculated	<a href="#">3971 MISC</a>
tenable -- comodo_antivirus	Comodo Antivirus versions up to 12.0.0.6810 are vulnerable to Arbitrary File Write due to Cavwp.exe handling of Comodo's Antivirus database. Cavwp.exe loads Comodo antivirus definition database in unsecured global section objects, allowing a local low privileged process to modify this data directly and change virus signatures.	2019-07-17	not yet calculated	<a href="#">CVE-2019-3970 MISC</a>
tinymce -- tinymce	inymce 4.7.11, 4.7.12 is affected by: CWE-79: Improper Neutralization of Input During Web Page Generation. The impact is: JavaScript code execution. The component is: Media element. The attack vector is: The victim must paste malicious content to media element's embed tab.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010091 MISC</a>
tp-link -- archer_c1200	CMD_SET_CONFIG_COUNTRY in the TP-Link Device Debug protocol in TP-Link Archer C1200 1.0.0 Build 20180502 rel.45702 and earlier is prone to a stack-based buffer overflow, which allows a remote attacker to achieve code execution or denial of service by sending a crafted payload to the listening server.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13614 MISC</a>
tp-link -- wireless_router_archer_router	CMD_FTEST_CONFIG in the TP-Link Device Debug protocol in TP-Link Wireless Router Archer Router version 1.0.0 Build 20180502 rel.45702 (EU) and earlier is prone to a stack-based buffer overflow, which allows a remote attacker to achieve code execution or denial of service by sending a crafted payload to the listening server.	2019-07-17	not yet calculated	<a href="#">CVE-2019-13613 MISC</a>
ulaunchelf_project -- ulaunchelf	uLaunchELF < commit 170827a is affected by: Buffer Overflow. The impact is: Possible code execution and denial of service. The component is: Loader program (loader.c) overly trusts the arguments provided via command line.	2019-07-15	not yet calculated	<a href="#">CVE-2019-1010039 MISC</a>
univenton -- univenton_corporate_server	Univenton Corporate Server univenton-directory-notifier 12.0.1-3 and earlier is affected by: CWE-213: Intentional Information Exposure. The impact is: Loss of Confidentiality. The component is: function data_on_connection() in src/callback.c. The attack vector is: network connectivity. The fixed version is: 12.0.1-4 and later.	2019-07-17	not yet calculated	<a href="#">CVE-2019-1010283 MISC</a>
videolan -- vlc_media_player	avc_CopyPicture in modules/codecs/avcodec/video.c in VideoLAN VLC media player through 3.0.7 has a heap-based buffer over-read because it does not properly validate the width and height.	2019-07-18	not yet calculated	<a href="#">CVE-2019-13962 MISC</a>
wordpress -- wordpress	TechyTalk Quick Chat WordPress Plugin All up to the latest is affected by: SQL Injection. The impact is: Access to the database. The component is: like_escape is used in Quick-chat.php line 399. The attack vector is: Crafted ajax request.	2019-07-18	not yet calculated	<a href="#">CVE-2019-1010104 MISC</a>
wordpress -- wordpress	A SQL injection vulnerability exists in the Icegram Email Subscribers & Newsletters plugin through 4.1.7 for WordPress. Successful exploitation of this vulnerability would allow a remote attacker to execute arbitrary SQL commands on the affected system.	2019-07-19	not yet calculated	<a href="#">CVE-2019-13569 MISC</a>
wordpress -- wordpress	An issue was discovered in the wp-code-highlightjs plugin through 0.6.2 for WordPress. wp-admin/options-general.php?page=wp-code-highlight-js allows CSRF, as demonstrated by an XSS payload in the hljs_additional_css parameter.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12934 MISC</a>
zeek -- zeek	In Zeek Network Security Monitor (formerly known as Bro) before 2.6.2, a NULL pointer dereference in the Kerberos (aka KRB) protocol parser leads to DoS because a case-type index is mishandled.	2019-07-17	not yet calculated	<a href="#">CVE-2019-12175 CONFIRM</a>
zeroshell -- zeroshell	Zeroshell 3.9.0 is prone to a remote command execution vulnerability. Specifically, this issue occurs because the web application mishandles a few HTTP parameters. An unauthenticated attacker can exploit this issue by injecting OS commands inside the vulnerable parameters.	2019-07-19	not yet calculated	<a href="#">CVE-2019-12725 MISC</a>
zipios_project -- zipios	Zipios before 0.1.7 does not properly handle certain malformed zip archives and can go into an infinite loop, causing a denial of service. This is related to zipheadio.h:readUInt32() and zipfile.cpp:Zipfile::Zipfile().	2019-07-17	not yet calculated	<a href="#">CVE-2019-13453 BID MISC CONFIRM</a>
zmartzone -- iam_auth_openidc	ZmartZone IAM mod_auth_openidc 2.3.10.1 and earlier is affected by: Cross Site Scripting (XSS). The impact is: Redirecting the user to a phishing page or interacting with the application on behalf of the user. The component is: File: src/mod_auth_openidc.c, Line: 3109. The fixed version is: 2.3.10.2.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010247 MISC MISC MISC</a>
zzcms -- zzmcms	zzcms zzmcms 8.3 and earlier is affected by: File Delete to getshell. The impact is: getshell. The component is: user/ppsave.php.	2019-07-19	not yet calculated	<a href="#">CVE-2019-1010151 MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nrcis.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



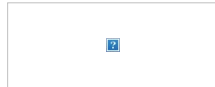
#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)



From: [US-CERT](mailto:US-CERT@nmap.org)  
To: [tmcc@nmap.org](mailto:tmcc@nmap.org), [nmap@nmap.org](mailto:nmap@nmap.org)  
Subject: Vulnerability Summary for the Week of July 8, 2019  
Date: Monday, July 15, 2019 2:32:13 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## Vulnerability Summary for the Week of July 8, 2019

07/15/2019 06:26 AM EDT

Original release date: July 15, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the [NIST NVD](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit the [NIST NVD](#) for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
contao -- contao	Contao 4.x allows SQL Injection. Fixed in Contao 4.4.39 and Contao 4.7.5.	2019-07-09	7.5	<a href="#">CVE-2019-11512</a> MISC
dlink -- central_wifimanager	/web/Lib/Action/IndexAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to execute arbitrary PHP code via a cookie because a cookie's username field allows eval injection, and an empty password bypasses authentication.	2019-07-06	7.5	<a href="#">CVE-2019-13372</a> MISC CONFIRM MISC
dlink -- central_wifimanager	An issue was discovered in the D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6. Input does not get validated and arbitrary SQL statements can be executed in the database via the /web/Public/Conn.php parameter dbSQL.	2019-07-06	7.5	<a href="#">CVE-2019-13373</a> MISC CONFIRM MISC
dlink -- central_wifimanager	A SQL Injection was discovered in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 in PayAction.class.php with the index.php/Pay/passcodeAuth parameter passcode. The vulnerability does not need any authentication.	2019-07-06	7.5	<a href="#">CVE-2019-13375</a> MISC CONFIRM MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow remote attackers to execute arbitrary commands via shell metacharacters in the online_firmware_check.cgi check_fw_url parameter.	2019-07-11	10.0	<a href="#">CVE-2019-13561</a> MISC MISC MISC
dlink -- dir-818lw_firmware	An issue was discovered on D-Link DIR-818LW devices with firmware 2.06betab01. There is a command injection in HNAp1 (exploitable with Authentication) via shell metacharacters in the MTU field to SetWanSettings.	2019-07-10	9.0	<a href="#">CVE-2019-13481</a> BID MISC
dlink -- dir-818lw_firmware	An issue was discovered on D-Link DIR-818LW devices with firmware 2.06betab01. There is a command injection in HNAp1 (exploitable with Authentication) via shell metacharacters in the Type field to SetWanSettings.	2019-07-10	10.0	<a href="#">CVE-2019-13482</a> BID MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices allow remote attackers to execute arbitrary commands via a crafted parameter to a CGI script, as demonstrated by sed injection in cgi-bin/camctrl_save_profile.cgi (save parameter) and cgi-bin/ddns.cgi.	2019-07-07	9.0	<a href="#">CVE-2019-13398</a> MISC
google -- android	In ihevcd_sao_shift_ctb of ihevcd_sao.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130023983.	2019-07-08	9.3	<a href="#">CVE-2019-2106</a> CONFIRM
google -- android	In ihevcd_parse_pps of ihevcd_parse_headers.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130024844.	2019-07-08	9.3	<a href="#">CVE-2019-2107</a> CONFIRM
google -- android	In MakeMPEG4VideoCodecSpecificData of AVIExtractor.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1. Android ID: A-130651570.	2019-07-08	9.3	<a href="#">CVE-2019-2109</a> CONFIRM
google -- android	In loop of DnsTlsSocket.cpp, there is a possible heap memory corruption due to a use after free. This could lead to remote code execution in the netd server with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122856181.	2019-07-08	7.5	<a href="#">CVE-2019-2111</a> CONFIRM
google -- android	In several functions of alarm.cc, there is possible memory corruption due to a use after free. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-117997080.	2019-07-08	7.2	<a href="#">CVE-2019-2112</a> CONFIRM
hidea -- az_admin	hidea.com AZ Admin 1.0 has news_det.php?cod= SQL Injection.	2019-07-11	7.5	<a href="#">CVE-2019-13507</a> MISC
hsycms -- hsycms	An issue was discovered in Hsycms V1.1. There is a SQL injection vulnerability via a /news/*.html page.	2019-07-10	7.5	<a href="#">CVE-2019-10653</a> MISC
oniguruma_project -- oniguruma	A use-after-free in onig_new_deluxe() in regex.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.	2019-07-10	7.5	<a href="#">CVE-2019-13224</a> CONFIRM
strong_password_project -- strong_password	The strong_password gem 0.0.7 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. The current version, without this backdoor, is 0.0.6.	2019-07-08	7.5	<a href="#">CVE-2019-13354</a> MISC MISC MISC MISC
teclib-edition -- fields	An issue was discovered in the Teclib Fields plugin through 1.9.2 for GLPI. It allows SQL Injection via container_id and old_order parameters to ajax/reorder.php by an unauthenticated user.	2019-07-10	7.5	<a href="#">CVE-2019-12723</a> MISC MISC CONFIRM
trape_project -- trape	Trape through 2019-05-08 has SQL injection via the data[2] variable in core/db.py, as demonstrated by the /bs t parameter.	2019-07-10	7.5	<a href="#">CVE-2019-13489</a> MISC
typo3 -- typo3	TYPO3 8.x through 8.7.26 and 9.x through 9.5.7 allows Deserialization of Untrusted Data.	2019-07-09	7.5	<a href="#">CVE-2019-12747</a> CONFIRM
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow Remote Command Injection, related to BusyBox and wget.	2019-07-10	10.0	<a href="#">CVE-2018-14494</a> MISC MISC
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow Remote Command Injection, aka "another command injection vulnerability in our target device," a different issue than CVE-2018-14494.	2019-07-10	10.0	<a href="#">CVE-2018-14495</a> MISC

				MISC
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow remote memory corruption and remote code execution because of a stack-based buffer overflow, related to sprintf, vocal_buff_4326, and set_getparam.cgi.	2019-07-10	7.5	<a href="#">CVE-2018-14496</a> MISC MISC
yoast -- yoast_seo	The Yoast SEO plugin before 11.6-RC5 for WordPress does not properly restrict unfiltered HTML in term descriptions.	2019-07-09	7.5	<a href="#">CVE-2019-13478</a> MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alsa-project -- alsa	posix/JackSocket.cpp in libjack in JACK2 1.9.1 through 1.9.12 (as distributed with alsa-plugins 1.1.7 and later) has a "double file descriptor close" issue during a failed connection attempt when jackd2 is not running. Exploitation success depends on multithreaded timing of that double close, which can result in unintended information disclosure, crashes, or file corruption due to having the wrong file associated with the file descriptor.	2019-07-05	6.8	<a href="#">CVE-2019-13351</a> MISC MISC
apachefriends -- xampp	lart.php in XAMPP 1.7.0 has XSS, a related issue to CVE-2008-3569.	2019-07-09	4.3	<a href="#">CVE-2019-8920</a> BID MISC
cesanta -- mongoose	mq_parse_http in mongoose.c in Mongoose 6.15 has a heap-based buffer over-read.	2019-07-10	5.0	<a href="#">CVE-2019-13503</a> MISC MISC
cisco -- unified_communications_manager	A vulnerability in the Session Initiation Protocol (SIP) protocol implementation of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of input SIP traffic. An attacker could exploit this vulnerability by sending a malformed SIP packet to an affected Cisco Unified Communications Manager. A successful exploit could allow the attacker to trigger a new registration process on all connected phones, temporarily disrupting service.	2019-07-05	5.0	<a href="#">CVE-2019-1887</a> CISCO
codedoc_project -- codedoc	Codedoc v3.2 has a stack-based buffer overflow in add_variable in codedoc.c, related to codedoc_strlcpy.	2019-07-06	6.8	<a href="#">CVE-2019-13362</a> MISC
crudlab -- wp_like_button	An authentication bypass vulnerability in the CRUDLab WP Like Button plugin through 1.6.0 for WordPress allows unauthenticated attackers to change settings. The contains() function in wp_like_button.php did not check if the current request is made by an authorized user, thus allowing any unauthenticated user to successfully update settings, as demonstrated by the wp-admin/admin.php?page=facebook-like-button each_page_url or code_snippet parameter.	2019-07-05	5.0	<a href="#">CVE-2019-13344</a> MISC MISC MISC
custom4web -- wp_open_graph	Cross-site request forgery (CSRF) vulnerability in WP Open Graph 1.6.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5960</a> JVN
digisol -- dg-hr-3300_firmware	Digisol Wireless Wifi Home Router HR-3300 allows XSS via the userid or password parameter to the admin login page.	2019-07-05	4.3	<a href="#">CVE-2018-14027</a> MISC
dlink -- central_wifimanager	A cross-site scripting (XSS) vulnerability in resource view in PayAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to inject arbitrary web script or HTML via the index.php/Pay/passcodeAuth passcode parameter.	2019-07-06	4.3	<a href="#">CVE-2019-13374</a> MISC CONFIRM MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow remote attackers to force a blank password via the apply_sec.cgi setup_wizard parameter.	2019-07-11	5.0	<a href="#">CVE-2019-13560</a> MISC MISC MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow XSS, as demonstrated by the /www/ping_response.cgi ping_ipaddr parameter, the /www/ping6_response.cgi ping6_ipaddr parameter, and the /www/apply_sec.cgi html_response_return_page parameter.	2019-07-11	4.3	<a href="#">CVE-2019-13562</a> MISC MISC MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow CSRF for the entire management console.	2019-07-11	6.8	<a href="#">CVE-2019-13563</a> MISC MISC MISC
dropbox -- dropbox	Dropbox.exe (and QtWebEngineProcess.exe in the Web Helper) in the Dropbox desktop application 71.4.108.0 store cleartext credentials in memory upon successful login or new account creation. These are not securely freed in the running process.	2019-07-08	4.3	<a href="#">CVE-2019-12171</a> MISC MISC
dwbooster -- appointment_hour_booking	The Appointment Hour Booking plugin 1.1.44 for WordPress allows XSS via the E-mail field, as demonstrated by email_1.	2019-07-11	4.3	<a href="#">CVE-2019-13505</a> MISC MISC
enhancesoft -- osticket	Unauthenticated Stored XSS in oSTicket 1.10.1 allows a remote attacker to gain admin privileges by injecting arbitrary web script or HTML via arbitrary file extension while creating a support ticket.	2019-07-09	4.3	<a href="#">CVE-2019-13397</a> MISC
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/switch.php has an Open Redirect via the current_page parameter.	2019-07-05	5.8	<a href="#">CVE-2018-12621</a> MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. htdocs/ajax/update.php has XSS via the field_name parameter.	2019-07-10	4.3	<a href="#">CVE-2018-12622</a> MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. htdocs/switch.php has XSS via the current_page parameter.	2019-07-10	4.3	<a href="#">CVE-2018-12623</a> MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/validate.php has XSS via the values parameter.	2019-07-10	4.3	<a href="#">CVE-2018-12625</a> MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/popup.php has XSS via the cat parameter.	2019-07-10	4.3	<a href="#">CVE-2018-12626</a> MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/list.php has XSS via the show_notification_list_issues or show_authorized_issues parameter.	2019-07-10	4.3	<a href="#">CVE-2018-12627</a> MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. CSRF in htdocs/manage/users.php allows creating another user with admin privileges.	2019-07-10	6.8	<a href="#">CVE-2018-12628</a> MISC CONFIRM
exiv2 -- exiv2	There is an out-of-bounds read in Exiv2::MrwImage::readMetadata in mrwimage.cpp in Exiv2 through 0.27.2.	2019-07-10	4.3	<a href="#">CVE-2019-13504</a> BID MISC MISC
ffmpeg -- ffmpeg	In FFmpeg 4.1.3, there is a division by zero at adx_write_trailer in libavformat/rawenc.c. This may be related to two NULL pointers passed as arguments at libavcodec/frame_thread_encoder.c.	2019-07-07	4.3	<a href="#">CVE-2019-13390</a> BID MISC MISC MISC MISC
fla-shop -- html5_maps	Cross-site request forgery (CSRF) vulnerability in HTML5 Maps 1.6.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5983</a> MISC MISC MISC
flarum -- flarum	Flarum before 0.1.0-beta.9 allows CSRF against all POST endpoints, as demonstrated by changing admin settings.	2019-07-07	6.8	<a href="#">CVE-2019-13183</a> CONFIRM MISC

				CONFIRM
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices have a hard-coded SSL/TLS key that is used during an administrator's SSL conversation.	2019-07-07	4.3	<a href="#">CVE-2019-13399</a> MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 use /etc/appWeb/appweb.pass to store administrative web-interface credentials in cleartext. These credentials can be retrieved via cgi-bin/getuserinfo.cgi?mode=info.	2019-07-07	5.0	<a href="#">CVE-2019-13400</a> MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices have CSRF in all scripts under cgi-bin/.	2019-07-07	6.8	<a href="#">CVE-2019-13401</a> MISC
fortinet -- fcm-mb40_firmware	/usr/sbin/default.sh and /usr/apache/htdocs/cgi-bin/admin/hardfactorydefault.cgi on Dynacolor FCM-MB40 v1.2.0.0 devices implement an incomplete factory-reset process. A backdoor can persist because neither system accounts nor the set of services is reset.	2019-07-07	6.5	<a href="#">CVE-2019-13402</a> MISC
gitea -- gitea	Gitea 1.7.2, 1.7.3 is affected by: Cross Site Scripting (XSS). The impact is: execute JavaScript in victim's browser, when the vulnerable repo page is loaded. The component is: repository's description. The attack vector is: victim must navigate to public and affected repo page.	2019-07-11	4.3	<a href="#">CVE-2019-1010314</a> MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is a persistent XSS vulnerability in the environment pages due to a lack of input validation and output encoding.	2019-07-10	4.3	<a href="#">CVE-2018-19493</a> BID CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access vulnerability that allows an unauthorized user to view private group names.	2019-07-10	4.0	<a href="#">CVE-2018-19494</a> CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an SSRF vulnerability in the Prometheus integration.	2019-07-10	4.0	<a href="#">CVE-2018-19495</a> CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access control vulnerability that permits a user with insufficient privileges to promote a project milestone to a group milestone.	2019-07-10	4.0	<a href="#">CVE-2018-19496</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.8 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an authorization vulnerability that allows access to the web-UI as a user using a Personal Access Token of any scope.	2019-07-10	6.5	<a href="#">CVE-2018-19569</a> BID CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.18 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an SSRF vulnerability in webhooks.	2019-07-10	4.0	<a href="#">CVE-2018-19571</a> MISC MISC
gitlab -- gitlab	GitLab CE 8.17 and later and EE 8.3 and later have a symlink time-of-check-to-time-of-use race condition that would allow unauthorized access to files in the GitLab Pages chroot environment. This is fixed in versions 11.5.1, 11.4.8, and 11.3.11.	2019-07-10	4.3	<a href="#">CVE-2018-19572</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 10.1 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an insecure direct object reference issue that allows a user to make comments on a locked issue.	2019-07-10	4.0	<a href="#">CVE-2018-19575</a> BID CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an access control issue that allows a Guest user to make changes to or delete their own comments on an issue, after the issue was made Confidential.	2019-07-10	6.4	<a href="#">CVE-2018-19576</a> MISC MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an incorrect access control vulnerability that displays to an unauthorized user the title and namespace of a confidential issue.	2019-07-10	5.0	<a href="#">CVE-2018-19577</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, version 11.5 before 11.5.1, is vulnerable to an insecure object reference issue that permits a user with Reporter privileges to view the Jaeger Tracing Operations page.	2019-07-10	4.0	<a href="#">CVE-2018-19578</a> CONFIRM MISC
gitlab -- gitlab	All versions of GitLab prior to 11.5.1, 11.4.8, and 11.3.11 do not send an email to the old email address when an email address change is made.	2019-07-10	5.0	<a href="#">CVE-2018-19580</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 8.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure object reference vulnerability that allows a Guest user to set the weight of an issue they create.	2019-07-10	5.0	<a href="#">CVE-2018-19581</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 11.4 before 11.4.8 and 11.5 before 11.5.1, is affected by an insecure direct object reference vulnerability that permits an unauthorized user to publish the draft merge request comments of another user.	2019-07-10	4.0	<a href="#">CVE-2018-19582</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.0 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, would log access tokens in the Workhorse logs, permitting administrators with access to the logs to see another user's token.	2019-07-10	4.0	<a href="#">CVE-2018-19583</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure direct object reference vulnerability that allows authenticated, but unauthorized, users to view members and milestone details of private groups.	2019-07-10	5.0	<a href="#">CVE-2018-19584</a> CONFIRM MISC
google -- android	In FileInputStream::Read of file_input_stream.cc, there is a possible memory corruption due to uninitialized data. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-116114182.	2019-07-08	6.8	<a href="#">CVE-2019-2105</a> CONFIRM
google -- android	In save_attr_seq of sdp_discovery.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-117105007.	2019-07-08	5.0	<a href="#">CVE-2019-2116</a> CONFIRM
helpy.io -- helpy	Helpy before 2.2.0 allows agents to edit admins.	2019-07-10	6.5	<a href="#">CVE-2018-20851</a> MISC MISC
ibm -- cloud_application_performance_management	IBM Application Performance Management (IBM Monitoring 8.1.4) could allow a remote attacker to induce the application to perform server-side DNS lookups of arbitrary domain names. IBM X-Force ID: 158270.	2019-07-11	5.0	<a href="#">CVE-2019-4131</a> XF CONFIRM
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3 and 1.1.3.2 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-force ID: 159032.	2019-07-11	5.0	<a href="#">CVE-2019-4193</a> CONFIRM XF
idoors -- idoors_reader	IDoors Reader 2.10.17 and earlier allows an attacker on the same network segment to bypass authentication to access the management console and operate the product via unspecified vectors.	2019-07-05	5.8	<a href="#">CVE-2019-5964</a> MISC MISC
ignitedcms_project -- ignitedcms	index.php/admin/permissions in Ignited CMS through 2017-02-19 allows CSRF to add an administrator.	2019-07-06	6.8	<a href="#">CVE-2019-13370</a> MISC
imagemagick -- imagemagick	In ImageMagick 7.0.8-50 Q16, ComplexImages in MagicCore/fourier.c has a heap-based buffer over-read because of incorrect calls to GetCacheViewVirtualPixels.	2019-07-07	6.8	<a href="#">CVE-2019-13391</a> MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-54 Q16 allows Division by Zero in RemoveDuplicateLayers in MagicCore/layer.c.	2019-07-09	4.3	<a href="#">CVE-2019-13454</a> BID MISC MISC MISC
intersystems -- cache	InterSystems Cache 2017.2.2.865.0 allows XSS.	2019-07-11	4.3	<a href="#">CVE-2018-17150</a> MISC
intersystems -- cache	InterSystems Cache 2017.2.2.865.0 has Incorrect Access Control.	2019-07-11	5.5	<a href="#">CVE-2018-17151</a> MISC
intersystems -- cache	InterSystems Cache 2017.2.2.865.0 allows XXE.	2019-07-11	5.5	<a href="#">CVE-2018-17152</a> MISC
invoxia -- nvx220_firmware	Invoxia NVX220 devices allow access to /bin/sh via escape from a restricted CLI, leading to disclosure of password hashes.	2019-07-05	5.0	<a href="#">CVE-2018-14529</a> MISC



jurori -- jurori_cms_2017	Cross-site scripting vulnerability in Jurori CMS 2017 Release2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	<a href="#">CVE-2019-5967</a> MISC MISC
jurori -- jurori_mail	Open redirect vulnerability in Jurori Mail 2.1.4 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-07-05	5.8	<a href="#">CVE-2019-5965</a> MISC MISC
jurori -- jurori_mail	Joruri Mail 2.1.4 and earlier does not properly manage sessions, which allows remote attackers to impersonate an arbitrary user and alter/discard the information via unspecified vectors.	2019-07-05	5.8	<a href="#">CVE-2019-5966</a> MISC MISC
keynto -- team_password_manager	KEYNTO Team Password Manager 1.5.0 allows XSS because data saved from websites is mishandled in the online vault.	2019-07-09	4.3	<a href="#">CVE-2019-13380</a> FULLDISC
libpng -- libpng	An issue has been found in third-party PNM decoding associated with libpng 1.6.35. It is a stack-based buffer overflow in the function get_token in pnm2png.c in pnm2png.	2019-07-10	6.8	<a href="#">CVE-2018-14550</a> MISC MISC
mailvelope -- mailvelope	Mailvelope prior to 3.1.0 is vulnerable to a clickjacking attack against the settings page. As the settings page is intended to be accessible from web applications, the browser's extension isolation mechanisms are disabled (web_accessible_resources). Mailvelope implements additional measures to prevent web applications from directly embedding the settings page, but this mechanism can be bypassed.	2019-07-09	4.3	<a href="#">CVE-2019-9147</a> CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 accepts or operates with invalid PGP public keys: Mailvelope allows importing keys that contain users without a valid self-certification. Keys that are obviously invalid are not rejected during import. An attacker that is able to get a victim to import a manipulated key could claim to have signed a message that originates from another person.	2019-07-09	4.3	<a href="#">CVE-2019-9148</a> CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 allows private key operations without user interaction via its client-API. By modifying an URL parameter in Mailvelope, an attacker is able to sign (and encrypt) arbitrary messages with Mailvelope, assuming the private key password is cached. A second vulnerability allows an attacker to decrypt an arbitrary message when the GnuPG backend is used in Mailvelope.	2019-07-09	6.4	<a href="#">CVE-2019-9149</a> CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 does not require user interaction to import public keys shown on web page. This functionality can be tricked to either hide a key import from the user or obscure which key was imported.	2019-07-09	5.0	<a href="#">CVE-2019-9150</a> CONFIRM
mastodon-tootdon -- tootdon_for_mastodon	The Android App 'Tootdon for Mastodon' version 3.4.1 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-07-05	5.8	<a href="#">CVE-2019-5961</a> MISC MISC
mediawiki -- mediawiki	Wikimedia MediaWiki through 1.32.1 allows CSRF.	2019-07-10	6.8	<a href="#">CVE-2019-12466</a> CONFIRM MISC BUGTRAQ DEBIAN
mediawiki -- mediawiki	Wikimedia MediaWiki 1.23.0 through 1.32.1 has an information leak. Privileged API responses that include whether a recent change has been patrolled may be cached publicly. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	5.0	<a href="#">CVE-2019-12474</a> CONFIRM MISC BUGTRAQ DEBIAN
odoo -- odoo	The Odoo Community Association (OCA) dbfilter_from_header module makes Odoo 8.x, 9.x, 10.x, and 11.x vulnerable to ReDoS (regular expression denial of service) under certain circumstances.	2019-07-05	5.0	<a href="#">CVE-2018-14733</a> CONFIRM MISC MISC MISC
oniguruma_project -- oniguruma	A NULL Pointer Dereference in match_at() in regex.c in Oniguruma 6.9.2 allows attackers to potentially cause denial of service by providing a crafted regular expression. Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.	2019-07-10	5.0	<a href="#">CVE-2019-13225</a> CONFIRM
opencats -- opencats	lib/DocumentToText.php in OpenCats before 0.9.4-3 has XXE that allows remote users to read files on the underlying operating system. The attacker must upload a file in the docx or odt format.	2019-07-05	4.3	<a href="#">CVE-2019-13358</a> MISC MISC MISC
otrs -- otrs	An issue was discovered in Open Ticket Request System (OTRS) 6.0.x through 6.0.7. A carefully constructed email could be used to inject and execute arbitrary stylesheet or JavaScript code in a logged in customer's browser in the context of the OTRS customer panel application.	2019-07-08	4.9	<a href="#">CVE-2018-11563</a> CONFIRM CONFIRM MISC
paypal -- adaptive_payments_sdk	paypal/adaptivepayments-sdk-php v3.9.2 is vulnerable to a reflected XSS in the SetPaymentOptions.php resulting code execution	2019-07-10	4.3	<a href="#">CVE-2017-6217</a> MISC
phpwind -- phpwind	PHPWind 9.1.0 has XSS vulnerabilities in the c and m parameters of the index.php file.	2019-07-09	4.3	<a href="#">CVE-2019-13472</a> MISC
pingidentity -- agentless_integration_kit	XSS exists in Ping Identity Agentless Integration Kit before 1.5.	2019-07-11	4.3	<a href="#">CVE-2019-13564</a> CONFIRM
pyxtrlock_project -- pyxtrlock	pyxtrlock 0.3 and earlier is affected by: Incorrect Access Control. The impact is: False locking impression when run in a non-X11 session. The fixed version is: 0.4.	2019-07-11	4.6	<a href="#">CVE-2019-1010316</a> MISC
sap -- information_steward	SAP Information Steward, version 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	4.3	<a href="#">CVE-2019-0329</a> BID MISC CONFIRM
sony -- vaio_update	Improper authorization vulnerability in VAIO Update 7.3.0.03150 and earlier allows an attackers to execute arbitrary executable file with administrative privilege via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5981</a> MISC MISC
sony -- vaio_update	Improper download file verification vulnerability in VAIO Update 7.3.0.03150 and earlier allows remote attackers to conduct a man-in-the-middle attack via a malicious wireless LAN access point. A successful exploitation may result in a malicious file being downloaded/executed.	2019-07-05	5.4	<a href="#">CVE-2019-5982</a> MISC MISC
squid-cache -- squid	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.	2019-07-05	4.3	<a href="#">CVE-2019-13345</a> MISC MISC MLIST
sukimalab -- attendance_manager	Cross-site scripting vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	<a href="#">CVE-2019-5970</a> MISC MISC MISC MISC
sukimalab -- attendance_manager	Cross-site request forgery (CSRF) vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5971</a> MISC MISC MISC MISC
sukimalab -- online_lesson_booking	Cross-site scripting vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	<a href="#">CVE-2019-5972</a> MISC MISC MISC
teclib-edition -- fields	An issue was discovered in the Teclib News plugin through 1.5.2 for GLPI. It allows a stored XSS attack via the \$_POST[name] parameter.	2019-07-10	4.3	<a href="#">CVE-2019-12724</a> MISC MISC CONFIRM
trape_project -- trape	A cross-site scripting (XSS) vulnerability in static/js/trape.js in Trape through 2019-05-08 allows remote attackers to inject arbitrary web script or HTML via the country, query, or refer parameter to the /register URI, because the jQuery prepend() method is used.	2019-07-10	4.3	<a href="#">CVE-2019-13488</a> MISC
typo3 -- typo3	TYPO3 8.3.0 through 8.7.26 and 9.0.0 through 9.5.7 allows XSS.	2019-07-09	4.3	<a href="#">CVE-2019-12748</a> CONFIRM
				<a href="#">CVE-2019-5984</a>

waspthemes -- custom_css_pro	Cross-site request forgery (CSRF) vulnerability in Custom CSS Pro 1.0.3 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	MISC MISC MISC
weseek -- growi	Cross-site request forgery (CSRF) vulnerability in GROWI v3.4.6 and earlier allows remote attackers to hijack the authentication of administrators via updating user's 'Basic Info'.	2019-07-05	6.8	CVE-2019-5968 MISC MISC
weseek -- growi	Open redirect vulnerability in GROWI v3.4.6 and earlier allows remote attacker to redirect users to arbitrary web sites and conduct phishing attacks via the process of login.	2019-07-05	5.8	CVE-2019-5969 MISC MISC
wikindx_project -- wikindx	A cross-site scripting (XSS) vulnerability in noMenu() and noSubMenu() in core/navigation/MENU.php in WIKINDX prior to version 5.8.1 allows remote attackers to inject arbitrary web script or HTML via the method parameter.	2019-07-08	4.3	CVE-2019-12930 CONFIRM CONFIRM CONFIRM
zoho -- salesiq	Cross-site scripting vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	CVE-2019-5962 MISC MISC
zoho -- salesiq	Cross-site request forgery (CSRF) vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5963 MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via the RCSettings.do rdsName parameter.	2019-07-11	4.3	CVE-2019-12595 MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via SoftwareListView.do with the parameter swType or swComplianceType.	2019-07-11	4.3	CVE-2019-12596 MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via ResourcesAttachments.jsp with the parameter pageName.	2019-07-11	4.3	CVE-2019-12597 MISC MISC
zohocorp -- manageengine_servicedesk_plus	An issue was discovered in the Purchase component of Zoho ManageEngine ServiceDesk Plus. There is XSS via the SearchN.do search field, a different vulnerability than CVE-2019-12189.	2019-07-11	4.3	CVE-2019-12539 MISC MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/page-edit.php (content box), which can be used to get a user's cookie.	2019-07-05	3.5	CVE-2019-13339 MISC
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the content box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, CVE-2018-20520, and CVE-2019-13186.	2019-07-05	3.5	CVE-2019-13340 MISC
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/conf.php (comment box), which can be used to get a user's cookie.	2019-07-05	3.5	CVE-2019-13341 MISC
cyberpowersystems -- powerpanel	A stored XSS vulnerability in the Agent/Center component of CyberPower PowerPanel Business Edition 3.4.0 allows a privileged attacker to embed malicious JavaScript in the SNMP trap receivers form. Upon visiting the /agent/action_recipient Event Action/Recipient page, the embedded code will be executed in the browser of the victim.	2019-07-09	3.5	CVE-2019-13070 MISC MISC
gitlab -- gitlab	GitLab CE/EE, versions 11.3 before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via unrecognized HTML tags.	2019-07-10	3.5	CVE-2018-19570 CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 10.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via Mermaid.	2019-07-10	3.5	CVE-2018-19573 CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 7.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in the OAuth authorization page.	2019-07-10	3.5	CVE-2018-19574 MISC MISC
gitlab -- gitlab	GitLab EE version 11.5 is vulnerable to a persistent XSS vulnerability in the Operations page. This is fixed in 11.5.1.	2019-07-10	3.5	CVE-2018-19579 CONFIRM MISC
google -- android	In HIDL, safe_union, and other C++ structs/unions being sent to application processes, there are uninitialized fields. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-131356202	2019-07-08	2.1	CVE-2019-2104 CONFIRM
google -- android	In setup wizard there is a bypass of some checks when wifi connection is skipped. This could lead to factory reset protection bypass with no additional privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122597079.	2019-07-08	2.1	CVE-2019-2113 CONFIRM
google -- android	In checkQueryPermission of TelephonyProvider.java, there is a possible disclosure of secure data due to a missing permission check. This could lead to local information disclosure about carrier systems with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-124107808.	2019-07-08	2.1	CVE-2019-2117 CONFIRM
google -- android	In various functions of Parcel.cpp, there are uninitialized or partially initialized stack variables. These could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-130161842.	2019-07-08	2.1	CVE-2019-2118 CONFIRM
google -- android	In multiple functions of key_store_service.cpp, there is a possible Information Disclosure due to improper locking. This could lead to local information disclosure of protected data with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-131622568.	2019-07-08	2.1	CVE-2019-2119 CONFIRM
ibm -- multicloud_manager	IBM Multicloud Manager 3.1.0, 3.1.1, and 3.1.2 ibm-mcm-chart could allow a local attacker with admin privileges to obtain highly sensitive information upon deployment. IBM X-Force ID: 158144.	2019-07-11	2.1	CVE-2019-4118 CONFIRM XF
libosinfo -- libosinfo	libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to osinfo-install-script via the command line.	2019-07-05	2.1	CVE-2019-13313 MLIST MISC MISC MISC
nagios -- nagios_xi	Nagios XI before 5.5.4 has XSS in the auto login admin management page.	2019-07-10	3.5	CVE-2018-17147 BID MISC
redhat -- virt-bootstrap	virt-bootstrap 1.1.0 allows local users to discover a root password by listing a process, because this password may be present in the --root-password option to virt_bootstrap.py.	2019-07-05	2.1	CVE-2019-13314 MLIST MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary	Description	Published	CVSS	Source &
---------	-------------	-----------	------	----------

Vendor -- Product			Score	Patch Info
alarm.com -- adc-v522ir_devices	Alarm.com ADC-V522IR 0100b9 devices have Incorrect Access Control, a different issue than CVE-2018-19588. This occurs because of incorrect protection of VPN certificates (used for initiating a VPN session to the Alarm.com infrastructure) on the local camera device.	2019-07-11	not yet calculated	<a href="#">CVE-2019-9657</a> <a href="#">MISC</a>
alarm.com -- adc-v522ir_devices	Alarm.com ADC-V522IR 0100b9 devices have Incorrect Access Control.	2019-07-11	not yet calculated	<a href="#">CVE-2018-19588</a> <a href="#">MISC</a>
apache -- kafka	In Apache Kafka versions between 0.11.0.0 and 2.1.0, it is possible to manually craft a Produce request which bypasses transaction/idempotent ACL validation. Only authenticated clients with Write permission on the respective topics are able to exploit this vulnerability. Users should upgrade to 2.1.1 or later where this vulnerability has been fixed.	2019-07-11	not yet calculated	<a href="#">CVE-2018-17196</a> <a href="#">MISC</a>
apple -- macos	hide.me before 2.4.4 on macOS suffers from a privilege escalation vulnerability in the connectWithExecutablePath:configFilePath:configFileName method of the me_hide_vpnhelper.Helper class in the me.hide.vpnhelper macOS privilege helper tool. This method takes user-supplied input and can be used to escalate privileges, as well as obtain the ability to run any application on the system in the root context.	2019-07-08	not yet calculated	<a href="#">CVE-2019-12173</a> <a href="#">MISC</a>
arlo -- basestation	Arlo Basestation firmware 1.12.0.1_27940 and prior contain a hardcoded username and password combination that allows root access to the device when an onboard serial interface is connected to.	2019-07-09	not yet calculated	<a href="#">CVE-2019-3950</a> <a href="#">CONFIRM</a>
arlo -- basestation	Arlo Basestation firmware 1.12.0.1_27940 and prior firmware contain a networking misconfiguration that allows access to restricted network interfaces. This could allow an attacker to upload or download arbitrary files and possibly execute malicious code on the device.	2019-07-09	not yet calculated	<a href="#">CVE-2019-3949</a> <a href="#">CONFIRM</a>
avaya -- control_manager	A SQL injection vulnerability in the reporting component of Avaya Control Manager could allow an unauthenticated attacker to execute arbitrary SQL commands and retrieve sensitive data related to other users on the system. Affected versions of Avaya Control Manager include 7.x and 8.0.x versions prior to 8.0.4.0. Unsupported versions not listed here were not evaluated.	2019-07-11	not yet calculated	<a href="#">CVE-2019-7003</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
avtech -- room_alert_3e	On AVTECH Room Alert 3E devices before 2.2.5, an attacker with access to the device's web interface may escalate privileges from an unauthenticated user to administrator by performing a cmd.cgi?action=ResetDefaults&src=RA reset and using the default credentials to get in.	2019-07-07	not yet calculated	<a href="#">CVE-2019-18379</a> <a href="#">MISC</a> <a href="#">MISC</a>
bks -- bks_ebk_ethernet-buskoppler_pro	BKS EBK Ethernet-Buskoppler Pro before 3.01 allows Unrestricted Upload of a File with a Dangerous Type.	2019-07-05	not yet calculated	<a href="#">CVE-2019-12971</a> <a href="#">MISC</a>
blackberry -- qnx_software_development_platform	An information disclosure vulnerability leading to a potential local escalation of privilege in the procs service (the /proc filesystem) of BlackBerry QNX Software Development Platform version(s) 6.5.0 SP1 and earlier could allow an attacker to potentially gain unauthorized access to a chosen process address space.	2019-07-12	not yet calculated	<a href="#">CVE-2019-8998</a> <a href="#">MISC</a>
broadlearning -- eclass	Any URLs with download_attachment.php under templates or home folders can allow arbitrary files downloaded without login in BroadLearning eClass before version ip.2.5.10.2.1.	2019-07-11	not yet calculated	<a href="#">CVE-2019-9886</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
castle_rock_computing -- snmpc	nodeimp.exe in Castle Rock SNMPc before 9.0.12.1 and 10.x before 10.0.9 has a stack-based buffer overflow via a long variable string in a Map Objects text file.	2019-07-12	not yet calculated	<a href="#">CVE-2019-13494</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- adaptive_security_appliance_software_and_firepower_threat_defense_software	A vulnerability in the cryptographic driver for Cisco Adaptive Security Appliance Software (ASA) and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reboot unexpectedly. The vulnerability is due to incomplete input validation of a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) ingress packet header. An attacker could exploit this vulnerability by sending a crafted TLS/SSL packet to an interface on the targeted device. An exploit could allow the attacker to cause the device to reload, which will result in a denial of service (DoS) condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed and transparent firewall mode and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic. A valid SSL or TLS session is required to exploit this vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-1873</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- advanced_malware_protection_for_endpoints_for_windows	A vulnerability in Cisco Advanced Malware Protection (AMP) for Endpoints for Windows could allow an authenticated, local attacker with administrator privileges to execute arbitrary code. The vulnerability is due to insufficient validation of dynamically loaded modules. An attacker could exploit this vulnerability by placing a file in a specific location in the Windows filesystem. A successful exploit could allow the attacker to execute the code with the privileges of the AMP service.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1832</a> <a href="#">CISCO</a>
cisco -- email_security_appliance	A vulnerability in the attachment scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper input validation of the email body. An attacker could exploit this vulnerability by naming a malicious attachment with a specific pattern. A successful exploit could allow the attacker to bypass configured content filters that would normally block the attachment.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1921</a> <a href="#">CISCO</a>
cisco -- email_security_appliance	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device. The vulnerability is due to improper input validation of certain email fields. An attacker could exploit this vulnerability by sending a crafted email message to a recipient protected by the ESA. A successful exploit could allow the attacker to bypass configured message filters and inject arbitrary scripting code inside the email body. The malicious code is not executed by default unless the recipient's email client is configured to execute scripts contained in emails.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1933</a> <a href="#">CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker with administrator privileges to overwrite or read arbitrary files on the underlying operating system (OS) of an affected device. The vulnerability is due to improper input validation in NFVIS filesystem commands. An attacker could exploit this vulnerability by using crafted variables during the execution of an affected command. A successful exploit could allow the attacker to overwrite or read arbitrary files on the underlying OS.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1894</a> <a href="#">CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device as root. The vulnerability is due to insufficient input validation of a configuration file that is accessible to a local shell user. An attacker could exploit this vulnerability by including malicious input during the execution of this file. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS as root.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1893</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1931</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface	2019-07-05	not yet calculated	<a href="#">CVE-2019-1930</a> <a href="#">CISCO</a>

	to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.			
cisco -- ios_xr_software	A vulnerability in the implementation of Border Gateway Protocol (BGP) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to incorrect processing of certain BGP update messages. An attacker could exploit this vulnerability by sending BGP update messages that include a specific set of attributes to be processed by an affected system. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP traffic from explicitly defined peers only. To exploit this vulnerability, the malicious BGP update message would need to come from a configured, valid BGP peer or would need to be injected by the attacker into the victim's BGP network on an existing, valid TCP connection to a BGP peer.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1909</a> <a href="#">CISCO</a>
cisco -- ip_phone_7800_series_and_8800_series	A vulnerability in Cisco SIP IP Phone Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected phone. The vulnerability is due to insufficient validation of input Session Initiation Protocol (SIP) packets. An attacker could exploit this vulnerability by altering the SIP replies that are sent to the affected phone during the registration process. A successful exploit could allow the attacker to cause the phone to reboot and not complete the registration process.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1922</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the Secure Sockets Layer (SSL) input packet processor of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a memory corruption on an affected device. The vulnerability is due to improper validation of HTTPS packets. An attacker could exploit this vulnerability by sending a malformed HTTPS packet to the management web interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a denial of service (DoS) condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1892</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1891</a> <a href="#">CISCO</a>
cisco -- unified_communications_domain_manager	A vulnerability in the CLI of Cisco Unified Communications Domain Manager (Cisco Unified CDM) Software could allow an authenticated, local attacker to escape the restricted shell. The vulnerability is due to insufficient input validation of shell commands. An attacker could exploit this vulnerability by executing crafted commands in the shell. A successful exploit could allow the attacker to escape the restricted shell and access commands in the context of the restricted shell user, which does not have root privileges.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1911</a> <a href="#">CISCO</a>
citrix -- xenserver	The Windows Guest Tools in Citrix XenServer 6.2 SP1 and earlier allows remote attackers to cause a denial of service (guest OS crash) via a crafted Ethernet frame.	2019-07-11	not yet calculated	<a href="#">CVE-2014-3798</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">SECTRAK</a>
cloud_foundry -- uaa	Cloud Foundry UAA version prior to 73.3.0, contain endpoints that contains improper escaping. An authenticated malicious user with basic read privileges for one identity zone can extend those reading privileges to all other identity zones and obtain private information on users, clients, and groups in all other identity zones.	2019-07-11	not yet calculated	<a href="#">CVE-2019-11268</a> <a href="#">CONFIRM</a>
cloudera -- cloudera_manager	Cloudera Manager through 5.15 has Incorrect Access Control.	2019-07-11	not yet calculated	<a href="#">CVE-2018-11744</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
cohesity -- dataplatform	A man-in-the-middle vulnerability related to vCenter access was found in Cohesity DataPlatform version 5.x and 6.x prior to 6.1.1c. Cohesity clusters did not verify TLS certificates presented by vCenter. This vulnerability could expose Cohesity user credentials configured to access vCenter.	2019-07-12	not yet calculated	<a href="#">CVE-2019-11242</a> <a href="#">CONFIRM</a>
container_build_system -- osbs-client	A flaw was found in the yaml.load() function in the osbs-client versions since 0.46 before 0.56.1. Insecure use of the yaml.load() function allowed the user to load any suspicious object for code execution via the parsing of malicious YAML files.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10135</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
cyberpower -- powerpanel_business	CSRF in the Agent/Center component of CyberPower PowerPanel Business Edition 3.4.0 allows an attacker to submit POST requests to any forms in the web application. This can be exploited by tricking an authenticated user into visiting an attacker controlled web page.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13071</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
damicms -- damicms	An arbitrary file read vulnerability in DamiCMS v6.0.0 allows remote authenticated administrators to read any files in the server via a crafted /admin.php?s=Tpl/Add/Id/ URI.	2019-07-10	not yet calculated	<a href="#">CVE-2018-14831</a> <a href="#">MISC</a>
ddrt -- dashcom_live	Lack of authentication in file-viewing components in DDRT Dashcom Live 2019-05-09 allows anyone to remotely access all claim details by visiting easily guessable dashboard/uploads/claim_files/claim_id_ URLs.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11020</a> <a href="#">MISC</a> <a href="#">MISC</a>
ddrt -- dashcom_live	Lack of authentication in case-exporting components in DDRT Dashcom Live through 2019-05-08 allows anyone to remotely access all claim details by visiting easily guessable exportpdf/all_claim_detail.php?claim_id= URLs.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11019</a> <a href="#">MISC</a> <a href="#">MISC</a>
debian -- mediawiki	An Incorrect Access Control vulnerability was found in Wikimedia MediaWiki 1.18.0 through 1.32.1. It is possible to bypass the limits on IP range blocks (\$wgBlockCIDRLimit) by using the API. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12472</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
debian -- mediawiki	An Incorrect Access Control vulnerability was found in Wikimedia MediaWiki 1.27.0 through 1.32.1. Directly POSTing to Special:ChangeEmail would allow for bypassing re-authentication, allowing for potential account takeover.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12468</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	MediaWiki through 1.32.1 has Incorrect Access Control (issue 1 of 3). A spammer can use Special:ChangeEmail to send out spam with no rate limiting or ability to block them. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12467</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	Wikimedia MediaWiki 1.30.0 through 1.32.1 has XSS. Loading user JavaScript from a non-existent account allows anyone to create the account, and perform XSS on users loading that script. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12471</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	Wikimedia MediaWiki 1.27.0 through 1.32.1 might allow DoS. Passing invalid titles to the API could cause a DoS by querying the entire watchlist table. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12473</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
				<a href="#">CVE-2019-12470</a>

debian -- mediawiki	Wikimedia MediaWiki through 1.32.1 has Incorrect Access Control. Suppressed log in RevisionDelete page is exposed. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-11333</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	MediaWiki through 1.32.1 has Incorrect Access Control. Suppressed username or log in Special:EditTags are exposed. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12469</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- redis	A stack-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By corrupting a hyperloglog using the SETRANGE command, an attacker could cause Redis to perform controlled increments of up to 12 bytes past the end of a stack-allocated buffer.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10193</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- redis	A heap-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By carefully corrupting a hyperloglog using the SETRANGE command, an attacker could trick Redis interpretation of dense HLL encoding to write up to 3 bytes beyond the end of a heap-allocated buffer.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10192</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
digium -- asterisk	Buffer overflow in res_pjsip_messaging in Digium Asterisk versions 13.21-cert3, 13.27.0, 15.7.2, 16.4.0 and earlier allows remote authenticated users to crash Asterisk by sending a specially crafted SIP MESSAGE message.	2019-07-12	not yet calculated	<a href="#">CVE-2019-12827</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
digium -- asterisk	An issue was discovered in Asterisk Open Source through 13.27.0, 14.x and 15.x through 15.7.2, and 16.x through 16.4.0, and Certified Asterisk through 13.21-cert3. A pointer dereference in chan_sip while handling SDP negotiation allows an attacker to crash Asterisk when handling an SDP answer to an outgoing T.38 re-invite. To exploit this vulnerability an attacker must cause the chan_sip module to send a T.38 re-invite request to them. Upon receipt, the attacker must send an SDP answer containing both a T.38 UDPTL stream and another media stream containing only a codec (which is not permitted according to the chan_sip configuration).	2019-07-12	not yet calculated	<a href="#">CVE-2019-13161</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
e107 -- e107	In e107 v2.1.7, output without filtering results in XSS.	2019-07-10	not yet calculated	<a href="#">CVE-2018-11734</a> <a href="#">MISC</a>
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.9 and CCU3 devices before 3.43.16 have buffer overflows in the ReGa ise GmbH HTTP-Server 2.0 component, aka HMCCU-179. This may lead to remote code execution.	2019-07-10	not yet calculated	<a href="#">CVE-2019-10122</a> <a href="#">MISC</a> <a href="#">MISC</a>
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.16 use session IDs for authentication but lack authorization checks. An attacker can obtain a session ID via an invalid login attempt to the RemoteApi account, aka HMCCU-154. This leads to automatic login as admin.	2019-07-10	not yet calculated	<a href="#">CVE-2019-10119</a> <a href="#">MISC</a> <a href="#">MISC</a>
eq-3 -- homematic_ccu2_devices	On eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.16, automatic login configuration (aka setAutoLogin) can be achieved by continuing to use a session ID after a logout, aka HMCCU-154.	2019-07-10	not yet calculated	<a href="#">CVE-2019-10120</a> <a href="#">MISC</a> <a href="#">MISC</a>
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.15 use session IDs for authentication but lack authorization checks. An attacker can obtain a session ID via the user authentication dialogue, aka HMCCU-153. This leads to automatic login as admin.	2019-07-10	not yet calculated	<a href="#">CVE-2019-10121</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fasterxml -- jackson-databind	An issue was discovered in FasterXML Jackson-databind 2.0.0 through 2.9.5. Use of Jackson default typing along with a gadget class from IBatis allows exfiltration of content. Fixed in 2.7.9.4, 2.8.11.2, and 2.9.6.	2019-07-09	not yet calculated	<a href="#">CVE-2018-11307</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
field_test_gem_for_ruby_on_rails -- field_test_gem_for_ruby_on_rails	The field_test gem 0.3.0 for Ruby has unvalidated input. A method call that is expected to return a value from a certain set of inputs can be made to return any input, which can be dangerous depending on how applications use it. If an application treats arbitrary variants as trusted, this can lead to a variety of potential vulnerabilities like SQL injection or cross-site scripting (XSS).	2019-07-09	not yet calculated	<a href="#">CVE-2019-13146</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
flightpath -- flightpath	FlightPath 4.x and 5.0-x allows directory traversal and Local File Inclusion through the form_include parameter in an index.php?q=system-handle-form-submit POST request because of an include_once in system_handle_form_submit in modules/system/system.module.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13396</a> <a href="#">CONFIRM</a>
ge_healthcare -- aestiva_and_aespire	In GE Aestiva and Aespire versions 7100 and 7900, a vulnerability exists where serial devices are connected via an added unsecured terminal server to a TCP/IP network configuration, which could allow an attacker to remotely modify device configuration and silence alarms.	2019-07-10	not yet calculated	<a href="#">CVE-2019-10966</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
glpi_project -- glpi	GLPI GLPI Product 9.3.1 is affected by: Frame and Form tags Injection allowing admins to phish users by putting code in reminder description. The impact is: Admins can phish any user or group of users for credentials / credit cards. The component is: Tools > Reminder > Description .. Set the description to any iframe/form tags and apply. The attack vector is: The attacker puts a login form, the user fills it and clicks on submit .. the request is sent to the attacker domain saving the data. The fixed version is: 9.4.1.	2019-07-12	not yet calculated	<a href="#">CVE-2019-10103</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
glpi_project -- glpi	An issue was discovered in GLPI before 9.4.1. After a successful password reset by a user, it is possible to change that user's password again during the next 24 hours without any information except the associated email address.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13240</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
hewlett_packard_enterprise -- 3par_service_processor	HPE has identified a vulnerability in HPE 3PAR Service Processor (SP) version 4.1 through 4.4. HPE 3PAR Service Processor (SP) version 4.1 through 4.4 has a remote information disclosure vulnerability which can allow for the disruption of the confidentiality, integrity and availability of the Service Processor and any managed 3PAR arrays.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11981</a> <a href="#">CONFIRM</a>
huawei -- mate_20_and_mate_20_X_honor_magic_2	There is a Factory Reset Protection (FRP) bypass vulnerability on several smartphones. The system does not sufficiently verify the permission, an attacker could do a certain operation on certain step of setup wizard. Successful exploit could allow the attacker bypass the FRP protection. Affected products: Mate 20 X, versions earlier than Ever-AL00B 9.0.0.200(C00E200R2P1); Mate 20, versions earlier than Hima-AL00B/Hima-TL00B 9.0.0.200(C00E200R2P1); Honor Magic 2, versions earlier than Tony-AL00B/Tony-TL00B 9.0.0.182(C00E180R2P2).	2019-07-10	not yet calculated	<a href="#">CVE-2019-5220</a> <a href="#">CONFIRM</a>
huawei -- mate_20_x	There is a path traversal vulnerability on Huawei Share. The software does not properly validate the path, an attacker could crafted a file path when transporting file through Huawei Share, successful exploit could allow the attacker to transport a file to arbitrary path on the phone. Affected products: Mate 20 X versions earlier than Ever-L29B 9.1.0.300(C432E3R1P12), versions earlier than Ever-L29B 9.1.0.300(C636E3R2P1), and versions earlier than Ever-L29B 9.1.0.300(C185E3R3P1).	2019-07-10	not yet calculated	<a href="#">CVE-2019-5221</a> <a href="#">CONFIRM</a>
	In Huneson I-oneNet version 3.0.7 ~ 3.0.53 and 4.0.4 ~ 4.0.16, the specific upload web module doesn't verify the file extension and type, and an attacker can upload a webshell.	2019-07-	not yet	<a href="#">CVE-2019-</a>



huneson -- i-onenet	After the webshell upload, an attacker can use the webshell to perform remote code execution such as running a system command.	10	calculated	12803 <a href="#">CONFIRM</a>
huneson -- i-onenet	In Huneson i-oneNet version 3.0.7 ~ 3.0.53 and 4.0.4 ~ 4.0.16, due to the lack of update file integrity checking in the upgrade process, an attacker can craft malicious file and use it as an update.	2019-07-10	not yet calculated	CVE-2019-12804 <a href="#">CONFIRM</a>
ibm -- content_navigator	IBM Content Navigator 3.0CD is vulnerable to local file inclusion, allowing an attacker to access a configuration file in the ICN server. IBM X-Force ID: 160015.	2019-07-11	not yet calculated	CVE-2019-4263 <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 153749.	2019-07-11	not yet calculated	CVE-2018-1968 <a href="#">CONFIRM</a> <a href="#">XF</a>
intel -- processor_diagnostic_tool	Improper access control in the Intel(R) Processor Diagnostic Tool before version 4.1.2.24 may allow an authenticated user to potentially enable escalation of privilege, information disclosure or denial of service via local access.	2019-07-11	not yet calculated	CVE-2019-11133 <a href="#">BID</a> <a href="#">CONFIRM</a>
intel -- ssd_dc_s4500_and_s4600_devices	Improper authentication in firmware for Intel(R) SSD DC S4500 Series and Intel(R) SSD DC S4600 Series before SCV10150 may allow an unprivileged user to potentially enable escalation of privilege via physical access.	2019-07-11	not yet calculated	CVE-2018-18095 <a href="#">BID</a> <a href="#">CONFIRM</a>
intuit -- lacerte	Intuit Lacerte 2017 has Incorrect Access Control.	2019-07-09	not yet calculated	CVE-2018-14833 <a href="#">MISC</a> <a href="#">MISC</a>
invoxia -- nvx220_devices	Invoxia NVX220 devices allow TELNET access as admin with a default password.	2019-07-05	not yet calculated	CVE-2018-14528 <a href="#">MISC</a>
ivanti -- endpoint_manager	An issue was discovered in the Core Server in Ivanti Endpoint Manager (EPM) 2017.3 before SU7 and 2018.x before 2018.3 SU3, with remote code execution. In other words, the issue affects 2017.3, 2018.1, and 2018.3 installations that lack the April 2019 update.	2019-07-11	not yet calculated	CVE-2019-10651 <a href="#">CONFIRM</a>
jenkins -- jenkins	Jenkins Port Allocator Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	CVE-2019-10350 <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	A stored cross site scripting vulnerability in Jenkins Dependency Graph Viewer Plugin 0.13 and earlier allowed attackers able to configure jobs in Jenkins to inject arbitrary HTML and JavaScript in the plugin-provided web pages in Jenkins.	2019-07-11	not yet calculated	CVE-2019-10349 <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	Jenkins Gogs Plugin stored credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	CVE-2019-10348 <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	Jenkins Mashup Portlets Plugin stored credentials unencrypted on the Jenkins master where they can be viewed by users with access to the master file system.	2019-07-11	not yet calculated	CVE-2019-10347 <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	A reflected cross site scripting vulnerability in Jenkins Embeddable Build Status Plugin 2.0.1 and earlier allowed attackers inject arbitrary HTML and JavaScript into the response of this plugin.	2019-07-11	not yet calculated	CVE-2019-10346 <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Docker Plugin 1.1.6 and earlier in various 'fillCredentialsItems' methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2019-07-11	not yet calculated	CVE-2019-10342 <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Docker Plugin 1.1.6 and earlier in DockerAPI.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-07-11	not yet calculated	CVE-2019-10341 <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Docker Plugin 1.1.6 and earlier in DockerAPI.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-07-11	not yet calculated	CVE-2019-10340 <a href="#">MLIST</a> <a href="#">MISC</a>
jenkins -- jenkins	Jenkins Caliper CI Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	CVE-2019-10351 <a href="#">MLIST</a> <a href="#">MISC</a>
juniper -- junos_os	A vulnerability in the pfe-chassisd Chassis Manager (CMLC) daemon of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the EX4300 when specific valid broadcast packets create a broadcast storm condition when received on the me0 interface of the EX4300 Series device. A reboot of the device is required to restore service. Continued receipt of these valid broadcast packets will create a sustained Denial of Service (DoS) against the device. Affected releases are Juniper Networks Junos OS: 16.1 versions above and including 16.1R1 prior to 16.1R7-S5; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R2; 18.1 versions prior to 18.1R3; 18.2 versions prior to 18.2R2.	2019-07-11	not yet calculated	CVE-2019-0046 <a href="#">CONFIRM</a>
juniper -- junos_os	On EX4300 Series switches with TCAM optimization enabled, incoming multicast traffic matches an implicit loopback filter rule first, since it has high priority. This rule is meant for reserved multicast addresses 224.0.0.x, but incorrectly matches on 224.x.x.x. Due to this bug, when a firewall filter is applied on the loopback interface, other firewall filters might stop working for multicast traffic. The command 'show firewall filter' can be used to confirm whether the filter is working. This issue only affects the EX4300 switch. No other products or platforms are affected by this vulnerability. This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D51, 14.1X53-D115 on EX4300 Series; 17.1 versions prior to 17.1R3 on EX4300 Series; 17.2 versions prior to 17.2R3-S2 on EX4300 Series; 17.3 versions prior to 17.3R3-S3 on EX4300 Series; 17.4 versions prior to 17.4R2-S5, 17.4R3 on EX4300 Series; 18.1 versions prior to 18.1R3-S1 on EX4300 Series; 18.2 versions prior to 18.2R2 on EX4300 Series; 18.3 versions prior to 18.3R2 on EX4300 Series.	2019-07-11	not yet calculated	CVE-2019-0048 <a href="#">CONFIRM</a>
juniper -- junos_os	On Junos devices with the BGP graceful restart helper mode enabled or the BGP graceful restart mechanism enabled, a certain sequence of BGP session restart on a remote peer that has the graceful restart mechanism enabled may cause the local routing protocol daemon (RPD) process to crash and restart. Repeated crashes of the RPD process can cause prolonged Denial of Service (DoS). Graceful restart helper mode for BGP is enabled by default. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S3; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3; 17.2X75 versions prior to 17.2X75-D105; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R1-S7, 17.4R2-S2, 17.4R3; 18.1 versions prior to 18.1R3-S2; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30; 18.3 versions prior to 18.3R1-S4, 18.3R2. Junos OS releases prior to 16.1R1 are not affected.	2019-07-11	not yet calculated	CVE-2019-0049 <a href="#">CONFIRM</a>
juniper -- junos_os	The srpxpfe process may crash on SRX Series services gateways when the UTM module processes a specific fragmented HTTP packet. The packet is misinterpreted as a regular TCP packet which causes the processor to crash. This issue affects all SRX Series platforms that support URL-Filtering and have web-filtering enabled. Affected releases are Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D85 on SRX Series; 15.1X49 versions prior to 15.1X49-D181, 15.1X49-D190 on SRX Series; 17.3 versions on	2019-07-11	not yet calculated	CVE-2019-0052 <a href="#">CONFIRM</a>

	SRX Series; 17.4 versions prior to 17.4R1-S8, 17.4R2-S5, 17.4R3 on SRX Series; 18.1 versions prior to 18.1R3-S6 on SRX Series; 18.2 versions prior to 18.2R2-S1, 18.2R3 on SRX Series; 18.3 versions prior to 18.3R1-S2, 18.3R2 on SRX Series; 18.4 versions prior to 18.4R1-S1, 18.4R2 on SRX Series.			
juniper -- junos_os	Insufficient validation of environment variables in the telnet client supplied in Junos OS can lead to stack-based buffer overflows, which can be exploited to bypass verixec restrictions on Junos OS. A stack-based overflow is present in the handling of environment variables when connecting via the telnet client to remote telnet servers. This issue only affects the telnet client ? accessible from the CLI or shell ? in Junos OS. Inbound telnet services are not affected by this issue. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S13; 12.3X48 versions prior to 12.3X48-D80; 14.1X53 versions prior to 14.1X53-D130, 14.1X53-D49; 15.1 versions prior to 15.1F6-S12, 15.1R7-S4; 15.1X49 versions prior to 15.1X49-D170; 15.1X53 versions prior to 15.1X53-D237, 15.1X53-D496, 15.1X53-D591, 15.1X53-D69; 16.1 versions prior to 16.1R3-S11, 16.1R7-S4; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R2-S7, 17.2R3-S1; 17.3 versions prior to 17.3R3-S4; 17.4 versions prior to 17.4R1-S6, 17.4R2-S3, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S3; 18.2 versions prior to 18.2R1-S5, 18.2R2-S2, 18.2R3; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S3, 18.3R2; 18.4 versions prior to 18.4R1-S2, 18.4R2.	2019-07-11	not yet calculated	<a href="#">CVE-2019-0053</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
leanote -- leanote	Leanote prior to version 2.6 is affected by: Cross Site Scripting (XSS).	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010003</a> <a href="#">MISC</a>
libpng -- libpng	libpng before 1.6.32 does not properly check the length of chunks against the user limit.	2019-07-10	not yet calculated	<a href="#">CVE-2017-12652</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10638</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This attack can be carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID generation was changed to have a dependency on an address associated with a network namespace.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10639</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The openvpn_launcher.64 binary is setuid root. This binary executes /opt/pia/openvpn-64/openvpn, passing the parameters provided from the command line. Care was taken to programmatically disable potentially dangerous openvpn parameters; however, the --route-pre-down parameter can be used. This parameter accepts an arbitrary path to a script/program to be executed when OpenVPN exits. The --script-security parameter also needs to be passed to allow for this action to be taken, and --script-security is not currently in the disabled parameter list. A local unprivileged user can pass a malicious script/binary to the --route-pre-down option, which will be executed as root when openvpn is stopped.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12578</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The root_runner.64 binary is setuid root. This binary executes /opt/pia/ruby/64/ruby, which in turn attempts to load several libraries under /tmp/ruby-deploy.0ld/lib. A local unprivileged user can create a malicious library under this path to execute arbitrary code as the root user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12575</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux_and_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux and macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The PIA Linux/macOS binary openvpn_launcher.64 binary is setuid root. This binary accepts several parameters to update the system configuration. These parameters are passed to operating system commands using a "here" document. The parameters are not sanitized, which allow for arbitrary commands to be injected using shell metacharacters. A local unprivileged user can pass special crafted parameters that will be interpolated by the operating system calls.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12579</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux_and_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux and macOS could allow an authenticated, local attacker to overwrite arbitrary files. The openvpn_launcher binary is setuid root. This binary supports the --log option, which accepts a path as an argument. This parameter is not sanitized, which allows a local unprivileged user to overwrite arbitrary files owned by any user on the system, including root. This creates a denial of service condition and possible data loss if leveraged by a malicious local user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12573</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The openvpn_launcher binary is setuid root. This program is called during the connection process and executes several operating system utilities to configure the system. The networksetup utility is called using relative paths. A local unprivileged user can execute arbitrary commands as root by creating a networksetup trojan which will be executed during the connection process. This is possible because the PATH environment variable is not reset prior to executing the OS utility.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12576</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v0.9.8 beta (build 02099) for macOS could allow an authenticated, local attacker to overwrite arbitrary files. When the client initiates a connection, the XML /tmp/pia-watcher.plist file is created. If the file exists, it will be truncated and the contents completely overwritten. This file is removed on disconnect. An unprivileged user can create a hard or soft link to arbitrary files owned by any user on the system, including root. This creates a denial of service condition and possible data loss if leveraged by a malicious local user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12571</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The macOS binary openvpn_launcher.64 is setuid root. This binary creates /tmp/pia_upscript.sh when executed. Because the file creation mask (umask) is not reset, the umask value is inherited from the calling process. This value can be manipulated to cause the privileged binary to create files with world writable permissions. A local unprivileged user can modify /tmp/pia_upscript.sh during the connect process to execute arbitrary code as the root user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12577</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_windows	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v1.0 for Windows could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The PIA client is vulnerable to a DLL injection vulnerability during the software update process. The updater loads several libraries from a folder that authenticated users have write access to. A low privileged user can leverage this vulnerability to execute	2019-07-11	not yet calculated	<a href="#">CVE-2019-12574</a> <a href="#">MISC</a>

	arbitrary code as SYSTEM.			
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 was vulnerable to multiple directory traversal issues, with which authenticated users could add, remove, or potentially read files in arbitrary folders accessible by the IIS user. This could lead to reading other users' credentials including those of SYSADMIN accounts, reading other users' emails, or adding emails or files to other users' accounts.	2019-07-08	not yet calculated	<a href="#">CVE-2019-12925</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 did not use appropriate access control checks in a number of areas. As a result, it was possible to perform a number of actions, when logged in as a user, that that user should not have had permission to perform. It was also possible to gain access to areas within the application for which the accounts used were supposed to have insufficient access.	2019-07-08	not yet calculated	<a href="#">CVE-2019-12926</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 was vulnerable to stored and reflected cross-site scripting (XSS) attacks. Because the session cookie did not use the HttpOnly flag, it was possible to hijack the session cookie by exploiting this vulnerability.	2019-07-08	not yet calculated	<a href="#">CVE-2019-12927</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mailenable -- mailenable_enterprise_premium	MailEnable Enterprise Premium 10.23 was vulnerable to XML External Entity Injection (XXE) attacks that could be exploited by an unauthenticated user. It was possible for an attacker to use a vulnerability in the configuration of the XML processor to read any file on the host system. Because all credentials were stored in a cleartext file, it was possible to steal all users' credentials (including the highest privileged users).	2019-07-08	not yet calculated	<a href="#">CVE-2019-12924</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
mailenable -- mailenable_enterprise_premium	In MailEnable Enterprise Premium 10.23, the potential cross-site request forgery (CSRF) protection mechanism was not implemented correctly and it was possible to bypass it by removing the anti-CSRF token parameter from the request. This could allow an attacker to manipulate a user into unwittingly performing actions within the application (such as sending email, adding contacts, or changing settings) on behalf of the attacker.	2019-07-08	not yet calculated	<a href="#">CVE-2019-12923</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
matrixssl -- matrixssl	MatrixSSL before 4.2.1 has an out-of-bounds read during ASN.1 handling.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13470</a> <a href="#">MISC</a>
minimagick -- minimagick	In lib/mini_magick/image.rb in MiniMagick before 4.9.4, a fetched remote image filename could cause remote command execution because Image.open input is directly passed to Kernel#open, which accepts a ` ` character followed by a command.	2019-07-11	not yet calculated	<a href="#">CVE-2019-13574</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
mobatech -- mobaxterm	In MobaXterm 11.1, the mobaxterm: URI handler has an argument injection vulnerability that allows remote attackers to execute arbitrary commands when the user visits a specially crafted URL. Based on the available command-line arguments of the software, one can simply inject -exec to execute arbitrary commands. The additional arguments -hidterm and -exitwhendone in the payload make the attack less visible.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13475</a> <a href="#">MISC</a>
mybb -- mybb	An CSRF issue was discovered in the JN-Jones MyBB-2FA plugin through 2014-11-05 for MyBB. An attacker can forge a request to an installed mybb2fa plugin to control its state via usercp.php?action=mybb2fa&do=deactivate (or usercp.php?action=mybb2fa&do=activate). A deactivate operation lowers the security of the targeted account by disabling two factor authentication.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12363</a> <a href="#">MISC</a> <a href="#">MISC</a>
netfilter -- iptables	A buffer overflow in iptables-restore in netfilter iptables 1.8.2 allows an attacker to (at least) crash the program or potentially gain code execution via a specially crafted iptables-save file. This is related to add_param_to_argv in xshared.c.	2019-07-12	not yet calculated	<a href="#">CVE-2019-11360</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
netiq -- advanced_authentication_framework	A potential Man in the Middle attack (MITM) was found in NetIQ Advanced Authentication Framework versions prior to 6.0.	2019-07-10	not yet calculated	<a href="#">CVE-2019-11650</a> <a href="#">CONFIRM</a>
npmjs -- serve-here.js	Path traversal vulnerability in version up to v1.1.3 in serve-here.js npm module allows attackers to list any file in arbitrary folder.	2019-07-10	not yet calculated	<a href="#">CVE-2019-5444</a> <a href="#">MISC</a>
nuxt -- nuxt.js	@nuxt/devalue before 1.2.3, as used in Nuxt.js before 2.6.2, mishandles object keys, leading to XSS.	2019-07-11	not yet calculated	<a href="#">CVE-2019-13506</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
ovirt -- ovirt_metrics	Sensitive passwords used in deployment and configuration of oVirt Metrics, all versions, were found to be insufficiently protected. Passwords could be disclosed in log files (if playbooks are run with -v) or in playbooks stored on Metrics or Bastion hosts.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10194</a> <a href="#">CONFIRM</a>
patchwork -- patchwork	A Cross Site Scripting (XSS) vulnerability exists in the template tag used to render message ids in Patchwork v1.1 through v2.1.x. This allows an attacker to insert JavaScript or HTML into the patch detail page via an email sent to a mailing list consumed by Patchwork. This affects the function msgid in templatetags/patch.py. Patchwork versions v2.1.4 and v2.0.4 will contain the fix.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13122</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
php -- php	main/streams/xf_socket.c in PHP 7.x before 2017-03-07 misparses fsockopen calls, such as by interpreting fsockopen("127.0.0.1:80", 443) as if the address/port were 127.0.0.1:80:443, which is later truncated to 127.0.0.1:80. This behavior has a security risk if the explicitly provided port number (i.e., 443 in this example) is hardcoded into an application as a security policy, but the hostname argument (i.e., 127.0.0.1:80 in this example) is obtained from untrusted input.	2019-07-10	not yet calculated	<a href="#">CVE-2017-7189</a> <a href="#">MISC</a>
prestashop -- prestashop	In PrestaShop before 1.7.6.0 RC2, the id_address_delivery and id_address_invoice parameters are affected by an Insecure Direct Object Reference vulnerability due to a guessable value sent to the web application during checkout. An attacker could leak personal customer information. This is PrestaShop bug #14444.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13461</a> <a href="#">MISC</a> <a href="#">MISC</a>
project_redcap -- redcap	Multiple stored Cross-site scripting (XSS) issues in the admin panel and survey system in REDCap 8 before 8.10.20 and 9 before 9.1.2 allow an attacker to inject arbitrary malicious HTML or JavaScript code into a user's web browser.	2019-07-11	not yet calculated	<a href="#">CVE-2019-13029</a> <a href="#">MISC</a>
python -- python	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.	2019-07-13	not yet calculated	<a href="#">CVE-2018-20852</a> <a href="#">MISC</a> <a href="#">MISC</a>
quest -- kace	Quest KACE, all versions prior to version 8.0.x, 8.1.x, and 9.0.x, allows unintentional access to the appliance leveraging functions of the troubleshooting tools located in the administrator user interface.	2019-07-08	not yet calculated	<a href="#">CVE-2019-10973</a> <a href="#">BID</a> <a href="#">MISC</a>
rapid7 -- insight_agent	Rapid7 Insight Agent, version 2.6.3 and prior, suffers from a local privilege escalation due to an uncontrolled DLL search path. Specifically, when Insight Agent 2.6.3 and prior starts, the Python interpreter attempts to load python3.dll at "C:\DLLs\python3.dll," which normally is writable by locally authenticated users. Because of this, a malicious local user could use Insight Agent's startup conditions to elevate to SYSTEM privileges. This issue was fixed in Rapid7 Insight Agent 2.6.4.	2019-07-12	not yet calculated	<a href="#">CVE-2019-5629</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">BUGTRAQ</a>
	The RzSurroundVADStreamingService (RzSurroundVADStreamingService.exe) in Razer			

razor -- surround	Surround 1.1.63.0 runs as the SYSTEM user using an executable located in %PROGRAMDATA%\Razer\Synapse\Devices\Razer Surround\Driver\. The DACL on this folder allows any user to overwrite contents of files in this folder, resulting in Elevation of Privilege.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13142</a> <a href="#">MISC</a>
realization -- concerto_critical_chain_planner	Realization Concerto Critical Chain Planner (aka CCPM) 5.10.8071 has SQL Injection in at least in the taskupdt/taskdetails.aspx webpage via the projectname parameter.	2019-07-12	not yet calculated	<a href="#">CVE-2019-13027</a> <a href="#">MISC</a>
red_hat -- openshift_container_platform	A reflected XSS vulnerability exists in authorization flow of OpenShift Container Platform versions: openshift-online-3, openshift-enterprise-3.4 through 3.7 and openshift-enterprise-3.9 through 3.11. An attacker could use this flaw to steal authorization data by getting them to click on a malicious link.	2019-07-11	not yet calculated	<a href="#">CVE-2019-3889</a> <a href="#">CONFIRM</a>
rockwell_automation -- panelview_5510	In Rockwell Automation PanelView 5510 (all versions manufactured before March 13, 2019 that have never been updated to v4.003, v5.002, or later), a remote, unauthenticated threat actor with access to an affected PanelView 5510 Graphic Display, upon successful exploit, may boot-up the terminal and gain root-level access to the device's file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10970</a> <a href="#">BID</a> <a href="#">MISC</a>
sap -- abap_server_and_abap_platform	ABAP Server and ABAP Platform (SAP Basis), versions, 7.31, 7.4, 7.5, do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0321</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (BI Workspace) (Enterprise), versions 4.1, 4.2, 4.3, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0326</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- commerce_cloud	SAP Commerce Cloud (previously known as SAP Hybris Commerce), (HY_COM, versions 6.3, 6.4, 6.5, 6.6, 6.7, 1808, 1811), allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0322</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- diagnostic_agent	The OS Command Plugin in the transaction GPA_ADMIN and the OSCommand Console of SAP Diagnostic Agent (LM-Service), version 7.2, allow an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0330</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- erp_hcm	SAP ERP HCM (SAP_HRCES), version 3, does not perform necessary authorization checks for a report that reads payroll data of employees in a certain area. Due to this under certain conditions, the user that once had authorization to payroll data of an employee, which was later revoked, may retain access to the same data.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0325</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- netweaver_application_server	Under certain conditions SAP NetWeaver Application Server for Java (Startup Framework), versions 7.21, 7.22, 7.45, 7.49, and 7.53, allows an attacker to access information which would otherwise be restricted.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0318</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- netweaver_for_java_application_server	SAP NetWeaver for Java Application Server - Web Container, (engineapi, versions 7.1, 7.2, 7.3, 7.31, 7.4 and 7.5), (servercode, versions 7.2, 7.3, 7.31, 7.4, 7.5), allows an attacker to upload files (including script files) without proper file format validation.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0327</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- netweaver_process_integration	ABAP Tests Modules (SAP Basis, versions 7.0, 7.1, 7.3, 7.31, 7.4, 7.5) of SAP NetWeaver Process Integration enables an attacker the execution of OS commands with privileged rights. An attacker could thereby impact the integrity and availability of the system.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0328</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- sap_gateway	The SAP Gateway, versions 7.5, 7.51, 7.52 and 7.53, allows an attacker to inject content which is displayed in the form of an error message. An attacker could thus mislead a user to believe this information is from the legitimate service when it's not.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0319</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- sapui5_and_openui5	SAPUI5 and OpenUI5, before versions 1.38.39, 1.44.39, 1.52.25, 1.60.6 and 1.63.0, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0281</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
schedmd -- slurm	SchedMD Slurm 17.11.x, 18.08.0 through 18.08.7, and 19.05.0 allows SQL Injection.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12838</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
siemens -- simatic_pcs_7_and_simatic_wincc_products	A vulnerability has been identified in SIMATIC PCS 7 V8.0 and earlier (All versions), SIMATIC PCS 7 V8.1 (All versions), SIMATIC PCS 7 V8.2 (All versions < V8.2 SP1 with WinCC V7.4 SP1 Upd11), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP2 with WinCC V7.4 SP1 Upd11), SIMATIC WinCC Professional (TIA Portal V13) (All versions), SIMATIC WinCC Professional (TIA Portal V14) (All versions), SIMATIC WinCC Professional (TIA Portal V15) (All versions), SIMATIC WinCC Runtime Professional V13 (All versions), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC V7.2 and earlier (All versions), SIMATIC WinCC V7.3 (All versions), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Upd 11), SIMATIC WinCC V7.5 (All versions < V7.5 Upd 3). The SIMATIC WinCC DataMonitor web application of the affected products allows to upload arbitrary ASPX code. The security vulnerability could be exploited by an authenticated attacker with network access to the WinCC DataMonitor application. No user interaction is required to exploit this vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the affected device. At the stage of publishing this security advisory no public exploitation is known.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10935</a> <a href="#">BID</a> <a href="#">MISC</a>
siemens -- siprotec_5_devices	A vulnerability has been identified in SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.90). All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions), DIGSI 5 engineering software (All versions < V7.90). Specially crafted packets sent to port 443/TCP could cause a Denial of Service condition.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10931</a> <a href="#">MISC</a>
siemens -- siprotec_5_devices	A vulnerability has been identified in SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.90). All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions), DIGSI 5 engineering software (All versions < V7.90). A remote attacker could use specially crafted packets sent to port 443/TCP to upload, download or delete files in certain parts of the file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10930</a> <a href="#">MISC</a>
	A vulnerability has been identified in Spectrum Power 3 (Corporate User Interface) (All versions <= v3.11), Spectrum Power 4 (Corporate User Interface) (Version v4.75), Spectrum Power 5 (Corporate User Interface) (All versions <= v5.50), Spectrum Power 7 (Corporate User Interface) (All versions <= v2.20). The web server could allow Cross-Site	2019-07-	not yet	<a href="#">CVE-2019-</a>

siemens -- spectrum_power_products	Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. The user does not need to be logged into the web interface in order for the exploitation to succeed. At the stage of publishing this security advisory no public exploitation is known.	11	calculated	<a href="#">10933</a> <a href="#">MISC</a>
siemens -- tia_administrator	A vulnerability has been identified in TIA Administrator (All versions < V1.0 SP1 Upd1). The integrated configuration web application (TIA Administrator) allows to execute certain application commands without proper authentication. The vulnerability could be exploited by an attacker with local access to the affected system. Successful exploitation requires no privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality and integrity and availability of the affected system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10915</a> <a href="#">BID</a> <a href="#">MISC</a>
snapview -- mikogo	The Windows versions of Snapview Mikogo, versions before 5.10.2 are affected by insecure implementations which allow local attackers to escalate privileges.	2019-07-12	not yet calculated	<a href="#">CVE-2019-12731</a> <a href="#">MISC</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager before 3.17.0 has a weak default of giving any unauthenticated user read permissions on the repository files and images.	2019-07-08	not yet calculated	<a href="#">CVE-2019-9630</a> <a href="#">MISC</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager before 3.17.0 establishes a default administrator user with weak defaults (fixed credentials).	2019-07-08	not yet calculated	<a href="#">CVE-2019-9629</a> <a href="#">MISC</a>
sony -- bravia_smart_tv_devices	Sony BRAVIA Smart TV devices allow remote attackers to cause a denial of service (device hang) via a crafted web page over HbbTV.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11889</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sony -- bravia_smart_tv_devices	Sony Bravia Smart TV devices allow remote attackers to cause a denial of service (device hang or reboot) via a SYN flood attack over a wired or Wi-Fi LAN.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11890</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
spiderlabs -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) 3.0.2. Use of X.Filename instead of X_Filename can bypass some PHP Script Uploads rules, because PHP automatically transforms dots into underscores in certain contexts where dots are invalid.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13464</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid 4.0.23 through 4.7. When checking Basic Authentication with HttpHeader: getAuth, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length isn't greater than the buffer, leading to a heap-based buffer overflow with user controlled data.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12527</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
squid-cache -- squid	An issue was discovered in Squid 3.3.9 through 3.5.28 and 4.x through 4.7. When Squid is configured to use Digest authentication, it parses the header Proxy-Authorization. It searches for certain tokens such as domain, uri, and qop. Squid checks if this token's value starts with a quote and ends with one. If so, it performs a memcpy of its length minus 2. Squid never checks whether the value is just a single quote (which would satisfy its requirements), leading to a memcpy of its length minus 1.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12525</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
squid-cache -- squid	An issue was discovered in Squid 2.x through 2.7.STABLE9, 3.x through 3.5.28, and 4.x through 4.7. When Squid is configured to use Basic Authentication, the Proxy-Authorization header is parsed via uuencode. uuencode determines how many bytes will be decoded by iterating over the input and checking its table. The length is then used to start decoding the string. There are no checks to ensure that the length it calculates isn't greater than the input buffer. This leads to adjacent memory being decoded as well. An attacker would not be able to retrieve the decoded data unless the Squid maintainer had configured the display of usernames on error pages.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12529</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
stopzilla -- stopzilla_antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x8000205F.	2019-07-09	not yet calculated	<a href="#">CVE-2018-15738</a> <a href="#">MISC</a> <a href="#">MISC</a>
sunnet -- wmprom	The SUNNET WMProm v5.0 and v5.1 for eLearning system has OS Command Injection via "teach/course/doajaxfileupload.php". The target server can be exploited without authentication.	2019-07-11	not yet calculated	<a href="#">CVE-2019-11062</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
swift -- alliance_web_platform	An issue was discovered in SWIFT Alliance Web Platform 7.1.23. A log injection (and an arbitrary log filename) can be achieved via the PATH_INFO to swp/login/EJBRemoteService/, related to com.swift.ejbgwt.j2ee.client.EJBInvocationException error log information containing null@java.comp/env/ error messages.	2019-07-05	not yet calculated	<a href="#">CVE-2018-16386</a> <a href="#">MISC</a>
symantec -- messaging_gateway	Symantec Messaging Gateway, prior to 10.7.1, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12751</a> <a href="#">BID</a> <a href="#">MISC</a>
thoughtspot -- thoughtspot	An authorization bypass vulnerability in pinboard updates in ThoughtSpot 4.4.1 through 5.1.1 (before 5.1.2) allows a low-privilege user with write access to at least one pinboard to corrupt pinboards of another user in the application by spoofing GUIDs in pinboard update requests, effectively deleting them.	2019-07-09	not yet calculated	<a href="#">CVE-2019-12782</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains multiple stack-based buffer overflows when processing user input for the setup wizard, allowing an unauthenticated user to execute arbitrary code. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13279</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 allows an unauthenticated attacker to execute setup wizard functionality, giving this attacker the ability to change configuration values, potentially leading to a denial of service. The request can be made on the local intranet or remotely if remote administration is enabled.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13277</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains multiple command injections when processing user input for the setup wizard, allowing an unauthenticated user to run arbitrary commands on the device. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13278</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains a stack-based buffer overflow in the ssi binary. The overflow allows an unauthenticated user to execute arbitrary code by providing a sufficiently long query string when POSTing to any valid cgi, txt, asp, or js file. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13276</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains a stack-based buffer overflow while returning an error message to the user about failure to resolve a hostname during a ping or traceroute attempt. This allows an authenticated user to execute arbitrary code. The exploit can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13280</a> <a href="#">MISC</a>
u.s._army -- america's_army_proving_grounds	An issue was discovered in the America's Army Proving Grounds platform for the Unreal Engine. With a false packet sent via UDP, the application server responds with several bytes, giving the possibility of DoS amplification, even being able to be used in DDoS attacks.	2019-07-10	not yet calculated	<a href="#">CVE-2018-10631</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
umbiquiti_networks -- edgemax_edgeswitch	Command Injection in EdgeMAX EdgeSwitch prior to 1.8.2 allow an Admin user to execute commands as root.	2019-07-10	not yet calculated	<a href="#">CVE-2019-5446</a> <a href="#">MISC</a>



umbiquiti_networks -- edgemax_edgeswitch	DoS in EdgeMAX EdgeSwitch prior to 1.8.2 allow an Admin user to Crash the SSH CLI interface by using crafted commands.	2019-07-10	not yet calculated	<a href="#">CVE-2019-5445</a> MISC
vmware -- esxi	VMware ESXi 6.5 suffers from partial denial of service vulnerability in hostd process. Patch ESXi650-201907201-UG for this issue is available.	2019-07-11	not yet calculated	<a href="#">CVE-2019-5528</a> BID CONFIRM
wavpack -- wavpack	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseWave64HeaderConfig (wave64.c:211). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit <a href="https://github.com/dbry/WavPack/commit/33a0025d1d63ccd05d9dbaa6923d52b1446a62fe">https://github.com/dbry/WavPack/commit/33a0025d1d63ccd05d9dbaa6923d52b1446a62fe</a> .	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010319</a> MISC
wavpack -- wavpack	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseCaffHeaderConfig (caff.c:486). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit <a href="https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b">https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b</a> .	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010317</a> MISC
wavpack -- wavpack	WavPack 5.1 and earlier is affected by: CWE 369: Divide by Zero. The impact is: Divide by zero can lead to sudden crash of a software/service that tries to parse a .wav file. The component is: ParseDsdiffHeaderConfig (dsdiff.c:282). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit <a href="https://github.com/dbry/WavPack/commit/4c0faba32fddbd0745cbfaf1e1aeb3da5d35b9fc">https://github.com/dbry/WavPack/commit/4c0faba32fddbd0745cbfaf1e1aeb3da5d35b9fc</a> .	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010315</a> MISC
weseek -- growi	In WESEEK GROWI before 3.5.0, the site-wide basic authentication can be bypassed by adding a URL parameter access_token (this is the parameter used by the API). No valid token is required since it is not validated by the backend. The website can then be browsed as if no basic authentication is required.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13337</a> MISC
weseek -- growi	In WESEEK GROWI before 3.5.0, a remote attacker can obtain the password hash of the creator of a page by leveraging wiki access to make API calls for page metadata. In other words, the password hash can be retrieved even though it is not a publicly available field.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13338</a> MISC
wolfvision -- cynap	WolfVision Cynap before 1.30j uses a static, hard-coded cryptographic secret for generating support PINs for the 'forgot password' feature. By knowing this static secret and the corresponding algorithm for calculating support PINs, an attacker can reset the ADMIN password and thus gain remote access.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13352</a> MISC FULLDISC
wordpress -- wordpress	The Rencontre plugin before 3.1.3 for WordPress allows SQL Injection via inc/rencontre_widget.php.	2019-07-08	not yet calculated	<a href="#">CVE-2019-13413</a> MISC
wordpress -- wordpress	The Rencontre plugin before 3.1.3 for WordPress allows XSS via inc/rencontre_widget.php.	2019-07-08	not yet calculated	<a href="#">CVE-2019-13414</a> MISC
zeromq -- libzmq	In ZeroMQ libzmq before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.3.2, a remote, unauthenticated client connecting to a libzmq application, running with a socket listening with CURVE encryption/authentication enabled, may cause a stack overflow and overwrite the stack with arbitrary data, due to a buffer overflow in the library. Users running public servers with the above configuration are highly encouraged to upgrade as soon as possible, as there are no known mitigations.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13132</a> MIST CONFIRM CONFIRM MIST BUGTRAQ UBUNTU DEBIAN
zoho_manageengine -- assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via the SearchN.do search field.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12537</a> MISC
zoho_manageengine -- servicedesk_plus	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 10.5. There is XSS via the WorkOrder.do search field.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12540</a> MISC
zoom_video_communications -- zoom_client	In the Zoom Client before 4.4.2 on macOS, remote attackers can cause a denial of service (continual focus grabs) via a sequence of invalid launch?action=join&confno= requests to localhost port 19421.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13449</a> MISC MISC MISC MISC
zoom_video_communications -- zoom_client	The Zoom Client before 4.4.53932.0709 on macOS allows remote code execution, a different vulnerability than CVE-2019-13450. If the ZoomOpener daemon (aka the hidden web server) is running, but the Zoom Client is not installed or can't be opened, an attacker can remotely execute code with a maliciously crafted launch URL. NOTE: ZoomOpener is removed by the Apple Malware Removal Tool (MRT) if this tool is enabled and has the 2019-07-10 MRTConfigData.	2019-07-12	not yet calculated	<a href="#">CVE-2019-13567</a> MISC MISC MISC MISC
zoom_video_communications -- zoom_client_and_ringcentral	In the Zoom Client through 4.4.4 and RingCentral 7.0.136380.0312 on macOS, remote attackers can force a user to join a video call with the video camera active. This occurs because any web site can interact with the Zoom web server on localhost port 19421 or 19424. NOTE: a machine remains vulnerable if the Zoom Client was installed in the past and then uninstalled. Blocking exploitation requires additional steps, such as the ZDisableVideo preference and/or killing the web server, deleting the ~/.zoomus directory, and creating a ~/.zoomus plain file.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13450</a> BID MISC MISC MISC MISC MISC MISC
zte -- mw_nr8000	ZTE MW NR8000V2.4.4.03 and NR8000V2.4.4.04 are impacted by path traversal vulnerability. Due to path traversal, users can download any files.	2019-07-11	not yet calculated	<a href="#">CVE-2019-3415</a> MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notified call-on-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nrcis.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED

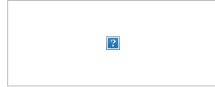


#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)



From: [US-CERT](#)  
To: [a\\_tarte@cs.mty.ale.ca.us](#)  
Subject: Vulnerability Summary for the Week of July 8, 2019  
Date: Monday, July 15, 2019 2:18:04 PM



National Cyber Awareness System:

## Vulnerability Summary for the Week of July 8, 2019

07/15/2019 06:26 AM EDT

Original release date: July 15, 2019

The CISA Weekly Vulnerability Summary Bulletin is created using information from the [NIST NVD](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit the [NIST NVD](#) for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
contao -- contao	Contao 4.x allows SQL Injection. Fixed in Contao 4.4.39 and Contao 4.7.5.	2019-07-09	7.5	<a href="#">CVE-2019-11512</a> MISC
dlink -- central_wifimanager	/web/Lib/Action/IndexAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to execute arbitrary PHP code via a cookie because a cookie's username field allows eval injection, and an empty password bypasses authentication.	2019-07-06	7.5	<a href="#">CVE-2019-13372</a> MISC CONFIRM MISC
dlink -- central_wifimanager	An issue was discovered in the D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6. Input does not get validated and arbitrary SQL statements can be executed in the database via the /web/Public/Conn.php parameter dbSQL.	2019-07-06	7.5	<a href="#">CVE-2019-13373</a> MISC CONFIRM MISC
dlink -- central_wifimanager	A SQL Injection was discovered in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 in PayAction.class.php with the index.php/Pay/passcodeAuth parameter passcode. The vulnerability does not need any authentication.	2019-07-06	7.5	<a href="#">CVE-2019-13375</a> MISC CONFIRM MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow remote attackers to execute arbitrary commands via shell metacharacters in the online_firmware_check.cgi check_fw_url parameter.	2019-07-11	10.0	<a href="#">CVE-2019-13561</a> MISC MISC MISC
dlink -- dir-818lw_firmware	An issue was discovered on D-Link DIR-818LW devices with firmware 2.06betab01. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the MTU field to SetWanSettings.	2019-07-10	9.0	<a href="#">CVE-2019-13481</a> BID MISC
dlink -- dir-818lw_firmware	An issue was discovered on D-Link DIR-818LW devices with firmware 2.06betab01. There is a command injection in HNAP1 (exploitable with Authentication) via shell metacharacters in the Type field to SetWanSettings.	2019-07-10	10.0	<a href="#">CVE-2019-13482</a> BID MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices allow remote attackers to execute arbitrary commands via a crafted parameter to a CGI script, as demonstrated by sed injection in cgi-bin/camctrl_save_profile.cgi (save parameter) and cgi-bin/ddns.cgi.	2019-07-07	9.0	<a href="#">CVE-2019-13398</a> MISC
google -- android	In ihexvd_sao_shift_ctb of ihexvd_sao.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130023983.	2019-07-08	9.3	<a href="#">CVE-2019-2106</a> CONFIRM
google -- android	In ihexvd_parse_pps of ihexvd_parse_headers.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-130024844.	2019-07-08	9.3	<a href="#">CVE-2019-2107</a> CONFIRM
google -- android	In MakeMPEG4VideoCodecSpecificData of AVIExtractor.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1. Android ID: A-130651570.	2019-07-08	9.3	<a href="#">CVE-2019-2109</a> CONFIRM
google -- android	In loop of DnsTlsSocket.cpp, there is a possible heap memory corruption due to a use after free. This could lead to remote code execution in the net server with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122856181.	2019-07-08	7.5	<a href="#">CVE-2019-2111</a> CONFIRM
google -- android	In several functions of alarm.cc, there is possible memory corruption due to a use after free. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-117997080.	2019-07-08	7.2	<a href="#">CVE-2019-2112</a> CONFIRM
hidea -- az_admin	hidea.com AZ Admin 1.0 has news_det.php?cod= SQL Injection.	2019-07-11	7.5	<a href="#">CVE-2019-13507</a> MISC
hsycms -- hsycms	An issue was discovered in Hsycms V1.1. There is a SQL injection vulnerability via a /news/" .html page.	2019-07-10	7.5	<a href="#">CVE-2019-10653</a> MISC
oniguruma_project -- oniguruma	A use-after-free in onig_new_deluxe() in regext.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.	2019-07-10	7.5	<a href="#">CVE-2019-13224</a> CONFIRM
strong_password_project -- strong_password	The strong_password gem 0.0.7 for Ruby, as distributed on RubyGems.org, included a code-execution backdoor inserted by a third party. The current version, without this backdoor, is 0.0.6.	2019-07-08	7.5	<a href="#">CVE-2019-13354</a> MISC MISC MISC MISC
teclib-edition -- fields	An issue was discovered in the Teclib Fields plugin through 1.9.2 for GLPI. It allows SQL Injection via container_id and old_order parameters to ajax/reorder.php by an unauthenticated user.	2019-07-10	7.5	<a href="#">CVE-2019-12723</a> MISC MISC CONFIRM
trape_project -- trape	Trape through 2019-05-08 has SQL injection via the data[2] variable in core/db.py, as demonstrated by the /bs t parameter.	2019-07-10	7.5	<a href="#">CVE-2019-13489</a> MISC
typo3 -- typo3	TYPO3 8.x through 8.7.26 and 9.x through 9.5.7 allows Deserialization of Untrusted Data.	2019-07-09	7.5	<a href="#">CVE-2019-12747</a> CONFIRM
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow Remote Command Injection, related to BusyBox and wget.	2019-07-10	10.0	<a href="#">CVE-2018-14494</a> MISC MISC
vivotek -- fd8136_firmware	Vivotek FD8136 devices allow Remote Command Injection, aka "another command injection vulnerability in our target device," a different issue than CVE-2018-14494.	2019-07-10	10.0	<a href="#">CVE-2018-14495</a> MISC MISC
	Vivotek FD8136 devices allow remote memory corruption and remote code execution because of a			<a href="#">CVE-2018-14496</a>

vivotek -- fd8136_firmware	stack-based buffer overflow, related to sprintf, vlocal_buff_4326, and set_getparam.cgi.	2019-07-10	7.5	MISC MISC
yoast -- yoast_seo	The Yoast SEO plugin before 11.6-RC5 for WordPress does not properly restrict unfiltered HTML in term descriptions.	2019-07-09	7.5	CVE-2019-13478 MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alsa-project -- alsa	posix/JackSocket.cpp in libjack in JACK2 1.9.1 through 1.9.12 (as distributed with alsa-plugins 1.1.7 and later) has a "double file descriptor close" issue during a failed connection attempt when jackd2 is not running. Exploitation success depends on multithreaded timing of that double close, which can result in unintended information disclosure, crashes, or file corruption due to having the wrong file associated with the file descriptor.	2019-07-05	6.8	CVE-2019-13351 MISC MISC
apachefriends -- xampp	lart.php in XAMPP 1.7.0 has XSS, a related issue to CVE-2008-3569.	2019-07-09	4.3	CVE-2019-8920 BID MISC
cesanta -- mongoose	mq_parse_http in mongoose.c in Mongoose 6.15 has a heap-based buffer over-read.	2019-07-10	5.0	CVE-2019-13503 MISC MISC
cisco -- unified_communications_manager	A vulnerability in the Session Initiation Protocol (SIP) protocol implementation of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of input SIP traffic. An attacker could exploit this vulnerability by sending a malformed SIP packet to an affected Cisco Unified Communications Manager. A successful exploit could allow the attacker to trigger a new registration process on all connected phones, temporarily disrupting service.	2019-07-05	5.0	CVE-2019-1887 CISCO
codedoc_project -- codedoc	Codedoc v3.2 has a stack-based buffer overflow in add_variable in codedoc.c, related to codedoc_strncpy.	2019-07-06	6.8	CVE-2019-13362 MISC
crudlab -- wp_like_button	An authentication bypass vulnerability in the CRUDLab WP Like Button plugin through 1.6.0 for WordPress allows unauthenticated attackers to change settings. The contains() function in wp_like_button.php did not check if the current request is made by an authorized user, thus allowing any unauthenticated user to successfully update settings, as demonstrated by the wp-admin/admin.php?page=facebook-like-button each_page_url or code_snippet parameter.	2019-07-05	5.0	CVE-2019-13344 MISC MISC MISC
custom4web -- wp_open_graph	Cross-site request forgery (CSRF) vulnerability in WP Open Graph 1.6.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5960 JVN
digisol -- dg-hr-3300_firmware	Digisol Wireless Wifi Home Router HR-3300 allows XSS via the userid or password parameter to the admin login page.	2019-07-05	4.3	CVE-2018-14027 MISC
dlink -- central_wifimanager	A cross-site scripting (XSS) vulnerability in resource view in PayAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to inject arbitrary web script or HTML via the index.php/Pay/passcodeAuth passcode parameter.	2019-07-06	4.3	CVE-2019-13374 MISC CONFIRM MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow remote attackers to force a blank password via the apply_sec.cgi setup_wizard parameter.	2019-07-11	5.0	CVE-2019-13560 MISC MISC MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow XSS, as demonstrated by the /www/ping_response.cgi ping_ipaddr parameter, the /www/ping6_response.cgi ping6_ipaddr parameter, and the /www/apply_sec.cgi html_response_return_page parameter.	2019-07-11	4.3	CVE-2019-13562 MISC MISC MISC
dlink -- dir-655_firmware	D-Link DIR-655 C devices before 3.02B05 BETA03 allow CSRF for the entire management console.	2019-07-11	6.8	CVE-2019-13563 MISC MISC MISC
dropbox -- dropbox	Dropbox.exe (and QtWebEngineProcess.exe in the Web Helper) in the Dropbox desktop application 71.4.108.0 store cleartext credentials in memory upon successful login or new account creation. These are not securely freed in the running process.	2019-07-08	4.3	CVE-2019-12171 MISC MISC
dwbooster -- appointment_hour_booking	The Appointment Hour Booking plugin 1.1.44 for WordPress allows XSS via the E-mail field, as demonstrated by email_1.	2019-07-11	4.3	CVE-2019-13505 MISC MISC
enhancesoft -- osticket	Unauthenticated Stored XSS in oSTicket 1.10.1 allows a remote attacker to gain admin privileges by injecting arbitrary web script or HTML via arbitrary file extension while creating a support ticket.	2019-07-09	4.3	CVE-2019-13397 MISC
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/switch.php has an Open Redirect via the current_page parameter.	2019-07-05	5.8	CVE-2018-12621 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. htdocs/ajax/update.php has XSS via the field_name parameter.	2019-07-10	4.3	CVE-2018-12622 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. htdocs/switch.php has XSS via the current_page parameter.	2019-07-10	4.3	CVE-2018-12623 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/validate.php has XSS via the values parameter.	2019-07-10	4.3	CVE-2018-12625 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/popup.php has XSS via the cat parameter.	2019-07-10	4.3	CVE-2018-12626 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/list.php has XSS via the show_notification_list_issues or show_authorized_issues parameter.	2019-07-10	4.3	CVE-2018-12627 MISC CONFIRM
eventum_project -- eventum	An issue was discovered in Eventum 3.5.0. CSRF in htdocs/manage/users.php allows creating another user with admin privileges.	2019-07-10	6.8	CVE-2018-12628 MISC CONFIRM
exiv2 -- exiv2	There is an out-of-bounds read in Exiv2::MrwImage::readMetadata in mrwimage.cpp in Exiv2 through 0.27.2.	2019-07-10	4.3	CVE-2019-13504 BID MISC MISC
ffmpeg -- ffmpeg	In FFmpeg 4.1.3, there is a division by zero at adx_write_trailer in libavformat/rawenc.c. This may be related to two NULL pointers passed as arguments at libavcodec/frame_thread_encoder.c.	2019-07-07	4.3	CVE-2019-13390 BID MISC MISC MISC MISC
fla-shop -- html5_maps	Cross-site request forgery (CSRF) vulnerability in HTML5 Maps 1.6.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	CVE-2019-5983 MISC MISC MISC
flarum -- flarum	Flarum before 0.1.0-beta.9 allows CSRF against all POST endpoints, as demonstrated by changing admin settings.	2019-07-07	6.8	CVE-2019-13183 CONFIRM MISC CONFIRM
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices have a hard-coded SSL/TLS key that is used during an	2019-07-07	4.3	CVE-2019-13399

	administrator's SSL conversation.			MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 use /etc/appWeb/appweb.pass to store administrative web-interface credentials in cleartext. These credentials can be retrieved via cgi-bin/getuserinfo.cgi?mode=info.	2019-07-07	5.0	<a href="#">CVE-2019-13400</a> MISC
fortinet -- fcm-mb40_firmware	Dynacolor FCM-MB40 v1.2.0.0 devices have CSRF in all scripts under cgi-bin/.	2019-07-07	6.8	<a href="#">CVE-2019-13401</a> MISC
fortinet -- fcm-mb40_firmware	/usr/sbin/default.sh and /usr/apache/htdocs/cgi-bin/admin/hardfactorydefault.cgi on Dynacolor FCM-MB40 v1.2.0.0 devices implement an incomplete factory-reset process. A backdoor can persist because neither system accounts nor the set of services is reset.	2019-07-07	6.5	<a href="#">CVE-2019-13402</a> MISC
gitea -- gitea	Gitea 1.7.2, 1.7.3 is affected by: Cross Site Scripting (XSS). The impact is: execute JavaScript in victim's browser, when the vulnerable repo page is loaded. The component is: repository's description. The attack vector is: victim must navigate to public and affected repo page.	2019-07-11	4.3	<a href="#">CVE-2019-1010314</a> MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is a persistent XSS vulnerability in the environment pages due to a lack of input validation and output encoding.	2019-07-10	4.3	<a href="#">CVE-2018-19493</a> BID CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access vulnerability that allows an unauthorized user to view private group names.	2019-07-10	4.0	<a href="#">CVE-2018-19494</a> CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an SSRF vulnerability in the Prometheus integration.	2019-07-10	4.0	<a href="#">CVE-2018-19495</a> CONFIRM MISC
gitlab -- gitlab	An issue was discovered in GitLab Community and Enterprise Edition 10.x and 11.x before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an incorrect access control vulnerability that permits a user with insufficient privileges to promote a project milestone to a group milestone.	2019-07-10	4.0	<a href="#">CVE-2018-19496</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.8 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an authorization vulnerability that allows access to the web-UI as a user using a Personal Access Token of any scope.	2019-07-10	6.5	<a href="#">CVE-2018-19569</a> BID CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.18 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an SSRF vulnerability in webhooks.	2019-07-10	4.0	<a href="#">CVE-2018-19571</a> MISC MISC
gitlab -- gitlab	GitLab CE 8.17 and later and EE 8.3 and later have a symlink time-of-check-to-time-of-use race condition that would allow unauthorized access to files in the GitLab Pages chroot environment. This is fixed in versions 11.5.1, 11.4.8, and 11.3.11.	2019-07-10	4.3	<a href="#">CVE-2018-19572</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 10.1 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an insecure direct object reference issue that allows a user to make comments on a locked issue.	2019-07-10	4.0	<a href="#">CVE-2018-19575</a> BID CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an access control issue that allows a Guest user to make changes to or delete their own comments on an issue, after the issue was made Confidential.	2019-07-10	6.4	<a href="#">CVE-2018-19576</a> MISC MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an incorrect access control vulnerability that displays to an unauthorized user the title and namespace of a confidential issue.	2019-07-10	5.0	<a href="#">CVE-2018-19577</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, version 11.5 before 11.5.1, is vulnerable to an insecure object reference issue that permits a user with Reporter privileges to view the Jaeger Tracing Operations page.	2019-07-10	4.0	<a href="#">CVE-2018-19578</a> CONFIRM MISC
gitlab -- gitlab	All versions of GitLab prior to 11.5.1, 11.4.8, and 11.3.11 do not send an email to the old email address when an email address change is made.	2019-07-10	5.0	<a href="#">CVE-2018-19580</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 8.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure object reference vulnerability that allows a Guest user to set the weight of an issue they create.	2019-07-10	5.0	<a href="#">CVE-2018-19581</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 11.4 before 11.4.8 and 11.5 before 11.5.1, is affected by an insecure direct object reference vulnerability that permits an unauthorized user to publish the draft merge request comments of another user.	2019-07-10	4.0	<a href="#">CVE-2018-19582</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 8.0 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, would log access tokens in the Workhorse logs, permitting administrators with access to the logs to see another user's token.	2019-07-10	4.0	<a href="#">CVE-2018-19583</a> CONFIRM MISC
gitlab -- gitlab	GitLab EE, versions 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, is vulnerable to an insecure direct object reference vulnerability that allows authenticated, but unauthorized, users to view members and milestone details of private groups.	2019-07-10	5.0	<a href="#">CVE-2018-19584</a> CONFIRM MISC
google -- android	In FileInputStream::Read of file_input_stream.cc, there is a possible memory corruption due to uninitialized data. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-116114182.	2019-07-08	6.8	<a href="#">CVE-2019-2105</a> CONFIRM
google -- android	In save_attr_seq of sdp_discovery.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-117105007.	2019-07-08	5.0	<a href="#">CVE-2019-2116</a> CONFIRM
helpy.io -- helpy	Helpy before 2.2.0 allows agents to edit admins.	2019-07-10	6.5	<a href="#">CVE-2018-20851</a> MISC MISC
ibm -- cloud_application_performance_management	IBM Application Performance Management (IBM Monitoring 8.1.4) could allow a remote attacker to induce the application to perform server-side DNS lookups of arbitrary domain names. IBM X-Force ID: 158270.	2019-07-11	5.0	<a href="#">CVE-2019-4131</a> XF CONFIRM
ibm -- jazz_for_service_management	IBM Jazz for Service Management 1.1.3 and 1.1.3.2 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-force ID: 159032.	2019-07-11	5.0	<a href="#">CVE-2019-4193</a> CONFIRM XF
idoors -- idoors_reader	iDoors Reader 2.10.17 and earlier allows an attacker on the same network segment to bypass authentication to access the management console and operate the product via unspecified vectors.	2019-07-05	5.8	<a href="#">CVE-2019-5964</a> MISC MISC
ignitedcms_project -- ignitedcms	index.php/admin/permissions in Ignited CMS through 2017-02-19 allows CSRF to add an administrator.	2019-07-06	6.8	<a href="#">CVE-2019-13370</a> MISC
imagemagick -- imagemagick	In ImageMagick 7.0.8-50 Q16, ComplexImages in MagickCore/fourier.c has a heap-based buffer over-read because of incorrect calls to GetCacheView/VirtualPixels.	2019-07-07	6.8	<a href="#">CVE-2019-13391</a> MISC MISC MISC
imagemagick -- imagemagick	ImageMagick 7.0.8-54 Q16 allows Division by Zero in RemoveDuplicateLayers in MagickCore/layer.c.	2019-07-09	4.3	<a href="#">CVE-2019-13454</a> BID MISC MISC MISC
intersystems -- cache	InterSystems Cache 2017.2.2.865.0 allows XSS.	2019-07-11	4.3	<a href="#">CVE-2018-17150</a> MISC
intersystems -- cache	InterSystems Cache 2017.2.2.865.0 has Incorrect Access Control.	2019-07-11	5.5	<a href="#">CVE-2018-17151</a> MISC
intersystems -- cache	InterSystems Cache 2017.2.2.865.0 allows XXE.	2019-07-11	5.5	<a href="#">CVE-2018-17152</a> MISC
invoxia -- nvx220_firmware	Invoxia NVX220 devices allow access to /bin/sh via escape from a restricted CLI, leading to disclosure of password hashes.	2019-07-05	5.0	<a href="#">CVE-2018-14529</a> MISC
loruri -- loruri_cms_2017	Cross-site scripting vulnerability in Loruri CMS 2017 Release2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	<a href="#">CVE-2019-5967</a> MISC MISC

jururi -- jururi_mail	Open redirect vulnerability in Jururi Mail 2.1.4 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-07-05	5.8	<a href="#">CVE-2019-5965</a> MISC MISC
jururi -- jururi_mail	Joruri Mail 2.1.4 and earlier does not properly manage sessions, which allows remote attackers to impersonate an arbitrary user and alter/disclose the information via unspecified vectors.	2019-07-05	5.8	<a href="#">CVE-2019-5966</a> MISC MISC
keynto -- team_password_manager	KEYNTO Team Password Manager 1.5.0 allows XSS because data saved from websites is mishandled in the online vault.	2019-07-09	4.3	<a href="#">CVE-2019-13380</a> FULLDISC
libpng -- libpng	An issue has been found in third-party PNM decoding associated with libpng 1.6.35. It is a stack-based buffer overflow in the function get_token in pnm2png.c in pnm2png.	2019-07-10	6.8	<a href="#">CVE-2018-14550</a> MISC MISC
mailvelope -- mailvelope	Mailvelope prior to 3.1.0 is vulnerable to a clickjacking attack against the settings page. As the settings page is intended to be accessible from web applications, the browser's extension isolation mechanisms are disabled (web_accessible_resources). Mailvelope implements additional measures to prevent web applications from directly embedding the settings page, but this mechanism can be bypassed.	2019-07-09	4.3	<a href="#">CVE-2019-9147</a> CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 accepts or operates with invalid PGP public keys: Mailvelope allows importing keys that contain users without a valid self-certification. Keys that are obviously invalid are not rejected during import. An attacker that is able to get a victim to import a manipulated key could claim to have signed a message that originates from another person.	2019-07-09	4.3	<a href="#">CVE-2019-9148</a> CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 allows private key operations without user interaction via its client-API. By modifying an URL parameter in Mailvelope, an attacker is able to sign (and encrypt) arbitrary messages with Mailvelope, assuming the private key password is cached. A second vulnerability allows an attacker to decrypt an arbitrary message when the GnuPG backend is used in Mailvelope.	2019-07-09	6.4	<a href="#">CVE-2019-9149</a> CONFIRM
mailvelope -- mailvelope	Mailvelope prior to 3.3.0 does not require user interaction to import public keys shown on web page. This functionality can be tricked to either hide a key import from the user or obscure which key was imported.	2019-07-09	5.0	<a href="#">CVE-2019-9150</a> CONFIRM
mastodon-tootdon -- tootdon_for_mastodon	The Android App 'Tootdon for Mastodon' version 3.4.1 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-07-05	5.8	<a href="#">CVE-2019-5961</a> MISC MISC
mediawiki -- mediawiki	Wikimedia MediaWiki through 1.32.1 allows CSRF.	2019-07-10	6.8	<a href="#">CVE-2019-12466</a> CONFIRM MISC BUGTRAQ DEBIAN
mediawiki -- mediawiki	Wikimedia MediaWiki 1.23.0 through 1.32.1 has an information leak. Privileged API responses that include whether a recent change has been patrolled may be cached publicly. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	5.0	<a href="#">CVE-2019-12474</a> CONFIRM MISC BUGTRAQ DEBIAN
odoo -- odoo	The Odoo Community Association (OCA) dbfilter_from_header module makes Odoo 8.x, 9.x, 10.x, and 11.x vulnerable to ReDoS (regular expression denial of service) under certain circumstances.	2019-07-05	5.0	<a href="#">CVE-2018-14733</a> CONFIRM MISC MISC MISC
oniguruma_project -- oniguruma	A NULL Pointer Dereference in match_at() in regex.c in Oniguruma 6.9.2 allows attackers to potentially cause denial of service by providing a crafted regular expression. Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.	2019-07-10	5.0	<a href="#">CVE-2019-13225</a> CONFIRM
opencats -- opencats	lib/DocumentToText.php in OpenCats before 0.9.4-3 has XXE that allows remote users to read files on the underlying operating system. The attacker must upload a file in the docx or odt format.	2019-07-05	4.3	<a href="#">CVE-2019-13358</a> MISC MISC MISC
otrs -- otrs	An issue was discovered in Open Ticket Request System (OTRS) 6.0.x through 6.0.7. A carefully constructed email could be used to inject and execute arbitrary stylesheet or JavaScript code in a logged in customer's browser in the context of the OTRS customer panel application.	2019-07-08	4.9	<a href="#">CVE-2018-11563</a> CONFIRM CONFIRM MISC
paypal -- adaptive_payments_sdk	paypal/adaptivepayments-sdk-php v3.9.2 is vulnerable to a reflected XSS in the SetPaymentOptions.php resulting code execution	2019-07-10	4.3	<a href="#">CVE-2017-6217</a> MISC
phpwind -- phpwind	PHPWind 9.1.0 has XSS vulnerabilities in the c and m parameters of the index.php file.	2019-07-09	4.3	<a href="#">CVE-2019-13472</a> MISC
pingidentity -- agentless_integration_kit	XSS exists in Ping Identity Agentless Integration Kit before 1.5.	2019-07-11	4.3	<a href="#">CVE-2019-13564</a> CONFIRM
pyxtrlock_project -- pyxtrlock	pyxtrlock 0.3 and earlier is affected by: Incorrect Access Control. The impact is: False locking impression when run in a non-X11 session. The fixed version is: 0.4.	2019-07-11	4.6	<a href="#">CVE-2019-1010316</a> MISC
sap -- information_steward	SAP Information Steward, version 4.2, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	4.3	<a href="#">CVE-2019-0329</a> BID MISC CONFIRM
sony -- vaio_update	Improper authorization vulnerability in VAIO Update 7.3.0.03150 and earlier allows an attackers to execute arbitrary executable file with administrative privilege via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5981</a> MISC MISC
sony -- vaio_update	Improper download file verification vulnerability in VAIO Update 7.3.0.03150 and earlier allows remote attackers to conduct a man-in-the-middle attack via a malicious wireless LAN access point. A successful exploitation may result in a malicious file being downloaded/executed.	2019-07-05	5.4	<a href="#">CVE-2019-5982</a> MISC MISC
squid-cache -- squid	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.	2019-07-05	4.3	<a href="#">CVE-2019-13345</a> MISC MISC MLIST
sukimalab -- attendance_manager	Cross-site scripting vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	<a href="#">CVE-2019-5970</a> MISC MISC MISC MISC
sukimalab -- attendance_manager	Cross-site request forgery (CSRF) vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5971</a> MISC MISC MISC MISC
sukimalab -- online_lesson_booking	Cross-site scripting vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	<a href="#">CVE-2019-5972</a> MISC MISC MISC
teclib-edition -- fields	An issue was discovered in the Teclib News plugin through 1.5.2 for GLPI. It allows a stored XSS attack via the \$_POST[name] parameter.	2019-07-10	4.3	<a href="#">CVE-2019-12724</a> MISC MISC CONFIRM
trape_project -- trape	A cross-site scripting (XSS) vulnerability in static/js/trape.js in Trape through 2019-05-08 allows remote attackers to inject arbitrary web script or HTML via the country, query, or refer parameter to the /register URI, because the jQuery prepend() method is used.	2019-07-10	4.3	<a href="#">CVE-2019-13488</a> MISC
typo3 -- typo3	TYPO3 8.3.0 through 8.7.26 and 9.0.0 through 9.5.7 allows XSS.	2019-07-09	4.3	<a href="#">CVE-2019-12748</a> CONFIRM
waspthemes -- custom_css_pro	Cross-site request forgery (CSRF) vulnerability in Custom CSS Pro 1.0.3 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5984</a> MISC MISC MISC



wesseek -- growi	Cross-site request forgery (CSRF) vulnerability in GROWI v3.4.6 and earlier allows remote attackers to hijack the authentication of administrators via updating user's 'Basic Info'.	2019-07-05	6.8	<a href="#">CVE-2019-5968</a> MISC MISC
wesseek -- growi	Open redirect vulnerability in GROWI v3.4.6 and earlier allows remote attackersto redirect users to arbitrary web sites and conduct phishing attacks via the process of login.	2019-07-05	5.8	<a href="#">CVE-2019-5969</a> MISC MISC
wikindx_project -- wikindx	A cross-site scripting (XSS) vulnerability in noMenu() and noSubMenu() in core/navigation/MENU.php in WIKINDX prior to version 5.8.1 allows remote attackers to inject arbitrary web script or HTML via the method parameter.	2019-07-08	4.3	<a href="#">CVE-2019-12930</a> CONFIRM CONFIRM CONFIRM
zoho -- salesiq	Cross-site scripting vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	4.3	<a href="#">CVE-2019-5962</a> MISC MISC
zoho -- salesiq	Cross-site request forgery (CSRF) vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5963</a> MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via the RCSettings.do rdsName parameter.	2019-07-11	4.3	<a href="#">CVE-2019-12595</a> MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via SoftwareListView.do with the parameter swType or swComplianceType.	2019-07-11	4.3	<a href="#">CVE-2019-12596</a> MISC MISC
zohocorp -- manageengine_assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via ResourcesAttachments.jsp with the parameter pageName.	2019-07-11	4.3	<a href="#">CVE-2019-12597</a> MISC MISC
zohocorp -- manageengine_servicedesk_plus	An issue was discovered in the Purchase component of Zoho ManageEngine ServiceDesk Plus. There is XSS via the SearchN.do search field, a different vulnerability than CVE-2019-12189.	2019-07-11	4.3	<a href="#">CVE-2019-12539</a> MISC MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/page-edit.php (content box), which can be used to get a user's cookie.	2019-07-05	3.5	<a href="#">CVE-2019-13339</a> MISC
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the content box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, CVE-2018-20520, and CVE-2019-13186.	2019-07-05	3.5	<a href="#">CVE-2019-13340</a> MISC
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/conf.php (comment box), which can be used to get a user's cookie.	2019-07-05	3.5	<a href="#">CVE-2019-13341</a> MISC
cyberpowersystems -- powerpanel	A stored XSS vulnerability in the Agent/Center component of CyberPower PowerPanel Business Edition 3.4.0 allows a privileged attacker to embed malicious JavaScript in the SNMP trap receivers form. Upon visiting the /agent/action_recipient Event Action/Recipient page, the embedded code will be executed in the browser of the victim.	2019-07-09	3.5	<a href="#">CVE-2019-13070</a> MISC MISC
gitlab -- gitlab	GitLab CE/EE, versions 11.3 before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via unrecognized HTML tags.	2019-07-10	3.5	<a href="#">CVE-2018-19570</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 10.3 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in Markdown fields via Mermaid.	2019-07-10	3.5	<a href="#">CVE-2018-19573</a> CONFIRM MISC
gitlab -- gitlab	GitLab CE/EE, versions 7.6 up to 11.x before 11.3.11, 11.4 before 11.4.8, and 11.5 before 11.5.1, are vulnerable to an XSS vulnerability in the OAuth authorization page.	2019-07-10	3.5	<a href="#">CVE-2018-19574</a> MISC MISC
gitlab -- gitlab	GitLab EE version 11.5 is vulnerable to a persistent XSS vulnerability in the Operations page. This is fixed in 11.5.1.	2019-07-10	3.5	<a href="#">CVE-2018-19579</a> CONFIRM MISC
google -- android	In HIDL, safe_union, and other C++ structs/unions being sent to application processes, there are uninitialized fields. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-131356202	2019-07-08	2.1	<a href="#">CVE-2019-2104</a> CONFIRM
google -- android	In setup wizard there is a bypass of some checks when wifi connection is skipped. This could lead to factory reset protection bypass with no additional privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122597079.	2019-07-08	2.1	<a href="#">CVE-2019-2113</a> CONFIRM
google -- android	In checkQueryPermission of TelephonyProvider.java, there is a possible disclosure of secure data due to a missing permission check. This could lead to local information disclosure about carrier systems with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-124107808.	2019-07-08	2.1	<a href="#">CVE-2019-2117</a> CONFIRM
google -- android	In various functions of Parcel.cpp, there are uninitialized or partially initialized stack variables. These could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-130161842.	2019-07-08	2.1	<a href="#">CVE-2019-2118</a> CONFIRM
google -- android	In multiple functions of key_store_service.cpp, there is a possible Information Disclosure due to improper locking. This could lead to local information disclosure of protected data with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-131622568.	2019-07-08	2.1	<a href="#">CVE-2019-2119</a> CONFIRM
ibm -- multicloud_manager	IBM Multicloud Manager 3.1.0, 3.1.1, and 3.1.2 ibm-mcm-chart could allow a local attacker with admin privileges to obtain highly sensitive information upon deployment. IBM X-Force ID: 158144.	2019-07-11	2.1	<a href="#">CVE-2019-4118</a> CONFIRM XF
libosinfo -- libosinfo	libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to osinfo-install-script via the command line.	2019-07-05	2.1	<a href="#">CVE-2019-13313</a> MLIST MISC MISC MISC
nagios -- nagios_xi	Nagios XI before 5.5.4 has XSS in the auto login admin management page.	2019-07-10	3.5	<a href="#">CVE-2018-17147</a> BID MISC
redhat -- virt-bootstrap	virt-bootstrap 1.1.0 allows local users to discover a root password by listing a process, because this password may be present in the --root-password option to virt_bootstrap.py.	2019-07-05	2.1	<a href="#">CVE-2019-13314</a> MLIST MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Alarm.com ADC-V522IR 0100b9 devices have Incorrect Access Control, a different issue than CVE-2018-19588. This occurs because of incorrect protection of VPN certificates	2019-07-	not yet	<a href="#">CVE-2019-</a>

alarm.com -- adc-v522ir_devices	(used for initiating a VPN session to the Alarm.com infrastructure) on the local camera device.	11	calculated	<a href="#">9657 MISC</a>
alarm.com -- adc-v522ir_devices	Alarm.com ADC-V522IR 0100b9 devices have Incorrect Access Control.	2019-07-11	not yet calculated	<a href="#">CVE-2018-19588 MISC</a>
apache -- kafka	In Apache Kafka versions between 0.11.0.0 and 2.1.0, it is possible to manually craft a Produce request which bypasses transaction/idempotent ACL validation. Only authenticated clients with Write permission on the respective topics are able to exploit this vulnerability. Users should upgrade to 2.1.1 or later where this vulnerability has been fixed.	2019-07-11	not yet calculated	<a href="#">CVE-2018-17196 MISC</a>
apple -- macos	hide.me before 2.4.4 on macOS suffers from a privilege escalation vulnerability in the connectWithExecutablePath.configFilePath.configFileName method of the me_hide_vpnhelper.Helper class in the me.hide.vpnhelper macOS privilege helper tool. This method takes user-supplied input and can be used to escalate privileges, as well as obtain the ability to run any application on the system in the root context.	2019-07-08	not yet calculated	<a href="#">CVE-2019-12174 MISC</a>
arlo -- basestation	Arlo Basestation firmware 1.12.0.1_27940 and prior contain a hardcoded username and password combination that allows root access to the device when an onboard serial interface is connected to.	2019-07-09	not yet calculated	<a href="#">CVE-2019-3950 CONFIRM</a>
arlo -- basestation	Arlo Basestation firmware 1.12.0.1_27940 and prior firmware contain a networking misconfiguration that allows access to restricted network interfaces. This could allow an attacker to upload or download arbitrary files and possibly execute malicious code on the device.	2019-07-09	not yet calculated	<a href="#">CVE-2019-3949 CONFIRM</a>
avaya -- control_manager	A SQL injection vulnerability in the reporting component of Avaya Control Manager could allow an unauthenticated attacker to execute arbitrary SQL commands and retrieve sensitive data related to other users on the system. Affected versions of Avaya Control Manager include 7.x and 8.0.x versions prior to 8.0.4.0. Unsupported versions not listed here were not evaluated.	2019-07-11	not yet calculated	<a href="#">CVE-2019-7003 BID CONFIRM</a>
avtech -- room_alert_3e	On AVTECH Room Alert 3E devices before 2.2.5, an attacker with access to the device's web interface may escalate privileges from an unauthenticated user to administrator by performing a cmd.cgi?action=ResetDefaults&src=RA reset and using the default credentials to get in.	2019-07-07	not yet calculated	<a href="#">CVE-2019-13379 MISC MISC</a>
bks -- bks_ebk_ethernet-buskoppler_pro	BKS EBK Ethernet-Buskoppler Pro before 3.01 allows Unrestricted Upload of a File with a Dangerous Type.	2019-07-05	not yet calculated	<a href="#">CVE-2019-12971 MISC</a>
blackberry -- qnx_software_development_platform	An information disclosure vulnerability leading to a potential local escalation of privilege in the procs service (the /proc filesystem) of BlackBerry QNX Software Development Platform version(s) 6.5.0 SP1 and earlier could allow an attacker to potentially gain unauthorized access to a chosen process address space.	2019-07-12	not yet calculated	<a href="#">CVE-2019-8998 MISC</a>
broadlearning -- eclass	Any URLs with download_attachment.php under templates or home folders can allow arbitrary files downloaded without login in BroadLearning eClass before version ip.2.5.10.2.1.	2019-07-11	not yet calculated	<a href="#">CVE-2019-9886 CONFIRM CONFIRM CONFIRM</a>
castle_rock_computing -- snmpc	nodeimp.exe in Castle Rock SNMPc before 9.0.12.1 and 10.x before 10.0.9 has a stack-based buffer overflow via a long variable string in a Map Objects text file.	2019-07-12	not yet calculated	<a href="#">CVE-2019-13494 MISC MISC</a>
cisco -- adaptive_security_appliance_software_and_firepower_threat_defense_software	A vulnerability in the cryptographic driver for Cisco Adaptive Security Appliance Software (ASA) and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reboot unexpectedly. The vulnerability is due to incomplete input validation of a Secure Sockets Layer (SSL) or Transport Layer Security (TLS) ingress packet header. An attacker could exploit this vulnerability by sending a crafted TLS/SSL packet to an interface on the targeted device. An exploit could allow the attacker to cause the device to reload, which will result in a denial of service (DoS) condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed and transparent firewall mode and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic. A valid SSL or TLS session is required to exploit this vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-1873 BID CISCO</a>
cisco -- advanced_malware_protection_for_endpoints_for_windows	A vulnerability in Cisco Advanced Malware Protection (AMP) for Endpoints for Windows could allow an authenticated, local attacker with administrator privileges to execute arbitrary code. The vulnerability is due to insufficient validation of dynamically loaded modules. An attacker could exploit this vulnerability by placing a file in a specific location in the Windows filesystem. A successful exploit could allow the attacker to execute the code with the privileges of the AMP service.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1932 CISCO</a>
cisco -- email_security_appliance	A vulnerability in the attachment scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper input validation of the email body. An attacker could exploit this vulnerability by naming a malicious attachment with a specific pattern. A successful exploit could allow the attacker to bypass configured content filters that would normally block the attachment.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1921 CISCO</a>
cisco -- email_security_appliance	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device. The vulnerability is due to improper input validation of certain email fields. An attacker could exploit this vulnerability by sending a crafted email message to a recipient protected by the ESA. A successful exploit could allow the attacker to bypass configured message filters and inject arbitrary scripting code inside the email body. The malicious code is not executed by default unless the recipient's email client is configured to execute scripts contained in emails.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1933 CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker with administrator privileges to overwrite or read arbitrary files on the underlying operating system (OS) of an affected device. The vulnerability is due to improper input validation in NFVIS filesystem commands. An attacker could exploit this vulnerability by using crafted variables during the execution of an affected command. A successful exploit could allow the attacker to overwrite or read arbitrary files on the underlying OS.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1894 CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device as root. The vulnerability is due to insufficient input validation of a configuration file that is accessible to a local shell user. An attacker could exploit this vulnerability by including malicious input during the execution of this file. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS as root.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1893 CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1931 CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1930 CISCO</a>

cisco -- ios_xr_software	A vulnerability in the implementation of Border Gateway Protocol (BGP) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to incorrect processing of certain BGP update messages. An attacker could exploit this vulnerability by sending BGP update messages that include a specific set of attributes to be processed by an affected system. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP traffic from explicitly defined peers only. To exploit this vulnerability, the malicious BGP update message would need to come from a configured, valid BGP peer or would need to be injected by the attacker into the victim's BGP network on an existing, valid TCP connection to a BGP peer.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1909</a> <a href="#">CISCO</a>
cisco -- ip_phone_7800_series_and_8800_series	A vulnerability in Cisco SIP IP Phone Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected phone. The vulnerability is due to insufficient validation of input Session Initiation Protocol (SIP) packets. An attacker could exploit this vulnerability by altering the SIP replies that are sent to the affected phone during the registration process. A successful exploit could allow the attacker to cause the phone to reboot and not complete the registration process.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1922</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the Secure Sockets Layer (SSL) input packet processor of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a memory corruption on an affected device. The vulnerability is due to improper validation of HTTPS packets. An attacker could exploit this vulnerability by sending a malformed HTTPS packet to the management web interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a denial of service (DoS) condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1892</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1891</a> <a href="#">CISCO</a>
cisco -- unified_communications_domain_manager	A vulnerability in the CLI of Cisco Unified Communications Domain Manager (Cisco Unified CDM) Software could allow an authenticated, local attacker to escape the restricted shell. The vulnerability is due to insufficient input validation of shell commands. An attacker could exploit this vulnerability by executing crafted commands in the shell. A successful exploit could allow the attacker to escape the restricted shell and access commands in the context of the restricted shell user, which does not have root privileges.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1911</a> <a href="#">CISCO</a>
citrix -- xenserver	The Windows Guest Tools in Citrix XenServer 6.2 SP1 and earlier allows remote attackers to cause a denial of service (guest OS crash) via a crafted Ethernet frame.	2019-07-11	not yet calculated	<a href="#">CVE-2014-3798</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">SECTRAK</a>
cloud_foundry -- uaa	Cloud Foundry UAA version prior to 73.3.0, contain endpoints that contains improper escaping. An authenticated malicious user with basic read privileges for one identity zone can extend those reading privileges to all other identity zones and obtain private information on users, clients, and groups in all other identity zones.	2019-07-11	not yet calculated	<a href="#">CVE-2019-11268</a> <a href="#">CONFIRM</a>
cloudera -- cloudera_manager	Cloudera Manager through 5.15 has Incorrect Access Control.	2019-07-11	not yet calculated	<a href="#">CVE-2018-11744</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
cohesity -- dataplatform	A man-in-the-middle vulnerability related to vCenter access was found in Cohesity DataPlatform version 5.x and 6.x prior to 6.1.1c. Cohesity clusters did not verify TLS certificates presented by vCenter. This vulnerability could expose Cohesity user credentials configured to access vCenter.	2019-07-12	not yet calculated	<a href="#">CVE-2019-11242</a> <a href="#">CONFIRM</a>
container_build_system -- osbs-client	A flaw was found in the yaml.load() function in the osbs-client versions since 0.46 before 0.56.1. Insecure use of the yaml.load() function allowed the user to load any suspicious object for code execution via the parsing of malicious YAML files.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10135</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
cyberpower -- powerpanel_business	CSRF in the Agent/Center component of CyberPower PowerPanel Business Edition 3.4.0 allows an attacker to submit POST requests to any forms in the web application. This can be exploited by tricking an authenticated user into visiting an attacker controlled web page.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13071</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
damicms -- damicms	An arbitrary file read vulnerability in DamiCMS v6.0.0 allows remote authenticated administrators to read any files in the server via a crafted /admin.php?s=Tpl/Add/id/ URI.	2019-07-10	not yet calculated	<a href="#">CVE-2018-14831</a> <a href="#">MISC</a>
ddrt -- dashcom_live	Lack of authentication in file-viewing components in DDRT Dashcom Live 2019-05-09 allows anyone to remotely access all claim details by visiting easily guessable dashboard/uploads/claim_files/claim_id_ URLs.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11020</a> <a href="#">MISC</a> <a href="#">MISC</a>
ddrt -- dashcom_live	Lack of authentication in case-exporting components in DDRT Dashcom Live through 2019-05-08 allows anyone to remotely access all claim details by visiting easily guessable exportpdf/all_claim_detail.php?claim_id= URLs.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11019</a> <a href="#">MISC</a> <a href="#">MISC</a>
debian -- mediawiki	An Incorrect Access Control vulnerability was found in Wikimedia MediaWiki 1.18.0 through 1.32.1. It is possible to bypass the limits on IP range blocks (\$wgBlockCIDRLimit) by using the API. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12472</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
debian -- mediawiki	An Incorrect Access Control vulnerability was found in Wikimedia MediaWiki 1.27.0 through 1.32.1. Directly POSTing to Special:ChangeEmail would allow for bypassing re-authentication, allowing for potential account takeover.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12468</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	MediaWiki through 1.32.1 has Incorrect Access Control (issue 1 of 3). A spammer can use Special:ChangeEmail to send out spam with no rate limiting or ability to block them. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12467</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	Wikimedia MediaWiki 1.30.0 through 1.32.1 has XSS. Loading user JavaScript from a non-existent account allows anyone to create the account, and perform XSS on users loading that script. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12471</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	Wikimedia MediaWiki 1.27.0 through 1.32.1 might allow DoS. Passing invalid titles to the API could cause a DoS by querying the entire watchlist table. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12473</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
debian -- mediawiki	Wikimedia MediaWiki through 1.32.1 has Incorrect Access Control. Suppressed log in RevisionDelete page is exposed. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	<a href="#">CVE-2019-12470</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>

				DEBIAN
debian -- mediawiki	MediaWiki through 1.32.1 has Incorrect Access Control. Suppressed username or log in Special:EditTags are exposed. Fixed in 1.32.2, 1.31.2, 1.30.2 and 1.27.6.	2019-07-10	not yet calculated	CVE-2019-12469 CONFIRM MISC BUGTRAQ DEBIAN
debian -- redis	A stack-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By corrupting a hyperloglog using the SETRANGE command, an attacker could cause Redis to perform controlled increments of up to 12 bytes past the end of a stack-allocated buffer.	2019-07-11	not yet calculated	CVE-2019-10193 CONFIRM MISC MISC MISC BUGTRAQ DEBIAN
debian -- redis	A heap-buffer overflow vulnerability was found in the Redis hyperloglog data structure versions 3.x before 3.2.13, 4.x before 4.0.14 and 5.x before 5.0.4. By carefully corrupting a hyperloglog using the SETRANGE command, an attacker could trick Redis interpretation of dense HLL encoding to write up to 3 bytes beyond the end of a heap-allocated buffer.	2019-07-11	not yet calculated	CVE-2019-10192 CONFIRM MISC MISC MISC BUGTRAQ DEBIAN
digium -- asterisk	Buffer overflow in res_pjsip_messaging in Digium Asterisk versions 13.21-cert3, 13.27.0, 15.7.2, 16.4.0 and earlier allows remote authenticated users to crash Asterisk by sending a specially crafted SIP MESSAGE message.	2019-07-12	not yet calculated	CVE-2019-12827 CONFIRM CONFIRM
digium -- asterisk	An issue was discovered in Asterisk Open Source through 13.27.0, 14.x and 15.x through 15.7.2, and 16.x through 16.4.0, and Certified Asterisk through 13.21-cert3. A pointer dereference in chan_sip while handling SDP negotiation allows an attacker to crash Asterisk when handling an SDP answer to an outgoing T.38 re-invite. To exploit this vulnerability an attacker must cause the chan_sip module to send a T.38 re-invite request to them. Upon receipt, the attacker must send an SDP answer containing both a T.38 UDPTL stream and another media stream containing only a codec (which is not permitted according to the chan_sip configuration).	2019-07-12	not yet calculated	CVE-2019-13161 CONFIRM CONFIRM
e107 -- e107	In e107 v2.1.7, output without filtering results in XSS.	2019-07-10	not yet calculated	CVE-2018-11734 MISC
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.9 and CCU3 devices before 3.43.16 have buffer overflows in the ReGa ise GmbH HTTP-Server 2.0 component, aka HMCCU-179. This may lead to remote code execution.	2019-07-10	not yet calculated	CVE-2019-10122 MISC MISC
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.16 use session IDs for authentication but lack authorization checks. An attacker can obtain a session ID via an invalid login attempt to the RemoteApi account, aka HMCCU-154. This leads to automatic login as admin.	2019-07-10	not yet calculated	CVE-2019-10119 MISC MISC
eq-3 -- homematic_ccu2_devices	On eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.16, automatic login configuration (aka setAutoLogin) can be achieved by continuing to use a session ID after a logout, aka HMCCU-154.	2019-07-10	not yet calculated	CVE-2019-10120 MISC MISC
eq-3 -- homematic_ccu2_devices	eQ-3 HomeMatic CCU2 devices before 2.41.8 and CCU3 devices before 3.43.15 use session IDs for authentication but lack authorization checks. An attacker can obtain a session ID via the user authentication dialogue, aka HMCCU-153. This leads to automatic login as admin.	2019-07-10	not yet calculated	CVE-2019-10121 MISC MISC MISC
fasterxml -- jackson-databind	An issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.5. Use of Jackson default typing along with a gadget class from IBatis allows exfiltration of content. Fixed in 2.7.9.4, 2.8.11.2, and 2.9.6.	2019-07-09	not yet calculated	CVE-2018-11307 CONFIRM MISC MISC MISC
field_test_gem_for_ruby_on_rails -- field_test_gem_for_ruby_on_rails	The field_test gem 0.3.0 for Ruby has unvalidated input. A method call that is expected to return a value from a certain set of inputs can be made to return any input, which can be dangerous depending on how applications use it. If an application treats arbitrary variants as trusted, this can lead to a variety of potential vulnerabilities like SQL injection or cross-site scripting (XSS).	2019-07-09	not yet calculated	CVE-2019-13146 BID MISC MISC
flightpath -- flightpath	FlightPath 4.x and 5.0-x allows directory traversal and Local File Inclusion through the form_include parameter in an index.php?q=system-handle-form-submit POST request because of an include_once in system_handle_form_submit in modules/system/system.module.	2019-07-10	not yet calculated	CVE-2019-13396 CONFIRM
ge_healthcare -- aestiva_and_aespire	In GE Aestiva and Aespire versions 7100 and 7900, a vulnerability exists where serial devices are connected via an added unsecured terminal server to a TCP/IP network configuration, which could allow an attacker to remotely modify device configuration and silence alarms.	2019-07-10	not yet calculated	CVE-2019-10966 BID MISC
glpi_project -- glpi	GLPI GLPI Product 9.3.1 is affected by: Frame and Form tags Injection allowing admins to phish users by putting code in reminder description. The impact is: Admins can phish any user or group of users for credentials / credit cards. The component is: Tools > Reminder > Description .. Set the description to any iframe/form tags and apply. The attack vector is: The attacker puts a login form, the user fills it and clicks on submit .. the request is sent to the attacker domain saving the data. The fixed version is: 9.4.1.	2019-07-12	not yet calculated	CVE-2019-1010310 MISC MISC
glpi_project -- glpi	An issue was discovered in GLPI before 9.4.1. After a successful password reset by a user, it is possible to change that user's password again during the next 24 hours without any information except the associated email address.	2019-07-10	not yet calculated	CVE-2019-13240 MISC MISC MISC MISC
hewlett_packard_enterprise -- 3par_service_processor	HPE has identified a vulnerability in HPE 3PAR Service Processor (SP) version 4.1 through 4.4. HPE 3PAR Service Processor (SP) version 4.1 through 4.4 has a remote information disclosure vulnerability which can allow for the disruption of the confidentiality, integrity and availability of the Service Processor and any managed 3PAR arrays.	2019-07-09	not yet calculated	CVE-2019-11981 CONFIRM
huawei -- mate_20_and_mate_20_x_honor_magic_2	There is a Factory Reset Protection (FRP) bypass vulnerability on several smartphones. The system does not sufficiently verify the permission, an attacker could do a certain operation on certain step of setup wizard. Successful exploit could allow the attacker bypass the FRP protection. Affected products: Mate 20 X, versions earlier than Ever-AL00B 9.0.0.200(C00E200R2P1); Mate 20, versions earlier than Hima-AL00B/Hima-TL00B 9.0.0.200(C00E200R2P1); Honor Magic 2, versions earlier than Tony-AL00B/Tony-TL00B 9.0.0.182(C00E180R2P2).	2019-07-10	not yet calculated	CVE-2019-5220 CONFIRM
huawei -- mate_20_x	There is a path traversal vulnerability on Huawei Share. The software does not properly validate the path, an attacker could crafted a file path when transporting file through Huawei Share, successful exploit could allow the attacker to transport a file to arbitrary path on the phone. Affected products: Mate 20 X versions earlier than Ever-L29B 9.1.0.300(C432E3R1P12), versions earlier than Ever-L29B 9.1.0.300(C636E3R2P1), and versions earlier than Ever-L29B 9.1.0.300(C185E3R3P1).	2019-07-10	not yet calculated	CVE-2019-5221 CONFIRM
huneson -- i-onenet	In Huneson i-oneNet version 3.0.7 ~ 3.0.53 and 4.0.4 ~ 4.0.16, the specific upload web module doesn't verify the file extension and type, and an attacker can upload a webshell. After the webshell upload, an attacker can use the webshell to perform remote code execution such as running a system command.	2019-07-10	not yet calculated	CVE-2019-12803 CONFIRM
	In Huneson i-oneNet version 3.0.7 ~ 3.0.53 and 4.0.4 ~ 4.0.16, due to the lack of update			CVE-2019-

huneson -- i-onenet	file integrity checking in the upgrade process, an attacker can craft malicious file and use it as an update.	2019-07-10	not yet calculated	<a href="#">12804 CONFIRM</a>
ibm -- content_navigator	IBM Content Navigator 3.0CD is vulnerable to local file inclusion, allowing an attacker to access a configuration file in the ICN server. IBM X-Force ID: 160015.	2019-07-11	not yet calculated	<a href="#">CVE-2019-4263 XF CONFIRM</a>
ibm -- security_identity_manager	IBM Security Identity Manager 7.0.1 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 153749.	2019-07-11	not yet calculated	<a href="#">CVE-2018-1968 CONFIRM XF</a>
intel -- processor_diagnostic_tool	Improper access control in the Intel(R) Processor Diagnostic Tool before version 4.1.2.24 may allow an authenticated user to potentially enable escalation of privilege, information disclosure or denial of service via local access.	2019-07-11	not yet calculated	<a href="#">CVE-2019-11133 BID CONFIRM</a>
intel -- ssd_dc_s4500_and_s4600_devices	Improper authentication in firmware for Intel(R) SSD DC S4500 Series and Intel(R) SSD DC S4600 Series before SCV10150 may allow an unprivileged user to potentially enable escalation of privilege via physical access.	2019-07-11	not yet calculated	<a href="#">CVE-2018-18095 BID CONFIRM</a>
intuit -- lacerte	Intuit Lacerte 2017 has Incorrect Access Control.	2019-07-09	not yet calculated	<a href="#">CVE-2018-14833 MISC MISC</a>
invoxia -- nvx220_devices	Invoxia NVX220 devices allow TELNET access as admin with a default password.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14528 MISC</a>
ivanti -- endpoint_manager	An issue was discovered in the Core Server in Ivanti Endpoint Manager (EPM) 2017.3 before SU7 and 2018.x before 2018.3 SU3, with remote code execution. In other words, the issue affects 2017.3, 2018.1, and 2018.3 installations that lack the April 2019 update.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10651 CONFIRM</a>
jenkins -- jenkins	Jenkins Port Allocator Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10350 MLIST MISC</a>
jenkins -- jenkins	A stored cross site scripting vulnerability in Jenkins Dependency Graph Viewer Plugin 0.13 and earlier allowed attackers able to configure jobs in Jenkins to inject arbitrary HTML and JavaScript in the plugin-provided web pages in Jenkins.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10349 MISC MLIST MISC</a>
jenkins -- jenkins	Jenkins Gogs Plugin stored credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10348 MLIST MISC</a>
jenkins -- jenkins	Jenkins Mashup Portlets Plugin stored credentials unencrypted on the Jenkins master where they can be viewed by users with access to the master file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10347 MLIST MISC</a>
jenkins -- jenkins	A reflected cross site scripting vulnerability in Jenkins Embeddable Build Status Plugin 2.0.1 and earlier allowed attackers inject arbitrary HTML and JavaScript into the response of this plugin.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10346 MLIST MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Docker Plugin 1.1.6 and earlier in various 'fillCredentialsItems' methods allowed users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10342 MLIST MISC</a>
jenkins -- jenkins	A missing permission check in Jenkins Docker Plugin 1.1.6 and earlier in DockerAPI.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10341 MLIST MISC</a>
jenkins -- jenkins	A cross-site request forgery vulnerability in Jenkins Docker Plugin 1.1.6 and earlier in DockerAPI.DescriptorImpl#doTestConnection allowed users with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10340 MLIST MISC</a>
jenkins -- jenkins	Jenkins Caliper CI Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10351 MLIST MISC</a>
juniper -- junos_os	A vulnerability in the pfe-chassisd Chassis Manager (CMLC) daemon of Juniper Networks Junos OS allows an attacker to cause a Denial of Service (DoS) to the EX4300 when specific valid broadcast packets create a broadcast storm condition when received on the me0 interface of the EX4300 Series device. A reboot of the device is required to restore service. Continued receipt of these valid broadcast packets will create a sustained Denial of Service (DoS) against the device. Affected releases are Juniper Networks Junos OS: 16.1 versions above and including 16.1R1 prior to 16.1R7-S5; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R2; 18.1 versions prior to 18.1R3; 18.2 versions prior to 18.2R2.	2019-07-11	not yet calculated	<a href="#">CVE-2019-0046 CONFIRM</a>
juniper -- junos_os	On EX4300 Series switches with TCAM optimization enabled, incoming multicast traffic matches an implicit loopback filter rule first, since it has high priority. This rule is meant for reserved multicast addresses 224.0.0.x, but incorrectly matches on 224.x.x.x. Due to this bug, when a firewall filter is applied on the loopback interface, other firewall filters might stop working for multicast traffic. The command 'show firewall filter' can be used to confirm whether the filter is working. This issue only affects the EX4300 switch. No other products or platforms are affected by this vulnerability. This issue affects: Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D51, 14.1X53-D115 on EX4300 Series; 17.1 versions prior to 17.1R3 on EX4300 Series; 17.2 versions prior to 17.2R3-S2 on EX4300 Series; 17.3 versions prior to 17.3R3-S3 on EX4300 Series; 17.4 versions prior to 17.4R2-S5, 17.4R3 on EX4300 Series; 18.1 versions prior to 18.1R3-S1 on EX4300 Series; 18.2 versions prior to 18.2R2 on EX4300 Series; 18.3 versions prior to 18.3R2 on EX4300 Series.	2019-07-11	not yet calculated	<a href="#">CVE-2019-0048 CONFIRM</a>
juniper -- junos_os	On Junos devices with the BGP graceful restart helper mode enabled or the BGP graceful restart mechanism enabled, a certain sequence of BGP session restart on a remote peer that has the graceful restart mechanism enabled may cause the local routing protocol daemon (RPD) process to crash and restart. Repeated crashes of the RPD process can cause prolonged Denial of Service (DoS). Graceful restart helper mode for BGP is enabled by default. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S3; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3; 17.2X75 versions prior to 17.2X75-D105; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R1-S7, 17.4R2-S2, 17.4R3; 18.1 versions prior to 18.1R3-S2; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D30; 18.3 versions prior to 18.3R1-S4, 18.3R2. Junos OS releases prior to 16.1R1 are not affected.	2019-07-11	not yet calculated	<a href="#">CVE-2019-0049 CONFIRM</a>
juniper -- junos_os	The srpxp process may crash on SRX Series services gateways when the UTM module processes a specific fragmented HTTP packet. The packet is misinterpreted as a regular TCP packet which causes the processor to crash. This issue affects all SRX Series platforms that support URL-Filtering and have web-filtering enabled. Affected releases are Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D85 on SRX Series; 15.1X49 versions prior to 15.1X49-D181, 15.1X49-D190 on SRX Series; 17.3 versions on SRX Series; 17.4 versions prior to 17.4R1-S8, 17.4R2-S5, 17.4R3 on SRX Series; 18.1 versions prior to 18.1R3-S6 on SRX Series; 18.2 versions prior to 18.2R2-S1, 18.2R3 on SRX Series; 18.3 versions prior to 18.3R1-S2, 18.3R2 on SRX Series; 18.4 versions prior	2019-07-11	not yet calculated	<a href="#">CVE-2019-0052 CONFIRM</a>



	to 18.4R1-S1, 18.4R2 on SRX Series.			
juniper -- junos_os	Insufficient validation of environment variables in the telnet client supplied in Junos OS can lead to stack-based buffer overflows, which can be exploited to bypass verixec restrictions on Junos OS. A stack-based overflow is present in the handling of environment variables when connecting via the telnet client to remote telnet servers. This issue only affects the telnet client ? accessible from the CLI or shell ? in Junos OS. Inbound telnet services are not affected by this issue. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S13; 12.3X48 versions prior to 12.3X48-D80; 14.1X53 versions prior to 14.1X53-D130, 14.1X53-D49; 15.1 versions prior to 15.1F6-S12, 15.1R7-S4; 15.1X49 versions prior to 15.1X49-D170; 15.1X53 versions prior to 15.1X53-D237, 15.1X53-D496, 15.1X53-D591, 15.1X53-D69; 16.1 versions prior to 16.1R3-S11, 16.1R7-S4; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R2-S7, 17.2R3-S1; 17.3 versions prior to 17.3R3-S4; 17.4 versions prior to 17.4R1-S6, 17.4R2-S3, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S3; 18.2 versions prior to 18.2R1-S5, 18.2R2-S2, 18.2R3; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S3, 18.3R2; 18.4 versions prior to 18.4R1-S2, 18.4R2.	2019-07-11	not yet calculated	<a href="#">CVE-2019-0053</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
leanote -- leanote	Leanote prior to version 2.6 is affected by: Cross Site Scripting (XSS).	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010003</a> <a href="#">MISC</a>
libpng -- libpng	libpng before 1.6.32 does not properly check the length of chunks against the user limit.	2019-07-10	not yet calculated	<a href="#">CVE-2017-12652</a> <a href="#">CONFIRM</a>
linux -- linux_kernel	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10638</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the IP ID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This attack can be carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because IP ID generation was changed to have a dependency on an address associated with a network namespace.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10639</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The openvpn_launcher.64 binary is setuid root. This binary executes /opt/pia/openvpn-64/openvpn, passing the parameters provided from the command line. Care was taken to programmatically disable potentially dangerous openvpn parameters; however, the --route-pre-down parameter can be used. This parameter accepts an arbitrary path to a script/program to be executed when OpenVPN exits. The --script-security parameter also needs to be passed to allow for this action to be taken, and --script-security is not currently in the disabled parameter list. A local unprivileged user can pass a malicious script/binary to the --route-pre-down option, which will be executed as root when openvpn is stopped.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12578</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The root_runner.64 binary is setuid root. This binary executes /opt/pia/ruby/64/ruby, which in turn attempts to load several libraries under /tmp/ruby-deploy.old/lib. A local unprivileged user can create a malicious library under this path to execute arbitrary code as the root user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12575</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux_and_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux and macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The PIA Linux/macOS binary openvpn_launcher.64 binary is setuid root. This binary accepts several parameters to update the system configuration. These parameters are passed to operating system commands using a "here" document. The parameters are not sanitized, which allow for arbitrary commands to be injected using shell metacharacters. A local unprivileged user can pass special crafted parameters that will be interpolated by the operating system calls.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12579</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_linux_and_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for Linux and macOS could allow an authenticated, local attacker to overwrite arbitrary files. The openvpn_launcher binary is setuid root. This binary supports the --log option, which accepts a path as an argument. This parameter is not sanitized, which allows a local unprivileged user to overwrite arbitrary files owned by any user on the system, including root. This creates a denial of service condition and possible data loss if leveraged by a malicious local user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12573</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The openvpn_launcher binary is setuid root. This program is called during the connection process and executes several operating system utilities to configure the system. The networksetup utility is called using relative paths. A local unprivileged user can execute arbitrary commands as root by creating a networksetup trojan which will be executed during the connection process. This is possible because the PATH environment variable is not reset prior to executing the OS utility.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12576</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v0.9.8 beta (build 02099) for macOS could allow an authenticated, local attacker to overwrite arbitrary files. When the client initiates a connection, the XML /tmp/pia-watcher.plist file is created. If the file exists, it will be truncated and the contents completely overwritten. This file is removed on disconnect. An unprivileged user can create a hard or soft link to arbitrary files owned by any user on the system, including root. This creates a denial of service condition and possible data loss if leveraged by a malicious local user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12571</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_macos	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v82 for macOS could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The macOS binary openvpn_launcher.64 is setuid root. This binary creates /tmp/pia_upscript.sh when executed. Because the file creation mask (umask) is not reset, the umask value is inherited from the calling process. This value can be manipulated to cause the privileged binary to create files with world writable permissions. A local unprivileged user can modify /tmp/pia_upscript.sh during the connect process to execute arbitrary code as the root user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12577</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_windows	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client v1.0 for Windows could allow an authenticated, local attacker to run arbitrary code with elevated privileges. The PIA client is vulnerable to a DLL injection vulnerability during the software update process. The updater loads several libraries from a folder that authenticated users have write access to. A low privileged user can leverage this vulnerability to execute arbitrary code as SYSTEM.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12574</a> <a href="#">MISC</a>
	MailEnable Enterprise Premium 10.23 was vulnerable to multiple directory traversal issues, with which authenticated users could add, remove, or potentially read files in arbitrary			<a href="#">CVE-2019-</a>



	Privilege.			
realization -- concerto_critical_chain_planner	Realization Concerto Critical Chain Planner (aka CCPM) 5.10.8071 has SQL Injection in at least in the taskupdt/taskdetails.aspx webpage via the projectname parameter.	2019-07-12	not yet calculated	<a href="#">CVE-2019-13027</a> <a href="#">MISC</a>
red_hat -- openshift_container_platform	A reflected XSS vulnerability exists in authorization flow of OpenShift Container Platform versions: openshift-online-3, openshift-enterprise-3.4 through 3.7 and openshift-enterprise-3.9 through 3.11. An attacker could use this flaw to steal authorization data by getting them to click on a malicious link.	2019-07-11	not yet calculated	<a href="#">CVE-2019-3889</a> <a href="#">CONFIRM</a>
rockwell_automation -- panelview_5510	In Rockwell Automation PanelView 5510 (all versions manufactured before March 13, 2019 that have never been updated to v4.003, v5.002, or later), a remote, unauthenticated threat actor with access to an affected PanelView 5510 Graphic Display, upon successful exploit, may boot-up the terminal and gain root-level access to the device's file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10970</a> <a href="#">BID</a> <a href="#">MISC</a>
sap -- abap_server_and_abap_platform	ABAP Server and ABAP Platform (SAP Basis), versions, 7.31, 7.4, 7.5, do not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0321</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- businessobjects_business_intelligence_platform	SAP BusinessObjects Business Intelligence Platform (BI Workspace) (Enterprise), versions 4.1, 4.2, 4.3, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0326</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- commerce_cloud	SAP Commerce Cloud (previously known as SAP Hybris Commerce), (HY_COM, versions 6.3, 6.4, 6.5, 6.6, 6.7, 1808, 1811), allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0322</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- diagnostic_agent	The OS Command Plugin in the transaction GPA_ADMIN and the OSCommand Console of SAP Diagnostic Agent (LM-Service), version 7.2, allow an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0330</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- erp_hcm	SAP ERP HCM (SAP_HRCES), version 3, does not perform necessary authorization checks for a report that reads payroll data of employees in a certain area. Due to this under certain conditions, the user that once had authorization to payroll data of an employee, which was later revoked, may retain access to the same data.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0325</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- netweaver_application_server	Under certain conditions SAP NetWeaver Application Server for Java (Startup Framework), versions 7.21, 7.22, 7.45, 7.49, and 7.53, allows an attacker to access information which would otherwise be restricted.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0318</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- netweaver_for_java_application_server	SAP NetWeaver for Java Application Server - Web Container, (engineapi, versions 7.1, 7.2, 7.3, 7.31, 7.4 and 7.5), (servercode, versions 7.2, 7.3, 7.31, 7.4, 7.5), allows an attacker to upload files (including script files) without proper file format validation.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0327</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- netweaver_process_integration	ABAP Tests Modules (SAP Basis, versions 7.0, 7.1, 7.3, 7.31, 7.4, 7.5) of SAP NetWeaver Process Integration enables an attacker the execution of OS commands with privileged rights. An attacker could thereby impact the integrity and availability of the system.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0328</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- sap_gateway	The SAP Gateway, versions 7.5, 7.51, 7.52 and 7.53, allows an attacker to inject content which is displayed in the form of an error message. An attacker could thus mislead a user to believe this information is from the legitimate service when it's not.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0319</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
sap -- sapui5_and_openui5	SAPUI5 and OpenUI5, before versions 1.38.39, 1.44.39, 1.52.25, 1.60.6 and 1.63.0, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-07-10	not yet calculated	<a href="#">CVE-2019-0281</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
schedmd -- slurm	SchedMD Slurm 17.11.x, 18.08.0 through 18.08.7, and 19.05.0 allows SQL Injection.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12838</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
siemens -- simatic_pcs_7_and_simatic_wincc_products	A vulnerability has been identified in SIMATIC PCS 7 V8.0 and earlier (All versions), SIMATIC PCS 7 V8.1 (All versions), SIMATIC PCS 7 V8.2 (All versions < V8.2 SP1 with WinCC V7.4 SP1 Upd11), SIMATIC PCS 7 V9.0 (All versions < V9.0 SP2 with WinCC V7.4 SP1 Upd11), SIMATIC WinCC Professional (TIA Portal V13) (All versions), SIMATIC WinCC Professional (TIA Portal V14) (All versions), SIMATIC WinCC Professional (TIA Portal V15) (All versions), SIMATIC WinCC Runtime Professional V13 (All versions), SIMATIC WinCC Runtime Professional V14 (All versions), SIMATIC WinCC Runtime Professional V15 (All versions), SIMATIC WinCC V7.2 and earlier (All versions), SIMATIC WinCC V7.3 (All versions), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Upd 11), SIMATIC WinCC V7.5 (All versions < V7.5 Upd 3). The SIMATIC WinCC DataMonitor web application of the affected products allows to upload arbitrary ASPX code. The security vulnerability could be exploited by an authenticated attacker with network access to the WinCC DataMonitor application. No user interaction is required to exploit this vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the affected device. At the stage of publishing this security advisory no public exploitation is known.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10935</a> <a href="#">BID</a> <a href="#">MISC</a>
siemens -- siprotec_5_devices	A vulnerability has been identified in SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.90), All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions), DIGSI 5 engineering software (All versions < V7.90). Specially crafted packets sent to port 443/TCP could cause a Denial of Service condition.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10931</a> <a href="#">MISC</a>
siemens -- siprotec_5_devices	A vulnerability has been identified in SIPROTEC 5 device types 6MD85, 6MD86, 6MD89, 7UM85, 7SA87, 7SD87, 7SL87, 7VK87, 7SA82, 7SA86, 7SD82, 7SD86, 7SL82, 7SL86, 7SJ86, 7SK82, 7SK85, 7SJ82, 7SJ85, 7UT82, 7UT85, 7UT86, 7UT87 and 7VE85 with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions < V7.90), All other SIPROTEC 5 device types with CPU variants CP300 and CP100 and the respective Ethernet communication modules (All versions), SIPROTEC 5 relays with CPU variants CP200 and the respective Ethernet communication modules (All versions), DIGSI 5 engineering software (All versions < V7.90). A remote attacker could use specially crafted packets sent to port 443/TCP to upload, download or delete files in certain parts of the file system.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10930</a> <a href="#">MISC</a>
siemens -- spectrum_power_products	A vulnerability has been identified in Spectrum Power 3 (Corporate User Interface) (All versions <= v3.11), Spectrum Power 4 (Corporate User Interface) (Version v4.75), Spectrum Power 5 (Corporate User Interface) (All versions <= v5.50), Spectrum Power 7 (Corporate User Interface) (All versions <= v2.20). The web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. The user does not need to be logged into the web interface in order for the exploitation to succeed. At the stage of	2019-07-11	not yet calculated	<a href="#">CVE-2019-10933</a> <a href="#">MISC</a>

	publishing this security advisory no public exploitation is known.			
siemens -- tia_administrator	A vulnerability has been identified in TIA Administrator (All versions < V1.0 SP1 Upd1). The integrated configuration web application (TIA Administrator) allows to execute certain application commands without proper authentication. The vulnerability could be exploited by an attacker with local access to the affected system. Successful exploitation requires no privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality and integrity and availability of the affected system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2019-07-11	not yet calculated	<a href="#">CVE-2019-10915</a> <a href="#">BID</a> <a href="#">MISC</a>
snapview -- mikogo	The Windows versions of Snapview Mikogo, versions before 5.10.2 are affected by insecure implementations which allow local attackers to escalate privileges.	2019-07-12	not yet calculated	<a href="#">CVE-2019-12731</a> <a href="#">MISC</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager before 3.17.0 has a weak default of giving any unauthenticated user read permissions on the repository files and images.	2019-07-08	not yet calculated	<a href="#">CVE-2019-9630</a> <a href="#">MISC</a>
sonatype -- nexus_repository_manager	Sonatype Nexus Repository Manager before 3.17.0 establishes a default administrator user with weak defaults (fixed credentials).	2019-07-08	not yet calculated	<a href="#">CVE-2019-9629</a> <a href="#">MISC</a>
sony -- bravia_smart_tv_devices	Sony BRAVIA Smart TV devices allow remote attackers to cause a denial of service (device hang) via a crafted web page over HbbTV.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11889</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
sony -- bravia_smart_tv_devices	Sony Bravia Smart TV devices allow remote attackers to cause a denial of service (device hang or reboot) via a SYN flood attack over a wired or Wi-Fi LAN.	2019-07-09	not yet calculated	<a href="#">CVE-2019-11890</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
spiderlabs -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) 3.0.2. Use of X.Filename instead of X_Filename can bypass some PHP Script Uploads rules, because PHP automatically transforms dots into underscores in certain contexts where dots are invalid.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13464</a> <a href="#">MISC</a>
squid-cache -- squid	An issue was discovered in Squid 4.0.23 through 4.7. When checking Basic Authentication with HttpHeader: getAuth, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length isn't greater than the buffer, leading to a heap-based buffer overflow with user controlled data.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12527</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
squid-cache -- squid	An issue was discovered in Squid 3.3.9 through 3.5.28 and 4.x through 4.7. When Squid is configured to use Digest authentication, it parses the header Proxy-Authorization. It searches for certain tokens such as domain, uri, and qop. Squid checks if this token's value starts with a quote and ends with one. If so, it performs a memcpy of its length minus 2. Squid never checks whether the value is just a single quote (which would satisfy its requirements), leading to a memcpy of its length minus 1.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12525</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
squid-cache -- squid	An issue was discovered in Squid 2.x through 2.7.STABLE9, 3.x through 3.5.28, and 4.x through 4.7. When Squid is configured to use Basic Authentication, the Proxy-Authorization header is parsed via uudecode. uudecode determines how many bytes will be decoded by iterating over the input and checking its table. The length is then used to start decoding the string. There are no checks to ensure that the length it calculates isn't greater than the input buffer. This leads to adjacent memory being decoded as well. An attacker would not be able to retrieve the decoded data unless the Squid maintainer had configured the display of usernames on error pages.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12529</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
stopzilla -- stopzilla_antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x8000205F.	2019-07-09	not yet calculated	<a href="#">CVE-2018-15738</a> <a href="#">MISC</a> <a href="#">MISC</a>
sunnet -- wmprom	The SUNNET WMProm v5.0 and v5.1 for eLearning system has OS Command Injection via "/teach/course/oaajaxfileupload.php". The target server can be exploited without authentication.	2019-07-11	not yet calculated	<a href="#">CVE-2019-11062</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
swift -- alliance_web_platform	An issue was discovered in SWIFT Alliance Web Platform 7.1.23. A log injection (and an arbitrary log filename) can be achieved via the PATH_INFO to swp/login/EJBRemoteService/, related to com.swift.ejbgwtj2ee.client.EJBInvocationException error log information containing null@java:comp/env/ error messages.	2019-07-05	not yet calculated	<a href="#">CVE-2018-16386</a> <a href="#">MISC</a>
symantec -- messaging_gateway	Symantec Messaging Gateway, prior to 10.7.1, may be susceptible to a privilege escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12751</a> <a href="#">BID</a> <a href="#">MISC</a>
thoughtspot -- thoughtspot	An authorization bypass vulnerability in pinboard updates in ThoughtSpot 4.4.1 through 5.1.1 (before 5.1.2) allows a low-privilege user with write access to at least one pinboard to corrupt pinboards of another user in the application by spoofing GUIDs in pinboard update requests, effectively deleting them.	2019-07-09	not yet calculated	<a href="#">CVE-2019-12782</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains multiple stack-based buffer overflows when processing user input for the setup wizard, allowing an unauthenticated user to execute arbitrary code. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13279</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 allows an unauthenticated attacker to execute setup wizard functionality, giving this attacker the ability to change configuration values, potentially leading to a denial of service. The request can be made on the local intranet or remotely if remote administration is enabled.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13277</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains multiple command injections when processing user input for the setup wizard, allowing an unauthenticated user to run arbitrary commands on the device. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13278</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains a stack-based buffer overflow in the ssi binary. The overflow allows an unauthenticated user to execute arbitrary code by providing a sufficiently long query string when POSTing to any valid cgi, txt, asp, or js file. The vulnerability can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13276</a> <a href="#">MISC</a>
trendnet -- tew-827dru	TRENDnet TEW-827DRU with firmware up to and including 2.04B03 contains a stack-based buffer overflow while returning an error message to the user about failure to resolve a hostname during a ping or traceroute attempt. This allows an authenticated user to execute arbitrary code. The exploit can be exercised on the local intranet or remotely if remote administration is enabled.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13280</a> <a href="#">MISC</a>
u.s._army -- america's_army_proving_grounds	An issue was discovered in the America's Army Proving Grounds platform for the Unreal Engine. With a false packet sent via UDP, the application server responds with several bytes, giving the possibility of DoS amplification, even being able to be used in DDoS attacks.	2019-07-10	not yet calculated	<a href="#">CVE-2018-10531</a> <a href="#">MISC</a> <a href="#">MISC</a>
umbiquiti_networks -- edgemax_edgeswitch	Command Injection in EdgeMAX EdgeSwitch prior to 1.8.2 allow an Admin user to execute commands as root.	2019-07-10	not yet calculated	<a href="#">CVE-2019-5446</a> <a href="#">MISC</a>
umbiquiti_networks -- edgemax_edgeswitch	DoS in EdgeMAX EdgeSwitch prior to 1.8.2 allow an Admin user to Crash the SSH CLI interface by using crafted commands.	2019-07-10	not yet calculated	<a href="#">CVE-2019-5445</a> <a href="#">MISC</a>
				<a href="#">CVE-2019-</a>

vmware -- esxi	VMware ESXi 6.5 suffers from partial denial of service vulnerability in hostd process. Patch ESXi650-201907201-UG for this issue is available.	2019-07-11	not yet calculated	<a href="#">5528</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
wavpack -- wavpack	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseWave64HeaderConfig (wave64.c:211). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit <a href="https://github.com/dbry/WavPack/commit/33a0025d1d63ccd05d9dbaa6923d52b1446a62fe">https://github.com/dbry/WavPack/commit/33a0025d1d63ccd05d9dbaa6923d52b1446a62fe</a> .	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010319</a> <a href="#">MISC</a> <a href="#">MISC</a>
wavpack -- wavpack	WavPack 5.1.0 and earlier is affected by: CWE-457: Use of Uninitialized Variable. The impact is: Unexpected control flow, crashes, and segfaults. The component is: ParseCaffHeaderConfig (caff.c:486). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit <a href="https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b">https://github.com/dbry/WavPack/commit/f68a9555b548306c5b1ee45199ccdc4a16a6101b</a> .	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010317</a> <a href="#">MISC</a> <a href="#">MISC</a>
wavpack -- wavpack	WavPack 5.1 and earlier is affected by: CWE 369: Divide by Zero. The impact is: Divide by zero can lead to sudden crash of a software/service that tries to parse a .wav file. The component is: ParseDsdiffHeaderConfig (dsdiff.c:282). The attack vector is: Maliciously crafted .wav file. The fixed version is: After commit <a href="https://github.com/dbry/WavPack/commit/4c0faba32fd9bd0745cbfaf1e1aeb3da5d35b9fc">https://github.com/dbry/WavPack/commit/4c0faba32fd9bd0745cbfaf1e1aeb3da5d35b9fc</a> .	2019-07-11	not yet calculated	<a href="#">CVE-2019-1010315</a> <a href="#">MISC</a> <a href="#">MISC</a>
wesseek -- growi	In WESEEK GROWI before 3.5.0, the site-wide basic authentication can be bypassed by adding a URL parameter access_token (this is the parameter used by the API). No valid token is required since it is not validated by the backend. The website can then be browsed as if no basic authentication is required.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13337</a> <a href="#">MISC</a>
wesseek -- growi	In WESEEK GROWI before 3.5.0, a remote attacker can obtain the password hash of the creator of a page by leveraging wiki access to make API calls for page metadata. In other words, the password hash can be retrieved even though it is not a publicly available field.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13338</a> <a href="#">MISC</a>
wolfvision -- cynap	WolfVision Cynap before 1.30j uses a static, hard-coded cryptographic secret for generating support PINs for the 'forgot password' feature. By knowing this static secret and the corresponding algorithm for calculating support PINs, an attacker can reset the ADMIN password and thus gain remote access.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13352</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Rencontre plugin before 3.1.3 for WordPress allows SQL Injection via inc/rencontre_widget.php.	2019-07-08	not yet calculated	<a href="#">CVE-2019-13413</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Rencontre plugin before 3.1.3 for WordPress allows XSS via inc/rencontre_widget.php.	2019-07-08	not yet calculated	<a href="#">CVE-2019-13414</a> <a href="#">MISC</a> <a href="#">MISC</a>
zeromq -- libzmq	In ZeroMQ libzmq before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.3.2, a remote, unauthenticated client connecting to a libzmq application, running with a socket listening with CURVE encryption/authentication enabled, may cause a stack overflow and overwrite the stack with arbitrary data, due to a buffer overflow in the library. Users running public servers with the above configuration are highly encouraged to upgrade as soon as possible, as there are no known mitigations.	2019-07-10	not yet calculated	<a href="#">CVE-2019-13132</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">BUGTRAQ</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
zoho_manageengine -- assetexplorer	An issue was discovered in Zoho ManageEngine AssetExplorer. There is XSS via the SearchN.do search field.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12537</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- servicedesk_plus	An issue was discovered in Zoho ManageEngine ServiceDesk Plus 10.5. There is XSS via the WorkOrder.do search field.	2019-07-11	not yet calculated	<a href="#">CVE-2019-12540</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoom_video_communications -- zoom_client	In the Zoom Client before 4.4.2 on macOS, remote attackers can cause a denial of service (continual focus grabs) via a sequence of invalid launch?action=join&confno= requests to localhost port 19421.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13449</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoom_video_communications -- zoom_client	The Zoom Client before 4.4.53932.0709 on macOS allows remote code execution, a different vulnerability than CVE-2019-13450. If the ZoomOpener daemon (aka the hidden web server) is running, but the Zoom Client is not installed or can't be opened, an attacker can remotely execute code with a maliciously crafted launch URL. NOTE: ZoomOpener is removed by the Apple Malware Removal Tool (MRT) if this tool is enabled and has the 2019-07-10 MRTConfigData.	2019-07-12	not yet calculated	<a href="#">CVE-2019-13567</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoom_video_communications -- zoom_client_and_ringcentral	In the Zoom Client through 4.4.4 and RingCentral 7.0.136380.0312 on macOS, remote attackers can force a user to join a video call with the video camera active. This occurs because any web site can interact with the Zoom web server on localhost port 19421 or 19424. NOTE: a machine remains vulnerable if the Zoom Client was installed in the past and then uninstalled. Blocking exploitation requires additional steps, such as the ZDisableVideo preference and/or killing the web server, deleting the ~/.zoomus directory, and creating a ~/.zoomus plain file.	2019-07-09	not yet calculated	<a href="#">CVE-2019-13450</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
zte -- mw_nr8000	ZTE MW NR8000V2.4.4.03 and NR8000V2.4.4.04 are impacted by path traversal vulnerability. Due to path traversal, users can download any files.	2019-07-11	not yet calculated	<a href="#">CVE-2019-3415</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [sca1.go](#). If you need help or have questions, please send an email to [info@sca1.go](mailto:info@sca1.go). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nasa-us-cert.gov to your address book.

OTHER RESOURCES  
[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED



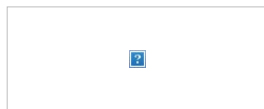
SUBSCRIBER SERVICES  
[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)





From: [US-CERT](#)  
To: [Tanner McGinnis](#)  
Subject: Vulnerability Summary for the Week of July 1, 2019  
Date: Monday, July 08, 2019 7:31:30 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## Vulnerability Summary for the Week of July 1, 2019

Original release date: July 8, 2019

The Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- web6000q_firmware	On Telus Actiontec WEB6000Q v1.1.02.22 devices, an attacker can login with root level access with the user "root" and password "admin" by using the enabled onboard UART headers.	2019-06-28	10.0	<a href="#">CVE-2018-15555</a> MISC <a href="#">FULLDISC</a>
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple heap-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution. Note: A different vulnerability than CVE-2019-10991.	2019-06-28	7.5	<a href="#">CVE-2019-10989</a> MISC MISC MISC
advantech -- webaccess	In WebAccess/SCADA, Versions 8.3.5 and prior, multiple stack-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	7.5	<a href="#">CVE-2019-10991</a> MISC MISC MISC MISC MISC MISC MISC
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple untrusted pointer dereference vulnerabilities may allow a remote attacker to execute arbitrary code.	2019-06-28	7.5	<a href="#">CVE-2019-10993</a> MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
chamilo -- chamilo_lms	Chamilo LMS 1.11.8 and 2.x allows remote code execution through an lp_upload.php unauthenticated file upload feature. It extracts a ZIP archive before checking its content, and once it has been extracted, does not check files in a recursive way. This means that by putting a .php file in a folder and then this folder in a ZIP archive, the server will accept this file without any checks. Because one can access this file from the website, it is remote code execution. This is related to a scorm/imsmanifest.xml file, the import_package function, and extraction in \$courseSysDir.\$newDir.	2019-06-30	7.5	<a href="#">CVE-2019-13082</a> MISC MISC
cszcms -- csz_cms	core/MY_Security.php in CSZ CMS 1.2.2 before 2019-06-20 has member/login/check SQL injection by sending a crafted HTTP User-Agent header and omitting the csrf_csz parameter.	2019-06-30	7.5	<a href="#">CVE-2019-13086</a> MISC
dosbox -- dosbox	DOSBox 0.74-2 has Incorrect Access Control.	2019-07-02	7.5	<a href="#">CVE-2019-12594</a> CONFIRM MLIST FEDORA MISC MISC
flowpaper -- flexpaper	The Publish Service in FlexPaper (later renamed FlowPaper) 2.3.6 allows remote code execution via setup.php and change_config.php.	2019-07-03	7.5	<a href="#">CVE-2018-11686</a> MISC MISC
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 could allow malicious user with access to the DB2 instance account to leverage a fenced execution process to execute arbitrary code as root. IBM X-Force ID: 156567.	2019-07-01	7.2	<a href="#">CVE-2019-4057</a> XF CONFIRM
	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1,			<a href="#">CVE-2019-4154</a>

ibm -- db2	10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 158519.	2019-07-01	7.2	<a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 161202.	2019-07-01	7.2	<a href="#">CVE-2019-4322</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
icon -- loopchain	In Loopchain through 2.2.1.3, an attacker can escalate privileges from a low-privilege shell by changing the environment (aka injection in the DEFAULT_SCORE_HOST environment variable).	2019-06-28	9.0	<a href="#">CVE-2019-12997</a> <a href="#">MISC</a>
lexmark -- 6500_firmware	Various Lexmark devices have a Buffer Overflow (issue 1 of 2).	2019-06-28	7.5	<a href="#">CVE-2018-15519</a> <a href="#">CONFIRM</a>
lexmark -- cx421_firmware	Various Lexmark devices have a Buffer Overflow (issue 2 of 2).	2019-06-28	7.5	<a href="#">CVE-2018-15520</a> <a href="#">CONFIRM</a>
matio_project -- matio	Multiple integer overflows exist in MATIO before 1.5.16, related to mat.c, mat4.c, mat5.c, mat73.c, and matvar_struct.c	2019-06-30	7.5	<a href="#">CVE-2019-13107</a> <a href="#">MISC</a>
netapp -- clustered_data_ontap	NetApp AFF A700s Baseboard Management Controller (BMC) firmware versions 1.22 and higher were shipped with a default account enabled that could allow unauthorized arbitrary command execution.	2019-07-01	7.5	<a href="#">CVE-2019-5497</a> <a href="#">CONFIRM</a>
nginx -- njs	njs through 0.3.3, used in NGINX, has a buffer over-read in nxt_utf8_decode in nxt/nxt_utf8.c. This issue occurs after the fix for CVE-2019-12207 is in place.	2019-06-29	7.5	<a href="#">CVE-2019-13067</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Authentication Bypass.	2019-07-02	7.5	<a href="#">CVE-2019-7266</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Authenticated Command Injection with root Code Execution.	2019-07-02	10.0	<a href="#">CVE-2019-7269</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Directory Traversal.	2019-07-02	7.5	<a href="#">CVE-2019-7253</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow File Inclusion.	2019-07-02	9.0	<a href="#">CVE-2019-7254</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Command Injections.	2019-07-02	10.0	<a href="#">CVE-2019-7256</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Unrestricted File Upload.	2019-07-02	7.5	<a href="#">CVE-2019-7257</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Hard-coded Credentials.	2019-07-02	10.0	<a href="#">CVE-2019-7261</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have a Version Control Failure.	2019-07-02	10.0	<a href="#">CVE-2019-7263</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow a Stack-based Buffer Overflow on the ARM platform.	2019-07-02	7.5	<a href="#">CVE-2019-7264</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Remote Code Execution (root access over SSH).	2019-07-02	10.0	<a href="#">CVE-2019-7265</a> <a href="#">MISC</a>
odoo -- odoo	Incorrect access control in the database manager component in Odoo Community 10.0 and 11.0 and Odoo Enterprise 10.0 and 11.0 allows a remote attacker to restore a database dump without knowing the super-admin password. An arbitrary password succeeds.	2019-06-28	7.5	<a href="#">CVE-2018-14885</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
optergy -- enterprise	Optergy Proton/Enterprise devices allow Authenticated File Upload with Code Execution as root.	2019-07-01	10.0	<a href="#">CVE-2019-7274</a> <a href="#">BID</a> <a href="#">MISC</a>
optergy -- enterprise	Optergy Proton/Enterprise devices allow Remote Root Code Execution via a Backdoor Console.	2019-07-01	10.0	<a href="#">CVE-2019-7276</a> <a href="#">BID</a> <a href="#">MISC</a>
optergy -- enterprise	Optergy Proton/Enterprise devices have Hard-coded Credentials.	2019-07-01	7.5	<a href="#">CVE-2019-7279</a> <a href="#">BID</a> <a href="#">MISC</a>
primasystems -- flexair	Prima Systems FlexAir devices allow Unauthenticated Command Injection resulting in Root Remote Code Execution.	2019-07-01	10.0	<a href="#">CVE-2019-7669</a> <a href="#">MISC</a>
primasystems -- flexair	Prima Systems FlexAir devices allow Authenticated Command Injection resulting in Root Remote Code Execution.	2019-07-01	9.0	<a href="#">CVE-2019-7670</a> <a href="#">MISC</a>
pulsesecure -- pulse_connect_secure	Session data between cluster nodes during cluster synchronization is not properly encrypted in Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX, PPS 5.2RX, or stand-alone devices.	2019-06-28	7.5	<a href="#">CVE-2018-20810</a> <a href="#">CONFIRM</a>
pulsesecure -- pulse_connect_secure	An input validation issue has been found with login_meeting.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2.	2019-06-28	7.5	<a href="#">CVE-2018-20813</a> <a href="#">CONFIRM</a>
redhat -- satellite	A path traversal flaw was found in spacewalk-proxy, all versions through 2.9, in the way the proxy processes cached client tokens. A remote, unauthenticated attacker could use this flaw to test the existence of arbitrary files, if they have access to the proxy's filesystem, or can execute arbitrary code in the context of the httpd process.	2019-07-02	7.5	<a href="#">CVE-2019-10137</a> <a href="#">CONFIRM</a>

synology -- calendar	OS command injection vulnerability in drivers_syno_import_user.php in Synology Calendar before 2.3.1-0617 allows remote attackers to execute arbitrary commands via the crafted 'X-Real-IP' header.	2019-06-30	<a href="#">7.5</a>	<a href="#">CVE-2019-11829 CONFIRM</a>
synology -- photo_station	SQL injection vulnerability in synophoto_csPhotoDB.php in Synology Photo Station before 6.8.11-3489 and before 6.3-2977 allows remote attackers to execute arbitrary SQL command via the type parameter.	2019-06-30	<a href="#">7.5</a>	<a href="#">CVE-2019-11821 CONFIRM</a>
toaruos -- toaruos	linker/linker.c in ToaruOS through 1.10.9 has insecure LD_LIBRARY_PATH handling in setuid applications.	2019-06-29	<a href="#">7.2</a>	<a href="#">CVE-2019-13046 MISC</a>
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 has incorrect access control in sys_sysfunc case 9 for TOARU_SYS_FUNC_SETHEAP, allowing arbitrary kernel pages to be mapped into user land, leading to root access.	2019-06-29	<a href="#">7.2</a>	<a href="#">CVE-2019-13047 MISC</a>
toaruos -- toaruos	An integer wrap in kernel/sys/syscall.c in ToaruOS 1.10.10 allows users to map arbitrary kernel pages into userland process space via TOARU_SYS_FUNC_MMAP, leading to escalation of privileges.	2019-06-29	<a href="#">7.2</a>	<a href="#">CVE-2019-13049 MISC</a>
web-gooroo -- cms_web-gooroo	SQL injection vulnerability in /wbq/core/_includes/authorization.inc.php in CMS Web-Gooroo through 2013-01-19 allows remote attackers to execute arbitrary SQL commands via the wbq_login parameter.	2019-07-03	<a href="#">7.5</a>	<a href="#">CVE-2017-18346 MISC EXPLOIT-DB</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x00000000000024ed.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13247 MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x0000000000002450.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13248 MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x00000000000b9e7a.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13249 MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x00000000000b9c2f.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13250 MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x00000000000c47ff.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13251 MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x00000000001172b0.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13252 MISC</a>
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, an out-of-bounds read vulnerability is caused by a lack of proper validation of user-supplied data. Exploitation of this vulnerability may allow disclosure of information.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2019-10983 MISC MISC</a>
advantech -- webaccess	In WebAccess/SCADA, Versions 8 3 5 and prior, a path traversal vulnerability is caused by a lack of proper validation of a user-supplied path prior to use in file operations. An attacker can leverage this vulnerability to delete files while posing as an administrator.	2019-06-28	<a href="#">6.4</a>	<a href="#">CVE-2019-10985 MISC MISC</a>
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple out-of-bounds write vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	<a href="#">6.8</a>	<a href="#">CVE-2019-10987 MISC MISC MISC</a>
advisto -- peel_shopping	Advisto PEEL SHOPPING 9.0.0 has CSRF via en/achat/caddie_ajout.php and en/achat/caddie_affichage.php, as demonstrated by an XSS payload in the couleurId[0] parameter to the latter.	2019-06-30	<a href="#">6.8</a>	<a href="#">CVE-2018-20848 MISC</a>
arastta -- ecommerce	Arastta eCommerce 1.6.2 is vulnerable to XSS via the PATH_INFO to the login/URI.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20849 MISC</a>
archon_project -- archon	packages/subjects/pub/subjects.php in Archon 3 21 rev-1 has XSS in the referer parameter in an index.php?subjectypeid=xxx request, aka Open Bug Bounty ID OBB-466362.	2019-07-03	<a href="#">4.3</a>	<a href="#">CVE-2017-17972 MISC</a>
audio_file_library_project -- audio_file_library	In Audio File Library (aka audiofile) 0.3.6, there exists one NULL pointer dereference bug in ulaw2linear_buf in G711.cpp in libmodules.a that allows an attacker to cause a denial of service via a crafted file.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-13147 MISC</a>
cyberpanel -- cyberpanel	An issue was discovered in CyberPanel through 1 8.4. On the user edit page, an attacker can edit the administrator's e-mail and password because of the lack of CSRF protection.	2019-07-02	<a href="#">6.8</a>	<a href="#">CVE-2019-13056 MISC MISC</a>
elitecms -- elite_cms	An issue was discovered in Elite CMS Pro 2 01. In /admin/add_sidebar.php, the ?page= parameter is vulnerable to SQL injection.	2019-07-03	<a href="#">6.5</a>	<a href="#">CVE-2018-12250 MISC MISC</a>
exiv2 -- exiv2	An integer overflow in Exiv2 through 0 27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted PNG image file, because PngImage::readMetadata mishandles a zero value for iccOffset.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13108 MISC MISC</a>
exiv2 -- exiv2	An integer overflow in Exiv2 through 0 27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted PNG image file, because PngImage::readMetadata mishandles a chunkLength - iccOffset subtraction.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13109 MISC MISC</a>
exiv2 -- exiv2	A ClffDirectory::readDirectory integer overflow and out-of-bounds read in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted CRW image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13110 MISC MISC</a>
exiv2 -- exiv2	A WebPImage::decodeChunks integer overflow in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (large heap allocation followed by a very long running loop) via a crafted WEBP image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13111 MISC MISC</a>
exiv2 -- exiv2	A PngChunk::parseChunkContent uncontrolled memory allocation in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (crash due to an std::bad_alloc exception) via a crafted PNG image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13112 MISC MISC</a>
exiv2 -- exiv2	Exiv2 through 0 27.1 allows an attacker to cause a denial of service (crash due to assertion failure) via an invalid data location in a CRW image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13113 MISC MISC</a>
	http.c in Exiv2 through 0.27.1 allows a malicious http server to cause a denial of			<a href="#">CVE-2019-13114</a>

exiv2 -- exiv2	service (crash due to a NULL pointer dereference) by returning a crafted response that lacks a space character.	2019-06-30	<a href="#">4.3</a>	<a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.5, 13.0 0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4 and BIG-IQ 6.0.0-6.1.0 and 5.1.0-5.4.0, an undisclosed iControl REST worker vulnerable to command injection for an Administrator user.	2019-07-02	<a href="#">6.5</a>	<a href="#">CVE-2019-6620</a> <a href="#">CONFIRM</a>
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.5, 13.0 0-13.1.1.4, 12.1.0-12.1.4.1, 11.6.1-11.6.3.4, and 11 5.1-11 5.8 and BIG-IQ 6.0.0-6.1.0 and 5.1.0-5.4.0, an undisclosed iControl REST worker is vulnerable to command injection by an admin/resource admin user. This issue impacts both iControl REST and tmsh implementations.	2019-07-02	<a href="#">6.5</a>	<a href="#">CVE-2019-6621</a> <a href="#">CONFIRM</a>
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.5, 13.0 0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4, an undisclosed iControl REST worker is vulnerable to command injection by an administrator or resource administrator user. This attack is only exploitable on multi-bladed systems.	2019-07-02	<a href="#">6.5</a>	<a href="#">CVE-2019-6622</a> <a href="#">CONFIRM</a>
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.4, 13.0 0-13.1.1.4, and 12.1.0-12.1.4, undisclosed traffic sent to BIG- P iSession virtual server may cause the Traffic Management Microkernel (TMM) to restart, resulting in a Denial-of-Service (DoS).	2019-07-02	<a href="#">5.0</a>	<a href="#">CVE-2019-6623</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.4, 13.0 0-13.1.1.4, and 12.1.0-12.1.4, an undisclosed traffic pattern sent to a BIG-IP UDP virtual server may lead to a denial-of-service (DoS).	2019-07-02	<a href="#">5.0</a>	<a href="#">CVE-2019-6624</a> <a href="#">CONFIRM</a>
f5 -- websafe_alert_server	A Cross Site Scripting (XSS) vulnerability in versions of F5 WebSafe Dashboard 3.9 x and earlier, aka F5 WebSafe Alert Server, allows an unauthenticated user to inject HTML via a crafted alert.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2016-5235</a> <a href="#">CONFIRM</a>
fla-shop -- html5_maps	Cross-site request forgery (CSRF) vulnerability in HTML5 Maps 1 6 5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	<a href="#">6.8</a>	<a href="#">CVE-2019-5983</a> <a href="#">MISC</a> <a href="#">MISC</a>
flightcrew_project -- flightcrew	An issue was discovered in FlightCrew v0.9.2 and earlier. A NULL pointer dereference occurs in GetRelativePathToNcx() or GetRelativePathsToXhtmlDocuments() when a NULL pointer is passed to xc::XMLUri::IsValidURI(). This affects third-party software (not Sigil) that uses FlightCrew as a library.	2019-06-28	<a href="#">4.3</a>	<a href="#">CVE-2019-13032</a> <a href="#">MISC</a>
gnome -- glib	The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.59.1 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used. This is similar to CVE-2019-12450.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2019-13012</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
grafana -- grafana	public/app/features/panel/panel_ctrl.ts in Grafana before 6.2.5 allows HTML Injection in panel drilldown links (via the Title or url field).	2019-06-29	<a href="#">4.3</a>	<a href="#">CVE-2019-13068</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- bigfix_inventory	IBM BigFix Inventory v9 (SUA v9 / LMT v9) discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161807.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2019-4369</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">XF</a>
ibm -- daeja_viewone	IBM Daeja ViewONE Professional, Standard & Virtual 5.0 through 5.0.5 could allow an unauthorized user to download server files resulting in sensitive information disclosure. IBM X-Force ID: 160012.	2019-07-02	<a href="#">5.0</a>	<a href="#">CVE-2019-4260</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. BM X-Force ID: 158092.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-4102</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158281.	2019-07-02	<a href="#">4.3</a>	<a href="#">CVE-2019-4134</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10.5 could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable web server. BM X-Force ID: 160698.	2019-07-02	<a href="#">6.5</a>	<a href="#">CVE-2019-4292</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8 0, 8 5, and 9 0 Admin Console could allow a remote attacker to obtain sensitive information when a specially crafted url causes a stack trace to be dumped. IBM X-Force ID: 160202.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2019-4269</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadBMPImage in coders/bmp.c.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-13133</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadVIFImage in coders/viff.c.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-13134</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability in the function ReadCUTImage in coders/cut.c.	2019-07-01	<a href="#">6.8</a>	<a href="#">CVE-2019-13135</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has an integer overflow vulnerability in the function TIFFSeekCustomStream in coders/tiff.c.	2019-07-01	<a href="#">6.8</a>	<a href="#">CVE-2019-13136</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadPSImage in coders/ps.c.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-13137</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
intelliants -- subrion	Subrion CMS before 4.1.4 has XSS.	2019-07-03	<a href="#">4.3</a>	<a href="#">CVE-2018-11317</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2019-13045</a>

irssi -- irssi	Irssi before 1.0.8, 1.1.x before 1.1.3, and 1.2.x before 1.2.1, when SASL is enabled, has a use after free when sending SASL login to the server.	2019-06-29	6.8	<a href="#">SUSE MISC MLIST BID MISC MISC BUGTRAQ UBUNTU</a>
istio -- istio	Istio before 1.2.2 mishandles certain access tokens, leading to "Epoch 0 terminated with an error" in Envoy. This is related to a jwt_authenticator.cc segmentation fault.	2019-06-28	5.0	<a href="#">CVE-2019-12995 MISC MISC MISC</a>
jetbrains -- teamcity	A reflected XSS on a user page was detected on one of the JetBrains TeamCity pages. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	4.3	<a href="#">CVE-2019-12842 CONFIRM</a>
jetbrains -- teamcity	The generated Kotlin DSL settings allowed usage of an unencrypted connection for resolving artifacts. The issue was fixed in JetBrains TeamCity 2018.2.3.	2019-07-03	5.0	<a href="#">CVE-2019-12845 MISC</a>
jetbrains -- teamcity	A user without the required permissions could gain access to some JetBrains TeamCity settings. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	4.0	<a href="#">CVE-2019-12846 CONFIRM</a>
kubevirt -- containerized-data-importer	A flaw was found in the containerized-data-importer in virt-cdi-cloner, version 1.4, where the host-assisted cloning feature does not determine whether the requesting user has permission to access the Persistent Volume Claim (PVC) in the source namespace. This could allow users to clone any PVC in the cluster into their own namespace, effectively allowing access to other user's data.	2019-06-28	4.0	<a href="#">CVE-2019-10175 CONFIRM</a>
lemonldap-ng -- lemonldap::	LemonLDAP: NG before 1.9.20 has an XML External Entity (XXE) issue when submitting a notification to the notification server. By default, the notification server is not enabled and has a "deny all" rule.	2019-06-28	6.8	<a href="#">CVE-2019-13031 MISC MLIST</a>
mod_auth_mellon_project -- mod_auth_mellon	mod_auth_mellon through 0.14.2 has an Open Redirect via the login?ReturnTo=substring, as demonstrated by omitting the // after http: in the target URL.	2019-06-29	4.3	<a href="#">CVE-2019-13038 MISC</a>
monstra -- monstra_cms	Monstra CMS before 3.0.4 has XSS via index.php.	2019-07-03	4.3	<a href="#">CVE-2018-11227 MISC MISC EXPLOIT-DB</a>
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Cross-Site Request Forgery (CSRF).	2019-07-02	6.8	<a href="#">CVE-2019-7270 MISC MISC</a>
nortekcontrol -- linear_emerge_5000p_firmware	Nortek Linear eMerge 50P/5000P devices have Default Credentials.	2019-07-01	5.0	<a href="#">CVE-2019-7271 MISC MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Default Credentials.	2019-07-02	5.0	<a href="#">CVE-2019-7252 MISC MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow XSS.	2019-07-02	4.3	<a href="#">CVE-2019-7255 MISC MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Privilege Escalation.	2019-07-02	6.5	<a href="#">CVE-2019-7258 MISC MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Authorization Bypass with Information Disclosure.	2019-07-02	4.0	<a href="#">CVE-2019-7259 MISC MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Cleartext Credentials in a Database.	2019-07-02	5.0	<a href="#">CVE-2019-7260 MISC MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Cross-Site Request Forgery (CSRF).	2019-07-02	6.8	<a href="#">CVE-2019-7262 MISC MISC</a>
novaksolutions -- infusionsoft-php-sdk	novaksolutions/infusionsoft-php-sdk v2016-10-31 is vulnerable to a reflected XSS in the leadscoring.php resulting code execution	2019-07-03	4.3	<a href="#">CVE-2017-6216 MISC</a>
odoo -- odoo	Improper data access control in Odoo Community 10.0 and 11.0 and Odoo Enterprise 10.0 and 11.0 allows authenticated users to perform a CSV export of the secure hashed passwords of other users.	2019-07-03	4.0	<a href="#">CVE-2018-14861 CONFIRM</a>
odoo -- odoo	Incorrect access control in the mail templating system in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated internal users to delete arbitrary menuitems via a crafted RPC request.	2019-07-03	5.5	<a href="#">CVE-2018-14862 CONFIRM</a>
odoo -- odoo	Incorrect access control in the RPC framework in Odoo Community 8.0 through 11.0 and Odoo Enterprise 9.0 through 11.0 allows authenticated users to call private functions via RPC.	2019-07-03	5.5	<a href="#">CVE-2018-14863 CONFIRM</a>
odoo -- odoo	Incorrect access control in asset bundles in Odoo Community 9.0 through 11.0 and earlier and Odoo Enterprise 9.0 through 11.0 and earlier allows remote authenticated users to inject arbitrary web script via a crafted attachment.	2019-07-03	4.0	<a href="#">CVE-2018-14864 CONFIRM</a>
odoo -- odoo	Report engine in Odoo Community 9.0 through 11.0 and earlier and Odoo Enterprise 9.0 through 11.0 and earlier does not use secure options when passing documents to wkhtmltopdf, which allows remote attackers to read local files.	2019-07-03	4.0	<a href="#">CVE-2018-14865 CONFIRM</a>
odoo -- odoo	Incorrect access control in the portal messaging system in Odoo Community 9.0 and 10.0 and Odoo Enterprise 9.0 and 10.0 allows remote attackers to post messages on behalf of customers, and to guess document attribute values, via crafted parameters.	2019-06-28	5.0	<a href="#">CVE-2018-14867 MISC CONFIRM</a>
odoo -- odoo	Incorrect access control in the Password Encryption module in Odoo Community 9.0 and Odoo Enterprise 9.0 allows authenticated users to change the password of other users without knowing their current password via a crafted RPC call.	2019-06-28	4.0	<a href="#">CVE-2018-14868 MISC CONFIRM</a>
odoo -- odoo	The module-description renderer in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier does not disable RST's local file inclusion, which allows privileged authenticated users to read local files via a crafted module description.	2019-06-28	4.0	<a href="#">CVE-2018-14886 MISC CONFIRM</a>



odoo -- odoo	Improper Host header sanitization in the dbfilter routing component in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows a remote attacker to deny access to the service and to disclose database names via a crafted request.	2019-06-28	5.8	<a href="#">CVE-2018-14887</a> MISC CONFIRM
open-xchange -- ox_guard	OX Guard 2.8.0 has CSRF.	2019-07-03	6.8	<a href="#">CVE-2018-10986</a> CONFIRM
optergy -- enterprise	Optergy Proton/Enterprise devices allow Username Disclosure.	2019-07-01	5.0	<a href="#">CVE-2019-7272</a> BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Cross-Site Request Forgery (CSRF).	2019-07-01	6.8	<a href="#">CVE-2019-7273</a> BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Open Redirect.	2019-07-01	5.8	<a href="#">CVE-2019-7275</a> BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Unauthenticated Internal Network Information Disclosure.	2019-07-01	5.0	<a href="#">CVE-2019-7277</a> BID MISC MISC
optergy -- enterprise	Optergy Proton/Enterprise devices have an Unauthenticated SMS Sending Service.	2019-07-01	6.4	<a href="#">CVE-2019-7278</a> BID MISC MISC
paloaltonetworks -- minemeld	Cross-site scripting vulnerability in Palo Alto Networks MineMeld version 0.9.60 and earlier may allow a remote attacker able to convince an authenticated MineMeld admin to type malicious input in the MineMeld UI could execute arbitrary JavaScript code in the admin's browser.	2019-07-01	4.3	<a href="#">CVE-2019-1578</a> CONFIRM
paloaltonetworks -- traps	Code injection vulnerability in Palo Alto Networks Traps 5.0.5 and earlier may allow an authenticated attacker to inject arbitrary JavaScript or HTML.	2019-07-01	6.5	<a href="#">CVE-2019-1577</a> BID CONFIRM
primasystems -- flexair	Prima Systems FlexAir devices have an Insufficient Session-ID Length.	2019-07-01	4.0	<a href="#">CVE-2019-7280</a> MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices allow Cross-Site Request Forgery (CSRF).	2019-07-01	6.8	<a href="#">CVE-2019-7281</a> MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices allow authentication with MD5 hashes directly.	2019-07-01	6.5	<a href="#">CVE-2019-7666</a> MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices allow unauthenticated download of the database configuration backup due to a predictable name, resulting in authentication bypass (a login authenticated with the MD5 hash of any user found in the database).	2019-07-01	6.4	<a href="#">CVE-2019-7667</a> MISC MISC
primasystems -- flexair	Prima Systems FlexAir devices have Default Credentials.	2019-07-01	5.0	<a href="#">CVE-2019-7668</a> MISC MISC
pulsesecure -- pulse_connect_secure	An XSS issue has been found with rd.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R3 due to improper header sanitization. This is not applicable to 8.1RX.	2019-06-28	4.3	<a href="#">CVE-2018-20808</a> CONFIRM
pulsesecure -- pulse_connect_secure	A crafted message can cause the web server to crash with Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R5 and Pulse Policy Secure 5.4RX before 5.4R5. This is not applicable to PCS 8.1RX.	2019-06-28	5.0	<a href="#">CVE-2018-20809</a> CONFIRM
pulsesecure -- pulse_connect_secure	A hidden RPC service issue was found with Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2 and 8.1RX before 8.1R12.	2019-06-28	5.0	<a href="#">CVE-2018-20811</a> CONFIRM
pulsesecure -- pulse_connect_secure	An XSS issue was found with Psaldownload.cgi in Pulse Secure Pulse Connect Secure (PCS) 8.3R2 before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX or PPS 5.2RX.	2019-06-28	4.3	<a href="#">CVE-2018-20814</a> BID CONFIRM
pulsesecure -- pulse_secure_desktop_client	An information exposure issue where IPv6 DNS traffic would be sent outside of the VPN tunnel (when Traffic Enforcement was enabled) exists in Pulse Secure Pulse Secure Desktop 9.0R1 and below. This is applicable only to dual-stack (IPv4/IPv6) endpoints.	2019-06-28	5.0	<a href="#">CVE-2018-20812</a> CONFIRM
rapid7 -- nexpose	A Cross-Site Request Forgery (CSRF) vulnerability was found in Rapid7 Nexpose InsightVM Security Console versions 6.5.0 through 6.5.68. This issue allows attackers to exploit CSRF vulnerabilities on API endpoints using Flash to circumvent a cross-domain pre-flight OPTIONS request.	2019-07-03	6.8	<a href="#">CVE-2019-5630</a> CONFIRM
redhat -- satellite	It was found that Spacewalk, all versions through 2.9, did not safely compute client token checksums. An attacker with a valid, but expired, authenticated set of headers could move some digits around, artificially extending the session validity without modifying the checksum.	2019-07-02	4.0	<a href="#">CVE-2019-10136</a> BID CONFIRM
rockoa -- rockoa	RockOA 1.8.7 allows remote attackers to obtain sensitive information because the webmain/webmainAction.php publictreestore method constructs a SQL WHERE clause unsafely by using the pidfields and idfields parameters, aka background SQL injection.	2019-06-28	4.0	<a href="#">CVE-2019-9846</a> MISC
seeddms -- seeddms	A stored XSS vulnerability was found in SeedDMS 5.1.11 due to poorly escaping the search result in the autocomplete search form placed in the header of out/out.Viewfolder.php.	2019-06-28	4.3	<a href="#">CVE-2019-12932</a> MISC
squirrelmail -- squirrelmail	XSS was discovered in SquirrelMail through 1.4.22 and 1.5.x through 1.5.2. Due to improper handling of RCDATA and RAWTEXT type elements, the built-in sanitization mechanism can be bypassed. Malicious script content from HTML e-mail can be executed within the application context via crafted use of (for example) a NOEMBED, NOFRAMES, NOSCRIPT, or TEXTAREA element.	2019-07-01	4.3	<a href="#">CVE-2019-12970</a> MISC BUGTRAQ MISC
	Symantec Endpoint Encryption, prior to SEE 11.3.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue that allows a user to			<a href="#">CVE-2019-9702</a>

symantec -- endpoint_encryption	gain elevated access to resources that are normally protected at lower access levels.	2019-07-01	4.6	<a href="#">CVE-2019-9703</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
symantec -- endpoint_encryption	Symantec Endpoint Encryption, prior to SEE 11.3.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue that allows a user to gain elevated access to resources that are normally protected at lower access levels.	2019-07-01	4.6	<a href="#">CVE-2019-9703</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
synology -- moments	Relative path traversal vulnerability in SYNO.PhotoTeam.Upload.Item in Synology Moments before 1.3.0-0691 allows remote authenticated users to upload arbitrary files via the name parameter.	2019-06-30	6.5	<a href="#">CVE-2019-11826</a> <a href="#">CONFIRM</a>
synology -- photo_station	Relative path traversal vulnerability in SYNO.PhotoStation.File in Synology Photo Station before 6.8.11-3489 and before 6.3-2977 allows remote attackers to upload arbitrary files via the uploadphoto parameter.	2019-06-30	4.0	<a href="#">CVE-2019-11822</a> <a href="#">CONFIRM</a>
tenable -- nessus	Content Injection vulnerability in Tenable Nessus prior to 8.5.0 may allow an authenticated, local attacker to exploit this vulnerability by convincing another targeted Nessus user to view a malicious URL and use Nessus to send fraudulent messages. Successful exploitation could allow the authenticated adversary to inject arbitrary text into the feed status, which will remain saved post session expiration.	2019-07-01	4.3	<a href="#">CVE-2019-3962</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 allows a denial of service upon a critical error in certain sys_sbrk allocation patterns (involving PAGE_SIZE, and a value less than PAGE_SIZE).	2019-06-29	4.9	<a href="#">CVE-2019-13048</a> <a href="#">MISC</a>
waspthemes -- custom_css_pro	Cross-site request forgery (CSRF) vulnerability in Custom CSS Pro 1.0.3 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5984</a> <a href="#">MISC</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000384e2a.	2019-06-30	6.8	<a href="#">CVE-2019-13083</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000026b739.	2019-06-30	6.8	<a href="#">CVE-2019-13084</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000030ecfa.	2019-06-30	6.8	<a href="#">CVE-2019-13085</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000385474.	2019-07-04	6.8	<a href="#">CVE-2019-13253</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e808.	2019-07-04	6.8	<a href="#">CVE-2019-13254</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000327464.	2019-07-04	6.8	<a href="#">CVE-2019-13255</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e849.	2019-07-04	6.8	<a href="#">CVE-2019-13256</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x00000000003273aa.	2019-07-04	6.8	<a href="#">CVE-2019-13257</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000328165.	2019-07-04	6.8	<a href="#">CVE-2019-13258</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e566.	2019-07-04	6.8	<a href="#">CVE-2019-13259</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000327a07.	2019-07-04	6.8	<a href="#">CVE-2019-13260</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000328384.	2019-07-04	6.8	<a href="#">CVE-2019-13261</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x00000000003283eb.	2019-07-04	6.8	<a href="#">CVE-2019-13262</a> <a href="#">MISC</a>
xpertsol -- server_status_by_hostname/ip	A SQL injection vulnerability in the Xpert Solution "Server Status by Hostname/ P" plugin 4.6 for WordPress allows an authenticated user to execute arbitrary SQL commands via GET parameters.	2019-07-03	6.5	<a href="#">CVE-2019-12570</a> <a href="#">MISC</a>
zoneminder -- zoneminder	Stored XSS in the Filters page (Name field) in ZoneMinder 1.32.3 allows a malicious user to embed and execute JavaScript code in the browser of any user who navigates to this page.	2019-06-29	4.3	<a href="#">CVE-2019-13072</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/page-edit.php (content box), which can be used to get a user's cookie.	2019-07-05	3.5	<a href="#">CVE-2019-13339</a> <a href="#">MISC</a>
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the content box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, CVE-2018-20520, and CVE-2019-13186.	2019-07-05	3.5	<a href="#">CVE-2019-13340</a> <a href="#">MISC</a>
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/conf.php (comment box), which can be used to get a user's cookie.	2019-07-05	3.5	<a href="#">CVE-2019-13341</a> <a href="#">MISC</a>
f5 -- websafe_alert_server	Cross-Site-Scripting (XSS) vulnerabilities in F5 WebSafe Dashboard 3.9.5 and earlier, aka F5 WebSafe Alert Server, allow privileged authenticated users to inject arbitrary web script or HTML when creating a new user, account or signature.	2019-07-01	3.5	<a href="#">CVE-2016-5236</a> <a href="#">CONFIRM</a>
fujielectric -- alpha7_pc_loader_firmware	An out-of-bounds read vulnerability has been identified in Fuji Electric Alpha7 PC Loader Versions 1.1 and prior, which may crash the system.	2019-07-02	3.3	<a href="#">CVE-2019-10975</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, and 19.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force	2019-07-01	3.5	<a href="#">CVE-2019-4410</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>

	ID: 162657.			
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.1, 10.5, and 11.1 is vulnerable to a denial of service. Users that have both EXECUTE on PD_GET_DIAG_HIST and access to the diagnostic directory on the DB2 server can cause the instance to crash. BM X-Force D: 158091.	2019-07-01	2.1	<a href="#">CVE-2019-4101</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect	IBM Tivoli Storage Manager Server ( BM Spectrum Protect 7.1 and 8.1) could allow a local user to replace existing databases by restoring old data. IBM X-Force ID: 158336.	2019-07-02	3.6	<a href="#">CVE-2019-4140</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
synology -- calendar	Cross-site scripting (XSS) vulnerability in Event Editor in Synology Calendar before 2.3.0-0615 allows remote attackers to inject arbitrary web script or HTML via the title parameter.	2019-06-30	3.5	<a href="#">CVE-2019-11825</a> <a href="#">CONFIRM</a>
synology -- note_station	Cross-site scripting (XSS) vulnerability in SYNO.NoteStation.Shard in Synology Note Station before 2.5.3-0863 allows remote attackers to inject arbitrary web script or HTML via the object_id parameter.	2019-06-30	3.5	<a href="#">CVE-2019-11827</a> <a href="#">CONFIRM</a>
synology -- office	Cross-site scripting (XSS) vulnerability in Chart in Synology Office before 3.1.4-2771 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2019-06-30	3.5	<a href="#">CVE-2019-11828</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a.t.works -- idoors_reader	Doors Reader 2.10.17 and earlier allows an attacker on the same network segment to bypass authentication to access the management console and operate the product via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5964</a> <a href="#">MISC</a> <a href="#">MISC</a>
amcrest -- ipm-721s_devices	On Amcrest PM-721S V2.420.AC00.16 R.20160909 devices, the users on the device are divided into 2 groups "admin" and "user". However, as a part of security analysis it was identified that a low privileged user who belongs to the "user" group and who has access to login in to the web administrative interface of the device can add a new administrative user to the interface using HTTP APIs provided by the device and perform all the actions as an administrative user by using that account. If the firmware version V2.420.AC00.16 R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable functions that performs the various action described in HTTP APIs. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function at address 0x00429084 in IDA pro is the one that processes the HTTP API request for "addUser" action. If one races the calls to this function, it can be clearly seen that the unction sub_41F38C at address 0x0041F588 parses the call received from the browser and passes it to the "addUser" unction without any authorization check.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8230</a> <a href="#">MISC</a> <a href="#">MISC</a>
amcrest -- ipm-721s_devices	The Amcrest IPM-721S Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322 allows HTTP requests that permit enabling various functionalities of the camera by using HTTP APIs, instead of the web management interface that is provided by the application. This HTTP API receives the credentials as base64 encoded in the Authorization HTTP header. However, a missing length check in the code allows an attacker to send a string of 1024 characters in the password field, and allows an attacker to exploit a memory corruption issue. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials. If the firmware version Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322 is dissected using the binwalk tool, one obtains a _user-x.squashfs img.extracted archive which contains the filesystem set up on the device that has many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the HTTP API specification. If we open this binary in DA Pro we will notice that this follows an ARM little-endian format. The function at address 00415364 in IDA Pro starts the HTTP authentication process. This function calls another function at sub_0042CCA0 at address 0041549C. This function performs a strchr operation after base64 decoding the credentials, and stores the result on the stack, which results in a stack-based buffer overflow.	2019-07-03	not yet calculated	<a href="#">CVE-2017-13719</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
amcrest -- ipm-721s_devices	Amcrest PM-721S V2.420.AC00.16 R.20160909 devices have default credentials that are hardcoded in the firmware and can be extracted by anyone who reverses the firmware to identify them. If the firmware version V2.420.AC00.16 R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If one opens this binary in DA-pro, one will notice that this follows a ARM little endian format. The unction sub_3DB2FC in DA pro is identified to be setting up the values at address 0x003DB5A6. The sub_5C057C then sets this value and adds it to the Configuration files in mnt/mt/Config/Account1 file.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8226</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>

amcrest -- ipm-721s_devices	Amcrest PM-721S V2.420.AC00.16.R.20160909 devices have a timeout policy to wait for 5 minutes in case 30 incorrect password attempts are detected using the Web and HTTP API interface provided by the device. However, if the same brute force attempt is performed using the ONVIF specification (which is supported by the same binary) then there is no account lockout or timeout executed. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials. If the firmware version V2.420.AC00.16.R.9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the ONVIF specification. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function at address 00671618 in IDA pro is parses the WSSE security token header. The sub_603D8 then performs the authentication check and if it is incorrect passes to the function sub_59F4C which prints the value "Sender not authorized."	2019-07-03	not yet calculated	<a href="#">CVE-2017-8227</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
amcrest -- ipm-721s_devices	Amcrest PM-721S V2.420.AC00.16.R.20160909 devices mishandle reboots within the past two hours. Amcrest cloud services does not perform a thorough verification when allowing the user to add a new camera to the user's account to ensure that the user actually owns the camera other than knowing the serial number of the camera. This can allow an attacker who knows the serial number to easily add another user's camera to an attacker's cloud account and control it completely. This is possible in case of any camera that is currently not a part of an Amcrest cloud account or has been removed from the user's cloud account. Also, another requirement for a successful attack is that the user should have rebooted the camera in the last two hours. However, both of these conditions are very likely for new cameras that are sold over the Internet at many ecommerce websites or vendors that sell the Amcrest products. The successful attack results in an attacker being able to completely control the camera which includes being able to view and listen on what the camera can see, being able to change the motion detection settings and also be able to turn the camera off without the user being aware of it. Note: The same attack can be executed using the Amcrest Cloud mobile application.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8228</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
amcrest -- ipm-721s_devices	Amcrest PM-721S V2.420.AC00.16.R.20160909 devices allow an unauthenticated attacker to download the administrative credentials. If the firmware version V2.420.AC00.16.R.9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function sub_436D6 in IDA pro is identified to be setting up the configuration for the device. If one scrolls to the address 0x000437C2 then one can see that /current_config is being set as an ALIAS for /mnt/mtd/Config folder on the device. If one TELNETs into the device and navigates to /mnt/mtd/Config folder, one can observe that it contains various files such as Account1, Account2, SHAACcount1, etc. This means that if one navigates to http://[Ipofcamera]/current_config/Sha1Account1 then one should be able to view the content of the files. The security researchers assumed that this was only possible only after authentication to the device. However, when unauthenticated access tests were performed for the same URL as provided above, it was observed that the device file could be downloaded without any authentication.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8229</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
arox -- school-erp_pro	AROX School-ERP Pro has a command execution vulnerability. import_stud.php and upload_file.php do not have session control. Therefore an unauthenticated user can execute a command on the system.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13294</a> <a href="#">MISC</a> <a href="#">MISC</a>
artica -- pandora_fms	Artica Pandora FMS 7.0 NG before 735 suffers from local privilege escalation due to improper permissions on C:\PandoraFMS and its sub-folders, allowing standard users to create new files. Moreover, the Apache service httpd.exe will try to execute cmd.exe from C:\PandoraFMS (the current directory) as NT AUTHORITY\SYSTEM upon web requests to the portal. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13035</a> <a href="#">MISC</a>
artifex -- mupdf	Artifex MuPDF 1.15.0 has a heap-based buffer overflow in z_append_display_node located at fitz/list-device.c, allowing remote attackers to execute arbitrary code via a crafted PDF file. This occurs with a large BDC property name that overflows the allocated size of a display list node.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13290</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
axiosys -- bento4	An issue was discovered in Bento4 1.5.1.0. A memory allocation failure is unhandled in Core/Api4SdpAtom.cpp and leads to crashes. When parsing input video, the program allocates a new buffer to parse an atom in the stream. The unhandled memory allocation failure causes a direct copy to a NULL pointer.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13238</a> <a href="#">MISC</a>
bks -- bks_ebk_ethernet_buskoppler_pro	BKS EBK Ethernet-Buskoppler Pro before 3.01 allows Unrestricted Upload of a File with a Dangerous Type.	2019-07-05	not yet calculated	<a href="#">CVE-2019-12971</a> <a href="#">MISC</a>
	It was discovered as a part of the research on IoT devices in the			

blipcare -- blipcare_wi-fi_blood_pressure_monitor	most recent firmware for Blipcare device that the device allows to connect to web management interface on a non-SSL connection using plain text HTTP protocol. The user uses the web management interface of the device to provide the user's Wi-Fi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is connected to the Blipcare's device wireless network to easily sniff these values using a MITM attack.	2019-07-02	not yet calculated	<a href="#">CVE-2017-11578</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
blipcare -- blipcare_wi-fi_blood_pressure_monitor	In the most recent firmware for Blipcare, the device provides an open Wireless network called "Blip" for communicating with the device. The user connects to this open Wireless network and uses the web management interface of the device to provide the user's Wi-Fi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is in vicinity of Wireless signal generated by the Blipcare device to easily sniff the credentials. Also, an attacker can connect to the open wireless network "Blip" exposed by the device and modify the HTTP response presented to the user by the device to execute other attacks such as convincing the user to download and execute a malicious binary that would infect a user's computer or mobile device with malware.	2019-07-02	not yet calculated	<a href="#">CVE-2017-11579</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
blipcare -- blipcare_wi-fi_blood_pressure_monitor	Blipcare Wifi blood pressure monitor BP700 10.1 devices allow memory corruption that results in Denial of Service. When connected to the "Blip" open wireless connection provided by the device, if a large string is sent as a part of the HTTP request in any part of the HTTP headers, the device could become completely unresponsive. Presumably this happens as the memory footprint provided to this device is very small. According to the specs from Rezolt, the Wi-Fi module only has 256k of memory. As a result, an incorrect string copy operation using either memcpy, strcpy, or any of their other variants could result in filling up the memory space allocated to the function executing and this would result in memory corruption. To test the theory, one can modify the demo application provided by the Cypress WICED SDK and introduce an incorrect "memcpy" operation and use the compiled application on the evaluation board provided by Cypress semiconductors with exactly the same Wi-Fi SOC. The results were identical where the device would completely stop responding to any of the ping or web requests.	2019-07-02	not yet calculated	<a href="#">CVE-2017-11580</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
blogengine -- blogengine net	BlogEngine.NET 3.3.7.0 allows /api/filemanager Directory Traversal via the path parameter.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10717</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
blogengine -- blogengine net	BlogEngine.NET 3.3.7.0 allows a Client Side URL Redirect via the returnUrl parameter, related to BlogEngine/BlogEngine.Core/Services/Security/Security.cs, login.aspx, and register.aspx.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10721</a> <a href="#">MISC</a> <a href="#">MISC</a>
calamares -- calamares	Calamares versions 3.1 through 3.2.10 copies a LUKS encryption keyfile from /crypto_keyfile.bin (mode 0600 owned by root) to /boot within a globally readable initramfs image with insecure permissions, which allows this originally protected file to be read by any user, thereby disclosing decryption keys for LUKS containers created with Full Disk Encryption.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13179</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
calamares -- calamares	modules/luksbootkeyfile/main.py in Calamares versions 3.1 through 3.2.10 has a race condition between the time when the LUKS encryption keyfile is created and when secure permissions are set.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13178</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon	Centreon V19.04 allows the attacker to execute arbitrary system commands by using the value "init_script"."Monitoring Engine Binary" in main.get.php to insert an arbitrary command into the database, and execute it by calling the vulnerable page www/include/configuration/configGenerate/xml/generateFiles.php which passes the inserted value to the database to shell_exec without sanitizing it, allowing one to execute system arbitrary commands).	2019-07-01	not yet calculated	<a href="#">CVE-2019-13024</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- 7800_and_8800_series_ip_phones	A vulnerability in Cisco SIP Phone Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected phone. The vulnerability is due to insufficient validation of input Session Initiation Protocol (SIP) packets. An attacker could exploit this vulnerability by altering the SIP replies that are sent to the affected phone during the registration process. A successful exploit could allow the attacker to cause the phone to reboot and not complete the registration process.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1922</a> <a href="#">CISCO</a>
cisco -- advanced_malware_protection_for_endpoints_for_windows	A vulnerability in Cisco Advanced Malware Protection (AMP) for Endpoints for Windows could allow an authenticated, local attacker with administrator privileges to execute arbitrary code. The vulnerability is due to insufficient validation of dynamically loaded modules. An attacker could exploit this vulnerability by	2019-07-05	not yet calculated	<a href="#">CVE-2019-1932</a> <a href="#">CISCO</a>



	placing a file in a specific location in the Windows filesystem. A successful exploit could allow the attacker to execute the code with the privileges of the AMP service.			
cisco -- application_policy_infrastructure_controller_software	A vulnerability in the REST API for software device management in Cisco Application Policy Infrastructure Controller (APIC) Software could allow an authenticated, remote attacker to escalate privileges to root on an affected device. The vulnerability is due to incomplete validation and error checking or the file path when specific software is uploaded. An attacker could exploit this vulnerability by uploading malicious software using the REST API. A successful exploit could allow an attacker to escalate their privilege level to root. The attacker would need to have the administrator role on the device.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1889</a> <a href="#">CISCO</a>
cisco -- email_security_appliance	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device. The vulnerability is due to improper input validation of certain email fields. An attacker could exploit this vulnerability by sending a crafted email message to a recipient protected by the ESA. A successful exploit could allow the attacker to bypass configured message filters and inject arbitrary scripting code inside the email body. The malicious code is not executed by default unless the recipient's email client is configured to execute scripts contained in emails.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1933</a> <a href="#">CISCO</a>
cisco -- email_security_appliance	A vulnerability in the attachment scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper input validation of the email body. An attacker could exploit this vulnerability by naming a malicious attachment with a specific pattern. A successful exploit could allow the attacker to bypass configured content filters that would normally block the attachment.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1921</a> <a href="#">CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFW Infrastructure Software (NFWIS) could allow an authenticated, remote attacker with administrator privileges to overwrite or read arbitrary files on the underlying operating system (OS) of an affected device. The vulnerability is due to improper input validation in NFWIS filesystem commands. An attacker could exploit this vulnerability by using crafted variables during the execution of an affected command. A successful exploit could allow the attacker to overwrite or read arbitrary files on the underlying OS.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1894</a> <a href="#">CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFW Infrastructure Software (NFWIS) could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device as root. The vulnerability is due to insufficient input validation of a configuration file that is accessible to a local shell user. An attacker could exploit this vulnerability by including malicious input during the execution of this file. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS as root.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1893</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1931</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1930</a> <a href="#">CISCO</a>
cisco -- ios_xr_software	A vulnerability in the implementation of Border Gateway Protocol (BGP) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to incorrect processing of certain BGP update messages. An attacker could exploit this vulnerability by sending BGP update messages that include a specific set of attributes to be processed by an affected system. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP traffic from explicitly defined peers only. To exploit this vulnerability, the malicious BGP update message would need to come from a configured, valid BGP peer or would need to be injected by the attacker into the victim's BGP network on an existing, valid TCP connection to a BGP peer.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1909</a> <a href="#">CISCO</a>

cisco -- jabber	A vulnerability in the loading mechanism of specific dynamic link libraries in Cisco Jabber for Windows could allow an authenticated, local attacker to perform a DLL preloading attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of the resources loaded by the application at run time. An attacker could exploit this vulnerability by crafting a malicious DLL file and placing it in a specific location on the targeted system. The malicious DLL file would execute when the Jabber application launches. A successful exploit could allow the attacker to execute arbitrary code on the target machine with the privileges of another user's account.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1855</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_switches	A vulnerability in the fabric infrastructure VLAN connection establishment of the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, adjacent attacker to bypass security validations and connect an unauthorized server to the infrastructure VLAN. The vulnerability is due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. An attacker could exploit this vulnerability by sending a malicious LLDP packet on the adjacent subnet to the Cisco Nexus 9000 Series Switch in ACI mode. A successful exploit could allow the attacker to connect an unauthorized server to the infrastructure VLAN, which is highly privileged. With a connection to the infrastructure VLAN, the attacker can make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1890</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1891</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the Secure Sockets Layer (SSL) input packet processor of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a memory corruption on an affected device. The vulnerability is due to improper validation of HTTPS packets. An attacker could exploit this vulnerability by sending a malformed HTTPS packet to the management web interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a denial of service (DoS) condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1892</a> <a href="#">CISCO</a>
cisco -- unified_communications_domain_manager	A vulnerability in the CLI of Cisco Unified Communications Domain Manager (Cisco Unified CDM) Software could allow an authenticated, local attacker to escape the restricted shell. The vulnerability is due to insufficient input validation of shell commands. An attacker could exploit this vulnerability by executing crafted commands in the shell. A successful exploit could allow the attacker to escape the restricted shell and access commands in the context of the restricted shell user, which does not have root privileges.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1911</a> <a href="#">CISCO</a>
cisco -- unified_communications_manager	A vulnerability in the Session Initiation Protocol (SIP) protocol implementation of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of input SIP traffic. An attacker could exploit this vulnerability by sending a malformed SIP packet to an affected Cisco Unified Communications Manager. A successful exploit could allow the attacker to trigger a new registration process on all connected phones, temporarily disrupting service.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1887</a> <a href="#">CISCO</a>
cisco -- web_security_appliance	A vulnerability in the HTTPS decryption feature of Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Secure Sockets Layer (SSL) server certificates. An attacker could exploit this vulnerability by installing a malformed certificate in a web server and sending a request to it through the Cisco WSA. A successful exploit could allow the attacker to cause an unexpected restart of the proxy process on an affected device.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1886</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- web_security_appliance	A vulnerability in the web proxy functionality of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation mechanisms for certain fields in HTTP/HTTPS requests sent through an affected device. A successful attacker could exploit this vulnerability by sending a malicious HTTP/HTTPS request through an affected device. An exploit could allow the attacker to force the device to stop processing traffic, resulting in a DoS condition.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1884</a> <a href="#">CISCO</a>
cloudera -- cloudera_manager	The keystore password for the Spark History Server may be exposed in unsecured files under the /var/run/cloudera-scm-agent directory managed by Cloudera Manager. The keystore file itself is not exposed.	2019-07-03	not yet calculated	<a href="#">CVE-2017-9326</a> <a href="#">CONF RM</a>
cloudera -- cloudera_manager	Secret data of processes managed by CM is not secured by file permissions.	2019-07-03	not yet calculated	<a href="#">CVE-2017-9327</a>

				CONF RM
cloudera -- data_science_workbench	Remote code execution is possible in Cloudera Data Science Workbench version 1.3.0 and prior releases via unspecified attack vectors.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11215</a> CONF RM
cloudera -- solr	The provided secure solrconfig.xml sample configuration does not enforce Sentry authorization on /update/json/docs.	2019-07-03	not yet calculated	<a href="#">CVE-2017-9325</a> CONF RM
codedoc -- codedoc	Codedoc v3.2 has a stack-based buffer overflow in add_variable in codedoc.c, related to codedoc_strncpy.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13362</a> MISC
codeigniter-restserver -- codeigniter-restserver	CodeIgniter Rest Server (aka codeigniter-restserver) 2.7.1 allows XXE attacks.	2019-07-03	not yet calculated	<a href="#">CVE-2015-3907</a> MISC
curl -- curl	A non-privileged user or program can put code and a config file in a known non-privileged path (under C:/usr/local/) that will make curl <= 7.65.1 automatically run the code (as an openssl "engine") on invocation. If that curl is invoked by a privileged user it can do anything it wants.	2019-07-02	not yet calculated	<a href="#">CVE-2019-5443</a> MLIST BID MISC
d-link -- central_wifi_manager	An issue was discovered in the D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6. Input does not get validated and arbitrary SQL statements can be executed in the database via the /web/Public/Conn.php parameter dbSQL.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13373</a> MISC MISC
d-link -- central_wifi_manager	A cross-site scripting (XSS) vulnerability in resource view in PayAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to inject arbitrary web script or HTML via the index.php/Pay/passcodeAuth passcode parameter.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13374</a> MISC MISC
d-link -- central_wifi_manager	A SQL Injection was discovered in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 in PayAction.class.php with the index.php/Pay/passcodeAuth parameter passcode. The vulnerability does not need any authentication.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13375</a> MISC MISC
d-link -- central_wifi_manager	/web/Lib/Action/IndexAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to execute arbitrary PHP code via a cookie because a cookie's username field allows eval injection, and an empty password bypasses authentication.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13372</a> MISC MISC
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The binary orthrus in /sbin folder of the device handles all the UPnP connections received by the device. It seems that the binary performs a sprintf operation at address 0x000A3E4 with the value in the command line parameter "-f" and stores it on the stack. Since there is no length check, this results in corrupting the registers for the function sub_A098 which results in memory corruption.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8414</a> MISC MISC BUGTRAQ
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1130 and DCS-1100 devices. The binary rtspd in /sbin folder of the device handles all the rtsp connections received by the device. It seems that the binary loads at address 0x00012CF4 a flag called "Authenticate" that indicates whether a user should be authenticated or not before allowing access to the video feed. By default, the value for this flag is zero and can be set/unset using the HTTP interface and network settings tab as shown below. The device requires that a user logging to the HTTP management interface of the device to provide a valid username and password. However, the device does not enforce the same restriction by default on RTSP URL due to the checkbox unchecked by default, thereby allowing any attacker in possession of external IP address of the camera to view the live video feed. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8405</a> MISC MISC BUGTRAQ
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The binary rtspd in /sbin folder of the device handles all the rtsp connections received by the device. It seems that the binary performs a memcpy operation at address 0x00011E34 with the value sent in the "Authorization: Basic" RTSP header and stores it on the stack. The number of bytes to be copied are calculated based on the length of the string sent in the RTSP header by the client. As a result, memcpy copies more data than it can hold on stack and this results in corrupting the registers for the caller function sub_F6CC which results in memory corruption. The severity of this attack is enlarged by the fact that the same value is then copied on the stack in the function 0x00011378 and this allows to overflow the buffer allocated and thus control the PC register which will result in arbitrary code execution on the device.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8410</a> MISC MISC BUGTRAQ
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device has a custom binary called mp4ts under the var/www/video folder. It seems that this binary dumps the HTTP VERB in the system logs. As a part of doing that it retrieves the HTTP VERB sent by the user and uses a vulnerable sprintf function at address 0x000C3D4 in the function sub_C210 to copy the value into a string and then into a log file. Since there is no bounds check being performed on the environment variable at address 0x000C360 this results in a stack overflow and overwrites the PC register allowing an attacker to execute buffer overflow or even a command injection attack.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8412</a> MISC MISC BUGTRAQ
	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device runs a custom daemon on UDP port 5978 which is called "dldps2121" and listens for broadcast packets			

d-link -- dcs-1100_and_dcs-1130_devices	<p>sent on 255 255 255 255. This daemon handles custom D-Link UDP based protocol that allows D-Link mobile applications and desktop applications to discover D-Link devices on the local network. The binary processes the received UDP packets sent from any device in "main" function. One path in the function reverses towards a block of code that handles commands to be executed on the device. The custom protocol created by D-Link follows the following pattern: Packetlen, Type of packet; M=MAC address of device or broadcast; D=Device Type; C=base64 encoded command string; test=1111. If a packet is received with the packet type being "S" or 0x53 then the string passed in the "C" parameter is base64 decoded and then executed by passing into a System API. We can see at address 0x00009B44 that the string received in packet type subtracts 0x31 or "1" from the packet type and is compared against 0x22 or "double quotes". If that is the case, then the packet is sent towards the block of code that executes a command. Then the value stored in "C" parameter is extracted at address 0x0000A1B0. Finally, the string received is base 64 decoded and passed on to the system API at address 0x0000A2A8 as shown below. The same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third-party application on the device to execute commands on the device without any authentication by sending just 1 UDP packet with custom base64 encoding.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8413</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device has a custom telnet daemon as a part of the busybox and retrieves the password from the shadow file using the function getsnam at address 0x00053894. Then performs a crypt operation on the password retrieved from the user at address 0x000538E0 and performs a strcmp at address 0x00053908 to check if the password is correct or incorrect. However, the /etc/shadow file is a part of CRAM-FS filesystem which means that the user cannot change the password and hence a hardcoded hash in /etc/shadow is used to match the credentials provided by the user. This is a salted hash of the string "admin" and hence it acts as a password to the device which cannot be changed as the whole filesystem is read only.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8415</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device runs a custom daemon on UDP port 5978 which is called "dldps2121" and listens for broadcast packets sent on 255 255 255 255. This daemon handles custom D-Link UDP based protocol that allows D-Link mobile applications and desktop applications to discover D-Link devices on the local network. The binary processes the received UDP packets sent from any device in "main" function. One path in the function reverses towards a block of code that processing of packets which does an unbounded copy operation which allows to overflow the buffer. The custom protocol created by Dlink follows the following pattern: Packetlen, Type of packet; M=MAC address of device or broadcast; D=Device Type; C=base64 encoded command string; test=1111 We can see at address 0x0000DBF8 handles the entire UDP packet and performs an insecure copy using strcpy function at address 0x0000DC88. This results in overflowing the stack pointer after 1060 characters and thus allows to control the PC register and results in code execution. The same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third-party application on the device to execute commands on the device without any authentication by sending just 1 UDP packet with custom base64 encoding.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8416</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device requires that a user logging into the device provide a username and password. However, the device allows D-Link apps on the mobile devices and desktop to communicate with the device without any authentication. As a part of that communication, the device uses custom version of base64 encoding to pass data back and forth between the apps and the device. However, the same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third party to retrieve the device's password without any authentication by sending just 1 UDP packet with custom base64 encoding. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8417</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1130 devices. The device requires that a user logging to the device to provide a username and password. However, the device does not enforce the same restriction on a specific URL thereby allowing any attacker in possession of that to view the live video feed. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8409</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
	<p>An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder or the video clippings recorded by the device. It seems that the POST parameters passed in this request (to test if email credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the function and thus result in command injection on the device. If the firmware version is dissected using binwalk tool, we obtain a cramfs-root archive which contains the filesystem set up on the</p>			

d-link -- dcs-1130_devices	device that contains all the binaries. The library "libmailutils so" is the one that has the vulnerable function "sub_1FC4" that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows an ARM little endian format. The function sub_1FC4 in DA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "receiver1" is extracted in function "sub_15AC" which is then passed to the vulnerable system API call. The vulnerable library function is accessed in "cgibox" binary at address 0x00023BCC which calls the "Send_mail" unction in "libmailutils so" binary as shown below which results in the vulnerable POST parameter being passed to the library which results in the command injection issue.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8411</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder or the video clippings recorded by the device. It seems that the GET parameters passed in this request (to test if SMB credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the unction and thus result in command injection on the device. If he firmware version is dissected using binwalk tool, we obtain a cramsfs-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "cgibox" is the one that has the vulnerable function "sub_7EAFD" that receives he values sent by the GET request. If we open this binary in IDA-pro we will notice that this follows a ARM little endian format. The function sub_7EAFD in IDA pro is identified to be receiving he values sent in the GET request and the value set in GET parameter "user" is extracted in function sub_7E49C which is hen passed to the vulnerable system API call.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8408</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of changing the administrative password for the web management interface. t seems that the device does not implement any cross-site request orgey protection mechanism which allows an attacker to trick a user who is logged in to the web management interface to change the user's password.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8407</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a crossdomain.xml file with no restrictions on who can access the webserver. This allows an hosted flash file on any domain to make calls to the device's webserver and pull any information that is stored on the device. In this case, user's credentials are stored in clear text on the device and can be pulled easily. t also seems that the device does not implement any cross-site scripting forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a cross-site flashing attack on the user's browser and execute any action on the device provided by the web management interface which steals the credentials from tools_admin.cgi file's response and displays it inside a Textfield.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8406</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder or the video clippings recorded by the device. It seems that the POST parameters passed in this request (to test if email credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the unction and thus result in command injection on the device. If he firmware version is dissected using binwalk tool, we obtain a cramsfs-root archive which contains the filesystem set up on the device that contains all the binaries. The library "libmailutils so" is he one that has the vulnerable function "sub_1FC4" that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows an ARM little endian format. The function sub_1FC4 in DA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "receiver1" is extracted in function "sub_15AC" which is then passed to the vulnerable system API call. The vulnerable library function is accessed in "cgibox" binary at address 0x0008F598 which calls the "mailLoginTest" unction in "libmailutils so" binary as shown below which results in the vulnerable POST parameter being passed to the library which results in the command injection issue.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8404</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dir-823g_devices	An issue was discovered on D-Link DIR-823G devices with firmware 1.02B03. There is a command injection in HNP1 exploitable with Authentication) via shell metacharacters in the IPAddress or Gateway field to SetStaticRouteSettings.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13128</a> <a href="#">MISC</a>
diffplug -- spotless	In DiffPlug Spotless before 1.20.0 (library and Maven plugin) and before 3.20.0 (Gradle plugin), the XML parser would resolve external entities over both HTTP and HTTPS and didn't respect he resolveExternalEntities setting. For example, this allows disclosure of file contents to a MITM attacker if a victim performs a spotlessApply operation on an untrusted XML file.	2019-06-28	not yet calculated	<a href="#">CVE-2019-9843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
digisol -- dg-hr3400_wireless_broadband_home_router	DIGISOL DG-HR3400 devices have XSS via a modified SSID when the apssid value is unchanged.	2019-07-03	not yet calculated	<a href="#">CVE-2018-12715</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
digisol -- hr-3300_wireless_wifi_home_router	Digisol Wireless Wifi Home Router HR-3300 allows XSS via the userid or password parameter to the admin login page.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14027</a>



				MISC
django -- django	An issue was discovered in Django 1.11 before 1.11.22, 2.1 before 2.1.10, and 2.2 before 2.2.3. An HTTP request is not redirected to HTTPS when the SECURE_PROXY_SSL_HEADER and SECURE_SSL_REDIRECT settings are used, and the proxy connects to Django via HTTPS. In other words, django.http.HttpRequest scheme has incorrect behavior when a client uses HTTP.	2019-07-01	not yet calculated	<a href="#">CVE-2019-12781</a> <a href="#">MLIST</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">CONF RM</a>
django_rest_registration -- django_rest_registration	verification.py in django-rest-registration (aka Django REST Registration library) before 0.5.0 relies on a static string for signatures (i.e., the Django Signing API is misused), which allows remote attackers to spoof the verification process. This occurs because incorrect code refactoring led to calling a security-critical function with an incorrect argument.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13177</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.2 incorrectly converts encryption key source values, resulting in lower than expected entropy. NOTE: this issue exists because of an incomplete fix for CVE-2018-15812.	2019-07-03	not yet calculated	<a href="#">CVE-2018-18326</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.2 uses a weak encryption algorithm to protect input parameters. NOTE: this issue exists because of an incomplete fix for CVE-2018-15811.	2019-07-03	not yet calculated	<a href="#">CVE-2018-18325</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.1 incorrectly converts encryption key source values, resulting in lower than expected entropy.	2019-07-03	not yet calculated	<a href="#">CVE-2018-15812</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.1 uses a weak encryption algorithm to protect input parameters.	2019-07-03	not yet calculated	<a href="#">CVE-2018-15811</a> <a href="#">MISC</a> <a href="#">MISC</a>
dosbox -- dosbox	A buffer overflow in DOSBox 0.74-2 allows attackers to execute arbitrary code.	2019-07-03	not yet calculated	<a href="#">CVE-2019-7165</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
eventum -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/switch.php has an Open Redirect via the current_page parameter.	2019-07-05	not yet calculated	eve
f5 -- big-ip	In BIG-IP 15.0.0, 14.0.0-14.1.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.2, and 11.5.2-11.6.4, BIG-IQ 6.0.0-6.1.0 and 5.1.0-5.4.0, Workflow 2.3.0, and Enterprise Manager 3.1.1, authenticated users with the ability to upload files (via scp, for example) can escalate their privileges to allow root shell access from within the TMOS Shell (tmsh) interface. The tmsh interface allows users to execute a secondary program via tools like sftp or scp.	2019-07-01	not yet calculated	<a href="#">CVE-2019-6642</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 12.1.0-12.1.4.1, undisclosed requests can cause Control REST processes to crash. The attack can only come from an authenticated user; all roles are capable of performing the attack. Unauthenticated users cannot perform this attack.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6641</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, SNMP exposes sensitive configuration objects over insecure transmission channels. This issue is exposed when a passphrase is inserted into various profile types and accessed using SNMPv2.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6640</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP (AFM, PEM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, an undisclosed TMUI pages for AFM and PEM Subscriber management are vulnerable to a stored cross-site scripting (XSS) issue. This is a control plane issue only and is not accessible from the data plane. The attack requires a malicious resource administrator to store the XSS.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6639</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, Malformed http requests made to an undisclosed iControl REST endpoint can lead to infinite loop of the restjavad process.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6638</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP (ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, Application logic abuse of ASM REST endpoints can lead to instability of BIG-IP system. Exploitation of this issue causes excessive memory consumption which results in the Linux kernel triggering OOM killer on arbitrary processes. The attack requires an authenticated user with role of "Guest" or greater privilege. Note: "No Access" cannot login so technically it's a role but a user with this access role cannot perform the attack.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6637</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP (AFM, ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, and 11.5.1-11.6.4, a stored cross-site scripting vulnerability in AFM feed list. In the worst case, an attacker can store a CSRF which results in code execution as the admin user. The level of user role which can perform this attack are resource administrator and administrator.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6636</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, when the BIG-IP system is licensed for Appliance mode, a user with either the Administrator or the Resource Administrator role can bypass Appliance mode restrictions.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6635</a> <a href="#">CONF RM</a>

f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, a high volume of malformed analytics report requests leads to instability in restjavad process. This causes issues with both iControl REST and some portions of TMUI. The attack requires an authenticated user with any role.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6634</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4, when the BIG-IP system is licensed with Appliance mode, user accounts with Administrator and Resource Administrator roles can bypass Appliance mode restrictions.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6633</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, under certain circumstances, attackers can decrypt configuration items that are encrypted because the vCMP configuration unit key is generated with insufficient randomness. The attack prerequisite is direct access to encrypted configuration and/or UCS files.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6632</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 11.5.1-11.6.4, iRules performing HTTP header manipulation may cause an interruption to service when processing traffic handled by a Virtual Server with an associated HTTP profile, in specific circumstances, when the requests do not strictly conform to RFCs.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6631</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP PEM 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, under certain conditions, the TMM process may terminate and restart while processing BIG-IP PEM traffic with the OpenVPN classifier.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6628</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP (AFM, Analytics, ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, and 11.5.1-11.6.3.4, A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the Configuration utility.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6626</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, and 11.5.1-11.6.4, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI) also known as the BIG-IP Configuration utility.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6625</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, undisclosed SSL traffic to a virtual server configured with a Client SSL profile may cause TMM to fail and restart. The Client SSL profile must have session tickets enabled and use DHE cipher suites to be affected. This only impacts the data plane, there is no impact to the control plane.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6629</a> <a href="#">CONF RM</a>
f5 -- f5_ssl_orchestrator	On F5 SSL Orchestrator 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, undisclosed traffic flow may cause TMM to restart under certain circumstances.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6630</a> <a href="#">CONF RM</a>
f5 -- f5_ssl_orchestrator	On F5 SSL Orchestrator 14.1.0-14.1.0.5, on rare occasions, specific to a certain race condition, TMM may restart when SSL Forward Proxy enforces the bypass action for an SSL Orchestrator transparent virtual server with SNAT enabled.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6627</a> <a href="#">CONF RM</a>
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x00000000001a95b1.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13245</a> <a href="#">MISC</a>
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x0000000000002d7d.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13244</a> <a href="#">MISC</a>
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x00000000001a9601.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13246</a> <a href="#">MISC</a>
ffmpeg -- ffmpeg	block_cmp() in libavcodec/zmbvenc.c in FFmpeg 4.1.3 has a heap-based buffer over-read.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13312</a> <a href="#">MISC</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349197 and 12.0-RELEASE before 12.0-RELEASE-p6, a bug in the non-default RACK TCP stack can allow an attacker to cause several linked lists to grow unbounded and cause an expensive list traversal on every packet being processed, leading to resource exhaustion and a denial of service.	2019-07-02	not yet calculated	<a href="#">CVE-2019-5599</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">FREEBSD</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349622, 12.0-RELEASE before 12.0-RELEASE-p7, 11.3-PRERELEASE before r349624, 11.3-RC3 before 11.3-RC3-p1, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in iconv implementation may allow an attacker to write past the end of an output buffer. Depending on the implementation, an attacker may be able to create a denial of service, provoke incorrect program behavior, or induce a remote code execution.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5600</a> <a href="#">MISC</a> <a href="#">FREEBSD</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349628, 12.0-RELEASE before 12.0-RELEASE-p7, 11.3-PRERELEASE before r349629, 11.3-RC3 before 11.3-RC3-p1, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in the cdrom driver allows users with read access to the cdrom device to arbitrarily overwrite kernel memory when media is present thereby allowing a malicious user in the operator group to gain root privileges.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5602</a> <a href="#">MISC</a> <a href="#">FREEBSD</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r347474, 12.0-RELEASE before 12.0-RELEASE-p7, 11.2-STABLE before r347475, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in the FFS	2019-07-	not yet	<a href="#">CVE-2019-5601</a>

	implementation causes up to three bytes of kernel stack memory to be written to disk as uninitialized directory entry padding.	03	calculated	MISC <a href="#">FREEBSD</a>
glpi_project -- glpi	nc/user.class.php in GLPI before 9.4.3 allows XSS via a user picture.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13239</a> MISC MISC MISC
gnome -- libxslt	In numbers.c in libxslt 1.1.33, a type holding grouping characters of an xsl:number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.	2019-06-30	not yet calculated	<a href="#">CVE-2019-13118</a> MISC MISC MISC
gnome -- libxslt	In numbers.c in libxslt 1.1.33, an xsl number with certain format strings could lead to a uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, I, i, or 0, or any other character.	2019-06-30	not yet calculated	<a href="#">CVE-2019-13117</a> MISC MISC MISC
grouptime -- teamwire_desktop_client	Grouptime Teamwire Desktop Client 1 5.1 prior to 1.9.0 on Windows allows code injection via a template, leading to remote code execution. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	<a href="#">CVE-2018-17170</a> MISC
grouptime -- teamwire_desktop_client	The admin interface of the Grouptime Teamwire Client 1.5.1 prior to 1 9.0 on-premises messenger server allows stored XSS. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	<a href="#">CVE-2018-17560</a> MISC
hawt -- hawtio	Hawt Hawtio through 2 5 0 is vulnerable to SSRF, allowing a remote attacker to trigger an HTTP request from an affected server to an arbitrary host via the initial /proxy/ substring of a URI.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9827</a> MISC
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 could allow an authenticated user to execute a function that would cause the server to crash. IBM X-Force ID: 162714.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4386</a> BID XF CONF RM
ibm -- infosphere_information_server	A Cross-Frame Scripting vulnerability in IBM InfoSphere Information Server 11 3, 11.5, and 11.7 can allow an attacker to load the vulnerable application inside an HTML iframe tag on a malicious page. IBM X-Force ID: 159419.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4237</a> XF CONF RM
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow an attacker to obtain sensitive information due to missing authentication in Ignite nodes. IBM X-Force ID: 161412.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4337</a> CONF RM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 161411.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4336</a> CONF RM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow a local user to obtain highly sensitive information from log files when debugging is enabled. IBM X-Force ID: 160765.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4299</a> CONF RM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 uses a high privileged PostgreSQL account for database access which could allow a local user to perform actions they should not have privileges to execute. IBM X-Force ID: 160764.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4298</a> CONF RM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow a remote authenticated attacker to conduct an LDAP injection. By using a specially crafted request, an attacker could exploit this vulnerability to make unauthorized queries or modify the LDAP content. IBM X-Force ID: 160761.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4297</a> CONF RM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 information disclosure could allow a local user to obtain e-mail contents from the client debug log file. IBM X-Force ID: 160759.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4296</a> CONF RM XF
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow an attacker with specialized access to obtain highly sensitive from the credential vault. IBM X-Force ID: 160758.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4295</a> CONF RM XF
ibm -- spectrum_protect_plus	When using IBM Spectrum Protect Plus 10.1.0, 10.1 2, and 10.1.3 to protect Oracle or MongoDB databases, a redirected restore operation may result in an escalation of user privileges. IBM X-Force ID: 162165.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4383</a> CONF RM BID XF
ibm -- spectrum_protect_plus	When using IBM Spectrum Protect Plus 10.1.0, 10.1 2, and 10.1.3 to protect Oracle, DB2 or MongoDB databases, a redirected restore operation specifying a target path may allow execution of arbitrary code on the system. IBM X-Force ID: 161667.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4357</a> CONF RM BID XF
ibm -- spectrum_protect_servers	IBM Spectrum Protect Operations Center 7.1 and 8.1 could allow a remote attacker to obtain sensitive information, caused by an error message containing a stack trace. By creating an error with a stack trace, an attacker could exploit this vulnerability to potentially obtain details on the Operations Center architecture. IBM X-Force ID: 158279.	2019-07-02	not yet calculated	<a href="#">CVE-2019-4129</a> CONF RM XF
ibm -- spectrum_protect_servers_and_storage_agents	IBM Spectrum Protect Servers 7.1 and 8.1 and Storage Agents are vulnerable to a stack-based buffer overflow, caused by improper bounds checking by servers and storage agents in response to specifically crafted communication exchanges. By	2019-07-	not yet	<a href="#">CVE-2019-4087</a>

	sending an overly long request, a remote attacker could overflow a buffer and execute arbitrary code on the system with instance d privileges or cause the server or storage agent to crash. BM X-Force ID: 157510.	02	calculated	<a href="#">CONF RM XF</a>
ibm -- spectrum_protect_servers_and_storage_agents	IBM Spectrum Protect Servers 7.1 and 8.1 and Storage Agents could allow a local attacker to gain elevated privileges on the system, caused by loading a specially crafted library loaded by the dsmqsan module. By setting up such a library, a local attacker could exploit this vulnerability to gain root privileges on the vulnerable system. BM X-Force ID: 157511.	2019-07-02	not yet calculated	<a href="#">CVE-2019-4088</a> <a href="#">CONF RM XF</a>
ignited_cms -- ignited_cms	ndex.php/admin/permissions in Ignited CMS through 2017-02-19 allows CSRF to add an administrator.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13370</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/fourier.c in ComplexImages.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13302</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of off-by-one errors.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13306</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of a wand/mogrify.c error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13311</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling rows.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13307</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced strncpy and an off-by-one error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13305</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced assignment.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/composite.c in CompositeImage.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13303</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks in AcquireMagickMemory because of an AnnotateImage error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13301</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling columns.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13300</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/pixel-accessor.h in GetPixelChannel.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13299</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/pixel-accessor.h in SetPixelViaPixelInfo because of a MagickCore/enhance.c error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13298</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a height of zero is mishandled.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13297</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has direct memory leaks in AcquireMagickMemory because of an error in CLIListOperatorImages in MagickWand/operation.c for a NULL value.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13296</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a width of zero is mishandled.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13295</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow in MagickCore/fourier.c in ComplexImage.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13308</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of mishandling the NoSuchImage error in CLIListOperatorImages in MagickWand/operation.c.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13309</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of an error in MagickWand/mogrify.c.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13310</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
invoxia -- nvx220_devices	Invoxia NVX220 devices allow access to /bin/sh via escape from a restricted CLI, leading to disclosure of password hashes.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14529</a> <a href="#">MISC</a>
invoxia -- nvx220_devices	Invoxia NVX220 devices allow TELNET access as admin with a default password.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14528</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.52 has a User Mode Write AV starting at mage00400000+0x0000000000249c6.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13243</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.52 has a User Mode Write AV starting at mage00400000+0x000000000013a98.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13242</a> <a href="#">MISC</a>
jack_audio -- jack2	posix/JackSocket.cpp in libjack in JACK2 1.9.1 through 1.9.12 as distributed with alsa-plugins 1.1.7 and later) has a "double file descriptor close" issue during a failed connection attempt when ackd2 is not running. Exploitation success depends on multithreaded timing of that double close, which can result in unintended information disclosure, crashes, or file corruption due o having the wrong file associated with the file descriptor.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13351</a> <a href="#">MISC</a> <a href="#">MISC</a>
jetbrains -- hub	In JetBrains Hub versions earlier than 2018.4.11298, the audit events for SMTPSettings show a cleartext password to the admin user. It is only relevant in cases where a password has not changed since 2017, and if the audit log still contains events rom before that period.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12847</a> <a href="#">CONF RM</a>
jetbrains -- intelliij_idea	In several JetBrains IntelliJ IDEA versions, creating remote run configurations of JavaEE application servers leads to saving a cleartext record of the server credentials in the DE configuration files. The issue has been fixed in the following versions: 2018.3.5, 2018.2.8, 2018.1.8.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9823</a> <a href="#">CONF RM</a>
jetbrains -- intelliij_idea	In several JetBrains IntelliJ IDEA versions, a Spring Boot run configuration with the default setting allowed remote attackers to execute code when the configuration is running, because a JMX server listens on all interfaces (instead of listening on only the ocalhost interface). This issue has been fixed in the following versions: 2019.1, 2018.3.4, 2018.2.8, 2018.1.8, and 2017.3.7.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9186</a> <a href="#">CONF RM</a>
jetbrains -- intelliij_idea	In several JetBrains IntelliJ IDEA Ultimate versions, an Application Server run configuration (for Tomcat, Jetty, Resin, or CloudBees) with the default setting allowed a remote attacker to execute code when the configuration is running, because a JMX server listened on all interfaces instead of localhost only. The issue has been fixed in the following versions: 2018.3.4, 2018.2.8, 2018.1.8, and 2017.3.7.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10104</a> <a href="#">CONF RM</a>
jetbrains -- intelliij_idea	JetBrains IntelliJ IDEA projects created using the Kotlin (JS Client/JVM Server) DE Template were resolving Gradle artifacts using an http connection, potentially allowing an MITM attack. This issue, which was fixed in Kotlin plugin version 1.3.30, is similar to CVE-2019-10101.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10103</a> <a href="#">CONF RM</a>
jetbrains -- intelliij_idea_ultimate	In several versions of JetBrains IntelliJ DEA Ultimate, creating un configurations for cloud application servers leads to saving a cleartext unencrypted record of the server credentials in the IDE configuration files. If the Settings Repository plugin was then used and configured to synchronize IDE settings using a public epository, these credentials were published to this repository. The issue has been fixed in the following versions: 2019.1, 2018.3.5, 2018.2.8, and 2018.1.8.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9872</a> <a href="#">CONF RM</a>
jetbrains -- intelliij_idea_ultimate	In several versions of JetBrains IntelliJ DEA Ultimate, creating Task Servers configurations leads to saving a cleartext unencrypted record of the server credentials in the IDE configuration files. The issue has been fixed in the following versions: 2019.1, 2018.3.5, 2018.2.8, and 2018.1.8.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9873</a> <a href="#">CONF RM</a>
jetbrains -- kotlin	JetBrains Ktor framework (created using the Kotlin IDE template) versions before 1.1.0 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack. This issue was fixed in Kotlin plugin version 1.3.30.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10102</a> <a href="#">MISC</a>
jetbrains -- kotlin	JetBrains Kotlin versions before 1.3.30 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10101</a> <a href="#">CONF RM</a>
jetbrains -- teamcity	A possible stored JavaScript injection requiring a deliberate server administrator action was detected. The issue was fixed in JetBrains TeamCity 2018.2.3.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12843</a> <a href="#">CONF RM</a>
jetbrains -- teamcity	Incorrect handling of user input in Z P extraction was detected in JetBrains TeamCity. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12841</a> <a href="#">CONF RM</a>
jetbrains -- teamcity	A possible stored JavaScript injection was detected on one of the JetBrains TeamCity pages. The issue was fixed in TeamCity 2018.2.3.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12844</a> <a href="#">MISC</a>
jetbrains -- youtrack	A query injection was possible in JetBrains YouTrack. The issue was fixed in YouTrack 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12850</a> <a href="#">CONF RM</a>
jetbrains -- youtrack	Certain actions could cause privilege escalation for issue attachments in JetBrains YouTrack. The issue was fixed in 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12867</a> <a href="#">CONF RM</a>



jetbrains -- youtrack	In JetBrains YouTrack Confluence plugin versions before 1.8.1.3, it was possible to achieve Server Side Template Injection. The attacker could add an Issue macro to the page in Confluence, and use a combination of a valid id field and specially crafted code in the link-text-template field to execute code remotely.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10100</a> MISC
jetbrains -- youtrack	A CSRF vulnerability was detected in one of the admin endpoints of JetBrains YouTrack. The issue was fixed in YouTrack 2018.4.49852.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12851</a> CONFIRM
jetbrains -- youtrack	An SSRF attack was possible on a JetBrains YouTrack server. The issue (1 of 2) was fixed in JetBrains YouTrack 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12852</a> CONFIRM
jetbrains -- youtrack	An Insecure Direct Object Reference, with Authorization Bypass through a User-Controlled Key, was possible in JetBrains YouTrack. The issue was fixed in 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12866</a> CONFIRM
jgraph -- mxgraph	An issue was discovered in mxGraph through 4.0.0, related to the "draw.io Diagrams" plugin before 8.3.14 for Confluence and other products. Improper input validation/sanitization of a color field leads to XSS. This is associated with <a href="#">avascrypt/examples/grapheditor/www/js/Dialogs.js</a> .	2019-07-01	not yet calculated	<a href="#">CVE-2019-13127</a> MISC MISC MISC
libosinfo -- libosinfo	libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to osinfo-install-script via the command line.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13313</a> MISC MISC MISC MISC
linux -- linux_kernel	In arch/x86/lib/insn-eval.c in the Linux kernel before 5.1.9, there is a use-after-free for access to an LDT entry because of a race condition between modify_ldt() and a #BR exception for an MPX bounds violation.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13233</a> MISC MISC MISC MISC
linux -- linux_kernel	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the PID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10638</a> MISC MISC MISC MISC MISC MISC MISC MISC
linux -- linux_kernel	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the PID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This attack can be carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because PID generation was changed to have a dependency on an address associated with a network namespace.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10639</a> MISC MISC MISC MISC
logitech -- r500_presentation_clicker	The Logitech R500 presentation clicker allows attackers to determine the AES key, leading to keystroke injection. On Windows, any text may be injected by using ALT+NUMPAD input to bypass the restriction on the characters A through Z.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13054</a> MISC
logitech -- unifying_devices	Certain Logitech Unifying devices allow attackers to dump AES keys and addresses, leading to the capability of live decryption of Radio Frequency transmissions, as demonstrated by an attack against a Logitech K360 keyboard.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13055</a> MISC
logitech -- unifying_devices	Logitech Unifying devices before 2016-02-26 allow keystroke injection, bypassing encryption, aka MouseJack.	2019-06-29	not yet calculated	<a href="#">CVE-2016-10761</a> MISC MISC
logitech -- unifying_devices	Logitech Unifying devices allow live decryption if the pairing of a keyboard to a receiver is sniffed.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13052</a> MISC
logitech -- unifying_devices	Logitech Unifying devices allow keystroke injection, bypassing encryption. The attacker must press a "magic" key combination while sniffing cryptographic data from a Radio Frequency transmission. NOTE: this issue exists because of an incomplete fix for CVE-2016-10761.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13053</a> MISC
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Arbitrary file deletion.	2019-06-28	not yet calculated	<a href="#">CVE-2018-14916</a> MISC FULLDISC FULLDISC
				<a href="#">CVE-2018-</a>

loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow XSS.	2019-06-28	not yet calculated	<a href="#">14919 MISC</a> <a href="#">FULLDISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Directory Traversal.	2019-06-28	not yet calculated	<a href="#">CVE-2018-14918</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
macafee -- epolicy_orchestrator	Information Disclosure vulnerability in the Agent Handler in McAfee ePolicy Orchestrator (ePO) 5.9.x and 5.10.0 prior to 5.10.0 update 4 allows remote unauthenticated attacker to view sensitive information in plain text via sniffing the traffic between the Agent Handler and the SQL server.	2019-07-03	not yet calculated	<a href="#">CVE-2019-3619</a> <a href="#">CONFIRM</a>
maxx -- waves_maxx_audio	WavesSysSvc in Waves MAXX Audio allows privilege escalation because the General registry key has Full Control access for the Users group, leading to DLL side loading. This affects WavesSysSvc64.exe 1.9.29.0.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13208</a> <a href="#">MISC</a>
medtronic -- minimed_508_and_paradigm_series_insulin_pumps	In Medtronic MinMed 508 and Medtronic Minimed Paradigm Insulin Pumps, Versions, MiniMed 508 pump ? All versions, MiniMed Paradigm 511 pump ? All versions, MiniMed Paradigm 512/712 pumps ? All versions, MiniMed Paradigm 712E pump ? All versions, MiniMed Paradigm 515/715 pumps ? All versions, MiniMed Paradigm 522/722 pumps ? All versions, MiniMed Paradigm 522K/722K pumps ? All versions, MiniMed Paradigm 523/723 pumps ? Software versions 2.4A or lower, MiniMed Paradigm 523K/723K pumps ? Software, versions 2.4A or lower, MiniMed Paradigm Veo 554/754 pumps ? Software versions 2.6A or lower, MiniMed Paradigm Veo 554CM and 754CM models only ? Software versions 2.7A or lower, the affected insulin pumps are designed to communicate using a wireless RF with other devices, such as blood glucose meters, glucose sensor transmitters, and CareLink USB devices. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with adjacent access to one of the affected insulin pump models can inject, replay, modify, and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.	2019-06-28	not yet calculated	<a href="#">CVE-2019-10964</a> <a href="#">BID</a> <a href="#">MISC</a>
mikrotik -- multiple_routers	A vulnerability in the FTP daemon on MikroTik routers through 6.44.3 could allow remote attackers to exhaust all available memory, causing the device to reboot because of uncontrolled resource management.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13074</a> <a href="#">MISC</a>
minicms -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the tags box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, and CVE-2018-20520.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13186</a> <a href="#">MISC</a>
ministry_of_interior_of_the_slovak_republic -- eid_client	An incorrect implementation of a local web server in eID client Windows version before 3.1.2, Linux version before 3.0.3 allows remote attackers to execute arbitrary code (.cgi, .pl, or .php) or delete arbitrary files via a crafted HTML page. This is a product from the Ministry of Interior of the Slovak Republic.	2019-06-28	not yet calculated	<a href="#">CVE-2019-13028</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
motorola -- cx2l_mwr04l_router	On the Motorola router CX2L MWR04L 1 01, there is a stack consumption (infinite recursion) issue in scopd via TCP port 8010 and UDP port 8080. It is caused by sprintf and inappropriate length handling.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13129</a> <a href="#">MISC</a>
moxa -- oncell_g3100-hspa_series_devices	There is Memory corruption in the web interface Moxa OnCell G3100-HSPA Series version 1.6 Build 17100315 and prior, different vulnerability than CVE-2018-11420.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11423</a> <a href="#">MISC</a>
moxa -- oncell_g3100-hspa_series_devices	Moxa OnCell G3100-HSPA Series version 1 6 Build 17100315 and prior use a proprietary monitoring protocol that does not provide confidentiality, integrity, and authenticity security controls. All information is sent in plain text, and can be intercepted and modified. The protocol is vulnerable to remote unauthenticated disclosure of sensitive information, including the administrator's password. Under certain conditions, it's also possible to retrieve additional information, such as content of HTTP requests to the device, or the previously used password, due to memory leakages.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11421</a> <a href="#">MISC</a>
moxa -- oncell_g3100-hspa_series_devices	A weak Cookie parameter is used in the web application of Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior. An attacker can brute force parameters required to bypass authentication and access the web interface to use all its functions except for password change.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11426</a> <a href="#">MISC</a>
moxa -- oncell_g3100-hspa_series_devices	CSRF tokens are not used in the web application of Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior, which makes it possible to perform CSRF attacks on the device administrator.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11427</a> <a href="#">MISC</a>
moxa -- oncell_g3100-hspa_series_devices	There is Memory corruption in the web interface of Moxa OnCell G3100-HSPA Series version 1.5 Build 17042015 and prior, a different vulnerability than CVE-2018-11423.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11420</a> <a href="#">MISC</a>
moxa -- oncell_g3100-hspa_series_devices	Moxa OnCell G3100-HSPA Series version 1 6 Build 17100315 and prior use a proprietary configuration protocol that does not provide confidentiality, integrity, and authenticity security controls. All information is sent in plain text, and can be intercepted and modified. Any commands (including device reboot, configuration download or upload, or firmware upgrade) are accepted and executed by the device without authentication.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11422</a> <a href="#">MISC</a>
moxa -- oncell_g3470a-lte_series_devices	There is Memory corruption in the web interface of Moxa OnCell G3470A-LTE Series version 1.6 Build 18021314 and prior, a	2019-07-	not yet	<a href="#">CVE-2018-11424</a>

	different vulnerability than CVE-2018-11425.	03	calculated	<a href="#">MISC</a>
moxa -- oncell_g3470a-lte_series_devices	Memory corruption issue was discovered in Moxa OnCell G3470A-LTE Series version 1.6 Build 18021314 and prior, a different vulnerability than CVE-2018-11424.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11425</a> <a href="#">MISC</a>
nlnet_labs -- nsd	nsd-checkzone in NLnet Labs NSD 4.2.0 has a Stack-based Buffer Overflow in the dname_concatenate() function in dname.c.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13207</a> <a href="#">MISC</a>
nortek_security_and_control -- linear_emerge_50p/5000p_devices	Linear eMerge 50P/5000P devices allow Cookie Path Traversal.	2019-07-02	not yet calculated	<a href="#">CVE-2019-7267</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortek_security_and_control -- linear_emerge_50p/5000p_devices	Linear eMerge 50P/5000P devices allow Unauthenticated File Upload.	2019-07-02	not yet calculated	<a href="#">CVE-2019-7268</a> <a href="#">MISC</a> <a href="#">MISC</a>
npm -- fstream	stream before 1.0.12 is vulnerable to Arbitrary File Overwrite. Extracting tarballs containing a hardlink to a file that already exists in the system, and a file that matches the hardlink, will overwrite the system's file with the contents of the extracted file. The fstream.DirWriter() function is vulnerable.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13173</a> <a href="#">MISC</a> <a href="#">MISC</a>
odoo -- community_and_enterprise	Incorrect access control in the TransientModel framework in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated attackers to access data in transient records that they do not own by making an RPC call before garbage collection occurs.	2019-07-03	not yet calculated	<a href="#">CVE-2018-14866</a> <a href="#">CONF RM</a>
odoo -- community_and_enterprise	Improper sanitization of dynamic user expressions in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated privileged users to escape from the dynamic expression sandbox and execute arbitrary code on the hosting system.	2019-07-03	not yet calculated	<a href="#">CVE-2018-14860</a> <a href="#">CONF RM</a>
odoo -- community_and_enterprise	Incorrect access control in the password reset component in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated users to reset the password of other users by being the first party to use the secure token.	2019-07-03	not yet calculated	<a href="#">CVE-2018-14859</a> <a href="#">CONF RM</a>
odoo_community_association -- dbfilter_from_header module	The Odoo Community Association (OCA) dbfilter_from_header module makes Odoo 8.x, 9.x, 10.x, and 11.x vulnerable to ReDoS (regular expression denial of service) under certain circumstances.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14733</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
opencats -- opencats	ib/DocumentToText.php in OpenCats before 0.9.4-3 has XXE that allows remote users to read files on the underlying operating system. The attacker must upload a file in the docx or odt format.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13358</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
panduit -- intravue	An insecure login process was discovered in Panduit IntraVUE before 3.2.0.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13044</a> <a href="#">MISC</a>
qemu -- qemu	qemu-bridge-helper.c in QEMU 4.0.0 does not ensure that a network interface name (obtained from bridge.conf or a --br=bridge option) is limited to the IFNAMSIZ size, which can lead to an ACL bypass.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13164</a> <a href="#">MLIST</a> <a href="#">MISC</a>
read_the_docs -- read_the_docs	Read the Docs before 3.5.1 has an Open Redirect if certain user-defined redirects are used. This affects private instances of Read the Docs (in addition to the public readthedocs.org web sites).	2019-07-02	not yet calculated	<a href="#">CVE-2019-13175</a> <a href="#">MISC</a>
riello -- netman_204	An issue was discovered in Riello NetMan 204 14-2 and 15-2. The issue is with the login script and wrongpass Python script used for authentication. When calling wrongpass, the variables \$VAL0 and \$VAL1 should be enclosed in quotes to prevent the potential for Bash command injection. Further to this, VAL0 and VAL1 should be sanitised to ensure they do not contain malicious characters. Passing it the username of ' ' will cause it to time out and log the user in because of poor error handling. This will log the attacker in as an administrator where the telnet / ssh services can be enabled, and the credentials for local users can be reset. Also, login.cgi accepts the username as a GET parameter, so login can be achieved by browsing to the /cgi-bin/login.cgi?username=%20a URI.	2019-07-03	not yet calculated	<a href="#">CVE-2017-6900</a> <a href="#">MISC</a> <a href="#">MISC</a>
sdl2_image -- sdl2_image	An exploitable heap-based buffer overflow vulnerability exists when loading a PCX file in SDL2_image, version 2.0.4. A missing error handler can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5051</a> <a href="#">MISC</a>
sdl2_image -- sdl2_image	An exploitable integer overflow vulnerability exists when loading a PCX file in SDL2_image 2.0.4. A specially crafted file can cause an integer overflow, resulting in too little memory being allocated, which can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5052</a> <a href="#">MISC</a>
sick -- msc800_devices	SICK MSC800 all versions prior to Version 4.0, the affected firmware versions contain a hard-coded customer account password.	2019-07-01	not yet calculated	<a href="#">CVE-2019-10979</a> <a href="#">BID</a> <a href="#">MISC</a>
sigil-ebook -- flightcrew	FlightCrew v0.9.2 and older are vulnerable to a directory traversal, allowing attackers to write arbitrary files via a . / (dot dot slash) in a ZIP archive entry that is mishandled during	2019-07-04	not yet calculated	<a href="#">CVE-2019-13241</a> <a href="#">MISC</a>

	extraction.			
sitebridge -- joruri_cms	Cross-site scripting vulnerability in Joruri CMS 2017 Release2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5967</a> <a href="#">MISC</a> <a href="#">MISC</a>
sitebridge -- joruri_mail	Open redirect vulnerability in Joruri Mail 2.1.4 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5965</a> <a href="#">MISC</a> <a href="#">MISC</a>
sitebridge -- joruri_mail	Joruri Mail 2.1.4 and earlier does not properly manage sessions, which allows remote attackers to impersonate an arbitrary user and alter/disclose the information via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5966</a> <a href="#">MISC</a> <a href="#">MISC</a>
skys_keyserver_network -- skys-keyserver_code_and_gnupg	Interaction between the skys-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.16, makes it risky to have a GnuPG keyserver configuration line referring to a host on the SKS keyserver network. Retrieving data from this network may cause a persistent denial of service, because of a Certificate Spamming Attack.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13050</a> <a href="#">MISC</a>
sony -- vaio_update	Improper download file verification vulnerability in VAIO Update 7.3.0.03150 and earlier allows remote attackers to conduct a man-in-the-middle attack via a malicious wireless LAN access point. A successful exploitation may result in a malicious file being downloaded/executed.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5982</a> <a href="#">MISC</a> <a href="#">MISC</a>
sony -- vaio_update	Improper authorization vulnerability in VAIO Update 7.3.0.03150 and earlier allows an attackers to execute arbitrary executable file with administrative privilege via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5981</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13345</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
stormshield -- stormshield_network_security	Stormshield Network Security 2.0.0 through 2.13.0 and 3.0.0 through 3.7.1 has self-XSS in the command line interface of the SNS web server.	2019-07-04	not yet calculated	<a href="#">CVE-2018-20850</a> <a href="#">MISC</a>
supermicro -- superdoctor_5	Super Micro SuperDoctor 5, when restrictions are not implemented in agent.cfg, allows remote attackers to execute arbitrary commands via NRPE.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13131</a> <a href="#">MISC</a>
swift -- alliance_web_platform	An issue was discovered in SWIFT Alliance Web Platform 7.1.23. A log injection (and an arbitrary log filename) can be achieved via the PATH_INFO to swp/login/EJBRemoteService/, related to com.swift.ejbgwt.j2ee.client.EJBInvocationException error log information containing null@java:comp/env/ error messages.	2019-07-05	not yet calculated	<a href="#">CVE-2018-16386</a> <a href="#">MISC</a>
tencent -- habo	HaboMalHunter through 2.0.0.3 in Tencent Habo allows attackers to evade dynamic malware analysis via PIE compilation.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13125</a> <a href="#">MISC</a>
tor_project -- tor_browser	Tor Browser through 8.5.3 has an information exposure vulnerability. It allows remote attackers to detect the browser's language via vectors involving an FRAME element, because text n that language is included in the title attribute of a LINK element or a non-HTML page. This is related to a behavior of Firefox before 68.	2019-06-30	not yet calculated	<a href="#">CVE-2019-13075</a> <a href="#">MISC</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the Private Port in Add Virtual Server.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13153</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the IP Address in Add Gaming Rule.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13152</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the UDP Ports To Open in Add Gaming Rule.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13148</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the key passwd in Routing RIP Settings.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13149</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the IP Address in Add Virtual Server.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13155</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication). The command injection exists in the key ip_addr.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13150</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the action set_sta_enrollee_pin_5g and the key wps_sta_enrollee_pin.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13151</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the TCP Ports To Open in Add Gaming Rule.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13154</a> <a href="#">MISC</a>
	The Android App 'Tootdon for Mastodon' version 3.4.1 and			<a href="#">CVE-2019-</a>

tsukurito -- tootdon_for_mastodon	earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-07-05	not yet calculated	<a href="#">5961 MISC MISC</a>
unzip -- unzip	Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a "better zip bomb" issue.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13232 MISC MLIST MISC</a>
virt-manager -- virt-bootstrap	virt-bootstrap 1.1.0 allows local users to discover a root password by listing a process, because this password may be present in the --root-password option to virt_bootstrap.py.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13314 MISC MISC</a>
virt-manager -- virt-manager	Virt-install(1) utility used to provision new virtual machines has introduced an option '--unattended' to create VMs without user interaction. This option accepts guest VM password as command line arguments, thus leaking them to other users on the system via process listing. It was introduced recently in the virt-manager v2.2.0 release.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10183 BID CONF RM</a>
weberp -- weberp	A SQL Injection issue was discovered in webERP 4.15. Payments.php accepts payment data in base64 format. After this is decoded, it is deserialized. Then, this deserialized data goes directly into a SQL query, with no sanitizing checks.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13292 MISC</a>
weseek -- growi	Cross-site request forgery (CSRF) vulnerability in GROWI v3.4.6 and earlier allows remote attackers to hijack the authentication of administrators via updating user's 'Basic Info'.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5968 MISC MISC</a>
weseek -- growi	Open redirect vulnerability in GROWI v3.4.6 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the process of login.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5969 MISC MISC</a>
wolfvision -- cynap	WolfVision Cynap before 1.30j uses a static, hard-coded cryptographic secret for generating support PINs for the 'forgot password' feature. By knowing this static secret and the corresponding algorithm for calculating support PINs, an attacker can reset the ADMIN password and thus gain remote access.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13352 MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5971 MISC MISC MISC</a>
wordpress -- wordpress	Cross-site scripting vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5962 MISC MISC</a>
wordpress -- wordpress	A Cross-Site-Request-Forgery (CSRF) vulnerability in widget_logic.php in the 2by2host Widget Logic plugin before 5.10.2 for WordPress allows remote attackers to execute PHP code via snippets (that are attached to widgets and then eval'd to dynamically determine their visibility) by crafting a malicious POST request that tricks administrators into adding the code.	2019-07-01	not yet calculated	<a href="#">CVE-2019-12826 MISC CONF RM</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Personalized WooCommerce Cart Page 2.4 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5979 MISC MISC</a>
wordpress -- wordpress	Cross-site scripting vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5970 MISC MISC MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Contest Gallery versions prior to 10.4.5 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5974 MISC MISC</a>
wordpress -- wordpress	An authentication bypass vulnerability in the CRUDLab WP Like Button plugin through 1.6.0 for WordPress allows unauthenticated attackers to change settings. The contains() function in wp_like_button.php did not check if the current request is made by an authorized user, thus allowing any unauthenticated user to successfully update settings, as demonstrated by the wp-admin/admin.php?page=facebook-like-button&each_page_url or code_snippet parameter.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13344 MISC MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in WP Open Graph 1.6.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5960 JVN</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5963 MISC MISC</a>
wordpress -- wordpress	Cross-site scripting vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5972 MISC MISC MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Related YouTube Videos versions prior to 1.9.9 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5980 MISC MISC</a>



wordpress -- wordpress	An issue was discovered in the VeronaLabs wp-statistics plugin before 12.6.7 for WordPress. The v1/hit endpoint of the API, when the non-default "use cache plugin" setting is enabled, is vulnerable to unauthenticated blind SQL Injection.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13275</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5973</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wuhan_deepin_technology -- deepin-clone	In GUI mode, deepin-clone before 1.1.3 creates a log file at the fixed path /tmp/deepin-clone.log as root, and follows symlinks here. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13227</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a fixed path /tmp/partclone.log in the Helper::getPartitionSizeInfo() function to write a log file as root, and follows symlinks there. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13229</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a predictable path /tmp/deepin-clone/mount/<block-dev-basename> in the Helper::temporaryMountDevice() function to temporarily mount a file system as root. An unprivileged user can prepare a symlink at this location to have the file system mounted in an arbitrary location. By winning a race condition, the attacker can also enter the mount point, thereby preventing a subsequent unmount of the file system.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13226</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a fixed path /tmp/repo.iso in the BootDoctor::fix() function to download an ISO file, and follows symlinks there. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled. By winning a race condition to replace the /tmp/repo.iso symlink by an attacker controlled ISO file, further privilege escalation may be possible.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13228</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, there is an out-of-bounds read vulnerability in the function SplashXPath::strokeAdjust() located at splash/SplashXPath.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an attacker to cause Information Disclosure. This is related to CVE-2018-16368.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13287</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, a heap-based buffer overflow could be triggered in DCTStream::decodeImage() in Stream.cc when writing to rameBuf memory. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service, an information leak, or possibly unspecified other impact.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13281</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, there is a heap-based buffer over-read in the function JBIG2Stream::readTextRegionSeg() located at JBIG2Stream.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an attacker to cause Information Disclosure.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13286</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, a heap-based buffer over-read could be triggered in SampledFunction::transform in Function.cc when using a large index for samples. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13282</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, there is a heap-based buffer over-read in the function JBIG2Stream::readScan() located at Stream.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftops tool. It might allow an attacker to cause Information Disclosure.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13291</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, the Parser::getObj() function in Parser.cc may cause infinite recursion via a crafted file. A remote attacker can leverage this for a DoS attack. This is similar to CVE-2018-16646.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13288</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, there is a use-after-free vulnerability in the function JBIG2Stream::close() located at JBIG2Stream.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13289</a> <a href="#">MISC</a>
xpdf -- xpdf	In Xpdf 4.01 01, a heap-based buffer over-read could be triggered in strncpy from FoFiType1::parse in fofi/FoFiType1.cc because it does not ensure the source string has a valid length before making a fixed-length copy. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13283</a> <a href="#">MISC</a>

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

OTHER RESOURCES:  
[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:  


SUBSCRIBER SERVICES:  
[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [tmcginnis@sunnyvale.ca.gov](mailto:tmcginnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [US-CERT](#)  
**To:** [weburates@ci.sunnyvale.ca.us](mailto:weburates@ci.sunnyvale.ca.us)  
**Subject:** Vulnerability Summary for the Week of July 1, 2019  
**Date:** Monday, July 08, 2019 6:38:19 PM



National Cyber Awareness System:

## Vulnerability Summary for the Week of July 1, 2019

Original release date: July 8, 2019

The Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- web6000q_firmware	On Telus Actiontec WEB6000Q v1.1.02.22 devices, an attacker can login with root level access with the user "root" and password "admin" by using the enabled onboard UART headers.	2019-06-28	10.0	<a href="#">CVE-2018-15555</a> MISC FULLDISC
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple heap-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution. Note: A different vulnerability than CVE-2019-10989.	2019-06-28	7.5	<a href="#">CVE-2019-10989</a> MISC MISC MISC
advantech -- webaccess	In WebAccess/SCADA, Versions 8 3 5 and prior, multiple stack-based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	7.5	<a href="#">CVE-2019-10991</a> MISC MISC MISC MISC MISC MISC MISC
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple untrusted pointer dereference vulnerabilities may allow a remote attacker to execute arbitrary code.	2019-06-28	7.5	<a href="#">CVE-2019-10993</a> MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
chamilo -- chamilo_lms	Chamilo LMS 1.11 8 and 2.x allows remote code execution through an lp_upload.php unauthenticated file upload feature. It extracts a ZIP archive before checking its content, and once it has been extracted, does not check files in a recursive way. This means that by putting a .php file in a folder and then this folder in a ZIP archive, the server will accept this file without any checks. Because one can access this file from the website, it is remote code execution. This is related to a scorm imsmanifest.xml file, the import_package function, and extraction in \$courseSysDir.\$newDir.	2019-06-30	7.5	<a href="#">CVE-2019-13082</a> MISC MISC
cszcms -- csz_cms	core/MY_Security.php in CSZ CMS 1.2 2 before 2019-06-20 has member/login/check SQL injection by sending a crafted HTTP User-Agent header and omitting the csrf_csz parameter.	2019-06-30	7.5	<a href="#">CVE-2019-13086</a> MISC
dosbox -- dosbox	DOSBox 0.74-2 has Incorrect Access Control.	2019-07-02	7.5	<a href="#">CVE-2019-12594</a> CONFIRM MLIST FEDORA MISC MISC
flowpaper -- flexpaper	The Publish Service in FlexPaper (later renamed FlowPaper) 2 3.6 allows remote code execution via setup.php and change_config.php.	2019-07-03	7.5	<a href="#">CVE-2018-11686</a> MISC MISC
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 could allow malicious user with access to the DB2 instance account to leverage a fenced execution process to execute arbitrary code as root. IBM X-Force ID: 156567.	2019-07-01	7.2	<a href="#">CVE-2019-4057</a> XF CONFIRM
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 158519.	2019-07-01	7.2	<a href="#">CVE-2019-4154</a> BID XF CONFIRM

ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 161202.	2019-07-01	7.2	<a href="#">CVE-2019-4322</a> BID XF CONFIRM
icon -- loopchain	In Loopchain through 2.2.1.3, an attacker can escalate privileges from a low-privilege shell by changing the environment (aka injection in the DEFAULT_SCORE_HOST environment variable).	2019-06-28	9.0	<a href="#">CVE-2019-12997</a> MISC
lexmark -- 6500_firmware	Various Lexmark devices have a Buffer Overflow (issue 1 of 2).	2019-06-28	7.5	<a href="#">CVE-2018-15519</a> CONFIRM
lexmark -- cx421_firmware	Various Lexmark devices have a Buffer Overflow (issue 2 of 2).	2019-06-28	7.5	<a href="#">CVE-2018-15520</a> CONFIRM
matio_project -- matio	Multiple integer overflows exist in MATIO before 1.5.16, related to mat.c, mat4.c, mat5.c, mat73.c, and matvar_struct.c	2019-06-30	7.5	<a href="#">CVE-2019-13107</a> MISC
netapp -- clustered_data_ontap	NetApp AFF A700s Baseboard Management Controller (BMC) firmware versions 1.22 and higher were shipped with a default account enabled that could allow unauthorized arbitrary command execution.	2019-07-01	7.5	<a href="#">CVE-2019-5497</a> CONFIRM
nginx -- njs	njs through 0.3.3, used in NGINX, has a buffer over-read in nxt_utf8_decode in nxt/nxt_utf8.c. This issue occurs after the fix for CVE-2019-12207 is in place.	2019-06-29	7.5	<a href="#">CVE-2019-13067</a> MISC
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Authentication Bypass.	2019-07-02	7.5	<a href="#">CVE-2019-7266</a> MISC
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Authenticated Command Injection with root Code Execution.	2019-07-02	10.0	<a href="#">CVE-2019-7269</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Directory Traversal.	2019-07-02	7.5	<a href="#">CVE-2019-7253</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow File Inclusion.	2019-07-02	9.0	<a href="#">CVE-2019-7254</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Command Injections.	2019-07-02	10.0	<a href="#">CVE-2019-7256</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Unrestricted File Upload.	2019-07-02	7.5	<a href="#">CVE-2019-7257</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Hard-coded Credentials.	2019-07-02	10.0	<a href="#">CVE-2019-7261</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have a Version Control Failure.	2019-07-02	10.0	<a href="#">CVE-2019-7263</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow a Stack-based Buffer Overflow on the ARM platform.	2019-07-02	7.5	<a href="#">CVE-2019-7264</a> MISC
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Remote Code Execution (root access over SSH).	2019-07-02	10.0	<a href="#">CVE-2019-7265</a> MISC
odoo -- odoo	Incorrect access control in the database manager component in Odoo Community 10.0 and 11.0 and Odoo Enterprise 10.0 and 11.0 allows a remote attacker to restore a database dump without knowing the super-admin password. An arbitrary password succeeds.	2019-06-28	7.5	<a href="#">CVE-2018-14885</a> MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Authenticated File Upload with Code Execution as root.	2019-07-01	10.0	<a href="#">CVE-2019-7274</a> BID MISC
optergy -- enterprise	Optergy Proton/Enterprise devices allow Remote Root Code Execution via a Backdoor Console.	2019-07-01	10.0	<a href="#">CVE-2019-7276</a> BID MISC
optergy -- enterprise	Optergy Proton/Enterprise devices have Hard-coded Credentials.	2019-07-01	7.5	<a href="#">CVE-2019-7279</a> BID MISC
primasystems -- flexair	Prima Systems FlexAir devices allow Unauthenticated Command Injection resulting in Root Remote Code Execution.	2019-07-01	10.0	<a href="#">CVE-2019-7669</a> MISC
primasystems -- flexair	Prima Systems FlexAir devices allow Authenticated Command Injection resulting in Root Remote Code Execution.	2019-07-01	9.0	<a href="#">CVE-2019-7670</a> MISC
pulsesecure -- pulse_connect_secure	Session data between cluster nodes during cluster synchronization is not properly encrypted in Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX, PPS 5.2RX, or stand-alone devices.	2019-06-28	7.5	<a href="#">CVE-2018-20810</a> CONFIRM
pulsesecure -- pulse_connect_secure	An input validation issue has been found with login_meeting.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2.	2019-06-28	7.5	<a href="#">CVE-2018-20813</a> CONFIRM
redhat -- satellite	A path traversal flaw was found in spacewalk-proxy, all versions through 2.9, in the way the proxy processes cached client tokens. A remote, unauthenticated attacker could use this flaw to test the existence of arbitrary files, if they have access to the proxy's filesystem, or can execute arbitrary code in the context of the httpd process.	2019-07-02	7.5	<a href="#">CVE-2019-10137</a> CONFIRM
synology -- calendar	OS command injection vulnerability in drivers_syno_import_user.php in Synology Calendar before 2.3.1-0617 allows remote attackers to execute arbitrary commands via the crafted 'X-Real-IP' header.	2019-06-30	7.5	<a href="#">CVE-2019-11829</a> CONFIRM

synology -- photo_station	SQL injection vulnerability in synophoto_csPhotoDB.php in Synology Photo Station before 6.8.11-3489 and before 6.3-2977 allows remote attackers to execute arbitrary SQL command via the type parameter.	2019-06-30	<a href="#">7.5</a>	<a href="#">CVE-2019-11821</a> <a href="#">CONFIRM</a>
toaruos -- toaruos	linker/linker.c in ToaruOS through 1.10.9 has insecure LD_LIBRARY_PATH handling in setuid applications.	2019-06-29	<a href="#">7.2</a>	<a href="#">CVE-2019-13046</a> <a href="#">MISC</a>
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 has incorrect access control in sys_sysfunc case 9 for TOARU_SYS_FUNC_SETHEAP, allowing arbitrary kernel pages to be mapped into user land, leading to root access.	2019-06-29	<a href="#">7.2</a>	<a href="#">CVE-2019-13047</a> <a href="#">MISC</a>
toaruos -- toaruos	An integer wrap in kernel/sys/syscall.c in ToaruOS 1.10.10 allows users to map arbitrary kernel pages into userland process space via TOARU_SYS_FUNC_MMAP, leading to escalation of privileges.	2019-06-29	<a href="#">7.2</a>	<a href="#">CVE-2019-13049</a> <a href="#">MISC</a>
web-gooroo -- cms_web-gooroo	SQL injection vulnerability in /wbq/core/_includes/authorization.inc.php in CMS Web-Gooroo through 2013-01-19 allows remote attackers to execute arbitrary SQL commands via the wbq_login parameter.	2019-07-03	<a href="#">7.5</a>	<a href="#">CVE-2017-18346</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x00000000000024ed.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13247</a> <a href="#">MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd!JPEGTransW+0x0000000000002450.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13248</a> <a href="#">MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x000000000000b9e7a.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13249</a> <a href="#">MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x000000000000b9c2f.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13250</a> <a href="#">MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x000000000000c47ff.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13251</a> <a href="#">MISC</a>
acdsee -- acdsee	ACDSee Free 1.1 21 has a User Mode Write AV starting at IDE_ACDStd! EP_SetColorProfile+0x0000000000001172b0.	2019-07-04	<a href="#">6.8</a>	<a href="#">CVE-2019-13252</a> <a href="#">MISC</a>
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, an out-of-bounds read vulnerability is caused by a lack of proper validation of user-supplied data. Exploitation of this vulnerability may allow disclosure of information.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2019-10983</a> <a href="#">MISC</a> <a href="#">MISC</a>
advantech -- webaccess	In WebAccess/SCADA, Versions 8 3 5 and prior, a path traversal vulnerability is caused by a lack of proper validation of a user-supplied path prior to use in file operations. An attacker can leverage this vulnerability to delete files while posing as an administrator.	2019-06-28	<a href="#">6.4</a>	<a href="#">CVE-2019-10985</a> <a href="#">MISC</a> <a href="#">MISC</a>
advantech -- webaccess	In WebAccess/SCADA Versions 8.3.5 and prior, multiple out-of-bounds write vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution.	2019-06-28	<a href="#">6.8</a>	<a href="#">CVE-2019-10987</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
advisto -- peel_shopping	Advisto PEEL SHOPPING 9.0.0 has CSRF via en/achat/caddie_ajout.php and en/achat/caddie_affichage.php, as demonstrated by an XSS payload in the couleurId[0] parameter to the latter.	2019-06-30	<a href="#">6.8</a>	<a href="#">CVE-2018-20848</a> <a href="#">MISC</a>
arastta -- ecommerce	Arastta eCommerce 1.6.2 is vulnerable to XSS via the PATH_INFO to the login/URI.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20849</a> <a href="#">MISC</a>
archon_project -- archon	packages/subjects/pub/subjects.php in Archon 3 21 rev-1 has XSS in the referer parameter in an index.php?subjectypeid=xxx request, aka Open Bug Bounty ID OBB-466362.	2019-07-03	<a href="#">4.3</a>	<a href="#">CVE-2017-17972</a> <a href="#">MISC</a>
audio_file_library_project -- audio_file_library	In Audio File Library (aka audiofile) 0.3.6, there exists one NULL pointer dereference bug in ulaw2linear_buf in G711.cpp in libmodules.a that allows an attacker to cause a denial of service via a crafted file.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-13147</a> <a href="#">MISC</a>
cyberpanel -- cyberpanel	An issue was discovered in CyberPanel through 1 8.4. On the user edit page, an attacker can edit the administrator's e-mail and password because of the lack of CSRF protection.	2019-07-02	<a href="#">6.8</a>	<a href="#">CVE-2019-13056</a> <a href="#">MISC</a> <a href="#">MISC</a>
elitecms -- elite_cms	An issue was discovered in Elite CMS Pro 2 01. In /admin/add_sidebar.php, the ?page= parameter is vulnerable to SQL injection.	2019-07-03	<a href="#">6.5</a>	<a href="#">CVE-2018-12250</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	An integer overflow in Exiv2 through 0 27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted PNG image file, because PngImage::readMetadata mishandles a zero value for iccOffset.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13108</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	An integer overflow in Exiv2 through 0 27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted PNG image file, because PngImage::readMetadata mishandles a chunkLength - iccOffset subtraction.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13109</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	A ClifDirectory::readDirectory integer overflow and out-of-bounds read in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (SIGSEGV) via a crafted CRW image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13110</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	A WebPImage::decodeChunks integer overflow in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (large heap allocation followed by a very long running loop) via a crafted WEBP image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13111</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	A PngChunk::parseChunkContent uncontrolled memory allocation in Exiv2 through 0.27.1 allows an attacker to cause a denial of service (crash due to an std::bad_alloc exception) via a crafted PNG image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13112</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	Exiv2 through 0 27.1 allows an attacker to cause a denial of service (crash due to assertion failure) via an invalid data location in a CRW image file.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13113</a> <a href="#">MISC</a> <a href="#">MISC</a>
exiv2 -- exiv2	http.c in Exiv2 through 0.27.1 allows a malicious http server to cause a denial of service (crash due to a NULL pointer dereference) by returning a crafted response that lacks a space character.	2019-06-30	<a href="#">4.3</a>	<a href="#">CVE-2019-13114</a> <a href="#">MISC</a> <a href="#">MISC</a>
	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.5, 13.0 0-13.1.1.4, 12.1.0-12.1.4.1, and			



f5 -- big-ip_access_policy_manager	11.5.1-11.6.4 and BIG-IQ 6.0.0-6.1.0 and 5.1.0-5.4.0, an undisclosed iControl REST worker vulnerable to command injection for an Administrator user.	2019-07-02	6.5	<a href="#">CVE-2019-6620</a> CONFIRM
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.5, 13.0 0-13.1.1.4, 12.1.0-12.1.4.1, 11.6.1-11.6.3.4, and 11 5.1-11 5.8 and BIG-IQ 6.0.0-6.1 0 and 5.1.0-5.4 0, an undisclosed iControl REST worker is vulnerable to command injection by an admin/resource admin user. This issue impacts both iControl REST and tmsh implementations.	2019-07-02	6.5	<a href="#">CVE-2019-6621</a> CONFIRM
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.5, 13.0 0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4, an undisclosed iControl REST worker is vulnerable to command injection by an administrator or resource administrator user. This attack is only exploitable on multi-bladed systems.	2019-07-02	6.5	<a href="#">CVE-2019-6622</a> CONFIRM
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.4, 13.0 0-13.1.1.4, and 12.1.0-12.1.4, undisclosed traffic sent to BIG- P iSession virtual server may cause the Traffic Management Microkernel (TMM) to restart, resulting in a Denial-of-Service (DoS).	2019-07-02	5.0	<a href="#">CVE-2019-6623</a> BID CONFIRM
f5 -- big-ip_access_policy_manager	On BIG- P 14.1.0-14.1.0.5, 14 0.0-14.0.0.4, 13.0 0-13.1.1.4, and 12.1.0-12.1.4, an undisclosed traffic pattern sent to a BIG-IP UDP virtual server may lead to a denial-of-service (DoS).	2019-07-02	5.0	<a href="#">CVE-2019-6624</a> CONFIRM
f5 -- websafe_alert_server	A Cross Site Scripting (XSS) vulnerability in versions of F5 WebSafe Dashboard 3.9 x and earlier, aka F5 WebSafe Alert Server, allows an unauthenticated user to inject HTML via a crafted alert.	2019-07-01	4.3	<a href="#">CVE-2016-5235</a> CONFIRM
fla-shop -- html5_maps	Cross-site request forgery (CSRF) vulnerability in HTML5 Maps 1 6 5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5983</a> MISC MISC
flightcrew_project -- flightcrew	An issue was discovered in FlightCrew v0.9 2 and earlier. A NULL pointer dereference occurs in GetRelativePathToNcx() or GetRelativePathsToXhtmlDocuments() when a NULL pointer is passed to xc::XMLUri::IsValidURL(). This affects third-party software (not Sigil) that uses FlightCrew as a library.	2019-06-28	4.3	<a href="#">CVE-2019-13032</a> MISC
gnome -- glib	The keyfile settings backend in GNOME GLib (aka glib2.0) before 2.59.1 creates directories using g_file_make_directory_with_parents (kfsb->dir, NULL, NULL) and files using g_file_replace_contents (kfsb->file, contents, length, NULL, FALSE, G_FILE_CREATE_REPLACE_DESTINATION, NULL, NULL, NULL). Consequently, it does not properly restrict directory (and file) permissions. Instead, for directories, 0777 permissions are used; for files, default file permissions are used. This is similar to CVE-2019-12450.	2019-06-28	5.0	<a href="#">CVE-2019-13012</a> MISC MISC MISC
grafana -- grafana	public/app/features/panel/panel_ctrl.ts in Grafana before 6.2.5 allows HTML Injection in panel drilldown links (via the Title or url field).	2019-06-29	4.3	<a href="#">CVE-2019-13068</a> MISC MISC
ibm -- bigfix_inventory	IBM BigFix Inventory v9 (SUA v9 / LMT v9) discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 161807.	2019-06-28	5.0	<a href="#">CVE-2019-4369</a> CONFIRM BID XF
ibm -- daeja_viewone	IBM Daeja ViewONE Professional, Standard & Virtual 5.0 through 5 0.5 could allow an unauthorized user to download server files resulting in sensitive information disclosure. IBM X-Force ID: 160012.	2019-07-02	5.0	<a href="#">CVE-2019-4260</a> CONFIRM XF
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. BM X-Force ID: 158092.	2019-07-01	4.3	<a href="#">CVE-2019-4102</a> BID XF CONFIRM
ibm -- planning_analytics	IBM Planning Analytics 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158281.	2019-07-02	4.3	<a href="#">CVE-2019-4134</a> XF CONFIRM
ibm -- security_guardium	IBM Security Guardium 10.5 could allow a remote attacker to upload arbitrary files, which could allow the attacker to execute arbitrary code on the vulnerable web server. BM X-Force D: 160698.	2019-07-02	6.5	<a href="#">CVE-2019-4292</a> BID XF CONFIRM
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8 0, 8 5, and 9 0 Admin Console could allow a remote attacker to obtain sensitive information when a specially crafted url causes a stack trace to be dumped. IBM X-Force ID: 160202.	2019-06-28	5.0	<a href="#">CVE-2019-4269</a> BID XF CONFIRM
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadBMPImage in coders/bmp.c.	2019-07-01	4.3	<a href="#">CVE-2019-13133</a> MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadVIFImage in coders/viff.c.	2019-07-01	4.3	<a href="#">CVE-2019-13134</a> MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability in the function ReadCUTImage in coders/cut.c.	2019-07-01	6.8	<a href="#">CVE-2019-13135</a> MISC MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has an integer overflow vulnerability in the function TIFFSeekCustomStream in coders/tiff.c.	2019-07-01	6.8	<a href="#">CVE-2019-13136</a> MISC MISC
imagemagick -- imagemagick	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadPSImage in coders/ps.c.	2019-07-01	4.3	<a href="#">CVE-2019-13137</a> MISC MISC MISC
intelliants -- subrion	Subrion CMS before 4.1.4 has XSS.	2019-07-03	4.3	<a href="#">CVE-2018-11317</a> MISC CONFIRM
				<a href="#">CVE-2019-13045</a> SUSE MISC MLIST

irssi -- irssi	Irssi before 1.0.8, 1.1.x before 1.1.3, and 1.2.x before 1.2.1, when SASL is enabled, has a use after free when sending SASL login to the server.	2019-06-29	6.8	<a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">UBUNTU</a>
istio -- istio	Istio before 1.2.2 mishandles certain access tokens, leading to "Epoch 0 terminated with an error" in Envoy. This is related to a jwt_authenticator.cc segmentation fault.	2019-06-28	5.0	<a href="#">CVE-2019-12995</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
jetbrains -- teamcity	A reflected XSS on a user page was detected on one of the JetBrains TeamCity pages. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	4.3	<a href="#">CVE-2019-12842</a> <a href="#">CONFIRM</a>
jetbrains -- teamcity	The generated Kotlin DSL settings allowed usage of an unencrypted connection for resolving artifacts. The issue was fixed in JetBrains TeamCity 2018.2.3.	2019-07-03	5.0	<a href="#">CVE-2019-12845</a> <a href="#">MISC</a>
jetbrains -- teamcity	A user without the required permissions could gain access to some JetBrains TeamCity settings. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	4.0	<a href="#">CVE-2019-12846</a> <a href="#">CONFIRM</a>
kubevirt -- containerized-data-importer	A flaw was found in the containerized-data-importer in virt-cdi-cloner, version 1.4, where the host-assisted cloning feature does not determine whether the requesting user has permission to access the Persistent Volume Claim (PVC) in the source namespace. This could allow users to clone any PVC in the cluster into their own namespace, effectively allowing access to other user's data.	2019-06-28	4.0	<a href="#">CVE-2019-10175</a> <a href="#">CONFIRM</a>
lemonldap-ng -- lemonldap::	LemonLDAP: NG before 1.9.20 has an XML External Entity (XXE) issue when submitting a notification to the notification server. By default, the notification server is not enabled and has a "deny all" rule.	2019-06-28	6.8	<a href="#">CVE-2019-13031</a> <a href="#">MISC</a> <a href="#">MLIST</a>
mod_auth_mellon_project -- mod_auth_mellon	mod_auth_mellon through 0.14.2 has an Open Redirect via the login?ReturnTo= substring, as demonstrated by omitting the // after http: in the target URL.	2019-06-29	4.3	<a href="#">CVE-2019-13038</a> <a href="#">MISC</a>
monstra -- monstra_cms	Monstra CMS before 3.0.4 has XSS via index.php.	2019-07-03	4.3	<a href="#">CVE-2018-11227</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
nortekcontrol -- linear_emerge_5000p_firmware	Linear eMerge 50P/5000P devices allow Cross-Site Request Forgery (CSRF).	2019-07-02	6.8	<a href="#">CVE-2019-7270</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_5000p_firmware	Nortek Linear eMerge 50P/5000P devices have Default Credentials.	2019-07-01	5.0	<a href="#">CVE-2019-7271</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Default Credentials.	2019-07-02	5.0	<a href="#">CVE-2019-7252</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow XSS.	2019-07-02	4.3	<a href="#">CVE-2019-7255</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Privilege Escalation.	2019-07-02	6.5	<a href="#">CVE-2019-7258</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Authorization Bypass with Information Disclosure.	2019-07-02	4.0	<a href="#">CVE-2019-7259</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices have Cleartext Credentials in a Database.	2019-07-02	5.0	<a href="#">CVE-2019-7260</a> <a href="#">MISC</a> <a href="#">MISC</a>
nortekcontrol -- linear_emerge_elite_firmware	Linear eMerge E3-Series devices allow Cross-Site Request Forgery (CSRF).	2019-07-02	6.8	<a href="#">CVE-2019-7262</a> <a href="#">MISC</a> <a href="#">MISC</a>
novaksolutions -- infusionsoft-php-sdk	novaksolutions/infusionsoft-php-sdk v2016-10-31 is vulnerable to a reflected XSS in the leadscoring.php resulting code execution	2019-07-03	4.3	<a href="#">CVE-2017-6216</a> <a href="#">MISC</a>
odoo -- odoo	Improper data access control in Odoo Community 10.0 and 11.0 and Odoo Enterprise 10.0 and 11.0 allows authenticated users to perform a CSV export of the secure hashed passwords of other users.	2019-07-03	4.0	<a href="#">CVE-2018-14861</a> <a href="#">CONFIRM</a>
odoo -- odoo	Incorrect access control in the mail templating system in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated internal users to delete arbitrary menuitems via a crafted RPC request.	2019-07-03	5.5	<a href="#">CVE-2018-14862</a> <a href="#">CONFIRM</a>
odoo -- odoo	Incorrect access control in the RPC framework in Odoo Community 8.0 through 11.0 and Odoo Enterprise 9.0 through 11.0 allows authenticated users to call private functions via RPC.	2019-07-03	5.5	<a href="#">CVE-2018-14863</a> <a href="#">CONFIRM</a>
odoo -- odoo	Incorrect access control in asset bundles in Odoo Community 9.0 through 11.0 and earlier and Odoo Enterprise 9.0 through 11.0 and earlier allows remote authenticated users to inject arbitrary web script via a crafted attachment.	2019-07-03	4.0	<a href="#">CVE-2018-14864</a> <a href="#">CONFIRM</a>
odoo -- odoo	Report engine in Odoo Community 9.0 through 11.0 and earlier and Odoo Enterprise 9.0 through 11.0 and earlier does not use secure options when passing documents to wkhtmltopdf, which allows remote attackers to read local files.	2019-07-03	4.0	<a href="#">CVE-2018-14865</a> <a href="#">CONFIRM</a>
odoo -- odoo	Incorrect access control in the portal messaging system in Odoo Community 9.0 and 10.0 and Odoo Enterprise 9.0 and 10.0 allows remote attackers to post messages on behalf of customers, and to guess document attribute values, via crafted parameters.	2019-06-28	5.0	<a href="#">CVE-2018-14867</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
odoo -- odoo	Incorrect access control in the Password Encryption module in Odoo Community 9.0 and Odoo Enterprise 9.0 allows authenticated users to change the password of other users without knowing their current password via a crafted RPC call.	2019-06-28	4.0	<a href="#">CVE-2018-14868</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
odoo -- odoo	The module-description renderer in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier does not disable RST's local file inclusion, which allows privileged authenticated users to read local files via a crafted module description.	2019-06-28	4.0	<a href="#">CVE-2018-14886</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
odoo -- odoo	Improper Host header sanitization in the dbfilter routing component in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows a remote attacker to deny access to the service and to disclose database names	2019-06-28	5.8	<a href="#">CVE-2018-14887</a> <a href="#">MISC</a>

	via a crafted request.			<a href="#">CONFIRM</a>
open-xchange -- ox_guard	OX Guard 2.8.0 has CSRF.	2019-07-03	<a href="#">6.8</a>	<a href="#">CVE-2018-10986</a> <a href="#">CONFIRM</a>
optergy -- enterprise	Optergy Proton/Enterprise devices allow Username Disclosure.	2019-07-01	<a href="#">5.0</a>	<a href="#">CVE-2019-7272</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
optergy -- enterprise	Optergy Proton/Enterprise devices allow Cross-Site Request Forgery (CSRF).	2019-07-01	<a href="#">6.8</a>	<a href="#">CVE-2019-7273</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
optergy -- enterprise	Optergy Proton/Enterprise devices allow Open Redirect.	2019-07-01	<a href="#">5.8</a>	<a href="#">CVE-2019-7275</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
optergy -- enterprise	Optergy Proton/Enterprise devices allow Unauthenticated Internal Network Information Disclosure.	2019-07-01	<a href="#">5.0</a>	<a href="#">CVE-2019-7277</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
optergy -- enterprise	Optergy Proton/Enterprise devices have an Unauthenticated SMS Sending Service.	2019-07-01	<a href="#">6.4</a>	<a href="#">CVE-2019-7278</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
paloaltonetworks -- minemeld	Cross-site scripting vulnerability in Palo Alto Networks MineMeld version 0.9.60 and earlier may allow a remote attacker able to convince an authenticated MineMeld admin to type malicious input in the MineMeld UI could execute arbitrary JavaScript code in the admin's browser.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-1578</a> <a href="#">CONFIRM</a>
paloaltonetworks -- traps	Code injection vulnerability in Palo Alto Networks Traps 5.0.5 and earlier may allow an authenticated attacker to inject arbitrary JavaScript or HTML.	2019-07-01	<a href="#">6.5</a>	<a href="#">CVE-2019-1577</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
primasystems -- flexair	Prima Systems FlexAir devices have an Insufficient Session-ID Length.	2019-07-01	<a href="#">4.0</a>	<a href="#">CVE-2019-7280</a> <a href="#">MISC</a> <a href="#">MISC</a>
primasystems -- flexair	Prima Systems FlexAir devices allow Cross-Site Request Forgery (CSRF).	2019-07-01	<a href="#">6.8</a>	<a href="#">CVE-2019-7281</a> <a href="#">MISC</a> <a href="#">MISC</a>
primasystems -- flexair	Prima Systems FlexAir devices allow authentication with MD5 hashes directly.	2019-07-01	<a href="#">6.5</a>	<a href="#">CVE-2019-7666</a> <a href="#">MISC</a> <a href="#">MISC</a>
primasystems -- flexair	Prima Systems FlexAir devices allow unauthenticated download of the database configuration backup due to a predictable name, resulting in authentication bypass (a login authenticated with the MD5 hash of any user found in the database).	2019-07-01	<a href="#">6.4</a>	<a href="#">CVE-2019-7667</a> <a href="#">MISC</a> <a href="#">MISC</a>
primasystems -- flexair	Prima Systems FlexAir devices have Default Credentials.	2019-07-01	<a href="#">5.0</a>	<a href="#">CVE-2019-7668</a> <a href="#">MISC</a> <a href="#">MISC</a>
pulsesecure -- pulse_connect_secure	An XSS issue has been found with rd.cgi in Pulse Secure Pulse Connect Secure 8.3RX before 8.3R3 due to improper header sanitization. This is not applicable to 8.1RX.	2019-06-28	<a href="#">4.3</a>	<a href="#">CVE-2018-20808</a> <a href="#">CONFIRM</a>
pulsesecure -- pulse_connect_secure	A crafted message can cause the web server to crash with Pulse Secure Pulse Connect Secure (PCS) 8.3RX before 8.3R5 and Pulse Policy Secure 5.4RX before 5.4R5. This is not applicable to PCS 8.1RX.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2018-20809</a> <a href="#">CONFIRM</a>
pulsesecure -- pulse_connect_secure	A hidden RPC service issue was found with Pulse Secure Pulse Connect Secure 8.3RX before 8.3R2 and 8.1RX before 8.1R12.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2018-20811</a> <a href="#">CONFIRM</a>
pulsesecure -- pulse_connect_secure	An XSS issue was found with Psaldownload.cgi in Pulse Secure Pulse Connect Secure (PCS) 8.3R2 before 8.3R2 and Pulse Policy Secure (PPS) 5.4RX before 5.4R2. This is not applicable to PCS 8.1RX or PPS 5.2RX.	2019-06-28	<a href="#">4.3</a>	<a href="#">CVE-2018-20814</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
pulsesecure -- pulse_secure_desktop_client	An information exposure issue where IPv6 DNS traffic would be sent outside of the VPN tunnel (when Traffic Enforcement was enabled) exists in Pulse Secure Pulse Secure Desktop 9.0R1 and below. This is applicable only to dual-stack (IPv4/IPv6) endpoints.	2019-06-28	<a href="#">5.0</a>	<a href="#">CVE-2018-20812</a> <a href="#">CONFIRM</a>
rapid7 -- nexpose	A Cross-Site Request Forgery (CSRF) vulnerability was found in Rapid7 Nexpose InsightVM Security Console versions 6.5.0 through 6.5.68. This issue allows attackers to exploit CSRF vulnerabilities on API endpoints using Flash to circumvent a cross-domain pre-flight OPTIONS request.	2019-07-03	<a href="#">6.8</a>	<a href="#">CVE-2019-5630</a> <a href="#">CONFIRM</a>
redhat -- satellite	It was found that Spacewalk, all versions through 2.9, did not safely compute client token checksums. An attacker with a valid, but expired, authenticated set of headers could move some digits around, artificially extending the session validity without modifying the checksum.	2019-07-02	<a href="#">4.0</a>	<a href="#">CVE-2019-10136</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
rockoa -- rockoa	RockOA 1.8.7 allows remote attackers to obtain sensitive information because the webmain/webmainAction.php publictreestore method constructs a SQL WHERE clause unsafely by using the pidfields and idfields parameters, aka background SQL injection.	2019-06-28	<a href="#">4.0</a>	<a href="#">CVE-2019-9846</a> <a href="#">MISC</a>
seeddms -- seeddms	A stored XSS vulnerability was found in SeedDMS 5.1.11 due to poorly escaping the search result in the autocomplete search form placed in the header of out/out.Viewfolder.php.	2019-06-28	<a href="#">4.3</a>	<a href="#">CVE-2019-12932</a> <a href="#">MISC</a>
squirrelmail -- squirrelmail	XSS was discovered in SquirrelMail through 1.4.22 and 1.5.x through 1.5.2. Due to improper handling of RCDATA and RAWTEXT type elements, the built-in sanitization mechanism can be bypassed. Malicious script content from HTML e-mail can be executed within the application context via crafted use of (for example) a NOEMBED, NOFRAMES, NOSCRIPT, or TEXTAREA element.	2019-07-01	<a href="#">4.3</a>	<a href="#">CVE-2019-12970</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
symantec -- endpoint_encryption	Symantec Endpoint Encryption, prior to SEE 11.3.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue that allows a user to gain elevated access to resources that are normally protected at lower access levels.	2019-07-01	<a href="#">4.6</a>	<a href="#">CVE-2019-9702</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

symantec -- endpoint_encryption	Symantec Endpoint Encryption, prior to SEE 11.3.0, may be susceptible to a privilege escalation vulnerability, which is a type of issue that allows a user to gain elevated access to resources that are normally protected at lower access levels.	2019-07-01	4.6	<a href="#">CVE-2019-9703</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
synology -- moments	Relative path traversal vulnerability in SYNO.PhotoTeam.Upload.Item in Synology Moments before 1.3.0-0691 allows remote authenticated users to upload arbitrary files via the name parameter.	2019-06-30	6.5	<a href="#">CVE-2019-11826</a> <a href="#">CONFIRM</a>
synology -- photo_station	Relative path traversal vulnerability in SYNO.PhotoStation.File in Synology Photo Station before 6.8.11-3489 and before 6.3-2977 allows remote attackers to upload arbitrary files via the uploadphoto parameter.	2019-06-30	4.0	<a href="#">CVE-2019-11822</a> <a href="#">CONFIRM</a>
tenable -- nessus	Content Injection vulnerability in Tenable Nessus prior to 8.5.0 may allow an authenticated, local attacker to exploit this vulnerability by convincing another targeted Nessus user to view a malicious URL and use Nessus to send fraudulent messages. Successful exploitation could allow the authenticated adversary to inject arbitrary text into the feed status, which will remain saved post session expiration.	2019-07-01	4.3	<a href="#">CVE-2019-3962</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
toaruos -- toaruos	kernel/sys/syscall.c in ToaruOS through 1.10.9 allows a denial of service upon a critical error in certain sys_sbrk allocation patterns (involving PAGE_SIZE, and a value less than PAGE_SIZE).	2019-06-29	4.9	<a href="#">CVE-2019-13048</a> <a href="#">MISC</a>
waspthemes -- custom_css_pro	Cross-site request forgery (CSRF) vulnerability in Custom CSS Pro 1.0.3 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	6.8	<a href="#">CVE-2019-5984</a> <a href="#">MISC</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000384e2a.	2019-06-30	6.8	<a href="#">CVE-2019-13083</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000026b739.	2019-06-30	6.8	<a href="#">CVE-2019-13084</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000030ecfa.	2019-06-30	6.8	<a href="#">CVE-2019-13085</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000385474.	2019-07-04	6.8	<a href="#">CVE-2019-13253</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e808.	2019-07-04	6.8	<a href="#">CVE-2019-13254</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000327464.	2019-07-04	6.8	<a href="#">CVE-2019-13255</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e849.	2019-07-04	6.8	<a href="#">CVE-2019-13256</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x00000000003273aa.	2019-07-04	6.8	<a href="#">CVE-2019-13257</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000328165.	2019-07-04	6.8	<a href="#">CVE-2019-13258</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x000000000032e566.	2019-07-04	6.8	<a href="#">CVE-2019-13259</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000327a07.	2019-07-04	6.8	<a href="#">CVE-2019-13260</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x0000000000328384.	2019-07-04	6.8	<a href="#">CVE-2019-13261</a> <a href="#">MISC</a>
xnview -- xnview	XnView Classic 2.48 has a User Mode Write AV starting at xnview+0x00000000003283eb.	2019-07-04	6.8	<a href="#">CVE-2019-13262</a> <a href="#">MISC</a>
xpertsol -- server_status_by_hostname/ip	A SQL injection vulnerability in the Xpert Solution "Server Status by Hostname/ P" plugin 4.6 for WordPress allows an authenticated user to execute arbitrary SQL commands via GET parameters.	2019-07-03	6.5	<a href="#">CVE-2019-12570</a> <a href="#">MISC</a>
zoneminder -- zoneminder	Stored XSS in the Filters page (Name field) in ZoneMinder 1.32.3 allows a malicious user to embed and execute JavaScript code in the browser of any user who navigates to this page.	2019-06-29	4.3	<a href="#">CVE-2019-13072</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/page-edit.php (content box), which can be used to get a user's cookie.	2019-07-05	3.5	<a href="#">CVE-2019-13339</a> <a href="#">MISC</a>
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the content box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, CVE-2018-20520, and CVE-2019-13186.	2019-07-05	3.5	<a href="#">CVE-2019-13340</a> <a href="#">MISC</a>
1234n -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/conf.php (comment box), which can be used to get a user's cookie.	2019-07-05	3.5	<a href="#">CVE-2019-13341</a> <a href="#">MISC</a>
f5 -- websafe_alert_server	Cross-Site-Scripting (XSS) vulnerabilities in F5 WebSafe Dashboard 3.9.5 and earlier, aka F5 WebSafe Alert Server, allow privileged authenticated users to inject arbitrary web script or HTML when creating a new user, account or signature.	2019-07-01	3.5	<a href="#">CVE-2016-5236</a> <a href="#">CONFIRM</a>
fujielectric -- alpha7_pc_loader_firmware	An out-of-bounds read vulnerability has been identified in Fuji Electric Alpha7 PC Loader Versions 1.1 and prior, which may crash the system.	2019-07-02	3.3	<a href="#">CVE-2019-10975</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- business_automation_workflow	IBM Business Automation Workflow 18.0.0.0, 18.0.0.1, 18.0.0.2, and 19.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 162657.	2019-07-01	3.5	<a href="#">CVE-2019-4410</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.1, 10.5, and 11.1 is vulnerable to a denial of service. Users that have both			<a href="#">CVE-2019-4101</a> <a href="#">BID</a>

ibm -- db2	EXECUTE on PD_GET_DIAG_HIST and access to the diagnostic directory on the DB2 server can cause the instance to crash. BM X-Force D: 158091.	2019-07-01	2.1	<a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- spectrum_protect	IBM Tivoli Storage Manager Server ( BM Spectrum Protect 7.1 and 8.1) could allow a local user to replace existing databases by restoring old data. IBM X-Force ID: 158336.	2019-07-02	3.6	<a href="#">CVE-2019-4140</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
synology -- calendar	Cross-site scripting (XSS) vulnerability in Event Editor in Synology Calendar before 2.3.0-0615 allows remote attackers to inject arbitrary web script or HTML via the title parameter.	2019-06-30	3.5	<a href="#">CVE-2019-11825</a> <a href="#">CONFIRM</a>
synology -- note_station	Cross-site scripting (XSS) vulnerability in SYNO.NoteStation.Shard in Synology Note Station before 2.5.3-0863 allows remote attackers to inject arbitrary web script or HTML via the object_id parameter.	2019-06-30	3.5	<a href="#">CVE-2019-11827</a> <a href="#">CONFIRM</a>
synology -- office	Cross-site scripting (XSS) vulnerability in Chart in Synology Office before 3.1.4-2771 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2019-06-30	3.5	<a href="#">CVE-2019-11828</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a.t.works -- idoors_reader	Doors Reader 2.10.17 and earlier allows an attacker on the same network segment to bypass authentication to access the management console and operate the product via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5964</a> <a href="#">MISC</a> <a href="#">MISC</a>
amcrest -- ipm-721s_devices	On Amcrest PM-721S V2.420.AC00.16.R.20160909 devices, the users on the device are divided into 2 groups "admin" and "user". However, as a part of security analysis it was identified that a low privileged user who belongs to the "user" group and who has access to login in to the web administrative interface of the device can add a new administrative user to the interface using HTTP APIs provided by the device and perform all the actions as an administrative user by using that account. If the firmware version V2.420.AC00.16.R.9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable functions that performs the various action described in HTTP APIs. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function at address 0x00429084 in IDA pro is the one that processes the HTTP API request for "addUser" action. If one traces the calls to this function, it can be clearly seen that the uncton sub_41F38C at address 0x0041F588 parses the call received from the browser and passes it to the "addUser" uncton without any authorization check.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8230</a> <a href="#">MISC</a> <a href="#">MISC</a>
amcrest -- ipm-721s_devices	The Amcrest IPM-721S Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322 allows HTTP requests that permit enabling various functionalities of the camera by using HTTP APIs, instead of the web management interface that is provided by the application. This HTTP API receives the credentials as base64 encoded in the Authorization HTTP header. However, a missing length check in the code allows an attacker to send a string of 1024 characters in the password field, and allows an attacker to exploit a memory corruption issue. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials. If the firmware version Amcrest_IPC-AWXX_Eng_N_V2.420.AC00.17.R.20170322 is dissected using the binwalk tool, one obtains a _user-x.squashfs img.extracted archive which contains the filesystem set up on the device that has many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the HTTP API specification. If we open this binary in DA Pro we will notice that this follows an ARM little-endian format. The function at address 00415364 in IDA Pro starts the HTTP authentication process. This function calls another function at sub_0042CCA0 at address 0041549C. This function performs a strchr operation after base64 decoding the credentials, and stores the result on the stack, which results in a stack-based buffer overflow.	2019-07-03	not yet calculated	<a href="#">CVE-2017-13719</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
amcrest -- ipm-721s_devices	Amcrest PM-721S V2.420.AC00.16.R.20160909 devices have default credentials that are hardcoded in the firmware and can be extracted by anyone who reverses the firmware to identify them. If the firmware version V2.420.AC00.16.R.9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If one opens this binary in DA-pro, one will notice that this follows a ARM little endian format. The uncton sub_3DB2FC in DA pro is identified to be setting up the values at address 0x003DB5A6. The sub_5C057C then sets this value and adds it to the Configuration files in mnt/mtd/Config/Account1 file.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8226</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
	Amcrest PM-721S V2.420.AC00.16.R.20160909 devices have a timeout policy to wait for 5 minutes in case 30 incorrect password attempts are detected using the Web and HTTP API interface			



amcrest -- ipm-721s_devices	provided by the device. However, if the same brute force attempt is performed using the ONVIF specification (which is supported by the same binary) then there is no account lockout or timeout executed. This can allow an attacker to circumvent the account protection mechanism and brute force the credentials. If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that performs the credential check in the binary for the ONVIF specification. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function at address 00671618 in IDA pro is parses the WSSE security token header. The sub_603D8 then performs the authentication check and if it is incorrect passes to the function sub_59F4C which prints the value "Sender not authorized."	2019-07-03	not yet calculated	<a href="#">CVE-2017-8227</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
amcrest -- ipm-721s_devices	Amcrest PM-721S V2.420.AC00.16.R.20160909 devices mishandle reboots within the past two hours. Amcrest cloud services does not perform a thorough verification when allowing the user to add a new camera to the user's account to ensure that the user actually owns the camera other than knowing the serial number of the camera. This can allow an attacker who knows the serial number to easily add another user's camera to an attacker's cloud account and control it completely. This is possible in case of any camera that is currently not a part of an Amcrest cloud account or has been removed from the user's cloud account. Also, another requirement for a successful attack is that the user should have rebooted the camera in the last two hours. However, both of these conditions are very likely for new cameras that are sold over the Internet at many ecommerce websites or vendors that sell the Amcrest products. The successful attack results in an attacker being able to completely control the camera which includes being able to view and listen on what the camera can see, being able to change the motion detection settings and also be able to turn the camera off without the user being aware of it. Note: The same attack can be executed using the Amcrest Cloud mobile application.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8228</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
amcrest -- ipm-721s_devices	Amcrest PM-721S V2.420.AC00.16.R.20160909 devices allow an unauthenticated attacker to download the administrative credentials. If the firmware version V2.420.AC00.16.R 9/9/2016 is dissected using binwalk tool, one obtains a _user-x.squashfs.img.extracted archive which contains the filesystem set up on the device that many of the binaries in the /usr folder. The binary "sonia" is the one that has the vulnerable function that sets up the default credentials on the device. If one opens this binary in IDA-pro one will notice that this follows a ARM little endian format. The function sub_436D6 in IDA pro is identified to be setting up the configuration for the device. If one scrolls to the address 0x000437C2 then one can see that /current_config is being set as an ALIAS for /mnt/mtd/Config folder on the device. If one TELNETs into the device and navigates to /mnt/mtd/Config folder, one can observe that it contains various files such as Account1, Account2, SHAACount1, etc. This means that if one navigates to http://[IPofcamera]/current_config/Sha1Account1 then one should be able to view the content of the files. The security researchers assumed that this was only possible only after authentication to the device. However, when unauthenticated access tests were performed for the same URL as provided above, it was observed that the device file could be downloaded without any authentication.	2019-07-03	not yet calculated	<a href="#">CVE-2017-8229</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
arox -- school-erp_pro	AROX School-ERP Pro has a command execution vulnerability. import_stud.php and upload_file.php do not have session control. Therefore an unauthenticated user can execute a command on the system.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13294</a> <a href="#">MISC</a> <a href="#">MISC</a>
artica -- pandora_fms	Artica Pandora FMS 7.0 NG before 735 suffers from local privilege escalation due to improper permissions on C:\PandoraFMS and its sub-folders, allowing standard users to create new files. Moreover, the Apache service httpd.exe will try to execute cmd.exe from C:\PandoraFMS (the current directory) as NT AUTHORITY\SYSTEM upon web requests to the portal. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13035</a> <a href="#">MISC</a>
artifex -- mupdf	Artifex MuPDF 1.15.0 has a heap-based buffer overflow in z_append_display_node located at fitz/list-device.c, allowing remote attackers to execute arbitrary code via a crafted PDF file. This occurs with a large BDC property name that overflows the allocated size of a display list node.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13290</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
axiosys -- bento4	An issue was discovered in Bento4 1.5.1.0. A memory allocation failure is unhandled in Core/Api4SdpAtom.cpp and leads to crashes. When parsing input video, the program allocates a new buffer to parse an atom in the stream. The unhandled memory allocation failure causes a direct copy to a NULL pointer.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13238</a> <a href="#">MISC</a>
bks -- bks_ebk_ethernet_buskoppler_pro	BKS EBK Ethernet-Buskoppler Pro before 3.01 allows Unrestricted Upload of a File with a Dangerous Type.	2019-07-05	not yet calculated	<a href="#">CVE-2019-12971</a> <a href="#">MISC</a>
	It was discovered as a part of the research on IoT devices in the most recent firmware for Blipcare device that the device allows to connect to web management interface on a non-SSL connection using plain text HTTP protocol. The user uses the web			<a href="#">CVE-2017-</a>

blipcare -- blipcare_wi-fi_blood_pressure_monitor	management interface of the device to provide the user's Wi-Fi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is connected to the Blipcare's device wireless network to easily sniff these values using a MITM attack.	2019-07-02	not yet calculated	<a href="#">11578</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
blipcare -- blipcare_wi-fi_blood_pressure_monitor	In the most recent firmware for Blipcare, the device provides an open Wireless network called "Blip" for communicating with the device. The user connects to this open Wireless network and uses the web management interface of the device to provide the user's Wi-Fi credentials so that the device can connect to it and have Internet access. This device acts as a Wireless Blood pressure monitor and is used to measure blood pressure levels of a person. This allows an attacker who is in vicinity of Wireless signal generated by the Blipcare device to easily sniff the credentials. Also, an attacker can connect to the open wireless network "Blip" exposed by the device and modify the HTTP response presented to the user by the device to execute other attacks such as convincing the user to download and execute a malicious binary that would infect a user's computer or mobile device with malware.	2019-07-02	not yet calculated	<a href="#">CVE-2017-11579</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
blipcare -- blipcare_wi-fi_blood_pressure_monitor	Blipcare Wifi blood pressure monitor BP700 10.1 devices allow memory corruption that results in Denial of Service. When connected to the "Blip" open wireless connection provided by the device, if a large string is sent as a part of the HTTP request in any part of the HTTP headers, the device could become completely unresponsive. Presumably this happens as the memory footprint provided to this device is very small. According to the specs from Rezolt, the Wi-Fi module only has 256k of memory. As a result, an incorrect string copy operation using either memcpy, strcpy, or any of their other variants could result in filling up the memory space allocated to the function executing and this would result in memory corruption. To test the theory, one can modify the demo application provided by the Cypress WICED SDK and introduce an incorrect "memcpy" operation and use the compiled application on the evaluation board provided by Cypress semiconductors with exactly the same Wi-Fi SOC. The results were identical where the device would completely stop responding to any of the ping or web requests.	2019-07-02	not yet calculated	<a href="#">CVE-2017-11580</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
blogengine -- blogengine net	BlogEngine.NET 3.3.7.0 allows /api/filemanager Directory Traversal via the path parameter.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10717</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
blogengine -- blogengine net	BlogEngine.NET 3.3.7.0 allows a Client Side URL Redirect via the returnUrl parameter, related to BlogEngine/BlogEngine.Core/Services/Security/Security.cs, login.aspx, and register.aspx.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10721</a> <a href="#">MISC</a> <a href="#">MISC</a>
calamares -- calamares	Calamares versions 3.1 through 3.2.10 copies a LUKS encryption keyfile from /crypto_keyfile.bin (mode 0600 owned by root) to /boot within a globally readable initramfs image with insecure permissions, which allows this originally protected file to be read by any user, thereby disclosing decryption keys for LUKS containers created with Full Disk Encryption.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13179</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
calamares -- calamares	modules/luksbootkeyfile/main.py in Calamares versions 3.1 through 3.2.10 has a race condition between the time when the LUKS encryption keyfile is created and when secure permissions are set.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13178</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
centreon -- centreon	Centreon V19.04 allows the attacker to execute arbitrary system commands by using the value "init_script"."Monitoring Engine Binary" in main get.php to insert a arbitrary command into the database, and execute it by calling the vulnerable page www/include/configuration/configGenerate/xml/generateFiles.php which passes the inserted value to the database to shell_exec without sanitizing it, allowing one to execute system arbitrary commands).	2019-07-01	not yet calculated	<a href="#">CVE-2019-13024</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- 7800_and_8800_series_ip_phones	A vulnerability in Cisco SIP Phone Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected phone. The vulnerability is due to insufficient validation of input Session Initiation Protocol (SIP) packets. An attacker could exploit this vulnerability by altering the SIP replies that are sent to the affected phone during the registration process. A successful exploit could allow the attacker to cause the phone to reboot and not complete the registration process.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1922</a> <a href="#">CISCO</a>
cisco -- advanced_malware_protection_for_endpoints_for_windows	A vulnerability in Cisco Advanced Malware Protection (AMP) for Endpoints for Windows could allow an authenticated, local attacker with administrator privileges to execute arbitrary code. The vulnerability is due to insufficient validation of dynamically loaded modules. An attacker could exploit this vulnerability by placing a file in a specific location in the Windows filesystem. A successful exploit could allow the attacker to execute the code with the privileges of the AMP service.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1932</a> <a href="#">CISCO</a>

cisco -- application_policy_infrastructure_controller_software	A vulnerability in the REST API for software device management in Cisco Application Policy Infrastructure Controller (APIC) Software could allow an authenticated, remote attacker to escalate privileges to root on an affected device. The vulnerability is due to incomplete validation and error checking or the file path when specific software is uploaded. An attacker could exploit this vulnerability by uploading malicious software using the REST API. A successful exploit could allow an attacker to escalate their privilege level to root. The attacker would need to have the administrator role on the device.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1889</a> <a href="#">CISCO</a>
cisco -- email_security_appliance	A vulnerability in the email message scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured filters on the device. The vulnerability is due to improper input validation of certain email fields. An attacker could exploit this vulnerability by sending a crafted email message to a recipient protected by the ESA. A successful exploit could allow the attacker to bypass configured message filters and inject arbitrary scripting code inside the email body. The malicious code is not executed by default unless the recipient's email client is configured to execute scripts contained in emails.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1933</a> <a href="#">CISCO</a>
cisco -- email_security_appliance	A vulnerability in the attachment scanning of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper input validation of the email body. An attacker could exploit this vulnerability by naming a malicious attachment with a specific pattern. A successful exploit could allow the attacker to bypass configured content filters that would normally block the attachment.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1921</a> <a href="#">CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, remote attacker with administrator privileges to overwrite or read arbitrary files on the underlying operating system (OS) of an affected device. The vulnerability is due to improper input validation in NFVIS filesystem commands. An attacker could exploit this vulnerability by using crafted variables during the execution of an affected command. A successful exploit could allow the attacker to overwrite or read arbitrary files on the underlying OS.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1894</a> <a href="#">CISCO</a>
cisco -- enterprise_nfv_infrastructure_software	A vulnerability in Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system (OS) of an affected device as root. The vulnerability is due to insufficient input validation of a configuration file that is accessible to a local shell user. An attacker could exploit this vulnerability by including malicious input during the execution of this file. A successful exploit could allow the attacker to execute arbitrary commands on the underlying OS as root.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1893</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1931</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	Multiple vulnerabilities in the RSS dashboard in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1930</a> <a href="#">CISCO</a>
cisco -- ios_xr_software	A vulnerability in the implementation of Border Gateway Protocol (BGP) functionality in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to incorrect processing of certain BGP update messages. An attacker could exploit this vulnerability by sending BGP update messages that include a specific set of attributes to be processed by an affected system. A successful exploit could allow the attacker to cause the BGP process to restart unexpectedly, resulting in a DoS condition. The Cisco implementation of BGP accepts incoming BGP traffic from explicitly defined peers only. To exploit this vulnerability, the malicious BGP update message would need to come from a configured, valid BGP peer or would need to be injected by the attacker into the victim's BGP network on an existing, valid TCP connection to a BGP peer.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1909</a> <a href="#">CISCO</a>
	A vulnerability in the loading mechanism of specific dynamic link libraries in Cisco Jabber for Windows could allow an authenticated, local attacker to perform a DLL preloading attack.			

cisco -- jabber	To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of the resources loaded by the application at run time. An attacker could exploit this vulnerability by crafting a malicious DLL file and placing it in a specific location on the targeted system. The malicious DLL file would execute when the Jabber application launches. A successful exploit could allow the attacker to execute arbitrary code on the target machine with the privileges of another user's account.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1855</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_switches	A vulnerability in the fabric infrastructure VLAN connection establishment of the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, adjacent attacker to bypass security validations and connect an unauthorized server to the infrastructure VLAN. The vulnerability is due to insufficient security requirements during the Link Layer Discovery Protocol (LLDP) setup phase of the infrastructure VLAN. An attacker could exploit this vulnerability by sending a malicious LLDP packet on the adjacent subnet to the Cisco Nexus 9000 Series Switch in ACI mode. A successful exploit could allow the attacker to connect an unauthorized server to the infrastructure VLAN, which is highly privileged. With a connection to the infrastructure VLAN, the attacker can make unauthorized connections to Cisco Application Policy Infrastructure Controller (APIC) services or join other host endpoints.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1890</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the web interface of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of requests sent to the web interface. An attacker could exploit this vulnerability by sending a malicious request to the web interface of an affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a DoS condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1891</a> <a href="#">CISCO</a>
cisco -- small_business_200_and_300_and_500_series_managed_switches	A vulnerability in the Secure Sockets Layer (SSL) input packet processor of Cisco Small Business 200, 300, and 500 Series Managed Switches could allow an unauthenticated, remote attacker to cause a memory corruption on an affected device. The vulnerability is due to improper validation of HTTPS packets. An attacker could exploit this vulnerability by sending a malformed HTTPS packet to the management web interface of the affected device. A successful exploit could allow the attacker to cause an unexpected reload of the device, resulting in a denial of service (DoS) condition.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1892</a> <a href="#">CISCO</a>
cisco -- unified_communications_domain_manager	A vulnerability in the CLI of Cisco Unified Communications Domain Manager (Cisco Unified CDM) Software could allow an authenticated, local attacker to escape the restricted shell. The vulnerability is due to insufficient input validation of shell commands. An attacker could exploit this vulnerability by executing crafted commands in the shell. A successful exploit could allow the attacker to escape the restricted shell and access commands in the context of the restricted shell user, which does not have root privileges.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1911</a> <a href="#">CISCO</a>
cisco -- unified_communications_manager	A vulnerability in the Session Initiation Protocol (SIP) protocol implementation of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of input SIP traffic. An attacker could exploit this vulnerability by sending a malformed SIP packet to an affected Cisco Unified Communications Manager. A successful exploit could allow the attacker to trigger a new registration process on all connected phones, temporarily disrupting service.	2019-07-05	not yet calculated	<a href="#">CVE-2019-1887</a> <a href="#">CISCO</a>
cisco -- web_security_appliance	A vulnerability in the HTTPS decryption feature of Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Secure Sockets Layer (SSL) server certificates. An attacker could exploit this vulnerability by installing a malformed certificate in a web server and sending a request to it through the Cisco WSA. A successful exploit could allow the attacker to cause an unexpected restart of the proxy process on an affected device.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1886</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- web_security_appliance	A vulnerability in the web proxy functionality of Cisco AsyncOS Software for Cisco Web Security Appliance (WSA) could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient input validation mechanisms for certain fields in HTTP/HTTPS requests sent through an affected device. A successful attacker could exploit this vulnerability by sending a malicious HTTP/HTTPS request through an affected device. An exploit could allow the attacker to force the device to stop processing traffic, resulting in a DoS condition.	2019-07-04	not yet calculated	<a href="#">CVE-2019-1884</a> <a href="#">CISCO</a>
cloudera -- cloudera_manager	The keystore password for the Spark History Server may be exposed in unsecured files under the /var/run/cloudera-scm-agent directory managed by Cloudera Manager. The keystore file itself is not exposed.	2019-07-03	not yet calculated	<a href="#">CVE-2017-9326</a> <a href="#">CONF RM</a>
cloudera -- cloudera_manager	Secret data of processes managed by CM is not secured by file permissions.	2019-07-03	not yet calculated	<a href="#">CVE-2017-9327</a> <a href="#">CONF RM</a>
cloudera -- data_science_workbench	Remote code execution is possible in Cloudera Data Science Workbench version 1.3.0 and prior releases via unspecified	2019-07-03	not yet calculated	<a href="#">CVE-2018-11215</a>

	attack vectors.			<a href="#">CONF RM</a>
cloudera -- solr	The provided secure solrconfig.xml sample configuration does not enforce Sentry authorization on /update/json/docs.	2019-07-03	not yet calculated	<a href="#">CVE-2017-9325</a> <a href="#">CONF RM</a>
codedoc -- codedoc	Codedoc v3.2 has a stack-based buffer overflow in add_variable in codedoc.c, related to codedoc_strncpy.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13362</a> <a href="#">MISC</a>
codeigniter-restserver -- codeigniter-restserver	CodeIgniter Rest Server (aka codeigniter-restserver) 2.7.1 allows XXE attacks.	2019-07-03	not yet calculated	<a href="#">CVE-2015-3907</a> <a href="#">MISC</a>
curl -- curl	A non-privileged user or program can put code and a config file in a known non-privileged path (under C:/usr/local/) that will make curl <= 7.65.1 automatically run the code (as an openssl "engine") on invocation. If that curl is invoked by a privileged user it can do anything it wants.	2019-07-02	not yet calculated	<a href="#">CVE-2019-5443</a> <a href="#">MLIST</a> <a href="#">BID</a> <a href="#">MISC</a>
d-link -- central_wifi_manager	An issue was discovered in the D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6. Input does not get validated and arbitrary SQL statements can be executed in the database via the /web/Public/Conn.php parameter dbSQL.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13373</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- central_wifi_manager	A cross-site scripting (XSS) vulnerability in resource view in PayAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to inject arbitrary web script or HTML via the index.php/Pay/passcodeAuth passcode parameter.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13374</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- central_wifi_manager	A SQL Injection was discovered in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 in PayAction.class.php with the index.php/Pay/passcodeAuth parameter passcode. The vulnerability does not need any authentication.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13375</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- central_wifi_manager	web/Lib/Action/IndexAction.class.php in D-Link Central WiFi Manager CWM(100) before v1.03R0100_BETA6 allows remote attackers to execute arbitrary PHP code via a cookie because a cookie's username field allows eval injection, and an empty password bypasses authentication.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13372</a> <a href="#">MISC</a> <a href="#">MISC</a>
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The binary orthrus in /sbin folder of the device handles all the UPnP connections received by the device. It seems that the binary performs a sprintf operation at address 0x000A3E4 with the value in the command line parameter "-f" and stores it on the stack. Since there is no length check, this results in corrupting the registers for the function sub_A098 which results in memory corruption.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8414</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1130 and DCS-1100 devices. The binary rtspd in /sbin folder of the device handles all the rtsp connections received by the device. It seems that the binary loads at address 0x00012CF4 a flag called "Authenticate" that indicates whether a user should be authenticated or not before allowing access to the video feed. By default, the value for this flag is zero and can be set/unset using the HTTP interface and network settings tab as shown below. The device requires that a user logging to the HTTP management interface of the device to provide a valid username and password. However, the device does not enforce the same restriction by default on RTSP URL due to the checkbox unchecked by default, thereby allowing any attacker in possession of external IP address of the camera to view the live video feed. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8405</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The binary rtspd in /sbin folder of the device handles all the rtsp connections received by the device. It seems that the binary performs a memcpy operation at address 0x00011E34 with the value sent in the "Authorization: Basic" RTSP header and stores it on the stack. The number of bytes to be copied are calculated based on the length of the string sent in the RTSP header by the client. As a result, memcpy copies more data than it can hold on stack and this results in corrupting the registers for the caller function sub_F6CC which results in memory corruption. The severity of this attack is enlarged by the fact that the same value is then copied on the stack in the function 0x00011378 and this allows to overflow the buffer allocated and thus control the PC register which will result in arbitrary code execution on the device.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8410</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device has a custom binary called mp4ts under the var/www/video folder. It seems that this binary dumps the HTTP VERB in the system logs. As a part of doing that it retrieves the HTTP VERB sent by the user and uses a vulnerable sprintf function at address 0x000C3D4 in the function sub_C210 to copy the value into a string and then into a log file. Since there is no bounds check being performed on the environment variable at address 0x000C360 this results in a stack overflow and overwrites the PC register allowing an attacker to execute buffer overflow or even a command injection attack.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8412</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
	An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device runs a custom daemon on UDP port 5978 which is called "dldps2121" and listens for broadcast packets sent on 255.255.255.255. This daemon handles custom D-Link UDP based protocol that allows D-Link mobile applications and desktop applications to discover D-Link devices on the local			



d-link -- dcs-1100_and_dcs-1130_devices	<p>network. The binary processes the received UDP packets sent from any device in "main" function. One path in the function reverses towards a block of code that handles commands to be executed on the device. The custom protocol created by D-Link follows the following pattern: Packetlen, Type of packet; M=MAC address of device or broadcast; D=Device Type; C=base64 encoded command string; test=1111. If a packet is received with the packet type being "S" or 0x53 then the string passed in the "C" parameter is base64 decoded and then executed by passing into a System API. We can see at address 0x00009B44 that the string received in packet type subtracts 0x31 or "1" from the packet type and is compared against 0x22 or "double quotes". If that is the case, then the packet is sent towards the block of code that executes a command. Then the value stored in "C" parameter is extracted at address 0x0000A1B0. Finally, the string received is base 64 decoded and passed on to the system API at address 0x0000A2A8 as shown below. The same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third-party application on the device to execute commands on the device without any authentication by sending just 1 UDP packet with custom base64 encoding.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8413</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device has a custom telnet daemon as a part of the busybox and retrieves the password from the shadow file using the function getsnam at address 0x00053894. Then performs a crypt operation on the password retrieved from the user at address 0x000538E0 and performs a strcmp at address 0x00053908 to check if the password is correct or incorrect. However, the /etc/shadow file is a part of CRAM-FS filesystem which means that the user cannot change the password and hence a hardcoded hash in /etc/shadow is used to match the credentials provided by the user. This is a salted hash of the string "admin" and hence it acts as a password to the device which cannot be changed as the whole filesystem is read only.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8415</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device runs a custom daemon on UDP port 5978 which is called "dldps2121" and listens for broadcast packets sent on 255.255.255.255. This daemon handles custom D-Link UDP based protocol that allows D-Link mobile applications and desktop applications to discover D-Link devices on the local network. The binary processes the received UDP packets sent from any device in "main" function. One path in the function reverses towards a block of code that processes packets which does an unbounded copy operation which allows to overflow the buffer. The custom protocol created by D-Link follows the following pattern: Packetlen, Type of packet; M=MAC address of device or broadcast; D=Device Type; C=base64 encoded command string; test=1111. We can see at address 0x0000DBF8 handles the entire UDP packet and performs an insecure copy using strcpy function at address 0x0000DC88. This results in overflowing the stack pointer after 1060 characters and thus allows to control the PC register and results in code execution. The same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third-party application on the device to execute commands on the device without any authentication by sending just 1 UDP packet with custom base64 encoding.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8416</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1100_and_dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1100 and DCS-1130 devices. The device requires that a user logging into the device provide a username and password. However, the device allows D-Link apps on the mobile devices and desktop to communicate with the device without any authentication. As a part of that communication, the device uses custom version of base64 encoding to pass data back and forth between the apps and the device. However, the same form of communication can be initiated by any process including an attacker process on the mobile phone or the desktop and this allows a third party to retrieve the device's password without any authentication by sending just 1 UDP packet with custom base64 encoding. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8417</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1130 devices. The device requires that a user logging to the device to provide a username and password. However, the device does not enforce the same restriction on a specific URL thereby allowing any attacker in possession of that to view the live video feed. The severity of this attack is enlarged by the fact that there more than 100,000 D-Link devices out there.</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8409</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	<p>An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder or the video clippings recorded by the device. It seems that the POST parameters passed in this request (to test if email credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the function and thus result in command injection on the device. If the firmware version is dissected using binwalk tool, we obtain a cramfs-root archive which contains the filesystem set up on the device that contains all the binaries. The library "libmailutils.so" is the one that has the vulnerable function "sub_1FC4" that receives the values sent by the POST request. If we open this</p>	2019-07-02	not yet calculated	<a href="#">CVE-2017-8411</a> <a href="#">MISC</a>

	binary in IDA-pro we will notice that this follows an ARM little endian format. The function sub_1FC4 in DA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "receiver1" is extracted in function "sub_15AC" which is then passed to the vulnerable system API call. The vulnerable library function is accessed in "cgibox" binary at address 0x00023BCC which calls the "Send_mail" unction in "libmailutils so" binary as shown below which results n the vulnerable POST parameter being passed to the library which results in the command injection issue.			<a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder or the video clippings recorded by the device. It seems that the GET parameters passed in this request (to test if SMB credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the unction and thus result in command injection on the device. If he firmware version is dissected using binwalk tool, we obtain a cramfs-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "cgibox" is the one that has the vulnerable function "sub_7EAFc" that receives he values sent by the GET request. If we open this binary in IDA-pro we will notice that this follows a ARM little endian format. The function sub_7EAFc in IDA pro is identified to be receiving he values sent in the GET request and the value set in GET parameter "user" is extracted in function sub_7E49C which is hen passed to the vulnerable system API call.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8408</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of changing the administrative password for the web management interface. t seems that the device does not implement any cross-site request orgey protection mechanism which allows an attacker to trick a user who is logged in to the web management interface to change the user's password.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8407</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a crossdomain.xml file with no restrictions on who can access the webserver. This allows an hosted flash file on any domain to make calls to the device's webserver and pull any information that is stored on the device. In this case, user's credentials are stored in clear text on the device and can be pulled easily. t also seems that the device does not implement any cross-site scripting forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a cross-site flashing attack on the user's browser and execute any action on the device provided by the web management interface which steals the credentials from tools_admin.cgi file's response and displays it inside a Textfield.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8406</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dcs-1130_devices	An issue was discovered on D-Link DCS-1130 devices. The device provides a user with the capability of setting a SMB folder or the video clippings recorded by the device. It seems that the POST parameters passed in this request (to test if email credentials and hostname sent to the device work properly) result in being passed as commands to a "system" API in the unction and thus result in command injection on the device. If he firmware version is dissected using binwalk tool, we obtain a cramfs-root archive which contains the filesystem set up on the device that contains all the binaries. The library "libmailutils so" is he one that has the vulnerable function "sub_1FC4" that ceives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows an ARM little endian format. The function sub_1FC4 in DA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "receiver1" is extracted in function "sub_15AC" which is then passed to the vulnerable system API call. The vulnerable library function is accessed in "cgibox" binary at address 0x0008F598 which calls the "mailLoginTest" unction in "libmailutils so" binary as shown below which results n the vulnerable POST parameter being passed to the library which results in the command injection issue.	2019-07-02	not yet calculated	<a href="#">CVE-2017-8404</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
d-link -- dir-823g_devices	An issue was discovered on D-Link DIR-823G devices with irmware 1.02B03. There is a command injection in HNAP1 exploitable with Authentication) via shell metacharacters in the IPAddress or Gateway field to SetStaticRouteSettings.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13128</a> <a href="#">MISC</a>
diffplug -- spotless	In DiffPlug Spotless before 1.20.0 (library and Maven plugin) and before 3.20.0 (Gradle plugin), the XML parser would resolve external entities over both HTTP and HTTPS and didn't respect he resolveExternalEntities setting. For example, this allows disclosure of file contents to a MITM attacker if a victim performs a spotlessApply operation on an untrusted XML file.	2019-06-28	not yet calculated	<a href="#">CVE-2019-9843</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
digisol -- dg-hr3400_wireless_broadband_home_router	DIGISOL DG-HR3400 devices have XSS via a modified SSID when the apssid value is unchanged.	2019-07-03	not yet calculated	<a href="#">CVE-2018-12715</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
digisol -- hr-3300_wireless_wifi_home_router	Digisol Wireless Wifi Home Router HR-3300 allows XSS via the userid or password parameter to the admin login page.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14027</a> <a href="#">MISC</a>
	An issue was discovered in Django 1.11 before 1.11.22, 2.1			<a href="#">CVE-2019-12781</a>

django -- django	before 2.1.10, and 2.2 before 2.2.3. An HTTP request is not redirected to HTTPS when the SECURE_PROXY_SSL_HEADER and SECURE_SSL_REDIRECT settings are used, and the proxy connects to Django via HTTPS. In other words, django.http.HttpRequest scheme has incorrect behavior when a client uses HTTP.	2019-07-01	not yet calculated	<a href="#">MLIST</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">CONFIRM</a>
django_rest_registration -- django_rest_registration	verification.py in django-rest-registration (aka Django REST Registration library) before 0.5.0 relies on a static string for signatures (i.e., the Django Signing API is misused), which allows remote attackers to spoof the verification process. This occurs because incorrect code refactoring led to calling a security-critical function with an incorrect argument.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13177</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.2 incorrectly converts encryption key source values, resulting in lower than expected entropy. NOTE: this issue exists because of an incomplete fix for CVE-2018-15812.	2019-07-03	not yet calculated	<a href="#">CVE-2018-18326</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.2 uses a weak encryption algorithm to protect input parameters. NOTE: this issue exists because of an incomplete fix for CVE-2018-15811.	2019-07-03	not yet calculated	<a href="#">CVE-2018-18325</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.1 incorrectly converts encryption key source values, resulting in lower than expected entropy.	2019-07-03	not yet calculated	<a href="#">CVE-2018-15812</a> <a href="#">MISC</a> <a href="#">MISC</a>
dnn_software -- dnn_platform	DNN (aka DotNetNuke) 9.2 through 9.2.1 uses a weak encryption algorithm to protect input parameters.	2019-07-03	not yet calculated	<a href="#">CVE-2018-15811</a> <a href="#">MISC</a> <a href="#">MISC</a>
dosbox -- dosbox	A buffer overflow in DOSBox 0.74-2 allows attackers to execute arbitrary code.	2019-07-03	not yet calculated	<a href="#">CVE-2019-7165</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
eventum -- eventum	An issue was discovered in Eventum 3.5.0. /htdocs/switch.php has an Open Redirect via the current_page parameter.	2019-07-05	not yet calculated	eve
f5 -- big-ip	In BIG-IP 15.0.0, 14.0.0-14.1.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.2, and 11.5.2-11.6.4, BIG-IQ 6.0.0-6.1.0 and 5.1.0-5.4.0, Workflow 2.3.0, and Enterprise Manager 3.1.1, authenticated users with the ability to upload files (via scp, for example) can escalate their privileges to allow root shell access from within the TMOS Shell (tmsh) interface. The tmsh interface allows users to execute a secondary program via tools like sftp or scp.	2019-07-01	not yet calculated	<a href="#">CVE-2019-6642</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 12.1.0-12.1.4.1, undisclosed requests can cause Control REST processes to crash. The attack can only come from an authenticated user; all roles are capable of performing the attack. Unauthenticated users cannot perform this attack.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6641</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, SNMP exposes sensitive configuration objects over insecure transmission channels. This issue is exposed when a passphrase is inserted into various profile types and accessed using SNMPv2.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6640</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP (AFM, PEM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, an undisclosed TMUI pages for AFM and PEM Subscriber management are vulnerable to a stored cross-site scripting (XSS) issue. This is a control plane issue only and is not accessible from the data plane. The attack requires a malicious resource administrator to store the XSS.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6639</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, Malformed http requests made to an undisclosed iControl REST endpoint can lead to infinite loop of the restjavad process.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6638</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP (ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, Application logic abuse of ASM REST endpoints can lead to instability of BIG-IP system. Exploitation of this issue causes excessive memory consumption which results in the Linux kernel triggering OOM killer on arbitrary processes. The attack requires an authenticated user with role of "Guest" or greater privilege. Note: "No Access" cannot login so technically it's a role but a user with this access role cannot perform the attack.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6637</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP (AFM, ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, and 11.5.1-11.6.4, a stored cross-site scripting vulnerability in AFM feed list. In the worst case, an attacker can store a CSRF which results in code execution as the admin user. The level of user role which can perform this attack are resource administrator and administrator.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6636</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.1-11.5.8, when the BIG-IP system is licensed for Appliance mode, a user with either the Administrator or the Resource Administrator role can bypass Appliance mode restrictions.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6635</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, a high volume of malformed analytics report requests leads to instability in restjavad process. This causes	2019-07-03	not yet calculated	<a href="#">CVE-2019-6634</a>

	issues with both iControl REST and some portions of TMUI. The attack requires an authenticated user with any role.			<a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4, when the BIG-IP system is licensed with Appliance mode, user accounts with Administrator and Resource Administrator roles can bypass Appliance mode restrictions.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6633</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, and 12.1.0-12.1.4.1, under certain circumstances, attackers can decrypt configuration items that are encrypted because the vCMP configuration unit key is generated with insufficient randomness. The attack prerequisite is direct access to encrypted configuration and/or UCS files.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6632</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 11.5.1-11.6.4, iRules performing HTTP header manipulation may cause an interruption to service when processing traffic handled by a Virtual Server with an associated HTTP profile, in specific circumstances, when the requests do not strictly conform to RFCs.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6631</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP PEM 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, under certain conditions, the TMM process may terminate and restart while processing BIG-IP PEM traffic with the OpenVPN classifier.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6628</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP (AFM, Analytics, ASM) 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.3.4, A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI), also known as the Configuration utility.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6626</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, 14.0.0-14.0.0.4, 13.0.0-13.1.1.4, 12.1.0-12.1.4.1, and 11.5.1-11.6.4, a reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Traffic Management User Interface (TMUI) also known as the BIG-IP Configuration utility.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6625</a> <a href="#">CONF RM</a>
f5 -- big-ip	On BIG-IP 14.1.0-14.1.0.5, undisclosed SSL traffic to a virtual server configured with a Client SSL profile may cause TMM to fail and restart. The Client SSL profile must have session tickets enabled and use DHE cipher suites to be affected. This only impacts the data plane, there is no impact to the control plane.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6629</a> <a href="#">CONF RM</a>
f5 -- f5_ssl_orchestrator	On F5 SSL Orchestrator 14.1.0-14.1.0.5 and 14.0.0-14.0.0.4, undisclosed traffic flow may cause TMM to restart under certain circumstances.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6630</a> <a href="#">CONF RM</a>
f5 -- f5_ssl_orchestrator	On F5 SSL Orchestrator 14.1.0-14.1.0.5, on rare occasions, specific to a certain race condition, TMM may restart when SSL Forward Proxy enforces the bypass action for an SSL Orchestrator transparent virtual server with SNAT enabled.	2019-07-03	not yet calculated	<a href="#">CVE-2019-6627</a> <a href="#">CONF RM</a>
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x000000000001a95b1.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13245</a> <a href="#">MISC</a>
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x00000000000002d7d.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13244</a> <a href="#">MISC</a>
faststone -- faststone_image_viewer	FastStone Image Viewer 7.0 has a User Mode Write AV starting at image00400000+0x000000000001a9601.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13246</a> <a href="#">MISC</a>
ffmpeg -- ffmpeg	block_cmp() in libavcodec/zmbvenc.c in FFmpeg 4.1.3 has a heap-based buffer over-read.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13312</a> <a href="#">MISC</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349197 and 12.0-RELEASE before 12.0-RELEASE-p6, a bug in the non-default RACK TCP stack can allow an attacker to cause several linked lists to grow unbounded and cause an expensive list traversal on every packet being processed, leading to resource exhaustion and a denial of service.	2019-07-02	not yet calculated	<a href="#">CVE-2019-5599</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a> <a href="#">FREEBSD</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349622, 12.0-RELEASE before 12.0-RELEASE-p7, 11.3-PRERELEASE before r349624, 11.3-RC3 before 11.3-RC3-p1, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in iconv implementation may allow an attacker to write past the end of an output buffer. Depending on the implementation, an attacker may be able to create a denial of service, provoke incorrect program behavior, or induce a remote code execution.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5600</a> <a href="#">MISC</a> <a href="#">FREEBSD</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r349628, 12.0-RELEASE before 12.0-RELEASE-p7, 11.3-PRERELEASE before r349629, 11.3-RC3 before 11.3-RC3-p1, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in the cdrom driver allows users with read access to the cdrom device to arbitrarily overwrite kernel memory when media is present thereby allowing a malicious user in the operator group to gain root privileges.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5602</a> <a href="#">MISC</a> <a href="#">FREEBSD</a>
freebsd -- freebsd	In FreeBSD 12.0-STABLE before r347474, 12.0-RELEASE before 12.0-RELEASE-p7, 11.2-STABLE before r347475, and 11.2-RELEASE before 11.2-RELEASE-p11, a bug in the FFS implementation causes up to three bytes of kernel stack memory to be written to disk as uninitialized directory entry padding.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5601</a> <a href="#">MISC</a> <a href="#">FREEBSD</a>
				<a href="#">CVE-2019-</a>

glpi_project -- glpi	nc/user.class.php in GLPI before 9.4.3 allows XSS via a user picture.	2019-07-04	not yet calculated	<a href="#">13239</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- libxslt	In numbers.c in libxslt 1.1.33, a type holding grouping characters of an xsl:number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.	2019-06-30	not yet calculated	<a href="#">CVE-2019-13118</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- libxslt	In numbers.c in libxslt 1.1.33, an xsl number with certain format strings could lead to a uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, l, i, or 0, or any other character.	2019-06-30	not yet calculated	<a href="#">CVE-2019-13117</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
grouptime -- teamwire_desktop_client	Grouptime Teamwire Desktop Client 1.5.1 prior to 1.9.0 on Windows allows code injection via a template, leading to remote code execution. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	<a href="#">CVE-2018-17170</a> <a href="#">MISC</a>
grouptime -- teamwire_desktop_client	The admin interface of the Grouptime Teamwire Client 1.5.1 prior to 1.9.0 on-premises messenger server allows stored XSS. All backend versions prior to prod-2018-11-13-15-00-42 are affected.	2019-06-28	not yet calculated	<a href="#">CVE-2018-17560</a> <a href="#">MISC</a>
hawt -- hawtio	Hawt Hawtio through 2.5.0 is vulnerable to SSRF, allowing a remote attacker to trigger an HTTP request from an affected server to an arbitrary host via the initial /proxy/ substring of a URI.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9827</a> <a href="#">MISC</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 could allow an authenticated user to execute a function that would cause the server to crash. IBM X-Force ID: 162714.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4386</a> <a href="#">BID</a> <a href="#">X-F</a> <a href="#">CONFIRM</a>
ibm -- infosphere_information_server	A Cross-Frame Scripting vulnerability in IBM InfoSphere Information Server 11.3, 11.5, and 11.7 can allow an attacker to load the vulnerable application inside an HTML iframe tag on a malicious page. IBM X-Force ID: 159419.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4237</a> <a href="#">X-F</a> <a href="#">CONFIRM</a>
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow an attacker to obtain sensitive information due to missing authentication in Ignite nodes. IBM X-Force ID: 161412.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4337</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 161411.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4336</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow a local user to obtain highly sensitive information from log files when debugging is enabled. IBM X-Force ID: 160765.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4299</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 uses a high privileged PostgreSQL account for database access which could allow a local user to perform actions they should not have privileges to execute. IBM X-Force ID: 160764.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4298</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow a remote authenticated attacker to conduct an LDAP injection. By using a specially crafted request, an attacker could exploit this vulnerability to make unauthorized queries or modify the LDAP content. IBM X-Force ID: 160761.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4297</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 information disclosure could allow a local user to obtain e-mail contents from the client debug log file. IBM X-Force ID: 160759.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4296</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 could allow an attacker with specialized access to obtain highly sensitive from the credential vault. IBM X-Force ID: 160758.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4295</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- spectrum_protect_plus	When using IBM Spectrum Protect Plus 10.1.0, 10.1.2, and 10.1.3 to protect Oracle or MongoDB databases, a redirected restore operation may result in an escalation of user privileges. IBM X-Force ID: 162165.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4383</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">X-F</a>
ibm -- spectrum_protect_plus	When using IBM Spectrum Protect Plus 10.1.0, 10.1.2, and 10.1.3 to protect Oracle, DB2 or MongoDB databases, a redirected restore operation specifying a target path may allow execution of arbitrary code on the system. IBM X-Force ID: 161667.	2019-07-01	not yet calculated	<a href="#">CVE-2019-4357</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">X-F</a>
ibm -- spectrum_protect_servers	IBM Spectrum Protect Operations Center 7.1 and 8.1 could allow a remote attacker to obtain sensitive information, caused by an error message containing a stack trace. By creating an error with a stack trace, an attacker could exploit this vulnerability to potentially obtain details on the Operations Center architecture. IBM X-Force ID: 158279.	2019-07-02	not yet calculated	<a href="#">CVE-2019-4129</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>
ibm -- spectrum_protect_servers_and_storage_agents	IBM Spectrum Protect Servers 7.1 and 8.1 and Storage Agents are vulnerable to a stack-based buffer overflow, caused by improper bounds checking by servers and storage agents in response to specifically crafted communication exchanges. By sending an overly long request, a remote attacker could overflow a buffer and execute arbitrary code on the system with instance d privileges or cause the server or storage agent to crash. IBM X-Force ID: 157510.	2019-07-02	not yet calculated	<a href="#">CVE-2019-4087</a> <a href="#">CONFIRM</a> <a href="#">X-F</a>



ibm -- spectrum_protect_servers_and_storage_agents	IBM Spectrum Protect Servers 7.1 and 8.1 and Storage Agents could allow a local attacker to gain elevated privileges on the system, caused by loading a specially crafted library loaded by the dsmsan module. By setting up such a library, a local attacker could exploit this vulnerability to gain root privileges on the vulnerable system. BM X-Force ID: 157511.	2019-07-02	not yet calculated	<a href="#">CVE-2019-4088</a> <a href="#">CONF RM</a> <a href="#">XF</a>
ignited_cms -- ignited_cms	index.php/admin/permissions in Ignited CMS through 2017-02-19 allows CSRF to add an administrator.	2019-07-06	not yet calculated	<a href="#">CVE-2019-13370</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/fourier.c in ComplexImages.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13302</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of off-by-one errors.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13306</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of a wand/mogrify.c error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13311</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling rows.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13307</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced strncpy and an off-by-one error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13305</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced assignment.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13304</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read in MagickCore/composite.c in CompositeImage.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13303</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks in AcquireMagickMemory because of an AnnotateImage error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13301</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling columns.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13300</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/pixel-accessor.h in GetPixelChannel.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13299</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/pixel-accessor.h in SetPixelViaPixelInfo because of a MagickCore/enhance.c error.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13298</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a height of zero is mishandled.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13297</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has direct memory leaks in AcquireMagickMemory because of an error in CLIListOperatorImages in MagickWand/operation.c for a NULL value.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13296</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a width of zero is mishandled.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13295</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow in MagickCore/fourier.c in ComplexImage.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13308</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of mishandling the NoSuchImage error in CLIListOperatorImages in MagickWand/operation.c.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13309</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
imagemagick -- imagemagick	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of an error in	2019-07-04	not yet calculated	<a href="#">CVE-2019-13310</a> <a href="#">MISC</a>

	MagickWand/mogrify.c.			MISC <a href="#">MISC</a>
invoxia -- nvx220_devices	Invoxia NVX220 devices allow access to /bin/sh via escape from a restricted CLI, leading to disclosure of password hashes.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14529</a> <a href="#">MISC</a>
invoxia -- nvx220_devices	Invoxia NVX220 devices allow TELNET access as admin with a default password.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14528</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.52 has a User Mode Write AV starting at mage00400000+0x0000000000249c6.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13243</a> <a href="#">MISC</a>
irfanview -- irfanview	IrfanView 4.52 has a User Mode Write AV starting at mage00400000+0x000000000013a98.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13242</a> <a href="#">MISC</a>
jack_audio -- jack2	posix/JackSocket.cpp in libjack in JACK2 1.9.1 through 1.9.12 as distributed with alsa-plugins 1.1.7 and later) has a "double file descriptor close" issue during a failed connection attempt when ackd2 is not running. Exploitation success depends on multithreaded timing of that double close, which can result in unintended information disclosure, crashes, or file corruption due o having the wrong file associated with the file descriptor.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13351</a> <a href="#">MISC</a> <a href="#">MISC</a>
jetbrains -- hub	In JetBrains Hub versions earlier than 2018.4.11298, the audit events for SMTPSettings show a cleartext password to the admin user. It is only relevant in cases where a password has not changed since 2017, and if the audit log still contains events rom before that period.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12847</a> <a href="#">CONF RM</a>
jetbrains -- intelliJ_idea	In several JetBrains IntelliJ IDEA versions, creating remote run configurations of JavaEE application servers leads to saving a cleartext record of the server credentials in the DE configuration files. The issue has been fixed in the following versions: 2018.3.5, 2018.2.8, 2018.1.8.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9823</a> <a href="#">CONF RM</a>
jetbrains -- intelliJ_idea	In several JetBrains IntelliJ IDEA versions, a Spring Boot run configuration with the default setting allowed remote attackers to execute code when the configuration is running, because a JMX server listens on all interfaces (instead of listening on only the ocalhost interface). This issue has been fixed in the following versions: 2019.1, 2018.3.4, 2018.2.8, 2018.1.8, and 2017.3.7.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9186</a> <a href="#">CONF RM</a>
jetbrains -- intelliJ_idea	In several JetBrains IntelliJ IDEA Ultimate versions, an Application Server run configuration (for Tomcat, Jetty, Resin, or CloudBees) with the default setting allowed a remote attacker to execute code when the configuration is running, because a JMX server listened on all interfaces instead of localhost only. The issue has been fixed in the following versions: 2018.3.4, 2018.2.8, 2018.1.8, and 2017.3.7.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10104</a> <a href="#">CONF RM</a>
jetbrains -- intelliJ_idea	JetBrains IntelliJ IDEA projects created using the Kotlin (JS Client/JVM Server) DE Template were resolving Gradle artifacts using an http connection, potentially allowing an MITM attack. This issue, which was fixed in Kotlin plugin version 1.3.30, is similar to CVE-2019-10101.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10103</a> <a href="#">CONF RM</a>
jetbrains -- intelliJ_idea_ultimate	In several versions of JetBrains IntelliJ DEA Ultimate, creating un configurations for cloud application servers leads to saving a cleartext unencrypted record of the server credentials in the IDE configuration files. If the Settings Repository plugin was then used and configured to synchronize IDE settings using a public epository, these credentials were published to this repository. The issue has been fixed in the following versions: 2019.1, 2018.3.5, 2018.2.8, and 2018.1.8.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9872</a> <a href="#">CONF RM</a>
jetbrains -- intelliJ_idea_ultimate	In several versions of JetBrains IntelliJ DEA Ultimate, creating Task Servers configurations leads to saving a cleartext unencrypted record of the server credentials in the IDE configuration files. The issue has been fixed in the following versions: 2019.1, 2018.3.5, 2018.2.8, and 2018.1.8.	2019-07-03	not yet calculated	<a href="#">CVE-2019-9873</a> <a href="#">CONF RM</a>
jetbrains -- kotlin	JetBrains Ktor framework (created using the Kotlin IDE template) versions before 1.1.0 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack. This issue was fixed in Kotlin plugin version 1.3.30.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10102</a> <a href="#">MISC</a>
jetbrains -- kotlin	JetBrains Kotlin versions before 1.3.30 were resolving artifacts using an http connection during the build process, potentially allowing an MITM attack.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10101</a> <a href="#">CONF RM</a>
jetbrains -- teamcity	A possible stored JavaScript injection requiring a deliberate server administrator action was detected. The issue was fixed in JetBrains TeamCity 2018.2.3.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12843</a> <a href="#">CONF RM</a>
jetbrains -- teamcity	Incorrect handling of user input in Z P extraction was detected in JetBrains TeamCity. The issue was fixed in TeamCity 2018.2.2.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12841</a> <a href="#">CONF RM</a>
jetbrains -- teamcity	A possible stored JavaScript injection was detected on one of the JetBrains TeamCity pages. The issue was fixed in TeamCity 2018.2.3.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12844</a> <a href="#">MISC</a>
jetbrains -- youtrack	A query injection was possible in JetBrains YouTrack. The issue was fixed in YouTrack 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12850</a> <a href="#">CONF RM</a>
jetbrains -- youtrack	Certain actions could cause privilege escalation for issue attachments in JetBrains YouTrack. The issue was fixed in 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12867</a> <a href="#">CONF RM</a>
jetbrains -- youtrack	In JetBrains YouTrack Confluence plugin versions before 1.8.1.3, it was possible to achieve Server Side Template Injection. The attacker could add an Issue macro to the page in Confluence,	2019-07-03	not yet calculated	<a href="#">CVE-2019-10100</a>

	and use a combination of a valid id field and specially crafted code in the link-text-template field to execute code remotely.			MISC
jetbrains -- youtrack	A CSRF vulnerability was detected in one of the admin endpoints of JetBrains YouTrack. The issue was fixed in YouTrack 2018.4.49852.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12851</a> <a href="#">CONFIRM</a>
jetbrains -- youtrack	An SSRF attack was possible on a JetBrains YouTrack server. The issue (1 of 2) was fixed in JetBrains YouTrack 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12852</a> <a href="#">CONFIRM</a>
jetbrains -- youtrack	An Insecure Direct Object Reference, with Authorization Bypass through a User-Controlled Key, was possible in JetBrains YouTrack. The issue was fixed in 2018.4.49168.	2019-07-03	not yet calculated	<a href="#">CVE-2019-12866</a> <a href="#">CONFIRM</a>
jgraph -- mxgraph	An issue was discovered in mxGraph through 4.0.0, related to the "draw.io Diagrams" plugin before 8.3.14 for Confluence and other products. Improper input validation/sanitization of a color field leads to XSS. This is associated with <code>avascript/examples/grapheditor/www/js/Dialogs.js</code> .	2019-07-01	not yet calculated	<a href="#">CVE-2019-13127</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
libosinfo -- libosinfo	libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to <code>osinfo-install-script</code> via the command line.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13313</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In <code>arch/x86/lib/insn-eval.c</code> in the Linux kernel before 5.1.9, there is a use-after-free for access to an LDT entry because of a race condition between <code>modify_ldt()</code> and a <code>#BR</code> exception for an MPX bounds violation.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13233</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	In the Linux kernel before 5.1.7, a device can be tracked by an attacker using the PID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). An attack may be conducted by hosting a crafted web page that uses WebRTC or gQUIC to force UDP traffic to attacker-controlled IP addresses.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10638</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	The Linux kernel 4.x (starting from 4.1) and 5.x before 5.0.8 allows Information Exposure (partial kernel address disclosure), leading to a KASLR bypass. Specifically, it is possible to extract the KASLR kernel image offset using the PID values the kernel produces for connection-less protocols (e.g., UDP and ICMP). When such traffic is sent to multiple destination IP addresses, it is possible to obtain hash collisions (of indices to the counter array) and thereby obtain the hashing key (via enumeration). This key contains enough bits from a kernel address (of a static variable) so when the key is extracted (via enumeration), the offset of the kernel image is exposed. This attack can be carried out remotely, by the attacker forcing the target device to send UDP or ICMP (or certain other) traffic to attacker-controlled IP addresses. Forcing a server to send UDP traffic is trivial if the server is a DNS server. ICMP traffic is trivial if the server answers ICMP Echo requests (ping). For client targets, if the target visits the attacker's web page, then WebRTC or gQUIC can be used to force UDP traffic to attacker-controlled IP addresses. NOTE: this attack against KASLR became viable in 4.1 because PID generation was changed to have a dependency on an address associated with a network namespace.	2019-07-05	not yet calculated	<a href="#">CVE-2019-10639</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
logitech -- r500_presentation_clicker	The Logitech R500 presentation clicker allows attackers to determine the AES key, leading to keystroke injection. On Windows, any text may be injected by using ALT+NUMPAD input to bypass the restriction on the characters A through Z.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13054</a> <a href="#">MISC</a>
logitech -- unifying_devices	Certain Logitech Unifying devices allow attackers to dump AES keys and addresses, leading to the capability of live decryption of Radio Frequency transmissions, as demonstrated by an attack against a Logitech K360 keyboard.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13055</a> <a href="#">MISC</a>
logitech -- unifying_devices	Logitech Unifying devices before 2016-02-26 allow keystroke injection, bypassing encryption, aka MouseJack.	2019-06-29	not yet calculated	<a href="#">CVE-2016-10761</a> <a href="#">MISC</a> <a href="#">MISC</a>
logitech -- unifying_devices	Logitech Unifying devices allow live decryption if the pairing of a keyboard to a receiver is sniffed.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13052</a> <a href="#">MISC</a>
logitech -- unifying_devices	Logitech Unifying devices allow keystroke injection, bypassing encryption. The attacker must press a "magic" key combination while sniffing cryptographic data from a Radio Frequency transmission. NOTE: this issue exists because of an incomplete fix for CVE-2016-10761.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13053</a> <a href="#">MISC</a>
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Arbitrary file deletion.	2019-06-28	not yet calculated	<a href="#">CVE-2018-14916</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">FULLDISC</a>
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow XSS.	2019-06-28	not yet calculated	<a href="#">CVE-2018-14919</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>

				<a href="#">FULLDISC MISC</a>
loytec -- lgate-902_devices	LOYTEC LGATE-902 6.3.2 devices allow Directory Traversal.	2019-06-28	not yet calculated	<a href="#">CVE-2018-14918 MISC FULLDISC</a>
macafee -- epolicy_orchestrator	Information Disclosure vulnerability in the Agent Handler in McAfee ePolicy Orchestrator (ePO) 5.9.x and 5.10.0 prior to 5.10.0 update 4 allows remote unauthenticated attacker to view sensitive information in plain text via sniffing the traffic between the Agent Handler and the SQL server.	2019-07-03	not yet calculated	<a href="#">CVE-2019-3619 CONF RM</a>
maxx -- waves_maxx_audio	WavesSysSvc in Waves MAXX Audio allows privilege escalation because the General registry key has Full Control access for the Users group, leading to DLL side loading. This affects WavesSysSvc64 exe 1.9.29.0.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13208 MISC</a>
medtronic -- minimed_508_and_paradigm_series_insulin_pumps	In Medtronic MinMed 508 and Medtronic Minimed Paradigm Insulin Pumps, Versions, MiniMed 508 pump ? All versions, MiniMed Paradigm 511 pump ? All versions, MiniMed Paradigm 512/712 pumps ? All versions, MiniMed Paradigm 712E pump? All versions, MiniMed Paradigm 515/715 pumps?All versions, MiniMed Paradigm 522/722 pumps ? All versions,MiniMed Paradigm 522K/722K pumps ? All versions, MiniMed Paradigm 523/723 pumps ? Software versions 2.4A or lower, MiniMed Paradigm 523K/723K pumps ? Software, versions 2.4A or lower, MiniMed Paradigm Veo 554/754 pumps ? Software versions 2.6A or lower, MiniMed Paradigm Veo 554CM and 754CM models only ? Software versions 2.7A or lower, the affected nsulin pumps are designed to communicate using a wireless RF with other devices, such as blood glucose meters, glucose sensor transmitters, and CareLink USB devices. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with adjacent access o one of the affected insulin pump models can inject, replay, modify, and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.	2019-06-28	not yet calculated	<a href="#">CVE-2019-10964 BID MISC</a>
mikrotik -- multiple_routers	A vulnerability in the FTP daemon on MikroTik routers through 6.44.3 could allow remote attackers to exhaust all available memory, causing the device to reboot because of uncontrolled esource management.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13074 MISC</a>
minicms -- minicms	In MiniCMS V1.10, stored XSS was found in mc-admin/post-edit.php via the tags box. An attacker can use it to get a user's cookie. This is different from CVE-2018-10296, CVE-2018-16233, and CVE-2018-20520.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13186 MISC</a>
ministry_of_interior_of_the_slovak_republic -- eid_client	An incorrect implementation of a local web server in eID client Windows version before 3.1.2, Linux version before 3.0.3) allows remote attackers to execute arbitrary code (.cgi, .pl, or .php) or delete arbitrary files via a crafted HTML page. This is a product from the Ministry of Interior of the Slovak Republic.	2019-06-28	not yet calculated	<a href="#">CVE-2019-13028 MISC MISC MISC</a>
motorola -- cx2l_mwr04L_router	On the Motorola router CX2L MWR04L 1 01, there is a stack consumption (infinite recursion) issue in scodp via TCP port 8010 and UDP port 8080. It is caused by sprintf and inappropriate ength handling.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13129 MISC</a>
moxa -- oncell_g3100-hspa_series_devices	There is Memory corruption in the web interface Moxa OnCell G3100-HSPA Series version 1.6 Build 17100315 and prior, different vulnerability than CVE-2018-11420.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11423 MISC</a>
moxa -- oncell_g3100-hspa_series_devices	Moxa OnCell G3100-HSPA Series version 1 6 Build 17100315 and prior use a proprietary monitoring protocol that does not provide confidentiality, integrity, and authenticity security controls. All information is sent in plain text, and can be intercepted and modified. The protocol is vulnerable to remote unauthenticated disclosure of sensitive information, including the administrator's password. Under certain conditions, it's also possible to retrieve additional information, such as content of HTTP requests to the device, or the previously used password, due to memory leakages.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11421 MISC</a>
moxa -- oncell_g3100-hspa_series_devices	A weak Cookie parameter is used in the web application of Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior. An attacker can brute force parameters required to bypass authentication and access the web interface to use all its unctions except for password change.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11426 MISC</a>
moxa -- oncell_g3100-hspa_series_devices	CSRF tokens are not used in the web application of Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior, which makes it possible to perform CSRF attacks on the device administrator.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11427 MISC</a>
moxa -- oncell_g3100-hspa_series_devices	There is Memory corruption in the web interface of Moxa OnCell G3100-HSPA Series version 1.5 Build 17042015 and prior, a different vulnerability than CVE-2018-11423.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11420 MISC</a>
moxa -- oncell_g3100-hspa_series_devices	Moxa OnCell G3100-HSPA Series version 1 6 Build 17100315 and prior use a proprietary configuration protocol that does not provide confidentiality, integrity, and authenticity security controls. All information is sent in plain text, and can be intercepted and modified. Any commands (including device reboot, configuration download or upload, or firmware upgrade) are accepted and executed by the device without authentication.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11422 MISC</a>
moxa -- oncell_g3470a-lte_series_devices	There is Memory corruption in the web interface of Moxa OnCell G3470A-LTE Series version 1.6 Build 18021314 and prior, a different vulnerability than CVE-2018-11425.	2019-07-03	not yet calculated	<a href="#">CVE-2018-11424 MISC</a>
	Memory corruption issue was discovered in Moxa OnCell	2019-07-	not yet	<a href="#">CVE-2018-</a>

moxa -- oncell_g3470a-lte_series_devices	G3470A-LTE Series version 1.6 Build 18021314 and prior, a different vulnerability than CVE-2018-11424.	03	calculated	<a href="#">11425 MISC</a>
nlnet_labs -- nsd	nsd-checkzone in NlNet Labs NSD 4.2.0 has a Stack-based Buffer Overflow in the dname_concatenate() function in dname.c.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13207 MISC</a>
nortek_security_and_control -- linear_emerge_50p/5000p_devices	Linear eMerge 50P/5000P devices allow Cookie Path Traversal.	2019-07-02	not yet calculated	<a href="#">CVE-2019-7267 MISC MISC</a>
nortek_security_and_control -- linear_emerge_50p/5000p_devices	Linear eMerge 50P/5000P devices allow Unauthenticated File Upload.	2019-07-02	not yet calculated	<a href="#">CVE-2019-7268 MISC MISC</a>
npm -- fstream	stream before 1.0.12 is vulnerable to Arbitrary File Overwrite. Extracting tarballs containing a hardlink to a file that already exists in the system, and a file that matches the hardlink, will overwrite the system's file with the contents of the extracted file. The fstream.DirWriter() function is vulnerable.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13173 MISC MISC</a>
odoo -- community_and_enterprise	Incorrect access control in the TransientModel framework in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated attackers to access data in transient records that they do not own by making an RPC call before garbage collection occurs.	2019-07-03	not yet calculated	<a href="#">CVE-2018-14866 CONF RM</a>
odoo -- community_and_enterprise	Improper sanitization of dynamic user expressions in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated privileged users to escape from the dynamic expression sandbox and execute arbitrary code on the hosting system.	2019-07-03	not yet calculated	<a href="#">CVE-2018-14860 CONF RM</a>
odoo -- community_and_enterprise	Incorrect access control in the password reset component in Odoo Community 11.0 and earlier and Odoo Enterprise 11.0 and earlier allows authenticated users to reset the password of other users by being the first party to use the secure token.	2019-07-03	not yet calculated	<a href="#">CVE-2018-14859 CONF RM</a>
odoo_community_association -- dbfilter_from_header module	The Odoo Community Association (OCA) dbfilter_from_header module makes Odoo 8.x, 9.x, 10.x, and 11.x vulnerable to ReDoS (regular expression denial of service) under certain circumstances.	2019-07-05	not yet calculated	<a href="#">CVE-2018-14733 CONF RM MISC MISC MISC</a>
opencats -- opencats	ib/DocumentToText.php in OpenCats before 0.9.4-3 has XXE that allows remote users to read files on the underlying operating system. The attacker must upload a file in the docx or odt format.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13358 MISC MISC MISC</a>
panduit -- intravue	An insecure login process was discovered in Panduit IntraVUE before 3.2.0.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13044 MISC</a>
qemu -- qemu	qemu-bridge-helper.c in QEMU 4.0.0 does not ensure that a network interface name (obtained from bridge.conf or a --br=bridge option) is limited to the IFNAMSIZ size, which can lead to an ACL bypass.	2019-07-03	not yet calculated	<a href="#">CVE-2019-13164 MLIST MISC</a>
read_the_docs -- read_the_docs	Read the Docs before 3.5.1 has an Open Redirect if certain user-defined redirects are used. This affects private instances of Read the Docs (in addition to the public readthedocs.org web sites).	2019-07-02	not yet calculated	<a href="#">CVE-2019-13175 MISC</a>
riello -- netman_204	An issue was discovered in Riello NetMan 204 14-2 and 15-2. The issue is with the login script and wrongpass Python script used for authentication. When calling wrongpass, the variables \$VAL0 and \$VAL1 should be enclosed in quotes to prevent the potential for Bash command injection. Further to this, VAL0 and VAL1 should be sanitised to ensure they do not contain malicious characters. Passing it the username of ' ' will cause it to time out and log the user in because of poor error handling. This will log the attacker in as an administrator where the telnet / ssh services can be enabled, and the credentials for local users can be reset. Also, login.cgi accepts the username as a GET parameter, so login can be achieved by browsing to the /cgi-bin/login.cgi?username=%20a URI.	2019-07-03	not yet calculated	<a href="#">CVE-2017-6900 MISC MISC</a>
sdl2_image -- sdl2_image	An exploitable heap-based buffer overflow vulnerability exists when loading a PCX file in SDL2_image, version 2.0.4. A missing error handler can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5051 MISC</a>
sdl2_image -- sdl2_image	An exploitable integer overflow vulnerability exists when loading a PCX file in SDL2_image 2.0.4. A specially crafted file can cause an integer overflow, resulting in too little memory being allocated, which can lead to a buffer overflow and potential code execution. An attacker can provide a specially crafted image file to trigger this vulnerability.	2019-07-03	not yet calculated	<a href="#">CVE-2019-5052 MISC</a>
sick -- msc800_devices	SICK MSC800 all versions prior to Version 4.0, the affected firmware versions contain a hard-coded customer account password.	2019-07-01	not yet calculated	<a href="#">CVE-2019-10979 BID MISC</a>
sigil-ebook -- flightcrew	FlightCrew v0.9.2 and older are vulnerable to a directory traversal, allowing attackers to write arbitrary files via a . / (dot slash) in a ZIP archive entry that is mishandled during extraction.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13241 MISC</a>
sitebridge -- joruri_cms	Cross-site scripting vulnerability in Joruri CMS 2017 Release2	2019-07-	not yet	<a href="#">CVE-2019-5967</a>



	and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	05	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
sitebridge -- joruri_mail	Open redirect vulnerability in Joruri Mail 2.1.4 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5965</a> <a href="#">MISC</a> <a href="#">MISC</a>
sitebridge -- joruri_mail	Joruri Mail 2.1.4 and earlier does not properly manage sessions, which allows remote attackers to impersonate an arbitrary user and alter/discard the information via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5966</a> <a href="#">MISC</a> <a href="#">MISC</a>
sks_keyserver_network -- sks-keyserver_code_and_gnupg	Interaction between the sks-keyserver code through 1.2.0 of the SKS keyserver network, and GnuPG through 2.2.16, makes it risky to have a GnuPG keyserver configuration line referring to a host on the SKS keyserver network. Retrieving data from this network may cause a persistent denial of service, because of a Certificate Spamming Attack.	2019-06-29	not yet calculated	<a href="#">CVE-2019-13050</a> <a href="#">MISC</a>
sony -- vaio_update	Improper download file verification vulnerability in VAIO Update 7.3.0.03150 and earlier allows remote attackers to conduct a man-in-the-middle attack via a malicious wireless LAN access point. A successful exploitation may result in a malicious file being downloaded/executed.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5982</a> <a href="#">MISC</a> <a href="#">MISC</a>
sony -- vaio_update	Improper authorization vulnerability in VAIO Update 7.3.0.03150 and earlier allows an attacker to execute arbitrary executable file with administrative privilege via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5981</a> <a href="#">MISC</a> <a href="#">MISC</a>
squid-cache -- squid	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13345</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
stormshield -- stormshield_network_security	Stormshield Network Security 2.0.0 through 2.13.0 and 3.0.0 through 3.7.1 has self-XSS in the command line interface of the SNS web server.	2019-07-04	not yet calculated	<a href="#">CVE-2018-20850</a> <a href="#">MISC</a>
supermicro -- superdoctor_5	Super Micro SuperDoctor 5, when restrictions are not implemented in agent.cfg, allows remote attackers to execute arbitrary commands via NRPE.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13131</a> <a href="#">MISC</a>
swift -- alliance_web_platform	An issue was discovered in SWIFT Alliance Web Platform 7.1.23. A log injection (and an arbitrary log filename) can be achieved via the PATH_INFO to swp/login/EJBRemoteService/, related to com.swift.ejbgtw.j2ee.client.EJBInvocationException error log information containing null@java:comp/env/ error messages.	2019-07-05	not yet calculated	<a href="#">CVE-2018-16386</a> <a href="#">MISC</a>
tencent -- habo	HaboMailHunter through 2.0.0.3 in Tencent Habo allows attackers to evade dynamic malware analysis via PIE compilation.	2019-07-01	not yet calculated	<a href="#">CVE-2019-13125</a> <a href="#">MISC</a>
tor_project -- tor_browser	Tor Browser through 8.5.3 has an information exposure vulnerability. It allows remote attackers to detect the browser's language via vectors involving an <FRAME> element, because text in that language is included in the title attribute of a <LINK> element or a non-HTML page. This is related to a behavior of Firefox before 68.	2019-06-30	not yet calculated	<a href="#">CVE-2019-13075</a> <a href="#">MISC</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the Private Port in Add Virtual Server.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13153</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the IP Address in Add Gaming Rule.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13152</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the UDP Ports To Open in Add Gaming Rule.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13148</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the key passwd in Routing RIP Settings.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13149</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the IP Address in Add Virtual Server.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13155</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication). The command injection exists in the key ip_addr.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13150</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the action set_sta_enrollee_pin_5g and the key wps_sta_enrollee_pin.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13151</a> <a href="#">MISC</a>
trendnet -- tew-827dru	An issue was discovered in TRENDnet TEW-827DRU firmware before 2.05B11. There is a command injection in apply.cgi (exploitable with authentication) via the TCP Ports To Open in Add Gaming Rule.	2019-07-02	not yet calculated	<a href="#">CVE-2019-13154</a> <a href="#">MISC</a>
tsukurito -- tootdon_for_mastodon	The Android App 'Tootdon for Mastodon' version 3.4.1 and earlier does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain	2019-07-05	not yet calculated	<a href="#">CVE-2019-5961</a> <a href="#">MISC</a>

	sensitive information via a crafted certificate.			MISC
unzip -- unzip	Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a "better zip bomb" issue.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13232</a> MISC MLIST MISC
virt-manager -- virt-bootstrap	virt-bootstrap 1.1.0 allows local users to discover a root password by listing a process, because this password may be present in the --root-password option to virt_bootstrap.py.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13314</a> MISC MISC
virt-manager -- virt-manager	Virt-install(1) utility used to provision new virtual machines has introduced an option '--unattended' to create VMs without user interaction. This option accepts guest VM password as command line arguments, thus leaking them to other users on the system via process listing. It was introduced recently in the virt-manager v2.2.0 release.	2019-07-03	not yet calculated	<a href="#">CVE-2019-10183</a> BID CONFIRM
weberp -- weberp	A SQL Injection issue was discovered in webERP 4.15. Payments.php accepts payment data in base64 format. After this is decoded, it is deserialized. Then, this deserialized data goes directly into a SQL query, with no sanitizing checks.	2019-07-04	not yet calculated	<a href="#">CVE-2019-13292</a> MISC
weseeek -- growi	Cross-site request forgery (CSRF) vulnerability in GROWI v3.4.6 and earlier allows remote attackers to hijack the authentication of administrators via updating user's 'Basic Info'.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5968</a> MISC MISC
weseeek -- growi	Open redirect vulnerability in GROWI v3.4.6 and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the process of login.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5969</a> MISC MISC
wolfvision -- cynap	WolfVision Cynap before 1.30j uses a static, hard-coded cryptographic secret for generating support PINs for the 'forgot password' feature. By knowing this static secret and the corresponding algorithm for calculating support PINs, an attacker can reset the ADMIN password and thus gain remote access.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13352</a> MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5971</a> MISC MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5962</a> MISC MISC
wordpress -- wordpress	A Cross-Site-Request-Forgery (CSRF) vulnerability in widget_logic.php in the 2by2host Widget Logic plugin before 5.10.2 for WordPress allows remote attackers to execute PHP code via snippets (that are attached to widgets and then eval'd to dynamically determine their visibility) by crafting a malicious POST request that tricks administrators into adding the code.	2019-07-01	not yet calculated	<a href="#">CVE-2019-12826</a> MISC CONFIRM
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Personalized WooCommerce Cart Page 2.4 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5979</a> MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Attendance Manager 0.5.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5970</a> MISC MISC MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Contest Gallery versions prior to 10.4.5 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5974</a> MISC MISC
wordpress -- wordpress	An authentication bypass vulnerability in the CRUDLab WP Like Button plugin through 1.6.0 for WordPress allows unauthenticated attackers to change settings. The contains() function in wp_like_button.php did not check if the current request is made by an authorized user, thus allowing any unauthenticated user to successfully update settings, as demonstrated by the wp-admin/admin.php?page=facebook-like-button&each_page_url or code_snippet parameter.	2019-07-05	not yet calculated	<a href="#">CVE-2019-13344</a> MISC MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in WP Open Graph 1.6.1 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5960</a> JVN
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Zoho SalesIQ 1.0.8 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5963</a> MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5972</a> MISC MISC MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Related YouTube Videos versions prior to 1.9.9 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	<a href="#">CVE-2019-5980</a> MISC MISC
wordpress -- wordpress	An issue was discovered in the VeronaLabs wp-statistics plugin before 12.6.7 for WordPress. The v1/hit endpoint of the API,	2019-07-	not yet	<a href="#">CVE-2019-13275</a>

	when the non-default "use cache plugin" setting is enabled, is vulnerable to unauthenticated blind SQL Injection.	04	calculated	MISC MISC MISC
wordpress -- wordpress	Cross-site request forgery (CSRF) vulnerability in Online Lesson Booking 0.8.6 and earlier allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2019-07-05	not yet calculated	CVE-2019-5973 MISC MISC MISC
wuhan_deepin_technology -- deepin-clone	In GUI mode, deepin-clone before 1.1.3 creates a log file at the fixed path /tmp/deepin-clone.log as root, and follows symlinks here. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled.	2019-07-04	not yet calculated	CVE-2019-13227 MLIST MISC MISC
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a fixed path /tmp/partclone.log in the Helper::getPartitionSizeInfo() function to write a log file as root, and follows symlinks there. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled.	2019-07-04	not yet calculated	CVE-2019-13229 MLIST MISC MISC
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a predictable path /tmp/deepin-clone/mount/<block-dev-basename> in the Helper::temporaryMountDevice() function to temporarily mount a file system as root. An unprivileged user can prepare a symlink at this location to have the file system mounted in an arbitrary location. By winning a race condition, the attacker can also enter the mount point, thereby preventing a subsequent unmount of the file system.	2019-07-04	not yet calculated	CVE-2019-13226 MLIST MISC MISC
wuhan_deepin_technology -- deepin-clone	deepin-clone before 1.1.3 uses a fixed path /tmp/repo.iso in the BootDoctor::fix() function to download an ISO file, and follows symlinks there. An unprivileged user can prepare a symlink attack there to create or overwrite files in arbitrary file system locations. The content is not attacker controlled. By winning a race condition to replace the /tmp/repo.iso symlink by an attacker controlled ISO file, further privilege escalation may be possible.	2019-07-04	not yet calculated	CVE-2019-13228 MLIST MISC MISC
xpdf -- xpdf	In Xpdf 4.01 01, there is an out-of-bounds read vulnerability in the function SplashXPath::strokeAdjust() located at splash/SplashXPath.cc. t can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. t might allow an attacker to cause Information Disclosure. This is related to CVE-2018-16368.	2019-07-04	not yet calculated	CVE-2019-13287 MISC
xpdf -- xpdf	In Xpdf 4.01 01, a heap-based buffer overflow could be triggered in DCTStream::decodeImage() in Stream.cc when writing to rameBuf memory. t can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service, an information leak, or possibly unspecified other impact.	2019-07-04	not yet calculated	CVE-2019-13281 MISC
xpdf -- xpdf	In Xpdf 4.01 01, there is a heap-based buffer over-read in the function JBIG2Stream::readTextRegionSeg() located at JBIG2Stream.cc. t can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool. It might allow an attacker to cause Information Disclosure.	2019-07-04	not yet calculated	CVE-2019-13286 MISC
xpdf -- xpdf	In Xpdf 4.01 01, a heap-based buffer over-read could be triggered in SampledFunction::transform in Function.cc when using a large index for samples. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact.	2019-07-04	not yet calculated	CVE-2019-13282 MISC
xpdf -- xpdf	In Xpdf 4.01 01, there is a heap-based buffer over-read in the function DCTStream::readScan() located at Stream.cc. It can, for example, be triggered by sending a crafted PDF document to the pdftops tool. t might allow an attacker to cause Information Disclosure.	2019-07-04	not yet calculated	CVE-2019-13291 MISC
xpdf -- xpdf	In Xpdf 4.01 01, the Parser::getObj() function in Parser.cc may cause infinite recursion via a crafted file. A remote attacker can leverage this for a DoS attack. This is similar to CVE-2018-16646.	2019-07-04	not yet calculated	CVE-2019-13288 MISC
xpdf -- xpdf	In Xpdf 4.01 01, there is a use-after-free vulnerability in the function JBIG2Stream::close() located at JBIG2Stream.cc. t can, for example, be triggered by sending a crafted PDF document to the pdftoppm tool.	2019-07-04	not yet calculated	CVE-2019-13289 MISC
xpdf -- xpdf	In Xpdf 4.01 01, a heap-based buffer over-read could be triggered in strncpy from FoFiType1::parse in fofi/FoFiType1.cc because it does not ensure the source string has a valid length before making a fixed-length copy. It can, for example, be triggered by sending a crafted PDF document to the pdftotext tool. It allows an attacker to use a crafted pdf file to cause Denial of Service or an information leak, or possibly have unspecified other impact.	2019-07-04	not yet calculated	CVE-2019-13283 MISC

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add [US-CERT@ncaa.us-cert.gov](mailto:US-CERT@ncaa.us-cert.gov) to your address book.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to wgultarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) - 245 Murray Lane SW Bldg 410 - Washington, DC 20598 - (888) 282-0870



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fggurina@sunnyvale.ca.gov](mailto:fggurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for July 8, 2019  
**Date:** Monday, July 08, 2019 5:05:02 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Having trouble viewing this email? [Click here](#)





### **'Do not record'**

For those embroiled in the criminal legal system, this may come as no surprise: In January 2018, defense attorney Joel Garson discovered that his client's phone calls from the Orange County jail had been recorded and listened to by law enforcement. At the time of the recordings, Garson's client, Joshua Waring, was pro per, or representing himself, and the trial court had ordered that his calls not be monitored.

[The Appeal](#)

### **California seeks to end execution lawsuit, cites moratorium**

Gov. Gavin Newsom sought to end a long-running federal lawsuit challenging California's lethal injection process on Friday, arguing that it is no longer valid because of his moratorium on executions. Death penalty opponents are challenging the state's plan to use a single powerful barbiturate, instead of three drugs, to execute criminals.

[AP](#)

### **California prison guards can't sue state for time spent walking to their posts, court rules**

The California Supreme Court on Monday rejected most of an 11-year-old lawsuit in which tens of thousands of California state prison guards sought additional pay for work-related tasks they performed before and after their shifts. The decision greatly reduces the number of correctional officers who can pursue overtime claims against the state for work they carry out before reaching their posts inside California state prisons, such as retrieving weapons and moving through controlled check points.

[Sacramento Bee](#)

### **ACLU appeals order blocking lawsuit on deputy cheating**

An Orange County judge - who in February blocked a lawsuit pertaining to the sheriff's illegal use of jailhouse informants and then hiding evidence of their corruption - was misguided, according to an appeal filed today by the American Civil Liberties Union. Superior Court Judge Glenda Sanders ruled that advancement of the case might violate separation of powers principles, unduly burden government officials with paperwork, tamper prosecutorial discretion and give an unworthy legal forum to the ACLU's clients, a group of Orange County taxpayers who've organized People For The Ethical Operation of Prosecutors and Law Enforcement.

[OC Weekly](#)

### **Suit against lawyers to recoup stolen funds not a SLAPP**

The Court of Appeal for this district yesterday affirmed the denial of an anti-SLAPP motion filed by an attorney and a law firm who are being sued by their clients' judgment creditors, saying that fees received by the lawyers in payment of the clients' criminal defense are moneys belonging to them. The holding came in an opinion that was not certified

for publication. Presiding Justice Frances Rothschild of Div. One was the author.

[Metropolitan News-Enterprise](#)

### **Justice accuses colleagues of evading California Supreme Court decision**

A man who menaced store employees with a set of car keys was properly convicted of assault with a deadly weapon, Div. Two of the Fourth District Court of Appeal declared yesterday in a majority opinion, with a dissenter accusing her colleagues of veering from the views expressed by the state Supreme Court. The case was first decided on July 17, 2018, with Acting Presiding Justice Art McKinster writing for the majority in affirming the conviction and Justice Marsha G. Slough dissenting.

[Metropolitan News-Enterprise](#)

### **Minnesota congressman is not immune to defamation suit**

The St. Paul city attorney can move forward with her defamation lawsuit against Congressman John Lesch for a letter he wrote questioning her suitability for a job, the Minnesota Court of Appeals ruled Monday. Lesch's position as a congressman does not make him immune from City Attorney Lyndsey Olson's defamation lawsuit stemming from a letter Lesch wrote to newly elected St. Paul Mayor Melvin Carter in January 2018, the three-judge panel ruled.

[Courthouse News Service](#)

### **No immunity for colleagues in immigrant-assault case**

Fleeing sexual violence in her home country, a Honduran mother found more of the same at U.S. immigration jail. With her caseworker in prison now for sexual assault, several more officials could be held liable for deliberate indifference. On Monday, the Third Circuit affirmed a ruling that sets the stage for a civil trial implicating the former colleagues of Daniel Sharkey at the Immigration Family Center in Leesport, Pennsylvania.

[Courthouse News Service](#)

### **Supreme Court expands confidentiality protections for private companies**

In Food Marketing Institute v. Argus Leader Media, the U.S. Supreme Court held that government agencies can withhold a private company's records from public disclosure under Exemption 4 of the Freedom of Information Act ("FOIA") if the company has treated the information as confidential and also received promises from the government agency to maintain the information's confidentiality.

[National Law Review](#)

### **Man's conviction for murdering roommate, burying body in the forest upheld**

A state appeals court panel Tuesday upheld a former Burbank resident's

conviction for the killing of a former roommate whose remains were buried in the Angeles National Forest. The three-justice panel from California's 2nd District Court of Appeal noted in its ruling that Donald Thurman is a "self-admitted con-man" who denied any involvement in the January 2013 beating death of Glendale resident Nicholas Carter.

[City News Service](#)

### **Judge denies motion to dismiss charges in Laguna Niguel murder case**

A man charged with a fatal stabbing at a Laguna Niguel bar lost a bid Tuesday to have the case dismissed based on allegations of outrageous governmental misconduct involving his arrest. Judge Richard Oberholzer, who was called in to preside over the evidentiary hearing because Orange County Superior Court jurists were recused from the case, ruled the alleged misconduct in the arrest of the defendant did not warrant dumping a murder charge.

[City News Service](#)

### **Court rules Amazon can be held liable for third-party sales**

A federal appeals court on Wednesday ruled online retail giant Amazon can be held liable for the products sold by third-party sellers on its platform. The 3rd U.S. Circuit Court of Appeals ruled 2-1 that customers can sue Amazon when they buy defective products from its platform, even if Amazon did not make those products. The decision could leave Amazon vulnerable to a slew of lawsuits.

[The Hill](#)

## **Prosecutors/ Prosecutions**

### **Veteran L.A. prosecutor takes courageous step to live her true identity as transgender woman**

As Pride month comes to a close, we shine a spotlight on why it's important. Yes, it's a celebration, but also an opportunity to talk about being understanding and accepting of all people, no matter their gender or sexuality. ABC7's David Ono sat down with a veteran deputy district attorney in Los Angeles who is incredibly courageous, not only because of what she does, but who she is.

[ABC7](#)

### **Woman charged in hit-and-run killing of holocaust survivor in Valley Village**

A 68-year-old woman has been charged in the hit-and-run death last month of a 91-year-old Holocaust survivor in Valley Village. Joyce B. McKinney was arrested June 21 in Burbank in the death of Gennady Bolotsky on June 17. She faces charges of assault with a deadly weapon, hit and run, and vehicular manslaughter, officials said.

[NBC4](#)

### **'John Doe DNA' from 1992 matched to California rape suspect**

California prosecutors said Monday that they used an unusual tactic to identify a suspect for three rapes committed more than 25 years ago, keeping the case alive long after the normal legal deadline would have expired. Investigators tucked away rape kit samples from the attacks between 1992 and 1994 in the Sacramento and Davis areas in hopes that the budding science would one day lead to a match.

[AP](#)

### **The new price of a plea bargain in California**

After the jury deadlocked in Victor Hugo Sanchez's murder trial in February, San Diego prosecutors offered him a deal: plead guilty to manslaughter and spend just 11 years in state prison. But there was an unusual catch. As part of the agreement, Sanchez had to sign away his right to benefit from any future legal changes, including legislation or court decisions that might reduce his sentence. He agreed.

[The Marshall Project](#)

### **Indictments charge widespread voting fraud scheme on Skid Row in Los Angeles**

An indictment unsealed in Los Angeles charged nine people accused of participating in voting fraud schemes - in which homeless people were allegedly offered cash or cigarettes in exchange for forged signatures on initiative petitions and voter registration forms. Seven of the accused pleaded not guilty early Friday. The two others have not yet appeared in court on the new case.

[NBC4](#)

### **The disastrous consequences of DA Larry Krasner's "reforms"**

It was an interesting social experiment: What happens in a major metropolitan city like Philadelphia when you elect a district attorney whose primary goal is releasing criminals rather than prosecuting them? The results, however, were all too predictable. Gun-related violent crime is rising in Philadelphia. The police force is demoralized. Victims of crimes, their families, and advocacy groups feel betrayed.

[Philadelphia Magazine](#)

### **LA District Attorney Jackie Lacey on her reelection bid**

Jackie Lacey has been the District Attorney of Los Angeles County for six years. She will seek re-election next year. But activists argue she hasn't done enough to push criminal justice reforms and prosecute officers accused of misconduct.

[KCRW](#)

### **Private prisons are archaic and cruel. California needs to stop using them**

As we contemplate ways to address the disproportionate number of people imprisoned in America, one potential impediment to change is the large corporations that profit from incarceration. Between 2000 and 2016, the number of people housed in private prisons in the United

States increased by 47% compared with an overall rise in the prison population of 9%, according to an analysis from the Sentencing Project.  
[Los Angeles Times](#)

### **Prosecutors challenged to prove Tyndall allegations**

A dozen investigators have amassed a trove of evidence against former University of Southern California gynecologist George Tyndall over the last year. They've interviewed hundreds of women who described disturbing behavior, from lurid comments to inappropriate touching, and collected photos the doctor kept of nude women taken in what appeared to be a medical exam room.

[Los Angeles Times](#)

### **City Attorney Mike Feuer addresses L.A.'s role in census battle, homelessness crisis**

The city of Los Angeles was part of a lawsuit over the citizenship question on the 2020 census. City Attorney Mike Feuer discussed the impact of the Supreme Court decision blocking the addition of the question he believes would deter participation by many of L.A.'s 3.5 million immigrants, losing millions in federal funding locally. "As a practical matter, that question is done. It's dead," Feuer said.

[ABC7](#)

### **Possible gang member charged in LA killing of USC student, an Oakland councilwoman's son**

A man who authorities suspect is a gang member was charged Tuesday in Los Angeles in the death of Victor McElhaney, son of Oakland city Councilwoman Lynette Gibson McElhaney. Ivan Hernandez, 23, faces one count of murder and one count of robbery, according to a news release from the Los Angeles County District Attorney's Office.

[Riverside Press-Enterprise](#)

### **LA City Attorney leads filing in support of LGBTQ workforce rights**

City Attorney Mike Feuer, along with the city of New York and government agencies and elected officials across the country, filed a brief with the U.S. Supreme Court today seeking to protect LGBTQ workers from employment discrimination. "Again, we're taking a stand for LGBTQ equality and against discrimination," Feuer said in a statement.

[City News Service](#)

### **Judge orders mistrial after jury deadlocks on whether Mongols member killed Pomona SWAT officer in 2014**

After nearly two months of testimony and deliberation, a Los Angeles Superior court judge on Friday declared a mistrial in the murder trial of a Mongols Motorcycle Club member after a jury deadlocked over whether he acted in self-defense when he fatally shot Pomona police SWAT officer Shaun Diamond in 2014.



[AP](#)

## Parole

### **Bruce Davis, former Manson family member, set to be released on parole after serving 47 years in jail**

Former Manson family member and killer Bruce Davis is set to be released on parole from jail in California. Following a five-hour-long hearing at the California Men's Colony in San Luis Obispo, the 76-year-old was cleared for release, reports the Daily Mail. Davis will now be allowed to go free after 120 days unless California Governor Gavin Newsom overturns the decision.

[MEAWW](#)

### **Parole agent creates path for former inmates to re-enter society, stay out of prison**

When a person is released from prison, they can come back into a world that's changed dramatically. Things like cell phones, email, job hunting and housing can be overwhelming. A Bay Area man has taken on the task of running a program to help former inmates re-enter society, and for years it's been a success. Peer Re-Entry Navigator Network, or PRNN, is the passion of Martin Figueroa, a San Francisco-based Parole Agent Supervisor.

[CBS SF Bay Area](#)

## Prop. 57, Prop 47 & AB 109

### **San Jose lawmaker questions whether measures led to rise in rapes**

San Jose lawmakers during a recent meeting peppered police with questions about the sharp rise in rapes citywide, but Councilmember Johnny Khamis had a request - study how a pair of controversial state measures might have contributed to the increase. Proposition 47, approved in 2014, redefined several nonviolent crimes as misdemeanors, and Proposition 57, approved in 2016, prioritized parole for nonviolent offenders who served their full sentences in California prisons and reduced sentences for good behavior.

[San Jose Spotlight](#)

### **Eastside residents voice concerns about illegal drug use in Plummer Park**

Residents of West Hollywood's Eastside are turning up the volume on complaints about drug use and drug paraphernalia found in Plummer Park. Brian Rubenstein, a local resident who walks his dogs in the park, recently shared with neighbors and several City Council members images of apparent drug users and of drugs and a needle and syringe apparently used to inject illegal drugs.

[WEHOville](#)

### **Why 'technical' violations are still sending ex-cons back to California lockups**

Missed appointments, failed drug screens and unpaid fines are still sending a large number of former convicts back behind bars for probation and parole violations, despite recent efforts by California to overhaul its sentencing rules and end a decades-long trend of mass incarceration. A new study by the Council of State Governments shows that a quarter of the people incarcerated in California in 2018 were previously on probation or parole.

[Sacramento Bee](#)

### **Grant to fund effort to keep mentally ill out of jail**

Santa Barbara County has received a grant of nearly \$6 million over three years from the Bureau of State and Community Corrections to provide mental health services, substance-use disorder treatment, and/or diversion programs for people in the criminal justice system. The award from Prop. 47 funds recognizes a significant collaborative effort between county stakeholders committed to preventing and reducing the incarceration of people with mental illness and substance abuse disorders.

[Santa Ynez Valley Star](#)

## **Public Safety**

### **California needs to provide better help for crime victims**

California provides money and other assistance to victims of violent crime, but the aid is available only to those who know to ask for it. Nearly 100 applications are denied each year because they're filed late, perhaps because it took too long for victims to learn of the program, or perhaps because they were too busy dealing with the trauma or other consequences of the crime. And, of course, it's impossible to know how many people never do learn they are eligible for compensation.

[Los Angeles Times](#)

### **City fights proposed ban on towing vehicles**

A number of California cities, including Redwood City, are protesting a bill in the state Legislature that would prohibit the towing of cars with five or more unpaid parking tickets and make cities wait longer to tow vehicles that haven't been moved in three days. Assembly Bill 516, by Assembly members David Chiu, D-San Francisco, and Miguel Santiago, D-Los Angeles, is intended to protect low-income residents from the impacts of having their cars towed.

[Palo Alto Daily Post](#)

### **How Amazon and the cops set up an elaborate sting operation that accomplished nothing**

For Amazon, fear is good for business. If customers fear their neighbors, and fear they might steal a package, customers are less likely to be mad at Amazon if they don't get a package they ordered. They're also more

likely to buy an Amazon-owned Ring doorbell camera, which is marketed as way of surveilling your stoop for package deliveries and package thieves - especially on Neighbors, the Ring-owned "neighborhood watch" app.

[Vice](#)

### **California gang leaders' prison cellphones reveal secrets that stayed in the dark for years**

Back in the '90s and early 2000s, if the leader of a prison gang wanted to call a hit, he had to rely on cunning methods: coded letters, hand signals in monitored prison visiting rooms or a cryptic language of double entendres. These days, all he has to do is reach for his contraband cellphone. California prison officials describe illicit phones as one of the biggest security threats facing the state's beleaguered prison system, with an estimated tens of thousands in circulation.

[Bay Area News Group](#)

## **Policy & Legal Issues**

### **State legislation would help homeless people living in vehicles**

Despite opposition from local officials, Assembly Bill 516 passed through the Senate Transportation Committee on Tuesday.

[Lodi News-Sentinel](#)

### **California cops are withholding public records despite new law saying they can't**

Sexual assault in jail. Domestic violence complaints against an officer ignored. Knocked out teeth followed by a cover up. Throw in tens of thousands of stolen bullets, an illegal choke hold, falsified police reports, and cavorting with sex workers and you've got an emerging picture of what California's new police transparency law has revealed in its first six months.

[LAist](#)

### **Coachella weed dispensary fight highlights lax monitoring of laws encouraging minority ownership**

A bitter dispute over ownership of a proposed cannabis dispensary and coffee shop exploded in plain view during a city council meeting, underscoring what some experts say is lax monitoring of California and city laws intended to encourage local or minority ownership in cannabis businesses. The Coachella City Council was set to vote this week on a conditional-use permit for the Roots cafe and dispensary, a 4,080-square foot cannabis shop with an adjacent coffeehouse.

[Palm Springs Desert Sun](#)

### **Employee settles suit alleging discrimination by police chief**

A longtime Beverly Hills police civilian employee who alleged he was discriminated against by Chief Sandra Spagnoli because he is in his 50s has settled his lawsuit against the city, court papers obtained Tuesday

show. Lawyers for Clark Fogg filed a notice of settlement Monday with Los Angeles Superior Court Judge Susan Bryant-Deason. No terms were divulged and the papers did not state if the settlement was subject to City Council approval.

[California News Wire Services](#)

### **California ends its long, costly shift of prisoners to other states**

For an issue that received so much publicity at its peak - images of prisoners in triple bunk beds and overflowing into multipurpose rooms - the end of California's prison crisis came quietly last week, when the state brought home the last of its inmates held in a private lockup northwest of Tucson. Making good on a pledge by Gov. Gavin Newsom to finish the process begun in 2012, state prison officials have wrapped up the contracts with all out-of-state prisons.

[Los Angeles Times](#)

### **Transparency-forward police body cam law goes into effect on July 1**

On Monday, July 1, a new state law will require law enforcement agencies in California to release footage from body-worn cameras within 45 days of a "critical incident" in which an officer has fired at a person or used force that resulted in death or serious injury. The measure, AB 748, will bring department protocols across the state in line with the Los Angeles Police Department's policy, updated in April 2018, through which the department must release footage within 45 days, unless there are extenuating circumstances.

[Witness LA](#)

### **Ruiz earmarks mental health funding for law enforcement in House spending bill**

The U.S. House of Representatives passed an appropriations bill June 25 that included an amendment authored by Rep. Raul Ruiz, D-Palm Desert, to increase funding for mental health initiatives for law enforcement. Nearly one in four officers have thought of suicide at some point in their careers, according to a 2008 study commissioned by the National Institute for Occupational Safety and Health.

[Palm Springs Desert Sun](#)

### **LAPD pioneered predicting crime with data. Many police don't think it works**

The Los Angeles Police Department took a revolutionary leap in 2010 when it became one of the first to employ data technology and information about past crimes to predict future unlawful activity. Other departments around the nation soon adopted predictive policing techniques.

[Los Angeles Times](#)

### **Far more women are being sent to prison for life than 10 years ago, especially in California**

California has the highest proportion of women serving life (or virtual life) sentences in state prisons - one out of every four female prisoners, according to a new fact sheet from the Sentencing Project. The state with the next highest rate of life imprisonment among women in prisons is Louisiana, where one in seven imprisoned women will spend her life behind bars.

[Witness LA](#)

### **A new state law is changing how courts treat the mentally ill, but in Humboldt it's not that easy**

As a deputy public defender for the County of Humboldt, Casey Russo has an insider's perspective on our criminal justice system, and when it comes to the treatment of people with mental health issues, Russo says we're doing it wrong. Too often, he said, people are getting cycled through the revolving doors of crime and incarceration because of untreated mental health diagnoses, including substance use disorders.

[Lost Coast Outpost](#)

### **OP-Ed: California's bail system might be bad, but no-bail is worse**

California Senate Bill 10, passed by the California legislature and signed by California's governor on August 28, 2018, provides for a drastic change in pretrial detentions of criminal defendants. The bill eliminates the cash bail system and replaces it with a risk assessment system with the goal of providing information on whether the defendant is likely to reoffend or not show up for court on the original criminal charge.

[Hanford Sentinel](#)

## **Crime**

### **Two felons arrested in Chico for possession of four loaded firearms**

Chico police arrested two felons in Chico on Friday for possession of four loaded firearms. Officers say the incident started at around 6:20 p.m. on Friday evening when officers with the street crimes D unit conducted a traffic stop at East 20th Street and Highway 99 in Chico. The driver, who police have identified as David Barnes, 51, was found to be on parole with the California Department of Corrections and Rehabilitation.

[KRCR News](#)

### **Suspect in violent California rapes captured in Atlanta**

A man accused of violently raping women in the Sacramento area in the early '90s is now behind bars after DNA gave him away and dogged police work brought him in, local law enforcement leaders say. Mark Manteuffel, 59, was arrested on Friday in suburban Atlanta. Sacramento law enforcement agencies traced him there after a break in a cold case. At a news conference Monday afternoon, the heads of law enforcement agencies involved gathered to announce the news.

[11Alive](#)



## **California DOJ data shows drop in police uses of force in 2018**

Police used force during encounters with civilians significantly fewer times in 2018 than in the previous two years, according to a new California Attorney General's Office report released Tuesday. The public data report is part of the CA Attorney General's transparency initiative, OpenJustice. In 2015, then-Attorney General Kamala Harris launched the OpenJustice data portal website to bring transparency to the state's justice system by publishing crime and policing statistics.

[Witness LA](#)

## **Los Angeles County**

### **Garbage piles and rats are stinking up LA's famed Fashion District**

LA's world-famous Fashion District has become the city's unofficial garbage can, anchored by a quickly expanding 12-ton mountain of trash that's the result of months of illegal dumping, creating a massive public health nightmare. Frustrated business owners contacted the I-Team to show us how a burned out commercial building on East Pico Boulevard, once a clothing showroom, has become a dumping ground for an estimated 12 tons of trash.

[NBC4](#)

### **Is Sheriff Villanueva going to kick ICE out of L.A.'s jails or isn't he?**

The most contentious part of Los Angeles County Sheriff Civilian Oversight Commission meetings generally comes at the beginning, during public comment, when anti-illegal-immigration activists voice their disgust at Sheriff Alex Villanueva for limiting his cooperation with federal immigration officers.

[Los Angeles Times](#)

### **Sheriff Villanueva continues to betray his campaign promises**

Like many others from communities across Los Angeles County, I rooted for Alex Villanueva to bring progressive criminal justice reform and police accountability to the Sheriff's office. Several months into his tenure, it's clear that he conned us all. Leading up to the election, there were high hopes around Villanueva's platform: cutting ties with federal immigration authorities, promoting diversion programs to lower the county jail population, and opposing a \$3.5 billion jail expansion to name a few.

[Los Angeles Daily News](#)

### **Reentry and Opportunity Center improves outcomes for probation clients**

The new Los Angeles County Reentry Opportunity Center aims to increase successful outcomes for probation clients. Described as a one-stop shop, the facility houses community and county service providers to

assist clients with a second chance to change the trajectory of their life. The DOORS or Developing Opportunities Offering Reentry Solutions section contains representatives to aid with housing, jobs, training, legal assistance, mental health services and more.

[Los Angeles Sentinel](#)

## Consumer

### **Federal Court ruling exposes Amazon to huge liability**

Consumer protection received a huge boost Wednesday when a federal appeals court ruled Amazon can be held liable for third-party sales on its website. The e-commerce giant previously dodged liability for about 60% of its sales which originate from unvetted Amazon worldwide marketplace sellers who flood the consumer market with an inexhaustible supply of counterfeit, fraudulent, pirated, and replica items.

[The Counterfeit Report](#)

### **Discount P&G Tide detergent: Real or a risk?**

Lori Sgaraglio does a lot of laundry in her Butler County home. She loves Liquid Tide, but says prices for the top rated detergent are insane. A 100-ounce jug or box can cost you \$12 - \$17 in most stores. So she was thrilled to stumble upon discounted Tide on Facebook Marketplace. "It's an incredible deal," she said. Many Facebook sellers are advertising five-gallon buckets of Tide for less than half the supermarket price.

[WCPO Cincinnati](#)

## California/National

### **Hate crimes in California dip in 2018 after 2017 bump**

The number of reported hate crimes and victims decreased last year in California, although the number of suspects increased, the state's attorney general reported Tuesday. Hate crime events fell 2.5% from 2017, down by about two-dozen reports to 1,066 in 2018, according to the annual report. That follows a 17% jump the prior year. The state defines hate crimes as those targeting victims because of their race or ethnicity, nationality, religion, sexual orientation, gender or a disability.

[NBC4](#)

### **California Senate passes 'Housing for Homeless,' bill with penalty component**

The Committee on Budget and Fiscal Review authored AB 101, which provides for statutory changes needed to enact the housing and homelessness-related provisions of the Budget Act of 2019. In short, the Legislature is making legislative changes to the legislatively-created housing and homeless problem in California, according to Sen. Jim Nielsen (R-Gerber).

[California Globe](#)

## **Criminal justice reform is proving a tricky subject for many of these 2020 Democrats**

From health care to climate change, the crowded field of Democratic presidential contenders has a number of complex subjects to tackle in stump speeches, interviews and debates. But few are proving as thorny as criminal justice reform, often for very personal reasons. For candidates like former Vice President Joe Biden and Vermont Sen. Bernie Sanders, it's their past record of voting for tough-on-crime legislation.

[Time](#)

## **Sentences/Convictions**

### **LAPD officer gets probation, community service after pleading no contest in workers' comp fraud case**

An LAPD officer was placed on three years of summary probation after entering a no contest plea in a workers' compensation fraud case, the Los Angeles County District Attorney's Office said Wednesday. Jason Gordon, 48, pleaded no contest to a misdemeanor count of workers' compensation insurance fraud on Tuesday, according to a statement from the DA's office.

[KTLA](#)

### **Felon sentenced to 55 years to life for attempt to kill officer**

A 34-year-old felon was sentenced Monday to more than 55 years to life in prison Monday for attempting to kill a Santa Ana police officer, who sustained a graze wound to the head in a gun battle with the defendant. Carlos Michael Rodriguez of Santa Ana was convicted March 5 of one count each of attempted murder on a peace officer, assault with a semiautomatic rifle and possession of a firearm by a felon and two counts of possession of drugs with the intent to sell.

[My News LA](#)

### **Stolen van driver sentenced for pursuit that ended in crash in Hollywood**

A man who led authorities on an erratic pursuit from the San Fernando Valley to Hollywood in a stolen work van earlier this year was sentenced on Friday, prosecutors said. Karapet Kirpichyan, 46, of North Hollywood, was sentenced to four years and eight months in state prison after negotiating a plea agreement with prosecutors, the Los Angeles County District Attorney's Office said in a news release.

[KTLA](#)

### **Boxer who live-streamed himself after DUI crash that killed a pregnant woman sentenced 10 years**

A former professional boxer will spend the next 10 years behind bars after killing a pregnant mother of four when he crashed into her Chrysler minivan while intoxicated. On Thursday, Marcos A. Forestal received his sentence of 10 years in state prison, KTLA and News Channel 3 report.

Forestal pleaded guilty to gross vehicular manslaughter in March following the horrific incident nearly a year ago, according to KTLA.

[People](#)

### **55 years for repairwoman's murder**

A Lancaster man was sentenced Thursday to 55 years to life in state prison for killing appliance repairwoman Lyndi Fisher when she came to his home to repair his refrigerator nearly two years ago. William Franklin Hughes III, 32, was sentenced after Los Angeles Superior Court Judge Carols Chung found him to have been sane during commission of the crime in the sanity trial phase, according to the Los Angeles County District Attorney's Office.

[Antelope Valley Press](#)

### **Teenager accused of rape deserves leniency because he's from a 'good family,' judge says**

The 16-year-old girl was visibly intoxicated, her speech slurred, when a drunk 16-year-old boy sexually assaulted her in a dark basement during an alcohol-fueled pajama party in New Jersey, prosecutors said. The boy filmed himself penetrating her from behind, her torso exposed, her head hanging down, prosecutors said. He later shared the cellphone video among friends, investigators said, and sent a text that said, "When your first time having sex was rape."

[New York Times](#)

## **Homeless**

### **Los Angeles allocates millions for new homeless outreach and cleanup**

The City Council Friday approved millions of dollars to be spent on an enhanced homeless-outreach and street-cleanup operation recently touted by the mayor as an overhaul of efforts to combat illegal dumping and providing hygiene services for the homeless. The council allocated more than \$6.5 million to the Los Angeles Bureau of Sanitation to cover costs of hygiene and health services, cleanup teams that will target high-need areas, bathroom and shower stations and more.

[My News LA](#)

### **The year homeless-related crime surged in Los Angeles**

As the number of people experiencing homelessness in the City of Los Angeles has swelled in the past decade, they have also increasingly wound up in the crime data. But in 2015 something unusual happened: The number of people experiencing homelessness grew by 12% from the year before, but crimes where homeless people were involved - as victim, suspect or both - grew by nearly 120%, according to the LAPD database.

[Crosstown](#)

### **Meth addiction is an epidemic, and it's complicating the**

### **homeless relief effort**

She was ravaged by drugs, a young woman turning old too soon. Her face was puffy and scabbed, her arms were scarred by needle marks, and an abscess the size of a kitchen sponge floated under tight skin near her elbow. On Thursday morning in downtown Los Angeles, the 26-year-old brunet walked into a needle exchange program asking for help. She said she had spent most of the previous several weeks living in a car.

[Los Angeles Times](#)

## **Guns**

### **A win for public safety or a government ploy? California set to require background check for ammo sales**

The bustle inside LAX Ammunition on the Friday before Father's Day betrayed the gloom of the outside sky. Employees inside the Los Angeles-area gun shop had their hands full chatting with customers who were looking to replenish their ammo supply before July 1, with some customers spending hundreds of dollars in the process.

[USA Today](#)

### **5 things to know about new California ammo law**

California has some of the most stringent gun laws in the country. Now, a far-reaching new initiative to curb violence will require background checks for every ammunition purchase. The law goes into effect Monday. California has 4.5 million registered gun owners. State officials estimate about 3 million are regular shooters and that they will buy ammunition four or five times each year.

[KCRA](#)

### **Federal judge moves forward suit over California gun registration**

A federal judge on Thursday refused to dismiss a lawsuit by California gun owners who claim they were unable to comply with the state's latest registration law because the state's internet-based registration system does not work properly. Judge Morrison England Jr. said the state's inability to maintain a working registration website leading up to the registration deadline violated procedural due process.

[The Washington Free Beacon](#)

### **California ATF says 'ghost guns' are a threat - some experts disagree**

California has a "ghost gun" problem, the Los Angeles Field Division of the Bureau of Alcohol, Tobacco Firearms and Explosives (ATF) says. A spokesperson for the ATF field division told The Trace and NBC that 30 percent of recovered firearms are homemade and untraceable. However, many Second Amendment attorneys, firearm experts, and pro-gun rights advocates think concerns are overblown.

[The Epoch Times](#)



## **Gun rights groups sue California over firearms sales ban to those under 21**

Second Amendment right groups sued the state of California Monday over the new law banning the sale of firearms to people under the age of 21. Fox News reports the groups, the Calguns Foundation and Firearms Policy Coalition, argued in a lawsuit filed in San Diego on behalf of individual gun owners that those 18 and over are adults and have a right to purchase a firearm.

[Fox News](#)

## **Media**

### **L.A. Times owner Patrick Soon-Shiong using newspaper to generate revenue for his private drug company**

The spirit of Mark H. Willes and Katherine Downing is apparently alive and well at the Los Angeles Times. Back in 1999, Times Publisher Kathryn M. Downing had to apologize for entering into a profit-sharing agreement between the Times Magazine and Staples Center, publishing an issue where the Staple's Center was the magazine's sole subject.

[Hews Media Group](#)

## **Pensions**

### **This time CalPERS plans for stock market drop**

When its investment fund had a huge loss during a stock market crash a decade ago, plunging from about \$260 billion to \$160 billion, CalPERS was caught by surprise and had to sell assets at a market bottom to pay bills. Despite a fund reaching \$368 billion last week during a record bull market, CalPERS is far from recovering its 100 percent funding in the year before the 2008 crash. It still has only 70 percent of the projected assets needed to pay growing future pension costs.

[Calpensions](#)

### **\$1.2 billion CalPERS lawsuit over long-term care gets go-ahead from judge**

Public workers and retirees who sued CalPERS over an 85 percent rate increase to long-term care insurance plans could find out next week whether their lawsuit will move forward. The lawsuit cleared a potential hurdle when a judge tentatively ruled that it shouldn't be thrown out based on how much time passed before it was filed, and a decision on a second piece of the trial is expected Monday or Tuesday.

[Sacramento Bee](#)

### **There's a new way to save for retirement in California. Here's how it works.**

Nearly half of Californians will retire into economic hardship, and half have no retirement assets, according to the UC Berkeley Labor Center. On Monday, the state unveiled a government-run retirement savings program, CalSavers, aimed at helping the 7.5 million

Californians who are on their own when it comes to retirement.  
[Sacramento Bee](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los  
Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [CLA Public Section](#)  
**To:** [Melissa Tronquet](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, June 28, 2019 3:26:49 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive](#) (858,115 articles)



[North America](#) | [Global](#)

**USA**

[North America](#)

[Employee Benefits & Pensions](#)



### **Jander v. IBM: an Aberration or the Start of a Plaintiff-Friendly Trend in ERISA Employer Stock Cases?**

**Thompson Hine LLP**

The Supreme Court decisions in *Dudenhoeffer* (2014) and *Amgen* (2016) made it more difficult, as a practical matter, for plaintiffs to bring ERISA duty...

### **IRS Shifts Gears on Pension Plan Retiree Lump-Sum Window Alternative Hall Benefits Law**

Paying attention to the shifts in how the IRS interprets its regulations is an important part of benefits administration. In recent Notice 2019-18...

### **Departments Issue Final Rules on Health Reimbursement Arrangements Winston & Strawn LLP**

The Departments of Treasury, Labor, and Health and Human Services (the Departments) recently issued final rules on the use of health reimbursement...

### **The Supreme Court Will Take Another Look At Its ERISA Stock-Drop Pleading Standard**

**Seyfarth Shaw LLP**

ERISA stock-drop litigation has diminished in recent years due to the Supreme Court's Dudenhoeffer decision (and a rising stock market). Now...

---

### **Labor and Employment Alert: Two New Options for Health Reimbursement Arrangements**

#### **Vorys Sater Seymour and Pease LLP**

A health reimbursement arrangement (HRA) is an arrangement whereby an employer reimburses eligible employees for their medical expenses up to a...

---

### **A Full House: Proposed Update to Investment Limited Partnership Structure to Further Enhance Ireland's Alternative Fund Offering**

#### **Dechert LLP**

On 20 June, 2019, Ireland's government released its proposed Investment Limited Partnerships (Amendment) Bill 2019 (the "Bill") that will update the...

---

### **How Multiemployer Pension Plans Continue To Extract More From Contributing Employers Than What They Bargained For**

#### **Jackson Lewis PC**

Contributing employers to multiemployer pension plans ("MEPPs") are commonly surprised that their obligations to such a plan can extend well beyond...

---

### **Is Repeal of the Cadillac Tax Inevitable?**

#### **Hall Benefits Law**

Many provisions of the Affordable Care Act (ACA) are still being debated, especially as our country decides what direction to go next and government...

---

### **How to Share the Wealth**

#### **Lane Powell PC**

Lillian had a problem. Against all odds, she'd managed to build a successful spirits business, selling her specialty, a truly weird (but utterly...

---

### **Military Retired Pay and Benefits Considerations in Divorce Proceedings**

#### **State Bar of Wisconsin**

ERISA vs. FSPA - what's the difference? It's a vital consideration for divorce practitioners, says James C. W. Bock. Find out what they are, and why...

---

### **Fiduciary Framework for Investment by Defined Contribution Plans in Alternative Assets**

#### **Mayer Brown**

With the maturing, growth and increasing importance of defined contribution plans to the retirement security of US employees, many plan fiduciaries...

---

### **Class Action Update from the U.S. Supreme Court's 2018-2019 Term**

#### **Pierce Atwood LLP**

The 2018-2019 term of the U.S. Supreme Court opened with a newly configured court in which Justice Kavanaugh joined as an Associate Justice following...

---



## **Seventh ERISA Case Filed Challenging Actuarial Assumptions Used in DB Plans** **Thompson Hine LLP**

Plaintiffs' lawyers have filed a series of cases challenging the lawfulness of the actuarial assumptions used in certain defined benefit retirement...

---

## **Supreme Court to Review ERISA Statute of Limitations Case**

### **Ogletree Deakins**

In late 2018, in *Sulyma v. Intel Corporation Investment Policy Committee*, the Ninth Circuit Court of Appeals held that a plaintiff's access to...

---

## **Are Manufacturer Drug Coupons and HDHPs a Good Fit?**

### **Kilpatrick Townsend & Stockton LLP**

In our last blog post, we discussed the recent rule finalized by Health and Human Services regarding the calculation of the annual cost-sharing...

---

## **Final Regulations Allow Employers to Pay For Employees' Health Insurance Premiums**

### **Taft Stettinius & Hollister LLP**

Health reimbursement arrangements (HRAs) are a very flexible type of group health plan—they allow employers to reimburse employees for certain...

---

## **Employee Benefit Plans with Master Trust Investments - Financial Statement Changes**

### **McDermott Will & Emery**

The Financial Accounting Standards Board (FASB) adopted changes to the required financial statement disclosures of employee benefit plans with...

---

## **Plan sponsors of hybrid defined benefit plans and certain merged retirement plans can apply for an IRS determination letter, starting September 1, 2019**

### **DLA Piper**

On May 1, 2019, the Internal Revenue Service (IRS) issued Rev. Proc. 2019-20, which provides for an expansion of the determination letter program...

---

## **Supreme Court Agrees to Hear Intel Case with Potentially Significant Implications for 401(k) Plan Fiduciaries**

### **Ropes & Gray LLP**

On June 10, 2019, the U.S. Supreme Court agreed to hear *Intel Corp. Investment Policy Committee et al. V. Sulyma* (No. 18-1116), and the outcome of...

---

## **Final Regulations Offer New Health Coverage Options for Employers**

### **Haynes and Boone LLP**

Final regulations were recently released by the U.S. Departments of Labor, Health and Human Services, and the Treasury (collectively, the...

---

Employment & Labor



Managing the employment relationship in Nevada

Nevada



### **Holland & Hart LLP**

A structured guide to managing the employment relationship in Nevada...

---

### **Employee termination law in Vermont** Vermont

#### **Downs Rachlin Martin PLLC**

A structured guide to employee termination law in Vermont

---

### **Managing the employment relationship in Arizona** Arizona

#### **Ogletree Deakins**

A structured guide to managing the employment relationship in Arizona...

---

### **Managing the employment relationship in Ohio** Ohio

#### **Taft Stettinius & Hollister LLP**

A structured guide to country specific laws, misclassification and contracts in Ohio

---

### **California's employment regulatory scheme: PAGA in wake of Epic Systems**

California

#### **Dentons**

As employers doing business in California know, California's employment regulatory scheme is the most comprehensive of any US state. In particular...

---

### **Updated Model Summary Annual Report**

#### **Haynes and Boone LLP**

The U.S. Department of Labor has released updated model Summary Annual Reports ("SARs") for retirement plans and for welfare benefit plans that are...

---

### **How to Craft a Non-Discriminatory Paternity Leave Policy** New York

#### **Law Office of Kristine A Sova**

Historically, many employers provided paid maternity leave to mothers, while providing little to no leave to fathers. While employers may provide...

---

### **Another EEO Audit Released - Looking at the FCC's Current EEO Obligations**

#### **Wilkinson Barker Knauer LLP**

The FCC yesterday released another of its regular EEO audit notices (available here), asking that approximately 80 radio stations, and the employment...

---

### **Additional Discovery Ordered to Determine Location of Exposure in Facility Defendant's Personal Jurisdiction Challenge** Louisiana

#### **Goldberg Segalla LLP**

The plaintiff, Frederico Lopez, filed suit against the defendants, alleging he developed mesothelioma from exposure to asbestos while...

---

### **New York Considering Gig Worker Protection Law** New York

#### **Fisher Phillips**

New York lawmakers just introduced the "Dependent Worker Act" into the Assembly and Senate this past week, which proposes to provide workers in the...

---

## **How to Conduct an International Internal Investigation**

### **Littler Mendelson PC**

Imagine an anonymous worker at a multinational's Egypt factory contacts the global whistleblower hotline and accuses the Cairo plant manager of...

---

## **Big trouble in New York State: Legislation would further expand sexual harassment and other discrimination laws**

New York

### **Constangy Brooks Smith & Prophete LLP**

In 2018, New York State and New York City lawmakers toughened their sexual harassment laws. But New York State lawmakers were not done. A few days...

---

## **Colorado bans the box**

Colorado

### **Constangy Brooks Smith & Prophete LLP**

Colorado has become the latest jurisdiction to join the "ban the box" movement. The Colorado Chance to Compete Act, signed into law by Gov. Jared...

---

## **Minnesota Employers: Don't be Caught Off Guard**

Minnesota

### **Spencer Fane LLP**

All companies and organizations with Minnesota-based employees must update their employment policies and practices due to recent state law changes...

---

## **Human Trafficking Training Required for Hotels/Motels in California by Year End**

### **Fox Rothschild LLP**

Another mid-year reminder: California hotels and motels must train all employees on human trafficking awareness by January 1, 2020. Per SB 970, hotel...

---

## **Maritime Law: Punitive Damages Are Not Available for an Unseaworthiness Claim**

### **Lane Powell PC**

This week, the United States Supreme Court released its landmark opinion in *Dutra Group v. Batterton*, Dkt. No. 18-266 (June 24, 2019), resolving the...

---

## **No Harm, No Foul? Not So, Under Illinois Biometric Privacy Law**

Illinois

### **DLA Piper**

Dozens of employment class actions have been filed against employers with operations in Illinois for alleged violations of the Illinois Biometric...

---

## **When is Obesity a Disability under the ADA?**

### **Cozen O'Connor**

Complying with the Americans with Disabilities Act poses difficult challenges for employers, and one of the toughest issues to come along in recent...

---

## **Department of Labor's Opinion Letter: FMLA Leave**

### **Taft Stettinius & Hollister LLP**

The Department of Labor (DOL) issued an opinion letter that provides employers with further guidance on Family and Medical Leave Act (FMLA) leaves...

---



## **New Jersey Becomes the Latest State to Propose a Ban on Discrimination Based on Hair and Hairstyle**

New Jersey

### **Saiber LLC**

If passed, the identical bills in the State Assembly and Senate would amend the Law Against Discrimination to ban discrimination based on hair...

---

## **New Personnel File Disclosure Requirements in Virginia**

Virginia

### **Odin Feldman & Pittleman PC**

Effective July 1, 2019, employers in Virginia will be subject to a new requirement to provide employees with copies of certain documents in their...

---

## **Minnesota Wage Theft Statute, Part II: New Notice, Disclosure, and Recordkeeping Requirements**

Minnesota

### **Ogletree Deakins**

In our previous article, we summarized the key provisions of Minnesota's new "wage theft" law. This article focuses specifically on the notices and...

---

## **Illinois' Legalization of Marijuana May Change the Drug-Free Workplace Landscape**

Illinois

### **Vedder Price PC**

Recreational cannabis is poised to become legal in Illinois in 2020, and Illinois employers should consider the impact now. In late May 2019, the...

---

## **NY Passes Dramatic Amendments to Workplace Discrimination Laws**

### **Fox Rothschild LLP**

Changes on the horizon will require employers throughout New York State to make significant changes to their workplace discrimination and harassment...

---

## **A Summary of the Latest Changes to the New York State Human Rights Law**

New

York

### **Mintz**

Just before the end of its session, the New York Legislature expanded protections against discrimination and harassment under the New York State Human...

---

## **Rat Eradication - Inflated and Otherwise**

New York

### **Vinson & Elkins LLP**

In late May, the New York Times ran a grim story entitled "Rats are Taking Over New York City," talking about the onslaught of rats in New York and...

---

## **Read This Now: New York's Groundbreaking Sexual Harassment Legislation**

New

York

### **Kelley Drye & Warren LLP**

Clichés like "seismic shift" and "paradigm change" do not begin to describe just how profoundly the New York Legislature changed the standards for...

---

## **Directed Verdict Reversed for Floor Tile Defendant Based on Admissibility of**

## Expert Opinion

### Goldberg Segalla LLP

The plaintiff, Robert Friedman, alleged that he developed mesothelioma from exposure to asbestos through remodeling work undertaken in...

---

## Evaluating and Addressing Retirement Plans' Cybersecurity

### Morgan Lewis

Employers who want to protect their retirement plan from a data breach — and limit their liability if one occurs — should evaluate and address sources...

---

## New York State Significantly Expands its Workplace Harassment Laws (Again)

New York

### Littler Mendelson PC

As its session draws to a close, the New York State Legislature substantially revised the State's anti-discrimination and anti-harassment laws this...

---

## Kentucky's new pregnancy accommodation law goes into effect

Kentucky

### Porter Wright Morris & Arthur LLP

Kentucky recently enacted the Pregnant Workers Act, which amends the Kentucky Civil Rights Act to provide accommodations to pregnant and lactating...

---

## Lawmakers Announce Three-Month Delay for Massachusetts Paid Family and Medical Leave Law

Massachusetts

### Hunton Andrews Kurth LLP

In a statement issued last week, Massachusetts Governor Charlie Baker, along with state house and senate leadership, announced that lawmakers had...

---

## Oregon Employers Face New Obligations Regarding Discrimination and Sexual Assault in Workplace

Oregon

### Holland & Knight LLP

Oregon Gov. Kate Brown has signed Senate Bill (SB) 726, which significantly changes Oregon employers' obligations with respect to handling...

---

## New York Lawmakers Pass Game-Changing Reforms to State Discrimination Laws

New York

### Fisher Phillips

Still grappling with the expansive sexual harassment reforms passed last year, New York businesses and employers will soon need to manage through yet...

---

## No "End Run" Around Brinker Under Section 17200

California

### Payne & Fears LLP

The California Court of Appeal has affirmed a complete victory by Safeway Inc. over a certified class of wage-and-hour plaintiffs. *Esparza v. Safeway*...

---

## Illinois Tackles Sexual Harassment

Illinois

### Kelley Drye & Warren LLP



On June 2, 2019, the Illinois General Assembly passed SB75, a legislative response to the #MeToo movement. Governor J. B. Pritzker is expected to...

---

### **The Interstate Medical Provider Claim: Unsettled Jurisdictional Questions Open the Floodgates in New Jersey**

New Jersey

#### **Goldberg Segalla LLP**

As overall filings in the New Jersey Workers' Compensation Courts have been falling, one particular type of claim is on the rise: the Medical Provider...

---

### **Massachusetts Paid Family and Medical Leave: Final Regulations, Updated Notices, and Educational Sessions**

Massachusetts

#### **Ogletree Deakins**

On June 18, 2019, the Massachusetts Department of Family and Medical Leave (DFML) issued final regulations regarding the Massachusetts Paid Family...

---

### **Oregon's New Workplace Fairness Act Limits the Use of Nondisclosure Agreements, Requires Written Antiharassment Policies, and Extends the Time for Filing Claims**

Oregon

#### **Littler Mendelson PC**

Oregon just enacted comprehensive legislation that will have a potentially surprising impact on most Oregon workplaces. On June 11, 2019, Governor...

---

### **Time's Up: New York Legislature Passes Sweeping Reform to Increase Workplace Protections Against Sexual Harassment and Other Forms of Discrimination**

New York

#### **Patterson Belknap Webb & Tyler LLP**

On June 19, 2019, the New York State Assembly passed sweeping legislation designed to increase protections against workplace sexual harassment. The...

---

### **New marijuana laws and court cases continue to provide inconsistent guidance for employers: a summary of recent developments in Illinois, Nevada, New Jersey and Michigan**

#### **Reed Smith LLP**

Over the past few years, 31 states have legalized some form of medical or recreational marijuana use and this wave of legalization continues to grow...

---

### **NLRB Rules Employers May Maintain Discipline Between Election and Certification**

#### **Barnes & Thornburg LLP**

After an election is held to determine whether a union will become the representative of a company's employees, there is a period of time in which...

---

### **Sweeping Pay Equity Laws On The Way For New York Employers**

New York

#### **Fisher Phillips**

This past week was a busy one for New York State lawmakers. In addition to passing game-changing legislation overhauling the state's discrimination...

---



## **Washington Healthcare Update- Jun 24, 2019**

Washington

### **McGuireWoods Consulting LLC**

Senate to hold hearing on the enforcement of antitrust laws, while the House plans to cover a number of health care bills that reauthorize a variety...

---

### **Supreme Court Upholds, Narrows Deference To Agency Interpretations Of Regulations**

#### **Mayer Brown**

In a 5-4 decision, the Supreme Court decided not to overrule the doctrine of Auer deference, which requires courts to defer to agency interpretations...

---

### **Case of the Big Bus Driver: Seventh Circuit Joins Other Circuits in Rejecting Obesity, without Other Physiological Condition, as ADA Impairment**

#### **Bradley Arant Boult Cummings LLP**

Obesity has been recognized as a disease by the American Medical Association, National Institutes of Health, and the World Health Organization. Does...

---

### **Regulatory Spring: Rulemaking by the Wage & Hour Division - June 21, 2019**

#### **Seyfarth Shaw LLP**

Last week, the comment period ended for the Department of Labor's Notice of Proposed Rulemaking seeking to revise and update the regulations...

---

### **New York State Poised to Expand Protections Against Discriminatory Pay Practices**

New York

#### **Proskauer Rose LLP**

The New York State legislature has passed a bill that, if signed by Governor Andrew Cuomo, will expand pay protections by requiring employers to...

---

### **Washington State Imposes Limits on Non-Compete Agreements**

Washington

#### **Fenwick & West LLP**

Washington is the latest state to shake up the non-competition landscape. Last month, Gov. Jay Inslee signed into law a bill that significantly...

---

### **\$2M Jury Award to Employee Vacationing While on Medical Leave Highlights Pitfalls for Employers**

Massachusetts

#### **McGuireWoods LLP**

It is no secret that employees sometimes abuse benefits under the Family and Medical Leave Act (FMLA). Nor is it a secret that pitfalls abound for...

---

### **Maryland Law Bars Enforcement of Non-Compete Agreements Against Low Wage Workers**

#### **Epstein Becker Green**

Maryland recently joined the ranks of states with laws limiting the enforcement of non-compete agreements against low wage workers. Maryland's...

---

### **Oregon Enacts Living Donor Leave Law**

Oregon

### **Jackson Lewis PC**

Earlier this month, Oregon Governor Kate Brown signed Senate Bill 796 into law —after it passed 28-1 in the state Senate, and unanimously in the...

---

### **U.S. Supreme Court Nixes Punitive Damages for Unseaworthiness**

#### **Winston & Strawn LLP**

Resolving a split between the Federal Circuit Courts of Appeals, the U.S. Supreme Court held in the case of *Dutra Group v. Batterton* that sailors...

---

### **Construction Conference Insights: Industry Leaders Lay the Foundation for Success**

#### **Ward and Smith, P.A.**

Three construction industry executives with nearly a century of experience among them freely shared the lessons they had learned and the keys to...

---

### **Workplace Safety in California, Episode 2: All About Cal/OSHA Citations**

California

Audio

#### **Ogletree Deakins**

In this Episode of the Workplace Safety in California series, Kevin Bland and Karen Tynan discuss the critical steps for employers to consider after...

---

### **Nevada Becomes the First State to Restrict Employer Use of Pre-Employment Cannabis Tests**

Nevada

#### **Seyfarth Shaw LLP**

Following closely on the heels of a similar law in New York City, effective January 1, 2020, it will be unlawful for Nevada employers to reject a job...

---

### **Penalizing the Employer for the EEOC's Mistake?**

#### **Shawe Rosenthal LLP**

A recent case caused me significant concern on behalf of employers. As you may know, before an employee may file a federal discrimination lawsuit...

---

### **Colorado Court of Appeals Permits Evidence of Billed Workers' Compensation Benefits at Trial**

Colorado

#### **Wilson Elser**

The Colorado Court of Appeals announced a recent published opinion in which, although the Court considered multiple issues on appeal, its opinion...

---

### **Tech-Tuned Workplace, Episode 1: Advanced Technologies**

Audio

#### **Ogletree Deakins**

In the first Episode of our "Tech-Tuned Workplace" series, Jennifer Betts and Ruthie Goodboe provide a high-level overview of advanced Technologies...

---

### **New York State Expected to Vastly Overhaul Harassment/Discrimination Laws Again**

New York

#### **Baker & Hostetler LLP**



Late on June 19, New York lawmakers passed a bill that makes wide-sweeping changes to New York State discrimination and harassment law. Gov. Andrew...

---

### **Mentor, Sponsor, Coach: Navigating Career Relationships**

#### **Association of Corporate Counsel**

How to find a mentor, sponsor and coach, and be open to these pivotal figures in your life...

---

### **How to Lower Risk by Cutting Harmful Company Documents**

#### **Jackson Lewis PC**

While company documents are necessary, some can expose a company to liability and other harms. Knowing how to identify and cut the harmful ones may...

---

### **Minnesota Employers Are Subject To New Record-Keeping And Notice Requirements**

Minnesota

#### **Fredrikson & Byron PA**

Minnesota employers are subject to several new record-keeping and notice requirements as a result of amendments made to several employment law...

---

### **Nevada Applicants and New Employees with Positive Marijuana Test Results Will Receive Legal Protections**

Nevada

#### **Littler Mendelson PC**

Beginning January 1, 2020, new legislation in Nevada will require employers to think carefully about whether and which applicants should be tested...

---

### **Viewpoint: A Road Map to Hiring Employees from Direct Competitors in California**

California

#### **Buchalter**

California strongly favors employee mobility. Laws enabling employees to work for direct competitors help drive California's economy. The ability of...

---

### **National Retailer Liable for Wage Statement Violations Under California Law**

California

#### **McGuireWoods LLP**

On May 31, 2019, the U.S. District Court for the Northern District of California awarded a \$102 million judgment against a national retailer for...

---

### **Harassment complaints in a post #metoo world: Four key guidelines for conducting an internal investigation**

#### **Fox Williams LLP**

The effect of the #metoo campaign continues to ripple across industries. The recent International Bar Association Us Too publication reported on...

---

### **Illinois Seeks to Impose Restrictions on the Use of Artificial Intelligence in Job Interviews**

Illinois

#### **Hunton Andrews Kurth LLP**

The Illinois legislature recently passed the Artificial Intelligence Video Interview

Act, which prohibits an Illinois employer from using artificial...

---

## **New York Lawmakers Upend the Employment Law Landscape...Again (Part 1)**

New York

### **Reed Smith LLP**

Late last week, New York legislators passed a series of sweeping changes to the State's employment laws. These drastic changes come on the heels of...

---

## **California Jury Awards \$15.4 Million to Former Jack in the Box Employee**

California

### **Proskauer Rose LLP**

In a decision unsurprising to anyone familiar with what California juries have been up to lately (see our reporting here), fast-food titan Jack in...

---

## **More than Enforcement: Exploring OSHA's On-Site Consultation Program**

### **Goldberg Segalla LLP**

Congress created OSHA to assure safe and healthful working conditions for workers by setting and enforcing standards and by providing training...

---

## **Recapping the Many Legal Developments Affecting Private Employers in New York and New Jersey, So Far, in 2019**

New Jersey

New York

### **Greenberg Traurig LLP**

There have been many significant developments in the first half of 2019 impacting private employers in New York and New Jersey. Federal, state, and...

---

## **New York State Set to Further Expand Protections Against Workplace Harassment**

New York

### **Proskauer Rose LLP**

New York State lawmakers have approved broad legislation that will lower the burden on plaintiffs seeking to prove claims of workplace harassment...

---

## **Forensic accounting skills in investigations**

### **Global Investigations Review**

Forensic analysis of data refers to analysis of electronically stored data. The most commonly analysed data are Accounting and financial, but several...

---

## **New Maine Law Requires Time Off From Work For Appointments at VA Medical Facilities**

Maine

### **Jackson Lewis PC**

State and local leave laws are changing weekly and sometimes even daily! For the second time this month, Maine is adjusting its leave laws. Employers...

---

## **New York Expands Harassment Laws**

New York

### **Jackson Lewis PC**

Major changes to New York's harassment laws were among the flurry of bills advanced and passed by the New York State Legislature in the final hours...

---



## **Connecticut Expands Harassment Training and Posting Obligations for Employers** Connecticut

### **Jackson Lewis PC**

Nearly all employers in Connecticut will now have to provide sexual harassment training to employees under Connecticut Public Act No. 19-16, also...

---

## **New York State Set to Enact Ban on Salary History Inquiries** New York

### **Proskauer Rose LLP**

In a continuation of its recent legislative push to expand the reach of anti-discrimination laws, New York State is set to be the latest jurisdiction...

---

## **New York To Curb Employer Use of Applicant and Employee Wage and Salary History** New York

### **Mintz**

Just days before concluding its legislative session, the New York Legislature enacted a law focusing on an employer's acquisition and use of applicant...

---

## **Massachusetts Department of Family and Medical Leave Provides New Worker Notices and Posters, and Issues Final Regulations** Massachusetts

### **Epstein Becker Green**

As previously reported, last week the Massachusetts Department of Family and Medical Leave ("DFML") announced several changes, both substantive and...

---

## **"Insurer Duty to Defend Against Sexual Misconduct Allegations Broadly Construed by SDNY," Insurance Law Update** New York

### **Jenner & Block LLP**

In a recent opinion, Brotherhood Mutual Insurance Company v. Kurt Ludwigsen, the US District Court for the Southern District of New York considered...

---

## **Illinois Legalizes Recreational Marijuana: Impact on Employers** Illinois

### **Proskauer Rose LLP**

Illinois will soon become the eleventh state to legalize the recreational use of marijuana. On June 25, 2019, Governor Pritzker signed into effect...

---

## **Credit on SLU Payments and Recovery of a Third-Party Action Lien: Why They Live Together in Perfect Harmony** New York

### **Goldberg Segalla LLP**

In New York, Workers' Compensation Law Section 15(4-a) provides a carrier the right to take a credit against a subsequently determined schedule award...

---

## **Update on State Fiduciary Duty Regulations** Massachusetts

### **Morgan Lewis**

As Massachusetts steps up to the plate, New Jersey extends comment period and announces public hearing. Just as the comment period on New Jersey's...

---

## **New Jersey Minimum Wage Hike on July 1, 2019** New Jersey



### **Jackson Lewis PC**

The New Jersey minimum wage will increase to \$10.00 per hour for many employees in the state on July 1, 2019....

---

### **NC Legislative Update: June 21, 2019**

North Carolina

#### **Nexsen Pruet**

House and Senate members continued their work towards a budget deal ahead of the approaching end of the fiscal year. Budget writers met several times...

---

### **Court Rejects MSHA's Revisions to Workplace Examination Rule**

#### **Ogletree Deakins**

Due to a recent court decision, metal/nonmetal mine operators are again facing the possibility of having to comply with two of the more onerous...

---

### **Class Action Trends Report Spring 2019**

#### **Jackson Lewis PC**

In the first federal circuit court decision to address a procedural matter of....

---

### **New York Passes Sweeping Changes to Anti-Harassment Law**

#### **Barnes & Thornburg LLP**

New York is on the cusp of passing one of the strictest anti-harassment laws in the country. In the past week, the New York Assembly and Senate have...

---

### **Colorado Enacts 'Ban the Box' Legislation to Take Effect in September 2019**

Colorado

#### **Jackson Lewis PC**

In an effort to prevent persons with criminal records from being automatically ruled out for job vacancies, Colorado Governor Jared Polis has signed...

---

### **Overcoming Organizational Resistance to Implementing Contract Management Software**

#### **ContractWorks**

Contract Management Software can help bring order to the otherwise unwieldy task of keeping track of your corporate agreements and the various...

---

### **Regulators Issue Senior Safe Act Fact Sheet**

#### **Kilpatrick Townsend & Stockton LLP**

To mark the one-year anniversary of the passage of The Senior Safe Act (the "Act"), the Securities and Exchange Commission ("SEC"), the North...

---

### **Third Thursdays with Ruthie: Negotiating Union Security and Dues Checkoff Provisions**

Audio

#### **Ogletree Deakins**

Union security and dues checkoff are both important subjects that come up during collective bargaining...

---

### **Taxation without a DC location - the District of Columbia's Universal Paid Leave**

**Act tax goes into effect July 1, 2019** [District of Columbia](#)

**Eversheds Sutherland (US) LLP**

In order to support the District of Columbia's new Universal Paid Leave Act (the Act), covered employers will be required to contribute to the...

---

**Are General Contractors Liable for Their Subcontractors' Actions or Inactions?**

[California](#)

**Jackson Lewis PC**

A general contractor in Southern California found itself on the hook for its subcontractor's failure to pay wages to its workers, even though the...

---

**UPDATE: Massachusetts Delays Paid Family and Medical Leave Law Deadlines**

[Massachusetts](#)

**Latham & Watkins LLP**

Employers now have until September 30, 2019, to provide individualized notice and October 1, 2019, to begin contributions. As covered in a previous...

---

**Advanced Technologies and the Workplace, Part I: A Primer**

**Ogletree Deakins**

You have probably heard the phrases "fourth industrial revolution" and the "future of work." Both refer to changes in the way people live, work, and...

---

**Alert for Employee Education: FBI Issues Warning About Exploitation of "Secure" Websites**

**Robinson & Cole LLP**

We all have been trained to look at website addresses with a critical eye to make sure they have "https," as those websites are supposed to be secure...

---

**Court of Appeals Says Police Officer's Promotion Can Be Rescinded Based on Pre-Promotion Misconduct** [California](#)

**Atkinson Andelson Loya Ruud & Romo**

On June 14, 2019, the California Court of Appeals, Second District, published a decision affirming the denial of a police officer's request for...

---

**Scabby the Rat Could Face Extermination under Labor Board General Counsel's Recommendation**

**Jackson Lewis PC**

A recent Advice Memorandum from the National Labor Relations Board's (NLRB) General Counsel's office (GC Office) has recommended that the Board...

---

**New Forms and Final Regulations Issued Under the Massachusetts Paid Family and Medical Leave Law** [Massachusetts](#)

**Littler Mendelson PC**

There has been much activity surrounding the Massachusetts Paid Family and Medical Leave law (PFML), which was enacted last summer as part of the...

---

**EEOC ready to accept comp data on July 15**



### **Constangy Brooks Smith & Prophete LLP**

Here's the timetable for EEO-1 comp data reporting. Late last week, the Equal Employment Opportunity Commission filed a status report in the case of...

---

### **Arbitration of Employment Claims Globally**

#### **Baker McKenzie**

While the benefits of arbitration clauses in employment documents with US employees are highly publicized and well known, arbitration clauses with...

---

### **Don't Freeze Up: Know What to Do When ICE Comes Knocking**

#### **Fox Rothschild LLP**

Employers should understand how to handle I-9 inspections by Immigration and Customs Enforcement (ICE) and proactively prepare for possible...

---

### **Labor and Employment Alert: Oregon Enacts an Expansive Workplace Protection Act**

[Oregon](#)

#### **Vorys Sater Seymour and Pease LLP**

Oregon recently enacted the Workplace Protection Act (WPA) to restrict the use of nondisclosure agreements in circumstances alleging employment...

---

### **Final Massachusetts Paid Family and Medical Leave Regulations Published and Other PFML Updates**

[Massachusetts](#)

#### **Proskauer Rose LLP**

The Massachusetts Department of Family and Medical Leave ("DFML") has posted the much-anticipated final regulations regarding Massachusetts' Paid...

---

### **What's Left of the De Minimis Doctrine in California? Ninth Circuit Court of Appeals May Soon Decide**

[California](#)

#### **Jackson Lewis PC**

Last year, the California Supreme Court held the federal "de minimis" doctrine does not apply to California state law claims for unpaid wages for...

---

### **NY Equal Pay Act Will Cover All Protected Characteristics**

[New Jersey](#)

#### **Fox Rothschild LLP**

New York State will vastly expand the scope of its Equal Pay Act to cover all characteristics protected under the New York Human Rights Law, including...

---

### **Digging into the New HRA Regulations Part 1 - Individual Coverage HRAs**

#### **Proskauer Rose LLP**

As discussed in our June 18th blog entry, the Departments of Labor, Health and Human Services, and Treasury (collectively, the "Departments")...

---

### **Building a Modern Slavery Strategy**

#### **Seyfarth Shaw LLP**

This is the fourth and last in a series of blogs by our Global Modern Slavery Team dealing with how companies can navigate the...

---

## **Department of Labor Releases Proposed Rule for Industry-Recognized Apprenticeship Programs**

**Little Mendelson PC**

On June 24, 2019, the Department of Labor made public its long-awaited proposed rule establishing a process for DOL to advance the development of...

---

## **SCOTUS keeps agency deference alive in *Kisor v. Wilkie*. But is it just a “stay of execution”?**

**Cooley LLP**

Today, SCOTUS decided *Kisor v. Wilkie*, an important case that raised the question of whether to overrule the decades-long deference of courts to the...

---

## **What ELSE is going on in Washington, DC? Legislative Update for Employers that Operate in the District of Columbia**

**Little Mendelson PC**

The District of Columbia Council has passed several pieces of legislation that impose significant obligations upon employers in the District of...

---

## **Extreme Obesity Not Necessarily a Disability Under ADA, Says Seventh Circuit**

**Barnes & Thornburg LLP**

The U.S. Court of Appeals for the Seventh Circuit recently held that extreme obesity is not an actionable “impairment” under the Americans with...

---

## **Colorado becomes the 13th State to “Ban the Box” - Prohibiting Employers from Inquiring about Criminal Convictions on Initial Employment Applications**

Colorado

**Cozen O'Connor**

Colorado employers should review and, if necessary, revise job applications to remove questions about criminal history. Colorado has joined a growing...

---

## **Massachusetts Paid Family and Medical Leave - Summary of Final Regulations**

Massachusetts

**Mintz**

On the heels of the welcome news that employers have three more months to prepare for Massachusetts Paid Family and Medical Leave (“MAPFML”), last...

---

## **Texas Legislature and Courts Clash With Cities Over Mandatory Sick Leave: What Employers Need to Know**

Texas

**Baker & Hostetler LLP**

Dallas has become the third city in Texas, following Austin and San Antonio, to pass a city ordinance requiring private-sector employers to offer...

---

## **National Labor Relations Board Limits Another Union Tactic (US)**

**Squire Patton Boggs**

On June 14, 2019, the National Labor Relations Board (“NLRB”) issued another favorable decision for employers who might find themselves facing union...

---



## **Oregon Adds Employee-Friendly Requirement to Existing Non-Compete Law... But Also Produces Company-Friendly Trade Secrets Law in Recent Court of Appeals Case**

[Oregon](#)

**Seyfarth Shaw LLP**

On May 14, 2019, Oregon Governor Kate Brown signed into law HB 2992, which, as of January 1, 2020, requires an employer to provide a terminated...

---

## **What Do Employers Need to Do to Accommodate Nursing Mothers?**

**Bryan Cave Leighton Paisner LLP**

The types of accommodations needed for nursing mothers is governed by state and municipal law, and, therefore, depends on where a company and its...

---

## **Be Careful, Your Bias is Showing**

**Graydon Head & Ritchey LLP**

Imagine you're a hiring manager. Candidates Chris, Jordan, and Nykesha apply for a job as an executive vice-president with your company. You learn...

---

## **Fox (Mostly) Remains In The Henhouse: SCOTUS Says Agencies (Sort Of) Know Best**

**Fisher Phillips**

By a 9-0 vote, the U.S. Supreme Court ruled today that by and large, the courts should continue deferring to a federal agency's reasonable...

---

## **Democrats Now Want White Collar Exemption Salary Level to Be Much Higher**

**Fox Rothschild LLP**

I blogged last week about the back and forth on the new USDOL proposed salary threshold for exempt status, at approximately \$35,000 per year. Well...

---

## **Substantial Changes Coming to New York Employment Discrimination Laws**

[New](#)

[York](#)

**Ogletree Deakins**

On the last day of the 2019-2020 legislative session, the New York State Senate and Assembly passed an omnibus bill. This legislation, once effective...

---

## **Final HRA regulations create new health coverage options for employers and employees**

**Stinson LLP**

On June 13, 2019 the Department of Health and Human Services, Department of Labor and Department of the Treasury released final regulations that...

---

## **One-Year Statue of Limitations Strictly Enforced in PAGA Suit**

[California](#)

**Hunton Andrews Kurth LLP**

Claims under California's Private Attorneys General Act (PAGA) are recently much in vogue. With the proliferation of arbitration agreements and class...

---

## **Supreme Court: Filing an EEOC Charge Is Not a Jurisdictional Requirement**

**Jones Day**



The Situation: The U.S. Supreme Court unanimously held that filing a charge of discrimination with the Equal Employment Opportunity...

---

### **New York State Legislature Enacts Sweeping Changes to Combat Sexual Harassment**

New York

#### **Sheppard Mullin Richter & Hampton LLP**

On June 19th, the New York State Senate and Assembly voted to pass omnibus legislation greatly strengthening protections against sexual harassment...

---

### **Does Your Arbitration Agreement Include a Carve-Out for Employee Access to the National Labor Relations Board? It Should.**

#### **Vinson & Elkins LLP**

Most employers mandating arbitration agreements as a condition of employment do not intend to prevent employees from filing unfair labor charges with...

---

### **Recreational Marijuana - Insights for Employers**

#### **Dinsmore & Shohl LLP**

On May 31, 2019, the House approved the Cannabis Regulation and Tax Act (Act), legalizing recreational use of marijuana in Illinois. This Act...

---

### **NY Passes Sweeping Employee Wage Lien Bill**

#### **Fox Rothschild LLP**

The New York State Assembly and Senate have passed a bill that would allow employees to obtain liens on their employers' personal and real property...

---

### **Paid Sick Leave in Texas Survives the Texas Legislature**

Texas

#### **Seyfarth Shaw LLP**

Employers in Austin, Dallas, and San Antonio expected the Texas Legislature to overturn their cities' recent foray into...

---

### **"California Dreamin"—Peculiar Laws To Consider When Crossing State Lines**

California

#### **Seyfarth Shaw LLP**

Like the singers in "California Dreamin," many out-of-state employers—on a winter's day and otherwise—might dream of operating in...

---

### **Timely Use It, or Lose It: Recent Supreme Court Case Provides Reminders for Employers, but Employees Still Need to File a Charge Before Filing Title VII Lawsuit**

#### **Bracewell LLP**

In *Fort Bend County, Texas v. Davis* (U.S. June 3, 2019), the U.S. Supreme Court (Court) held that the charge-filing requirement under Title VII of...

---

### **What Employers Can Expect With The EEOC**

#### **Seyfarth Shaw LLP**

As we approach the latter portion of the fiscal year, employers are beginning to see a significant spike in EEOC case filings over...

---

## **Texas Paid Sick Leave Ordinances in State of Confusion - What Are Employers to Do?** Texas

### **Ford & Harrison LLP**

Texas does not require private employers to provide paid sick leave to any employee. However, three major Texas cities - Dallas...

---

## **First Chemical Safety Board Report in Onshore Drilling Accident**

### **Step toe & Johnson LLP**

On June 12, 2019, the US Chemical Safety and Hazard Investigation Board (CSB) issued its first investigation report of an onshore drilling accident...

---

## **Uber Drivers Are Contractors, Not Employees, NLRB Memo Says**

### **Fox Rothschild LLP**

Since the emergence of the "gig economy" in the last decade, courts and government agencies have grappled with the question of whether gig workers...

---

## **Expansive Changes Coming to the New York State Human Rights Law** New York

### **Wilson Elser**

On June 19, 2019, the New York State Legislature passed Senate Bill S.6577, which upon Governor Cuomo's anticipated signature will significantly...

---

## **Changes to Come for Health Plans Due to Trump's Executive Order**

### **Graydon Head & Ritchey LLP**

On June 24, 2019, President Trump issued the "Executive Order on Improving Price and Quality Transparency in American Healthcare to Put Patients First..."

---

## **Confidential and Proprietary Information, and Trade Secrets**

### **Holland & Knight LLP**

A franchise is simply not marketable without intellectual property rights. Confidential, proprietary and trade secret information that is...

---

## **Washington Supreme Court Confirms Higher Standard for Harassment at a "Place of Public Accommodation"** Washington

### **Jackson Lewis PC**

Under the Washington State Law Against Discrimination ("WLAD"), the statute prohibits "places of public accommodation" discriminating against...

---

## **July 1, 2019 Minimum Wage Increases in California Counties and Municipalities**

### **Sheppard Mullin Richter & Hampton LLP**

Many California employees received a raise on January 1, 2019 when the state increased the minimum wage to \$12 per hour for large employers (26...

---

## **How Will SCOTUS' Upcoming Cases Affect Title VII?**

### **Haynsworth Sinkler Boyd PA**

The United States Supreme Court will decide three cases in October 2019 to determine if Title VII of the 1964 Civil Rights Act guarantees protections...



---

## **U.S. DOL Proposes New Joint Employer Test**

### **Holland & Hart LLP**

Employers often struggle to determine whether they might be considered "joint employers" with other entities under the Fair Labor Standards Act...

---

## **Riot games gender discrimination investigation accelerating**

### **Banner Witcoff**

The State of California Department of Fair Employment and Housing made a statement, on Wednesday, June 12th, that it would be progressing forward in...

---

## **The Next Wave? Serial Discrimination Filings from Prior Class Claims**

### **Jackson Lewis PC**

Notwithstanding the employers' victory at the U.S. Supreme Court in Epic Systems Corp. v. Lewis, which made it clear that arbitration and class...

---

## **The Aging Construction Industry: Keeping Skilled Employees Longer**

### **Jackson Lewis PC**

Workers in the construction industry tend to be older than those in other industries, according to the National Association of Home Builders. The...

---

## **Building with Pride: LGBTQ+ Issues**

### **Jackson Lewis PC**

Every year, June is "Pride Month," but LGBTQ+ issues challenge the construction industry year-round....

---

## **U.S. Supreme Court Reaffirms Primacy of Federal Law on Outer Continental Shelf**

### **Holland & Knight LLP**

U.S. Supreme Court reaffirms primacy of federal law on Outer Continental Shelf holding state law may not be adopted where federal law already...

---

## **D.C. Circuit Opinion Rules That Lacrosse Officials in Pennsylvania Are Independent Contractors**

### **Goldberg Segalla LLP**

The D.C. Circuit ruled on June 14, 2019, that lacrosse officials working for the Pennsylvania Interscholastic Athletic Association (PIAA) are...

---

インディアナ州の従業員は制服を着ていますか？ インディアナ州法の改正により 雇用主は制服の貸与に掛かる費用を従業員の給与から控除できるかもしれませんよ！

### **Masuda Funai Eifert & Mitchell Ltd**

Executive Summary Effective May 1, 2019, Indiana employers may deduct from an employee's paycheck the cost of renting uniform shirts, pants and...

---

## **New York City Considers Mandatory Vacation Time Law**

### **Manatt Phelps & Phillips LLP**

The New York City Council's Committee on Civil Service and Labor has proposed

a bill that would require New York City employers with five (5) or more...

---

### **Google: Demonstrating The Hazards Of Employment Discrimination From Every Angle**

**Seyfarth Shaw LLP**

Google's recent travails with simultaneous traditional and "reverse" discrimination claims signal a new era of dynamic employment discrimination risk...

---

### **Don't Know What You Got (Till It's Gone): Is OSHA Required to Give Managers and Supervisors Their Rights Before Interviewing Them?**

**Fisher Phillips**

When an inspector from the Occupational Safety and Health Administration (OSHA) shows up at your workplace, know this: everything&mdash;and we mean...

---

### **How to Navigate the Dallas and San Antonio Paid Sick Leave Ordinances** Texas

**Carrington Coleman**

Dallas and San Antonio recently passed city laws mandating paid sick leave. The status of these municipal ordinances remains unclear. That is because...

---

### **June's Notable Cases and Events in E-Discovery**

**Sidley Austin LLP**

This Sidley Update addresses the following recent developments and court decisions involving e-discovery issues...

---

### **Applicants may be required to declare citizenship status when filing for Ohio workers' compensation benefits** Ohio

**Porter Wright Morris & Arthur LLP**

The Ohio House of Representatives passed a two year \$645 million Workers' Compensation budget on June 5, 2019. As part of the budget bill, a...

---

### **Beltway Buzz, June 21, 2019**

**Ogletree Deakins**

Late last week, the National Labor Relations Board issued a decision involving the balancing of employees' statutory...

---

### **New York Extends Pay Equity Act to All Protected Classes** New York

**Mintz**

The New York State Legislature has passed an amendment to New York's Achieve Pay Equity Act (the "Act"), which will prohibit pay discrimination...

---

### **New York City to Prohibit Retaliation for Requesting Reasonable Accommodation** New York

**Jackson Lewis PC**

On June 13, 2019, the New York City Council passed Intro 799 to prohibit retaliation against individuals who make a request for a reasonable...

---



## **Dallas Enacts Paid Sick Leave Law**

### **Fox Rothschild LLP**

Dallas employers will soon be obligated to provide paid sick leave to eligible employees. Under the city's new ordinance, businesses with more than...

---

## **From the East to the West, Does Arbitration in Missouri Reign Best? Missouri Courts Uphold and Invalidate Arbitration Agreements**

Missouri

### **Baker Sterchi Cowden & Rice LLC**

This past May, the Missouri Supreme Court, Missouri Court of Appeals, and both United States District Courts in Missouri analyzed the validity and...

---

## **Court: Employers Can't Stall Subpoenas to Run out OSHA's Enforcement Clock**

### **Ogletree Deakins**

Employers consider many factors when choosing whether to challenge investigatory subpoenas. They now have an additional consideration: whether a...

---

## **New York Adopts Laws Aimed at Combating Salary Inequality and Race Discrimination**

New York

### **Jackson Lewis PC**

In the final days of its 2019 Session, the New York State Legislature passed three bills that, respectively, will bar employers from inquiring about...

---

## **New York State Legislature Passes Major Amendments To Anti-Discrimination and Anti-Harassment Laws**

New York

### **Seyfarth Shaw LLP**

The New York State Legislature has passed, and Governor Andrew M. Cuomo is expected to sign, a bill amending the state's...

---

## **Keep Out: NLRB Allows Further Restrictions of Union Access to Employers' Property**

### **Fox Rothschild LLP**

In a June 14, 2019 decision, the National Labor Relations Board clarified whether an employer may limit nonemployee union organizers from entering the...

---

## **Environment & Climate Change**



## **Another Study Finds Popular Cereals and Snack Products Contain Traces of Glyphosate**

### **Goldberg Segalla LLP**

The Environmental Working Group (EWG) - a consumer products testing and environmental advocacy organization - recently commissioned a new round of...

---

## **EDF Publishes Report On Trump EPA's Implementation Of The Lautenberg Act**

### **Bergeson & Campbell PC**

The Environmental Defense Fund (EDF) announced on June 17, 2019, a report entitled Toxic Consequences: Trump's attacks on Chemical Safety put our...

---



**Expanded A-901 Requirements Coming Soon? Sales Persons, Consultants and Soil Recyclers Should Prepare** [New Jersey](#)

**Riker Danzig Scherer Hyland & Perretti LLP**

There are extensive regulations in New Jersey governing businesses involved in the solid waste and recycling industries. Many people do not realize...

---

**New York State Passes Sweeping Climate Legislation That Could Affect Nearly All Sectors** [New York](#)

**Beveridge & Diamond PC**

The New York State Assembly and Senate this week passed one of the most sweeping pieces of climate change legislation in the United States and beyond...

---

**Supreme Court Decision Expands Scope of FOIA's Exemption for Confidential Information, with Significant Implications for EPA**

**Covington & Burling LLP**

The Supreme Court's June 24 decision in Food Marketing Institute v. Argus Leader Media has significantly expanded the confidential commercial...

---

**Monthly Update for April 2019**

**Bergeson & Campbell PC**

WEBINAR -- FIFRA Hot Topics In Pesticide, Biocides, And Other Agricultural Chemicals Regulation And Litigation, April 24, 2019, 1:00 p.m. - 2:00 p.m...

---

**NC Politics in the News- Jun 24, 2019** [North Carolina](#)

**McGuireWoods Consulting LLC**

Legislation designed to further develop North Carolina's fast-growing hemp industry, increase agritourism and make overhauling open-air waste storage...

---

**California Prop. 65 Regulation Exempts Certain Coffee Chemicals From Cancer Warning; Stay in Coffee Case Lifted** [California](#)

**Bryan Cave Leighton Paisner LLP**

California's Office of Environmental Health Hazard Assessment ("OEHHA") has finalized a highly anticipated Proposition 65 regulation relating to...

---

**US Bankruptcy Court Finds that CERCLA § 104(e) Request and National Priority Listing Do Not Constitute "Claims" Under New York Law** [New York](#)

**Beveridge & Diamond PC**

Buyers and sellers of contaminated properties will want to take note of the June 3, 2019 ruling from the U.S. Bankruptcy Court for the Northern...

---

**Commonwealth Court Upholds Environmental Hearing Board's Denial of Sierra Club's Fee Petition in Third-Party Permit Challenge** [Pennsylvania](#)

**Manko Gold Katcher & Fox**

On June 11, 2019 the Commonwealth Court of Pennsylvania upheld a decision by the Pennsylvania Environmental Hearing Board ("EHB") denying the Sierra...

---

## **New York State Climate Leadership and Community Protection Act** New York

### **Bryan Cave Leighton Paisner LLP**

On June 20, 2019, the New York State legislature enacted the Climate Leadership and Community Protection Act. Governor Andrew Cuomo is expected to...

---

## **EPA Proposes Regulation of Designated PBT Chemical Substances**

### **Keller and Heckman LLP**

On June 21, 2019 the U.S. Environmental Protection Agency (EPA) released a pre-publication copy of a proposed rule under section 6(h) of the Toxic...

---

## **Not So Cooperative Federalism? Washington Sues EPA Over Reversal in Long Running Human Health Criteria Saga** Washington

### **Beveridge & Diamond PC**

On June 6, Washington filed a lawsuit challenging EPA's May 10, 2019, decision to reverse its 2016 disapproval of Washington's proposed Human Health...

---

## **Environmental Considerations in Corporate Transactions**

### **Robinson & Cole LLP**

My partner Bob Melvin and I recently gave a presentation on environmental, health, and safety considerations in mergers and acquisitions. While it...

---

## **EPA Publishes Proposed PBT Chemicals Rule under TSCA**

### **Bergeson & Campbell PC**

The U.S. Environmental Protection Agency released on June 21, 2019, a proposed rule intended to reduce exposures to certain chemicals that are...

---

## **New Jersey Advances Clean Energy Agenda** New Jersey

### **Morgan Lewis**

New Jersey advanced several of the Murphy administration's Clean Energy goals during June 2019. Over the past month, the state released a draft of...

---

## **Energy & Infrastructure Insight- Summer 2019**

### **Shearman & Sterling LLP**

Masdar and Bee'ah are developing the Sharjah Project on a 50/50 basis, with Bee'ah supplying municipal solid waste (MSW) and Sharjah Electricity and...

---

## **Three New EPA Rules Will Affect Utility Coal Plants and State Resource Planning**

### **Morgan Lewis**

The US Environmental Protection Agency (EPA) issued three rules on June 19 that may give utilities new reasons to consider investing in certain plant...

---

## **EPA Issues Final Guidance for States for Consideration of PM2.5 Precursors**

### **Katten Muchin Rosenman LLP**

On May 30, 2019, the U.S. Environmental Protection Agency (EPA) issued a final memorandum on fine particulate matter (PM2.5) precursor demonstration...

---



## **Why EPA's Clean Water Act Section 401 Guidance Will Have No Practical Impact on Pipeline Projects**

### **Holland & Knight LLP**

The U.S. Environmental Protection Agency (EPA) recently announced the rollout of its new Clean Water Act Section 401 Guidance for Federal Agencies...

---

## **Monthly Update for May 2019**

### **Bergeson & Campbell PC**

Registration Now Open For "TSCA: Three Years Later": Bergeson & Campbell, P.C. (B&C®), the Environmental Law Institute (ELI), and the George...

---

## **U.S. EPA Region IV Proposes Alternative Policy for Exemptions During Startup, Shutdown and Malfunction Events: Five Things You Need to Know**

### **Sidley Austin LLP**

On June 5, 2019, the United States Environmental Protection Agency's (EPA) Region IV proposed an alternative startup, shutdown and malfunction (SSM)...

---

## **Monthly Update for June 2019**

### **Bergeson & Campbell PC**

EPA Issues Draft Revised Method For ESA Pesticide Assessments: On May 16, 2019, the U.S. Environmental Protection Agency (EPA) announced that it was...

---

## **The State AG Report Weekly Update June 20, 2019**

### **Cozen O'Connor**

California AG Xavier Becerra filed a lawsuit against country club owners and operators ClubCorp Holdings, Inc., ClubCorp Club Operations, Inc., CCA...

---

## **New EPA Rules Could Impact Decisions on US Generation Mix**

### **Morgan Lewis**

The Environmental Protection Agency (EPA) issued three rules on June 19, granting additional powers to states to determine their projected energy...

---

## **New York Food Waste Law Unlocks Economic Opportunity**

New York

### **Riker Danzig Scherer Hyland & Perretti LLP**

New York Food Waste Law Unlocks Economic Opportunity: State-level initiatives are essential to reducing food...

---

## **Mobile Sources Face an Increased Risk of Agency Enforcement and Citizen Suits**

### **Squire Patton Boggs**

On June 12, 2019, the US Environmental Protection Agency (US EPA) announced its seven enforcement and compliance assurance priority areas for fiscal...

---

## **E&S Disclosure Trends in SEC Filings 2018 - 2019**

### **White & Case LLP**

In light of the increased spotlight on environmental, social and governance ("ESG") disclosures, White & Case's Public Company Advisory Group...

---

## **The Impact the New Prop 65 Warning Regulations on Multi-Family Apartments and Other Prop 65 Updates**

California

### **Buchalter**

There have been recent developments in the enforcement of the California Safe Drinking Water and Toxic Enforcement Act of 1986 (also known as...

---

## **Trump Administration Issues Affordable Clean Energy Rule**

### **Wilmer Cutler Pickering Hale and Dorr LLP**

On June 19, 2019, the Environmental Protection Agency (EPA) released a final rule repealing the Obama-era "Clean Power Plan" (CPP) and replacing it...

---

## **PHMSA Seeks Public Comment on LNG by Rail Assessment**

### **Holland & Knight LLP**

On June 6, 2019, the Pipeline and Hazardous Materials Safety Administration of the U.S. Department of Transportation (PHMSA) announced the...

---

## **Danger or opportunity - why facing up to climate change makes business sense**

### **Lexology**

"Of all risks, it is in relation to the environment that the world is most clearly sleepwalking into catastrophe." You might be forgiven for thinking...

---

## **Fifteen States and State Associations Comment on EPA's Draft PFAS Guidance**

### **Holland & Knight LLP**

In the latest development in the federal government's efforts to develop a framework for addressing groundwater contaminated with perfluorooctanoic...

---

## **Democratic Senators Call on EPA to "Stop Undermining Key Chemical Safety Law"**

### **Bergeson & Campbell PC**

On June 20, 2019, Senators Tom Udall (D-NM), Cory Booker (D-NJ), Ed Markey (D-MA), Jeff Merkley (D-OR), and Sheldon Whitehouse (D-RI) sent a letter...

---

## **Changes Being Proposed to Washington's Industrial Stormwater Permit**

Washington

### **Davis Wright Tremaine LLP**

On May 1, 2019, the Washington State Department of Ecology published a draft of the new Industrial Stormwater General Permit (New Permit), asking for...

---

## **Environmental Groups Seek Protection for Mountain Lions in Southern California**

California

### **Nossaman LLP**

The Center for Biological Diversity and Mountain Lion Foundation submitted a petition to the California Fish and Game Commission (the "Commission")...

---

## **Court hears oral argument in case challenging EPA's prioritization and risk evaluation rules**



### **Bergeson & Campbell PC**

On May 16, 2019, the U.S. Court of Appeals for the Ninth Circuit heard oral arguments in a case filed by non-governmental organizations (NGO)...

---

### **Bipartisan Senate Efforts to Mandate Agencies Address Growing PFAS Crisis**

#### **Barnes & Thornburg LLP**

As more than two dozen federal legislative proposals to address PFAS elbow their way through the halls of Congress, the Senate is likely to pass the...

---

### **Rewetting the Ink on Washington's Industrial Stormwater General Permit: Significant Modifications Coming Down the Pipes**

Washington

#### **Beveridge & Diamond PC**

The Washington Department of Ecology (Ecology) released the draft 2020 Industrial Stormwater General Permit (ISGP) for public comment. The draft...

---

### **EPA Repeals Obama Administration's Power Plant CO2 Regulations and Issues Narrower Replacement Rule**

#### **Crowell & Moring LLP**

On June 19, 2019, EPA signed the final Affordable Clean Energy (ACE) Rule, addressing the emission of carbon dioxide and other greenhouse gases...

---

### **D.C. Circuit Says NEPA Requires FERC To Inquire Into Up and Downstream Effects of Pipeline Project**

#### **Sheppard Mullin Richter & Hampton LLP**

In a recent opinion, the D.C. Circuit suggested the Federal Energy Regulatory Commission (FERC) must attempt to obtain information necessary to...

---

### **EPA's New National Compliance Initiatives Reflect Shifting Enforcement Priorities and Methods**

#### **Sidley Austin LLP**

The U.S. Environmental Protection Agency's (EPA) enforcement office has announced its national...

---

### **6 Things to Know about EPA's Final ACE Rule**

#### **Latham & Watkins LLP**

In a significant and potentially precedent-setting action, EPA terminates the Clean Power Plan, narrows the scope of required controls to the...

---

### **Solar Energy Providers Should Protect Their Investments with Advanced DC Monitoring**

#### **Frost Brown Todd LLC**

As the scale of solar energy projects grows, the incorporation of advanced direct current (DC) monitoring into solar power systems becomes...

---

### **U.S. Senators Introduce Bipartisan Act Aiming To Increase Small Refinery Exemptions Transparency**

#### **Bergeson & Campbell PC**



On June 14, 2019, U.S. Senators Deb Fischer (R-NE) and Tammy Duckworth (D-IL) introduced the Renewable Fuel Standard (RFS) Integrity Act of 2019. This...

---

### **U.S. Forest Service Proposes to Revise NEPA Regulations**

#### **Beveridge & Diamond PC**

On June 13, 2019, the U.S. Forest Service issued a proposed rule to revise its regulations (36 CFR part 220) implementing the National Environmental...

---

### **US Forest Service Proposes NEPA Streamlining Rule: Implications for the Outdoor Recreation Industry**

#### **Wilmer Cutler Pickering Hale and Dorr LLP**

On June 13, the US Forest Service announced a proposal to streamline environmental review of proposed projects on National Forest System land.1 The...

---

### **New Jersey Legislature Passes Amendments to Site Remediation Reform Act**

New Jersey

#### **Manko Gold Katcher & Fox**

The Site Remediation Reform Act (SRRA), enacted in 2009, transformed the site remediation process in New Jersey through the creation of the licensed...

---

### **Washington Clean Energy Transformation Act Establishes Aggressive Mandates for Grid Decarbonization and Renewable Energy Production**

Washington

#### **Beveridge & Diamond PC**

After several years of fruitless effort, Washington's 2019 legislature passed and Governor Inslee signed the Washington Clean Energy Transformation...

---

## **Internet & Social Media**



**Privacy FAQs: If a company receives a right to be forgotten request, is it required to delete records that show whether an individual opted-in or opted-out from marketing?**

California

#### **Bryan Cave Leighton Paisner LLP**

The California Consumer Privacy Act ("CCPA") was enacted in early 2018 as a political compromise to stave off a poorly drafted, and plaintiff's...

---

### **Ninth Circuit Follows Fourth Circuit in Finding TCPA 'Debt Collection' Exemption Unconstitutional**

#### **Manatt Phelps & Phillips LLP**

Adding more fuel to an already raging fire, the Ninth Circuit has weighed in on a case that has the potential to make its way to the U.S. Supreme...

---

### **A Single Prior Art Reference Can Render a Patent Obvious**

#### **Knobbe Martens**

Game and Technology Co., Ltd. ("GAT") owns a patent directed to a method of customizing internet game characters in online games. Activision sought...

---

## **Nevada's Amended Privacy Law: Groundbreaking or More of the Same?**

Nevada

### **Sheppard Mullin Richter & Hampton LLP**

Nevada recently amended its existing online privacy law to give Nevada residents the ability - in certain circumstances - to opt out of the sale of...

---

## **After Months of Rumors, Facebook Officially Announces New Libra Cryptocurrency**

### **Blank Rome LLP**

Social networking giant Facebook has unveiled plans for a global digital currency, which the company hopes will "transform the global economy" by...

---

## **Benefit of the but-for bargain: Assessing economic tools for data privacy litigation**

### **Edgeworth Economics**

A theory of harm frequently asserted in data breach class actions is that plaintiffs did not receive the "benefit of the bargain" with defendants...

---

## **FBI Warns of Cybercrimes Targeting Seniors**

### **Duane Morris LLP**

World Elder Abuse Awareness Day took place last week on June 15. This Awareness Day highlights how older populations are vulnerable to various forms...

---

## **Implications from New Hampshire Lottery Commission v. Barr**

### **Hogan Lovells**

In a recent decision that inures to the benefit of the online gambling industry, a federal district court in New Hampshire held that the "the text...

---

## **另一种角度解读 个人信息出境安全评估办法（征求意见稿）**

### **AnJie Law Firm**

2019年6月13日，国家互联网信息办公室（以下简称"网信办"）发布通知对 个人信息出境安全评估办法（征求意见稿）（以下简称"征求意见稿"）公开征集意...

---

## **Overview of Blockchain Technology and US Blockchain Law**

### **Wolters Kluwer Legal & Regulatory**

In the past decade, blockchain technology has gone mainstream. It has rapidly evolved from a few Bitcoin software nodes in January 2009 to a...

---

## **CARU Takes Action Against Two More Mobile Apps**

### **Sheppard Mullin Richter & Hampton LLP**

We recently wrote about the Children's Advertising Review Unit's privacy-related enforcement against two mobile apps for children on our Eye on...

---

## **Nevada Amends Online Privacy Law to Add New Consumer Opt-Out Rights**

Nevada

### **Loeb & Loeb LLP**



Nevada recently amended its data privacy laws to provide consumers with greater protections. Nevada Senate Bill 220, which amends the existing Nevada...

---

**Recommended Practices to Detect Unauthorized Access on Company Networks**  
**Manatt Phelps & Phillips LLP**

The cyber threat landscape is continually evolving. Cybercriminals are using new and sophisticated methods to gain unauthorized access to networks...

---

**Just Ahead of CCPA, Ad Agency Fails to Secure Leads Data** California  
**Frankfurt Kurnit Klein & Selz PC**

An Internet advertising agency that specializes in lead generation for law firms failed to properly secure databases that included the records of...

---

**Judge Ramos: Text Message Exchange Doesn't Satisfy Writing Requirement of Statute of Frauds** New Jersey

**Steptoe & Johnson LLP**

In an opinion yesterday, Judge Ramos ruled that a real estate broker could not recover a commission because the agreement was not in writing as...

---

**Sen. Blumenthal Seeks FTC Action on Detox Teas, Influencers**

**Manatt Phelps & Phillips LLP**

Sen. Richard Blumenthal (D-Conn.) is calling on the Federal Trade Commission (FTC) to take a closer look at influencers, in a new letter in which he...

---

**FERC and NERC Advance Dramatically Expanded Mandatory Cybersecurity Reporting Standards**

**Holland & Knight LLP**

New Federal Energy Regulatory Commission (FERC) rule mandates new wide-ranging cybersecurity reporting standards in CIP 008-6. Mandatory reporting is...

---

**Privacy Report: Three Dating Apps Removed from App Store After Potential COPPA Violations**

**Arent Fox LLP**

Three dating apps—Meet24, FastMeet, and Meet4U, all operated by Wildec LLC—have been removed from Apple's App Store and Google's Google Play Store...

---

**Yoga Influencers' Disclosures Show Limits of Flexibility**

**Kelley Drye & Warren LLP**

The Electronic Retailing Self-Regulation Program (or "ERSP") recently announced a decision involving Alo Yoga's influencer campaign. The decision...

---

**Who's that bot? California requires clear disclosure starting 7/1/2019** California

**DLA Piper**

Starting July 1, 2019, California will require clear and conspicuous disclosures when bots are used to communicate or interact online with people in...

---

**California Court Finds Section 230 Protects Decision to Suspend and Ban Twitter**

## **Account**

### **Morrison & Foerster LLP**

A California Superior Court's recent ruling in *Murphy v. Twitter* held that Section 230 of the Communications Decency Act shielded Twitter from...

---

## **Facebook Rolls Out Political Advertising Tools Globally**

### **Frankfurt Kurnit Klein & Selz PC**

Yesterday, Facebook announced that it is rolling out, globally, transparency tools for advertisers who want to place political and issue-related...

---

## **Congress: Week in Review | June 20, 2019**

### **McGuireWoods Consulting LLC**

Canadian Prime Minister Justin Trudeau is in Washington today for separate meetings with the President, Senate Majority Leader Mitch McConnell (R-KY)...

---

## **Short-Term Rental Update: Disney works its magic for short-term rentals; Airbnb educates Seattle's short-term rental community**

### **Garvey Schubert Barer**

The Anaheim City Council is reversing its 2016 ban on short-term rentals after seemingly...

---

## **Lessons from the Lawsuit That Could Shake Up the Esports Industry**

### **Arent Fox LLP**

The esports industry has been rapidly growing since its inception in the 1990's. Viewership numbers for esports championship games exceed that of the...

---

## **What is Your Family Office Doing to Protect Itself From Security Threats? (Part II)**

### **McGuireWoods LLP**

Welcome back to our three-part series examining vulnerabilities surrounding family offices and steps they can take to mitigate those risks. In Part...

---

## **Tap Into Your Jurors' Reward System**

### **Holland & Hart LLP**

Next time you're in a public place, look around at all the people and what they're doing. Looking at their phones? Yes! Nearly all of them. Now, some...

---

## **Locksmiths Locked Out: Court Affirms Immunity for Use of Tools That Portray Third-Party Content Pictorially or as an Aggregate Metric**

### **Proskauer Rose LLP**

In the past few months, there have been a number of notable decisions affirming broad immunity under the Communications Decency Act (CDA), 47 U.S.C...

---

## **Let Americans break up Big Tech**

### **McCann FitzGerald**

Calls to break-up Big Tech grow louder. In recent weeks Chris Hughes, Facebook's co-founder, argued in a New York Times oped that it's time to break...



---

## Legislators Propose Narrowing § 230's Protections

### Morrison & Foerster LLP

As we have frequently noted on Socially Aware, Section 230 of the Communications Decency Act protects social media sites and other online platforms...

---

## Emerging Technologies Washington Update- Jun 20, 2019

District of Columbia

### McGuireWoods Consulting LLC

This Week: Senate Commerce Subcommittee convenes drone security hearing, Hawley introduces plan to amend Section 230, Senate Commerce Committee...

---

## Maine and Nevada's New Data Privacy Laws and the California Consumer Privacy Act Compared

California

Maine

Nevada

### Baker McKenzie

Selling or trading personal information -- a common practice in the adtech industry -- is increasingly under regulatory scrutiny and legislators...

---

## State Privacy Laws Continue to Proliferate

Maine

Nevada

New York

### Manatt Phelps & Phillips LLP

States continue to push forward with privacy laws, with new statutes in Nevada and Maine and a proposal currently pending in New York, which would...

---

## Browsewraps Could Be Enforced

California

### Sycamore Legal PC

The Tech Contracts Handbook warns website operators not to rely on browsewraps: contracts posted online without a click-to-agree requirement. In fact...

---

## California's Law Regulating Online Bots, Effective July 1, 2019

California

### Baker & Hostetler LLP

California's new "bot" law, Cal. Bus. & Prof. Code § 17940, et seq. (SB 1001) takes effect on July 1, 2019. This means that any company or individual...

---

## What is Your Family Office Doing to Protect Itself From Security Threats? (Part III)

### McGuireWoods LLP

Welcome back to our three-part series examining cyber vulnerabilities surrounding family offices and steps they can take to mitigate those risks. In...

---

## "Gonna stand my ground; And I won't back down" - The OPC charges forward with its controversial consultation on transborder dataflows/transfers for processing

### McMillan LLP

On June 11, 2019, the Office of the Privacy Commissioner of Canada ("OPC") published a reframed discussion document (the "Reframed Discussion")...

---



### **District Court Finds Use of Third-Party Hashtags Created Implied Association** **Hunton Andrews Kurth LLP**

Social media can be a minefield of intellectual property issues. The hashtag, for example, began as a searching tool, but now has evolved into its...

---

### **USTR Creates Website for Navigating the China Section 301 Tariff Process** **Thompson Hine LLP**

The Office of the U.S. Trade Representative (USTR) has created a website to assist persons in navigating the China Section 301 investigation and...

---

### **Customs + Border Patrol Vendor's Network Compromises Images and License Plate Data**

**Robinson & Cole LLP**

The United States Customs and Border Patrol (CBP) admitted last week that personal information that it collected from travelers crossing the U.S...

---

### **States Limit Employer Access to Employee Social Media and Other Internet Accounts**

**Frost Brown Todd LLC**

The U.S. State Department recently implemented a policy requiring visa applicants to submit information about any social media usernames, handles, and...

---

## **Legal Practice**



### **Source And Choice Of Privilege Law In Diversity Cases — Part III**

**McGuireWoods LLP**

The last two Privilege Points (Part I and Part II) addressed federal courts' identification of and choice of the appropriate state's privilege law in...

---

### **KTalks**

**Kilpatrick Townsend & Stockton LLP**

Welcome to our second KTalks. This series reaches out to leaders in the business and legal communities with five questions to seek their insight on...

---

### **Making Sense of the “Ethics” of Litigation Finance**

**Validity Finance**

Imagine you are a lawyer and a small business owner seeks your representation. She has a strong breach of contract claim against a supplier—but she...

---

### **Pennsylvania Expands Attorney Work-Product Protection for Disclosures to Third Parties**

**Pennsylvania**

**Pepper Hamilton LLP**

The Pennsylvania Supreme Court has adopted a new, expanded standard for preserving the protections of the attorney work-product doctrine, codified at...

---

### **NJ lawyer suspended for make-believe FINRA arbitration, hiding default against**

**firm** New Jersey

### **Thompson Hine LLP**

A New Jersey lawyer was suspended for six months for misrepresenting to clients for about eight years that their arbitration matter “was proceeding...

---

### **SCOTUS Overrules “State Compensation” Ripeness Requirement for Takings Claims**

#### **Robinson & Cole LLP**

Today, the United States Supreme Court issued its long-awaited decision in *Knick v. Township of Scott*. In a 5-4 decision, the Court overruled the...

---

### **Bringing contracts into the digital age**

#### **ThoughtRiver Ltd**

How Lexible, the universal contract language, is disrupting more than 1,000 years of legal contracts...

---

### **One Way to Waive an Attorney-Client Communication** Delaware

#### **Commonsense Construction Law LLC**

The judge’s decision on an injunction hearing provides a cautionary tale for attorneys preparing a privilege log. The underlying case arose when...

---

### **Finding "The One": Perspectives on Hiring a Divorce Attorney**

#### **Foster Swift Collins & Smith PC**

Divorce is an unpleasant experience for most, but a positive attorney-client relationship can ease the burden. Thoughtful, competent representation...

---

### **Using Computer-Assisted Billing to Find the Elusive Reasonable Fee**

#### **EffortlessLegal**

What is a “reasonable fee”? Articulating a concise yet all-encompassing definition is much more difficult than relying on Supreme Court Justice Potter...

---

## **Projects & Procurement**



### **OH SNAP! Supreme Court Rejects Substantial Competitive Harm Test For Key FOIA Exemption**

#### **Sheppard Mullin Richter & Hampton LLP**

On June 24, 2019, the Supreme Court ruled that Exemption 4 of the Freedom of Information Act (“FOIA”), which protects from public disclosure “trade...

---

### **Private Equity, Venture Capital, and Hedge Funds May Get Boost from SEC**

#### **Kilpatrick Townsend & Stockton LLP**

On June 18th, the SEC issued a Concept Release (the “Concept Release”) seeking public comment on ways to simplify, harmonize, and improve the rules...

---

### **Supreme Court Shakes Up FOIA Exemption for Confidential Information**

#### **Covington & Burling LLP**

On Monday, the Supreme Court significantly altered how government agencies



will treat confidential commercial information protected from disclosure by...

---

## **Investments in Renewable and Conventional Power Projects in Qualified Opportunity Zones**

### **King & Spalding LLP**

The Qualified Opportunity Zone rules under Section 1400Z of the Internal Revenue Code permit certain investors to realize substantial tax benefits if...

---

## **Maine Enacts New Law to Encourage Net Metering and Long-Term Contracts for Distributed Generation**

Maine

### **Pierce Atwood LLP**

Today, Governor Janet Mills signed new legislation to broaden customer access to net metering (known in Maine as net energy billing, or NEB) and to...

---

## **A New Frontier: ASBCA Issues First Ever CPAR Decision on the Merits**

### **Crowell & Moring LLP**

On June 3, 2019, the ASBCA published its first ever decision addressing the merits of a CPAR evaluation - i.e., whether CPAR ratings were "fair and...

---

## **World Bank Debars Chinese Engineering Company for Fraudulent Bidding Practices in Connection With Liberian Infrastructure Project**

### **Pepper Hamilton LLP**

On June 12, 2019, the World Bank announced that China-based Dongfang Electronics Co. Ltd. ("Dongfang") would be debarred for fifteen (15) months for...

---

## **DOE to Prohibit Contractors from Technical Collaboration with Certain Foreign Governments**

### **Morgan Lewis**

The US Department of Energy (DOE) issued Order No. 486.1 on June 7 prohibiting DOE employees and contractors from participating in the foreign...

---

## **Payers, Providers, and Patients - Oh My!: FCA Dismissals Under the Granston Memo**

Audio

### **Crowell & Moring LLP**

Payers, Providers, and Patients - Oh My! Is Crowell & Moring's biweekly health care podcast, discussing legal and regulatory issues that affect health...

---

## **NIST Announces and Seeks Public Comment on 800-171 Update and Related Documents**

### **Covington & Burling LLP**

On June 19, 2019, the National Institute of Standards and Technology ("NIST") announced the long-awaited update to Special Publication ("SP") 800-171...

---

## **Contractors' Cybersecurity Violations Potentially Actionable Under False Claims Act**

California

### **Bradley Arant Boult Cummings LLP**

A federal district court in California recently allowed a relator's False Claims Act

lawsuit against two federal contractors to proceed where the...

---

**Court of Federal Claims Disallows Section 1603 Grant for Development Fees**  
**Troutman Sanders LLP**

Attached are two decisions from the United States Court of Federal Claims, California Ridge Wind Energy LLC, v. United States of America, No. 14-250 C...

---

**Nota Bene Episode 39: Doing Business with the U.S. Government in an Era of Cybersecurity, Espionage and Executive Orders with Townsend Bourne** [Audio](#)  
**Sheppard Mullin Richter & Hampton LLP**

In an era of trade wars, espionage, and executive orders, how can companies who wish to dive into government procurement or are already involved in...

---

**FERC Approves Formula Rate and Transmission Incentives to Transmission-Only Company That Won Order No. 1000 Solicitation**  
**Troutman Sanders LLP**

On June 11, 2019, FERC accepted Republic Transmission LLC's ("Republic") proposed transmission formula rate ("Formula Rate") that will be incorporated...

---

**CMS Updates PACE Regulations on Elderly Care**  
**Greenberg Traurig LLP**

The Centers for Medicare & Medicaid Services (CMS) recently made several substantive and technical updates to the Programs of All-Inclusive Care for...

---

**Contractor's Challenge to Cost Accounting Regulation Hits Headwinds**  
**Crowell & Moring LLP**

On May 29, 2019, the U.S. Court of Federal Claims dismissed Boeing's complaint against the government, rejecting claims that the Defense Contract...

---

**New Green Bond Guidance Complements Existing Green Bond Principles**  
**Latham & Watkins LLP**

The Executive Committee for the Green Bond Principles recently published three documents providing key guidance complementing the Green Bond...

---

**National P3 Update: Water and Sewer Infrastructure**  
**Bilzin Sumberg**

We recently provided an update on the status of higher-education and social-infrastructure projects being delivered under the P3 model. This update...

---

**Third Circuit Provides Defense for FCA Claims Concerning Pre-2010 Conduct**  
**Pepper Hamilton LLP**

On June 18, the Third Circuit affirmed a District of Delaware decision dismissing a False Claims Act (FCA) case against Medco Health Solutions, Inc...

---

**Louisiana Business Pleads Guilty to \$48 Million Fraudulent Medical Reimbursement Scheme** [Louisiana](#)  
**Arent Fox LLP**



Louisiana-based company The Total Financial Group, Inc. ("TTFG") and its principles entered a guilty plea to a scheme involving a multiple employer...

---

### **Challenging a CPARS Rating at a Board of Contracts Appeals**

#### **Taft Stettinius & Hollister LLP**

Government contractors have long been able to challenge Contract Performance Assessment Reporting System (CPARS) ratings to the contracting officer...

---

### **Return Mail May Make COFC More Attractive To Patent Holders**

#### **Baker & Hostetler LLP**

In 2011 the Leahy-Smith America Invents Act created three new types of post-issuance...

---

Public



### **U.S. House Votes to Approve Measure Blocking Feds from Interfering with State Cannabis Laws**

#### **Wilson Elser**

On June 20, 2019, the House of Representatives passed a bipartisan amendment by a 267&minus;165 vote that would protect state-legal cannabis programs...

---

### **New Gainful Employment Program Disclosure Requirements Take Effect July 1, 2019**

#### **Drinker Biddle & Reath LLP**

After earlier delays in implementation, the U.S. Department of Education (the Department) has instructed postsecondary education institutions that...

---

### **OMB Releases Spring 2019 Unified Agenda of Regulatory Actions**

#### **Hogan Lovells**

The Office of Management and Budget (OMB) recently released the Spring 2019 Unified Agenda of Regulatory Actions, which outlines the rulemaking...

---

### **Financial Companies Should Review SCRA and MLA Requirements to Avoid Costly Issues**

#### **Holland & Knight LLP**

Israeli companies that want to do business in the U.S. and have business models based on, or include, lending money or other financial transactions...

---

### **Bill of Rights, Part 2: Religion and Expression**

Audio

#### **Patterson Belknap Webb & Tyler LLP**

Early colonists try to balance religious liberty with established state churches. John Peter Zenger goes to trial and suffers a pyrrhic loss. The...

---

### **New Law Makes Minor Changes to Indiana Uniform Commercial Code**

Indiana

#### **Barnes & Thornburg LLP**

On May 1, 2019, the Indiana State Legislature passed House Bill 1487 (HB 1487), which includes several minor changes to the Indiana Uniform...



---

## **Presidential Race Update: June 2019** [Audio](#)

### **Brownstein Hyatt Farber Schreck LLP**

With the first presidential debate nearly upon us, 20 Democratic candidates are about to present their policy platforms to a national audience. Drew...

---

## **Supreme Court Clarifies Broad Interpretation of FOIA Exemption for Confidential Commercial Information**

### **Sidley Austin LLP**

In a very significant FOIA decision for business, Food Mktg. Inst. V. Argus Leader Media, decided on June 24, 2019, the Supreme Court reversed 45...

---

## **Health Care in the Democratic Presidential Debates**

### **Brownstein Hyatt Farber Schreck LLP**

Health care—what to do next, and how to do it—is likely to be a flash point in the first debates of the 2020 Democratic presidential nomination...

---

## **Bill of Rights, Part 3: Military Amendments** [Audio](#)

### **Patterson Belknap Webb & Tyler LLP**

The Patterson team discusses the English and colonial antecedents of the Second Amendment, the fear of standing armies motivating its proposal, and...

---

## **Landmark Supreme Court ruling on FOIA protection favors business**

### **Hogan Lovells**

Yesterday, 24 June 2019, the U.S. Supreme Court issued a landmark decision, Food Mktg. Inst. v. Argus Leader Media, 139 S. Ct. 915 (2019), that...

---

## **Elder Abuse and Red Flags**

### **Holland & Knight LLP**

With the aging population and signs that elder abuse is on the rise, it seems that now is a time to provide a reminder of some red flags that could...

---

## **Next Week in Congress- June 21, 2019**

### **McGuireWoods Consulting LLC**

With one week remaining before the July 4 recess - and the August recess just around the corner - congressional leaders continue to negotiate towards...

---

## **TCPA Legislation on the Horizon?**

### **Drinker Biddle & Reath LLP**

While the FCC has a record open to adopt guidance and a new definition for what it considers as an “automatic telephone dialing system” (ATDS) and...

---

## **“Help Me, Help You”: Defense Department Advises Contractors That Cybersecurity Is An Allowable Cost** [Audio](#)

### **Jackson Lewis PC**

During a presentation at the Professional Services Council Federal Acquisition Conference on June 13, 2019, a high-ranking Department of Defense...

---

**North Carolina Legislate Update, June 21, 2019** North Carolina**Brooks Pierce McLendon Humphrey & Leonard LLP**

Budget negotiators from both chambers worked behind closed doors this week seeking to resolve differences on the budget bill. A conference committee...

---

**Change Is in the Air: Buerkle Withdraws Her Nomination to Chair the CPSC****Morrison & Foerster LLP**

This week, Acting Chairman Ann Marie Buerkle withdrew her nomination to serve as Chairman of the U.S. Consumer Product Safety Commission (CPSC). She...

---

**Everything Sucks! Lessons on How NOT to Behave in the Workplace****Ford & Harrison LLP**

Everything Sucks! Is a Netflix comedy series set in the mid-1990s at Boring High School. The show follows high school freshman Luke O'Neil, his...

---

**Cyber Update: DoD Contractor Cybersecurity Certification and 33 New Enhanced Controls to Combat the Advanced Persistent Threat****Sheppard Mullin Richter & Hampton LLP**

The Government remains intensely focused on how best to protect its Controlled Unclassified Information (CUI) once it is released to contractors. In...

---

**The Weekly Hill Update****Baker & Hostetler LLP**

Below is the Federal Policy team's weekly preview, posted when Congress is in session...

---

**Privacy Perils: Elder Abuse Awareness Day****Bass, Berry & Sims PLC**

With older adults increasingly targeted by financial scammers, Governor Bill Lee has proclaimed tomorrow, June 15, 2019, as Elder Abuse Awareness Day...

---

**Rubio's Huawei proposal should worry US tech, pharma companies****IAM**

Last week, US Senator Marco Rubio made a misguided foray into IP policy, proposing a measure that would deprive Huawei of its ability to enforce US...

---

**Introducing the Public Benefit LLC** Delaware**Morrison & Foerster LLP**

Four years after Delaware first enacted its Public Benefit Corporation (PBC) statute, the state has taken another step forward in advancing legal...

---

**Colorado Supreme Court Gives OK to Ballot Measure to Repeal TABOR** Colorado**Brownstein Hyatt Farber Schreck LLP**

The Colorado Supreme Court provided a big victory on Monday to proponents of a citizen-initiated statewide ballot measure that would ask voters...

---



## **U.S. Department of Education proposes regulations related to accreditation, state authorization, and other Title IV topics in "kitchen sink" rule-making**

**Hogan Lovells**

On 12 June 2019 the U.S. Department of Education (ED) published a notice of proposed rule-making (NPRM) in the Federal Register related to the...

---

## **Public M&A - resilient in a time of stress?**

**Allen & Overy LLP**

Public M&A activity would normally be expected to track the rest of the global transactions market and therefore be experiencing a period of slow...

---

## **Giving the Gift of Education**

**Think Defense APLC**

Let's reinstate Pell grants for people in prison. What are those? They are federal grants that help people pay for college...

---

## **Veterans Community Care Program Final Rule**

**Seyfarth Shaw LLP**

On June 6, 2019, the US Department of Veterans Affairs ("VA") issued final rules regarding the implementation of the Veterans Community Care Program...

---

## **CMS Proposes Changes to Medicare Wage Index that Would Increase Reimbursement Rates to Rural Hospitals at the Expense of Urban Hospitals**

**Sheppard Mullin Richter & Hampton LLP**

On May 3, 2019, the Centers for Medicare & Medicaid Services ("CMS") published a comprehensive proposed rule ("Proposed Rule") to revise the Medicare...

---

## **NCGA Week in Review- Jun 21, 2019**

North Carolina

**McGuireWoods Consulting LLC**

Time is of the essence these days at the North Carolina General Assembly. As the end of session draws closer and closer, legislators have been...



## **Global**

### **Employment & Labor**



## **Job interview 4.0 - legal considerations for automated face and speech recognition**

**Rihm Rechtsanwälte**

Many companies advertise and sell sophisticated video interview software to large companies for recruitment purposes. While applicants are interviewed...

### **Environment & Climate Change**



---

## **Oil and gas exploration and production laws in Lebanon**

### **Kouatly & Associates**

A structured guide to oil and gas regulation in Lebanon

---

## **Oil and gas exploration and production laws in Venezuela**

### **InterJuris Abogados**

A structured guide to oil and gas exploration and production laws in Venezuela

---

## **Proposed Revisions to Equator Principles Released for Review**

### **White & Case LLP**

The Equator Principles Association (EPA) has released the much-awaited draft text of Equator Principles 4 (EP4). Further consultation of the draft...

---

## **International Shipping Finance Goes Green**

### **Mayer Brown**

On June 18, 2019, a group of major ship finance banks<sup>1</sup> announced the launch of the “Poseidon Principles,” a framework for global responsible shipping...

---

## **Internet & Social Media**



## **Electronic marketing and internet use in Brazil**

### **Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados**

A structured guide to electronic marketing and internet use in Brazil

---

## **Telecoms privacy and data security provisions in Russia**

### **King & Spalding LLP**

A structured guide to privacy and data security provisions for telecoms services in Russia

---

## **Telecoms privacy and data security provisions in Germany**

### **Heuking Kühn Lüer Wojtek**

A structured guide to privacy and data security provisions for telecoms services in Germany

---

## **The launch of Libra**

### **DLA Piper**

Earlier this week Facebook launched a new currency “Libra” through its White Paper, setting out a vision to become a global provider of low cost...

---

## **TMT Horizons 2019**

### **Hogan Lovells**

The dynamism of the Technology, Media and Telecoms sector is set to continue. Challengers can reach scale seemingly overnight, forcing market change...

---

## **Privacy Tip #195 - Evite Announces Breach of Account Information of 10 Million Users**

### **Robinson & Cole LLP**



If you use Evite for e-invitations or social planning purposes, be aware that it announced last week that the account information for up to 10...

## Recht der Domainnamen

### Bardehle Pagenberg

Der Domainname ist heute viel mehr als eine Internet-Adresse. Er ist in aller Regel ein wichtiger Teil der Marken- sowie Kommunikationsstrategie und...

## Amazon TLD back in limbo as governments rail against e-commerce giant and ICANN

### World Trademark Review

Amazon's application for the '.Amazon' top-level domain (TLD) and two internationalised domains is back on hold after the Colombian government lodged...

## Legal Practice



## The future of data processing in driverless cars: the shift from connected to autonomous

### PrivacyPerfect

The shift from 'connected cars' (cars communicating with their manufacturers, traffic lights, surrounding vehicles etc.) to 'self-driving'...

## Projects & Procurement



## Africa Business in Brief - 11 JUN 2019

### ENSAfrica

Tirupati Graphite, the flake-graphite company with primary mining and processing projects in Madagascar and downstream processing projects in India...

## Democratic Republic of Congo

### ENSAfrica

TSXV-listed tin-focused mining company Alphamin Resources Corp. has commenced hot commissioning at its Bisie tin project. Construction of the mine...

## Africa Business in Brief - 17 JUN 2019

### ENSAfrica

The African Development Bank and its partners have launched the Africa Digital Financial Inclusion Facility (ADFI), designed to aid safety and...

## Public



## Private Bank Briefing: Issues Impacting the Private Bank Sector - June 2019

### Latham & Watkins LLP

The FCA and the PRA published their Business Plans for 2019/20 in April 2019. FCA Priorities As expected, with Brexit remaining a key focus, there are...



## **Linbert Spencer OBE - The Centre for Inclusive Leadership - ZebraTalk #37**

### **Taylor Vinters LLP**

Watch Linbert Spencer from The Centre for Inclusive Leadership speaking at the Zebra Project event 'Diversity and inclusion - from tokenism to...

---

## **Crossing Borders 10 (Chinese/English)**

### **King & Wood Mallesons**

In the last decade (2008 - 2018), investor-state dispute settlement (ISDS) is quite controversial. On the commercial side, however, the mechanism has...

---

## **What is the role of MI6 in International Criminal Law?**

### **Nyman Gibson Miralis**

The UK Secret Intelligence Service (SIS) - otherwise known as MI6 - conducts secret overseas operations and gathers intelligence to help protect UK...

---

## **Other top stories**

**Privacy Matters: A Website Privacy Policy is Good Governance**

---

**Time To Revisit Arbitration Agreements: Employers Dealt A Blow By Unanimous Labor Board**

---

**Texas prohibits collection actions and arbitrations on time-barred debt**

---

**Student Loans in Bankruptcy: What's on the Horizon?**

---

**Reincorporating a California corporation to a Delaware corporation**

---

**Future Securities Claims - The Bond Wave**

---

**Avoiding Inadvertent Disclosures of Privileged Information**

---

**Court Finds No Private Right of Action Under Michigan Medical Marijuana Act**

---

**Retailer Wins Lawsuit Against Its Merchant Processor**

---

**Employer Insights: Recreational Marijuana in Illinois**

---

## **International developments**

**Führungsaufgabe als zustimmungspflichtige Einstellung** DE

---

**Proposed Changes to School Board Executive Compensation**

---

**BAG zur Unterschrift bei Massenentlassungsanzeige** DE

---

**Teil 5: Alternative Gestaltungsmöglichkeiten beim Ablauf der Überlassungshöchstdauer** DE

---

**Automobile Newsletter No. 6**

---

**Observatorio contra el fraude a la Seguridad Social** ES

---

**Oil and gas exploration and production laws in Nigeria**

---

**Data security and breach notification in Canada**

---

**Real Estate in Ireland**

---

**Legal Aspects of Cloud Computing: Cloud Contracting**

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law

[Contact Lexology](#)

[About Lexology](#)



© 2006-2019 Globe Business Media Group

**From:** US-CERT  
**To:** Tanner McGinnis  
**Subject:** SB19-175: Vulnerability Summary for the Week of June 17, 2019  
**Date:** Monday, June 24, 2019 1:37:15 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## SB19-175: Vulnerability Summary for the Week of June 17, 2019

06/24/2019 06:54 AM EDT

Original release date: June 24, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- t2200h_firmware	An issue was discovered on Actiontec T2200H T2200H-31.128L.08 devices, as distributed by Telus. By attaching a UART adapter to the UART pins on the system board, an attacker can use a special key sequence (Ctrl-L) to obtain a shell with root privileges. After gaining root access, the attacker can mount the filesystem read-write and make permanent modifications to the device including bricking of the device, disabling vendor management of the device, preventing automatic upgrades, and permanently installing malicious code on the device.	2019-06-17	7.2	<a href="#">CVE-2019-12789</a> MISC MISC
advantech -- webaccess	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 10012 RPC call.	2019-06-18	7.5	<a href="#">CVE-2019-3953</a> MISC
advantech -- webaccess	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 81024 RPC call.	2019-06-18	7.5	<a href="#">CVE-2019-3954</a> MISC
arenam -- amgallery	SQL Injection exists in the AMGallery 1.2.3 component for Joomla! via the filter_category_id parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17398</a> MISC MISC
bubblesoftapps -- bubbleupnp	In BubbleUPnP 0.9 update 30, the XML parsing engine for SSDP/UPnP functionality is vulnerable to an XML External Entity Processing (XXE) attack. Remote, unauthenticated attackers can use this vulnerability to: (1) Access arbitrary files from the filesystem with the same permission as the user account running BubbleUPnP, (2) Initiate SMB connections to capture a NetNTLM challenge/response and crack the cleartext password, or (3) Initiate SMB connections to relay a NetNTLM challenge/response and achieve Remote Command Execution in Windows domains.	2019-06-19	7.5	<a href="#">CVE-2018-15506</a> CONFIRM
bzip -- bzip2	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.	2019-06-19	7.5	<a href="#">CVE-2019-12900</a> MISC
chronoscan -- chronoscan	SQL injection vulnerability in ChronoScan version 1.5.4.3 and earlier allows an unauthenticated attacker to execute arbitrary SQL commands via the wcr_machineid cookie.	2019-06-21	7.5	<a href="#">CVE-2018-15868</a> MISC MISC

cisco -- meeting_server	A vulnerability in the CLI configuration shell of Cisco Meeting Server could allow an authenticated, local attacker to inject arbitrary commands as the root user. The vulnerability is due to insufficient input validation during the execution of a vulnerable CLI command. An attacker with administrator-level credentials could exploit this vulnerability by injecting crafted arguments during command execution. A successful exploit could allow the attacker to perform arbitrary code execution as root on an affected product.	2019-06-19	7.2	<a href="#">CVE-2019-1623</a> <a href="#">BID</a> <a href="#">CISCO</a>
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, the BACnet daemon does not properly validate input, which could allow a remote attacker to send specially crafted packets causing the device to become unavailable.	2019-06-18	7.8	<a href="#">CVE-2018-18878</a> <a href="#">MISC</a> <a href="#">MISC</a>
deltaww -- devicenet_builder	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at image00400000+0x0000000000017a45e.	2019-06-19	7.5	<a href="#">CVE-2019-12898</a> <a href="#">MISC</a>
deltaww -- devicenet_builder	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at ntdll!RtlQueueWorkItem+0x00000000000005e3.	2019-06-19	7.5	<a href="#">CVE-2019-12899</a> <a href="#">MISC</a>
education_website_project -- education_website	SQL injection exists in Scriptzee Education Website 1.0 via the college_list.html subject, city, or country parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17840</a> <a href="#">MISC</a> <a href="#">MISC</a>
ethereum -- ethereumj	An issue was discovered in EthereumJ 1.8.2. There is Unsafe Deserialization in ois.readObject in mine/Ethash.java and decoder.readObject in crypto/ECKey.java. When a node syncs and mines a new block, arbitrary OS commands can be run on the server.	2019-06-20	10.0	<a href="#">CVE-2018-15890</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.	2019-06-18	7.8	<a href="#">CVE-2019-11477</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
flippa_marketplace_clone_project -- flippa_marketplace_clone	SQL injection exists in Scriptzee Flippa Marketplace Clone 1.0 via the site-search sortBy or sortDir parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17841</a> <a href="#">MISC</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	app/backup/index.php in the Backup Module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation, which allows authenticated administrative attackers to execute commands on the host.	2019-06-17	9.0	<a href="#">CVE-2019-11410</a> <a href="#">MISC</a> <a href="#">MISC</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device firmware file contains a file known as relay.sh which allows the device to create relay ports and connect the device to Vera servers. This is primarily used as a method of communication between the device and Vera servers so the devices can be communicated with even when the user is not at home. One of the parameters retrieved by this specific script is "remote_host". This parameter is not sanitized by the script correctly and is passed in a call to "eval" to execute another script where remote_host is concatenated to be passed a parameter to the second script. This allows an attacker to escape from the executed command and then execute any commands of his/her choice.	2019-06-17	9.0	<a href="#">CVE-2017-9384</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device firmware file contains a file known as proxy.sh which allows the device to proxy a specific request to and from another website. This is primarily used as a method of communication between the device and Vera website when the user is logged in to the https://home.getvera.com and allows the device to communicate between the device and website. One of the parameters retrieved by this specific script is "url". This parameter is not sanitized by the script correctly and is passed in a call to "eval" to execute "curl" functionality. This allows an attacker to escape from the executed command and then execute any commands of his/her choice.	2019-06-17	9.0	<a href="#">CVE-2017-9388</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device allows a user to install applications written in the Lua programming language. Also the interface allows any user to write his/her application in the Lua language. However, this functionality is not protected by authentication and this allows an attacker to run arbitrary Lua code on the device. The POST request is forwarded to LuaUPNP daemon on the device. This binary handles the received Lua code in the function "LU::JobHandler_LuaUPnP::RunLua(LU::JobHandler_LuaUPnP * __hidden this, LU::UPnPActionWrapper *)". The value in the "code"	2019-06-17	9.0	<a href="#">CVE-2017-9389</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>

	parameter is then passed to the function "LU::LuaInterface::RunCode(char const*)" which actually loads the Lua engine and runs the code.			
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "request_image" as one of the service actions for a normal user to retrieve an image from a camera that is controlled by the controller. It seems that the "URL" parameter passed in the query string is not sanitized and is stored on the stack which allows an attacker to overflow the buffer. The function "LU::Generic_IP_Camera_Manager::REQ_Image" is activated when the lu_request_image is passed as the "id" parameter in query string. This function then calls "LU::Generic_IP_Camera_Manager::GetUrlFromArguments" and passes a "pointer" to the function where it will be allowed to store the value from the URL parameter. This pointer is passed as the second parameter \$a2 to the function "LU::Generic_IP_Camera_Manager::GetUrlFromArguments". However, neither the callee or the caller in this case performs a simple length check and as a result an attacker who is able to send more than 1336 characters can easily overflow the values stored on the stack including the \$RA value and thus execute code on the device.	2019-06-17	9.0	<a href="#">CVE-2017-9391</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "request_image" as one of the service actions for a normal user to retrieve an image from a camera that is controlled by the controller. It seems that the "res" (resolution) parameter passed in the query string is not sanitized and is stored on the stack which allows an attacker to overflow the buffer. The function "LU::Generic_IP_Camera_Manager::REQ_Image" is activated when the lu_request_image is passed as the "id" parameter in the query string. This function then calls "LU::Generic_IP_Camera_Manager::GetUrlFromArguments". This function retrieves all the parameters passed in the query string including "res" and then uses the value passed in it to fill up buffer using the sprintf function. However, the function in this case lacks a simple length check and as a result an attacker who is able to send more than 184 characters can easily overflow the values stored on the stack including the \$RA value and thus execute code on the device.	2019-06-17	9.0	<a href="#">CVE-2017-9392</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
google -- android	In llcp_util_parse_connect of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-111660010	2019-06-19	7.1	<a href="#">CVE-2018-9561</a> <a href="#">MISC</a>
google -- android	In llcp_util_parse_cc of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-114237888	2019-06-19	7.1	<a href="#">CVE-2018-9563</a> <a href="#">MISC</a>
google -- android	In llcp_util_parse_link_params of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-114238578	2019-06-19	7.1	<a href="#">CVE-2018-9564</a> <a href="#">MISC</a>
google -- android	In findAvailSpellCheckerLocked of TextServicesManagerService.java, there is a possible way to bypass the warning dialog when selecting an untrusted spell checker due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0Android ID: A-118694079	2019-06-19	7.2	<a href="#">CVE-2019-1985</a> <a href="#">MISC</a>
google -- android	In ih264d_fmt_conv_420sp_to_420p of ih264d_format_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118399205	2019-06-19	9.3	<a href="#">CVE-2019-1989</a> <a href="#">MISC</a>
google -- android	In ihevcd_fmt_conv_420sp_to_420p of ihevcd_fmt_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118453553	2019-06-19	9.3	<a href="#">CVE-2019-1990</a> <a href="#">MISC</a>
google -- android	In addLinks of Linkify java, there is a possible phishing vector due to an unusual root cause. This could lead to remote code execution or misdirection of clicks with no additional execution privileges needed.	2019-06-19	9.3	<a href="#">CVE-2019-2003</a>



	User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116321860			<a href="#">MISC</a>
google -- android	In serviceDied of HalDeathHandlerHidl.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-116665972	2019-06-19	<a href="#">10.0</a>	<a href="#">CVE-2019-2006</a> <a href="#">MISC</a>
google -- android	In getReadIndex and getWriteIndex of FifoControllerBase.cpp, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-120789744	2019-06-19	<a href="#">10.0</a>	<a href="#">CVE-2019-2007</a> <a href="#">MISC</a>
google -- android	In createEffect of AudioFlinger.cpp, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-122309228	2019-06-19	<a href="#">7.6</a>	<a href="#">CVE-2019-2008</a> <a href="#">MISC</a>
google -- android	In l2c_lcc_proc_pdu of l2c_fcr.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120665616	2019-06-19	<a href="#">8.3</a>	<a href="#">CVE-2019-2009</a> <a href="#">MISC</a>
google -- android	In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118152591	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2010</a> <a href="#">MISC</a>
google -- android	In readNullableNativeHandleNoDup of Parcel.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-120084106	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2011</a> <a href="#">MISC</a>
google -- android	In rw_t3t_act_handle_fmt_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497437	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2012</a> <a href="#">MISC</a>
google -- android	In rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497583	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2013</a> <a href="#">MISC</a>
google -- android	In rw_t3t_handle_get_sc_poll_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120499324	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2014</a> <a href="#">MISC</a>
google -- android	In rw_t3t_act_handle_check_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120503926	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2015</a> <a href="#">MISC</a>
google -- android	In NFA_SendRawFrame of nfa_dm_api.cc, there is a possible out-of-bound write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120664978	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2016</a> <a href="#">MISC</a>
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-121035711	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2017</a> <a href="#">MISC</a>
google -- android	In resetPasswordInternal of DevicePolicyManagerService.java, there is a possible bypass of password reset protection due to an unusual root cause. Remote user interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-110172241	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2018</a> <a href="#">MISC</a>
google -- android	In ce_t4t_data_cback of ce_t4t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions:	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2019</a>

	Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-115635871			<a href="#">MISC</a>
google -- android	In llcp_dlc_proc_rr_rnr_pdu of llcp_dlc.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116788646	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2020</a> <a href="#">MISC</a>
google -- android	In rw_t3t_act_handle_ndef_detect_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120428041	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2021</a> <a href="#">MISC</a>
google -- android	In rw_t3t_act_handle_fmt_rsp and rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120506143	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2022</a> <a href="#">MISC</a>
google -- android	In ServiceManager::add function in the hardware service manager, there is an insecure permissions check based on the PID of the caller. This could allow an app to add or replace a HAL service with its own service, gaining code execution in a privileged process.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-121035042Upstream kernel	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2023</a> <a href="#">MISC</a>
google -- android	In em28xx_unregister_dvb of em28xx-dvb.c, there is a possible use after free issue. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-111761954References: Upstream kernel	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2024</a> <a href="#">MISC</a>
google -- android	In binder_thread_read of binder.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-116855682References: Upstream kernel	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2025</a> <a href="#">MISC</a>
healthnode_hospital_management_system_project -- healthnode_hospital_management_system	SQL Injection exists in HealthNode Hospital Management System 1.0 via the id parameter to dashboard/Patient/info.php or dashboard/Patient/patientdetails.php.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17393</a> <a href="#">MISC</a> <a href="#">MISC</a>
hotel_booking_engine_project -- hotel_booking_engine	SQL injection exists in Scriptzee Hotel Booking Engine 1.0 via the hotels_h_room_type parameter.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17842</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- control_desk	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbitrary commands on the system. IBM X-Force ID: 161680.	2019-06-19	<a href="#">8.5</a>	<a href="#">CVE-2019-4364</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool/impact	IBM Tivoli Netcool/Impact 7.1.0 allows for remote execution of command by low privileged User. Remote code execution allow to execute arbitrary code on system which lead to take control over the system. IBM X-Force ID: 158094.	2019-06-17	<a href="#">7.7</a>	<a href="#">CVE-2019-4103</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
infoblox -- nios	A privilege escalation vulnerability in the "support access" feature on Infoblox NIOS 6.8 through 8.4.1 could allow a locally authenticated administrator to temporarily gain additional privileges on an affected device and perform actions within the super user scope. The vulnerability is due to a weakness in the "support access" password generation algorithm. A locally authenticated administrative user may be able to exploit this vulnerability if the "support access" feature is enabled, they know the support access code for the current session, and they know the algorithm to generate the support access password from the support access code. "Support access" is disabled by default. When enabled, the access will be automatically disabled (and support access code will expire) after the 24 hours.	2019-06-17	<a href="#">7.2</a>	<a href="#">CVE-2018-10239</a> <a href="#">CONFIRM</a>
jimtlawl_project -- jimtlawl	SQL Injection exists in the Jimtlawl 2.2.7 component for Joomla! via the id parameter.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17399</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgd -- libgd	The GD Graphics Library (aka libgd) through 2.2.5 has a Double Free Vulnerability in the gdImageBmpPtr function.	2019-06-20	<a href="#">7.5</a>	<a href="#">CVE-2018-15878</a> <a href="#">MISC</a>
libgd -- libgd	The GD Graphics Library (aka libgd) through 2.2.5 has a Double Free Vulnerability in the gdImageBmpPtr function.	2019-06-20	<a href="#">7.5</a>	<a href="#">CVE-2018-15879</a> <a href="#">MISC</a>
linux -- linux_kernel	A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.	2019-06-14	<a href="#">7.5</a>	<a href="#">CVE-2019-10126</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">BUGTRAQ</a>

				DEBIAN
linux -- linux_kernel	A double-free can happen in <code>idr_remove_all()</code> in <code>lib/idr.c</code> in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS).	2019-06-18	7.2	<a href="#">CVE-2019-3896</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
onapp -- onapp	OnApp before 5.0.0-88, 5.5.0-93, and 6.0.0-196 allows an attacker to run arbitrary commands with root privileges on servers managed by OnApp for XEN/KVM hypervisors. To exploit the vulnerability an attacker has to have control of a single server on a given cloud (e.g. by renting one). From the source server, the attacker can craft any command and trigger the OnApp platform to execute that command with root privileges on a target server.	2019-06-19	8.5	<a href="#">CVE-2019-12491</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.0 and earlier has Incorrect Access Control.	2019-06-17	7.5	<a href="#">CVE-2019-7158</a> <a href="#">MISC</a>
open_faculty_evaluation_system_project -- open_faculty_evaluation_system	Open Faculty Evaluation System 5.6 for PHP 5.6 allows <code>submit_feedback.php</code> SQL Injection, a different vulnerability than CVE-2018-18758.	2019-06-19	7.5	<a href="#">CVE-2018-18757</a> <a href="#">MISC</a> <a href="#">MISC</a>
open_faculty_evaluation_system_project -- open_faculty_evaluation_system	Open Faculty Evaluation System 7 for PHP 7 allows <code>submit_feedback.php</code> SQL Injection, a different vulnerability than CVE-2018-18757.	2019-06-19	7.5	<a href="#">CVE-2018-18758</a> <a href="#">MISC</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-06-19	7.5	<a href="#">CVE-2019-2729</a> <a href="#">MISC</a>
ranksol -- twilio_web_to_fax_machine_system	SQL Injection exists in Twilio WEB To Fax Machine System 1.0 via the email or password parameter to <code>login_check.php</code> , or the id parameter to <code>add_email.php</code> or <code>edit_content.php</code> .	2019-06-19	7.5	<a href="#">CVE-2018-17388</a> <a href="#">MISC</a> <a href="#">MISC</a>
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7 x x and 8.0.0. A parameter in the web reports module is vulnerable to h2 SQL injection. This can be exploited to inject SQL queries and run standard h2 system functions.	2019-06-17	7.5	<a href="#">CVE-2018-20469</a> <a href="#">MISC</a> <a href="#">MISC</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of changing the administrative password for the web management interface. It seems that the device does not implement any cross site request forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface to change a user's password. Also this is a systemic issue.	2019-06-18	9.3	<a href="#">CVE-2017-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new routes to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in passing commands to a "popen" API in the function and thus result in command injection on the device. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a <code>cpio-root</code> archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function <code>sub_00420F38</code> in IDA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "dest" is extracted at address 0x00420FC4. The POST parameter "dest" is concatenated in a route add command and this is passed to a "popen" function at address 0x00421220. This allows an attacker to provide the payload of his/her choice and finally take control of the device.	2019-06-18	9.0	<a href="#">CVE-2017-8333</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
sophos -- sfos	A shell escape vulnerability in <code>/webconsole/Controller</code> in Admin Portal of Sophos XG firewall 17.0.8 MR-8 allow remote authenticated attackers to execute arbitrary OS commands via shell metacharacters in the "dbName" POST parameter.	2019-06-20	9.0	<a href="#">CVE-2018-16117</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
thephpfactory -- auction_factory	SQL Injection exists in the Auction Factory 4.5.5 component for Joomla! via the <code>filter_order_Dir</code> or <code>filter_order</code> parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17374</a> <a href="#">MISC</a> <a href="#">MISC</a>
thephpfactory -- dutch_auction_factory	SQL Injection exists in the Dutch Auction Factory 2.0.2 component for Joomla! via the <code>filter_order_Dir</code> or <code>filter_order</code> parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17381</a> <a href="#">MISC</a> <a href="#">MISC</a>
thephpfactory -- micro_deal_factory	SQL Injection exists in the Micro Deal Factory 2.4.0 component for Joomla! via the <code>id</code> parameter, or the <code>PATH_INFO</code> to <code>mydeals/</code> or <code>listdeals/</code> .	2019-06-19	7.5	<a href="#">CVE-2018-17386</a> <a href="#">MISC</a> <a href="#">MISC</a>
	An issue was discovered on TP-Link TL-WR1043ND V2 devices. An			<a href="#">CVE-2019-</a>

tp-link -- tl-wr1043nd_firmware	attacker can send a cookie in an HTTP authentication packet to the router management web interface, and fully control the router without knowledge of the credentials.	2019-06-19	<a href="#">10.0</a>	<a href="#">6971 MISC MISC</a>
videolan -- vlc_media_player	An issue was discovered in zlib_decompress_extra in modules/demux/mkv/util.cpp in VideoLAN VLC media player 3 x through 3.0.7. The Matroska demuxer, while parsing a malformed MKV file type, has a double free.	2019-06-18	<a href="#">7.5</a>	<a href="#">CVE-2019-12874 MISC</a>
webmin -- webmin	In Webmin through 1.910, any user authorized to the "Package Updates" module can execute arbitrary commands with root privileges via the data parameter to update.cgi.	2019-06-15	<a href="#">9.0</a>	<a href="#">CVE-2019-12840 MISC BID MISC MISC</a>
westerndigital -- my_book_live_firmware	Western Digital WD My Book Live (all versions) has a root Remote Command Execution bug via shell metacharacters in the /api/1.0/rest/language_configuration language parameter. t can be triggered by anyone who knows the IP address of the affected device.	2019-06-19	<a href="#">10.0</a>	<a href="#">CVE-2018-18472 MISC MISC</a>
whatsapp -- whatsapp	When receiving calls using WhatsApp for iOS, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for iOS prior to v2.18.90.24 and WhatsApp Business for iOS prior to v2.18.90.24.	2019-06-14	<a href="#">7.5</a>	<a href="#">CVE-2018-20655 BID MISC</a>
whatsapp -- whatsapp	An out-of-bounds read was possible in WhatsApp due to incorrect parsing of RTP extension headers. This issue affects WhatsApp for Android prior to 2.18.276, WhatsApp Business for Android prior to 2.18.99, WhatsApp for iOS prior to 2.18.100.6, WhatsApp Business for iOS prior to 2.18.100.2, and WhatsApp for Windows Phone prior to 2.18.224.	2019-06-14	<a href="#">7.5</a>	<a href="#">CVE-2018-6350 BID MISC</a>
zohocorp -- manageengine_adselfservice_plus	An authentication bypass vulnerability in the password reset functionality in Zoho ManageEngine ADSelfService Plus before 5.0.6 allows an attacker with physical access to gain a shell with SYSTEM privileges via the restricted thick client browser. The attack uses a long sequence of crafted keyboard input.	2019-06-17	<a href="#">7.2</a>	<a href="#">CVE-2019-12476 BID MISC MISC</a>
zohocorp -- manageengine_analytics_plus	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus.	2019-06-18	<a href="#">7.2</a>	<a href="#">CVE-2019-12133 MISC CONFIRM</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
afian -- filerun	FileRun 2019.05.21 allows XSS via the filename to the ?module=fileman&section=do&page=up URI.	2019-06-20	<a href="#">4.3</a>	<a href="#">CVE-2019-12905 MISC</a>
alpinelinux -- abuild	Alpine Linux abuild through 3.4.0 allows an unprivileged member of the abuild group to add an untrusted package via a --keys-dir option that causes acceptance of an untrusted signing key.	2019-06-18	<a href="#">4.0</a>	<a href="#">CVE-2019-12875 MISC MISC</a>
alternate-tools -- alternate_pic_view	Alternate Pic View 2.600 has a User Mode Write AV starting at PicViewer!PerfgrapFinalize+0x000000000000a8868.	2019-06-19	<a href="#">5.0</a>	<a href="#">CVE-2019-12893 MISC</a>
alternate-tools -- alternate_pic_view	Alternate Pic View 2.600 has a Read Access Violation at the Instruction Pointer after a call from PicViewer!PerfgrapFinalize+0x000000000000a9a1b.	2019-06-19	<a href="#">5.0</a>	<a href="#">CVE-2019-12894 MISC</a>
alternate-tools -- alternate_pic_view	In Alternate Pic View 2.600, the Exception Handler Chain is Corrupted starting at PicViewer!PerfgrapFinalize+0x000000000000b916d.	2019-06-19	<a href="#">5.0</a>	<a href="#">CVE-2019-12895 MISC</a>
apache -- allura	In Apache Allura prior to 1.11.0, a vulnerability exists for stored XSS on the user dropdown selector when creating or editing tickets. The XSS executes when a user engages with that dropdown on that page.	2019-06-18	<a href="#">4.3</a>	<a href="#">CVE-2019-10085 BID MISC MLIST</a>
artha_project -- artha	Artha ~ The Open Thesaurus 1.0.3.0 has a Buffer Overflow.	2019-06-18	<a href="#">5.0</a>	<a href="#">CVE-2018-18944 MISC MISC</a>
b3log -- solo	b3log Solo 2.9.3 has XSS in the Input page under the "Publish Articles" menu with an ID of "articleTags" stored in the "tag" JSON field, which allows remote attackers to inject arbitrary Web scripts or HTML via a carefully	2019-06-20	<a href="#">4.3</a>	<a href="#">CVE-2018-16248 MISC</a>

	crafted site name in an admin-authenticated HTTP request.			
cisco -- integrated_management_controller	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to access potentially sensitive system usage information. The vulnerability is due to a lack of proper data protection mechanisms. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow an attacker to view sensitive system data.	2019-06-19	5.0	<a href="#">CVE-2019-1631</a> BID CISCO
cisco -- prime_service_catalog	A vulnerability in the web-based management interface of Cisco Prime Service Catalog Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protection mechanisms on the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user.	2019-06-19	6.8	<a href="#">CVE-2019-1874</a> BID CISCO
cloudera -- data_science_workbench	An issue was discovered in Cloudera Data Science Workbench (CDSW) 1.2.x through 1.4.0. Unauthenticated users can get a list of user accounts.	2019-06-21	5.0	<a href="#">CVE-2018-15665</a> MISC CONFIRM
columbiaweather -- weather_microserver_firmware	In firmware version MS_2 6.9900 of Columbia Weather MicroServer, a readouts_rd.php directory traversal issue makes it possible to read any file present on the underlying operating system.	2019-06-18	5.0	<a href="#">CVE-2018-18876</a> MISC MISC
columbiaweather -- weather_microserver_firmware	In firmware version MS_2 6.9900 of Columbia Weather MicroServer, an authenticated web user can access an alternative configuration page config_main.php that allows manipulation of the device.	2019-06-18	6.5	<a href="#">CVE-2018-18877</a> MISC MISC
columbiaweather -- weather_microserver_firmware	In firmware version MS_2 6.9900 of Columbia Weather MicroServer, an authenticated web user can pipe commands directly to the underlying operating system as user input is not sanitized in networkdiags.php.	2019-06-18	6.5	<a href="#">CVE-2018-18879</a> MISC MISC
corel -- paintshop_pro_2019	An issue was discovered in Corel PaintShop Pro 2019 21 0.0.119. An integer overflow in the jp2 parsing library allows an attacker to overwrite memory and to execute arbitrary code.	2019-06-19	6.8	<a href="#">CVE-2019-6114</a> MISC
craftcms -- craft_cms	Craft CMS 3.1.30 has XSS.	2019-06-18	4.3	<a href="#">CVE-2019-12823</a> MISC CONFIRM
creativity -- witycms	A "search for user discovery" injection issue exists in Creativity wityCMS 0.6.2 via the "Utilisateur" menu. No input parameters are filtered, e.g., the /admin/user/users Nickname, email, firstname, lastname, and groupe parameters.	2019-06-20	4.0	<a href="#">CVE-2018-16251</a> MISC
debian -- debian_linux	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.7, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. An attacker could send a malicious email to an OTRS system. If a logged-in agent user quotes it, the email could cause the browser to load external image resources.	2019-06-17	4.3	<a href="#">CVE-2019-12248</a> CONFIRM MISC
dotcms -- dotcms	dotCMS before 5.1.6 is vulnerable to a SQL injection that can be exploited by an attacker of the role Publisher via view_unpushed_bundles.jsp.	2019-06-18	6.5	<a href="#">CVE-2019-12872</a> MISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows XML External Entity Blind Injection, related to pingback.axd and BlogEngine.Core/Web/HttpHandlers/PingbackHandler.cs.	2019-06-21	5.0	<a href="#">CVE-2019-10718</a> MISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution because file creation is mishandled, related to /api/upload and BlogEngine.NET/AppCode/Api/UploadController.cs. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714.	2019-06-21	6.5	<a href="#">CVE-2019-10719</a> MISC FULLDISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution via the theme cookie to the File Manager. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714.	2019-06-21	6.5	<a href="#">CVE-2019-10720</a> MISC FULLDISC MISC
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7 and earlier allows XXE via an apml file to syndication.axd.	2019-06-21	5.0	<a href="#">CVE-2019-11392</a> MISC
edrawsoft -- edraw_max	Edraw Max 7.9.3 has Heap Corruption starting at ntdll!RtlpNtMakeTemporaryKey+0x00000000000001a77.	2019-06-19	5.0	<a href="#">CVE-2019-12896</a> MISC
edrawsoft -- edraw_max	Edraw Max 7.9.3 has a Read Access Violation at the Instruction Pointer after a call from ObjectModule!Paint::Clear+0x0000000000000074.	2019-06-19	5.0	<a href="#">CVE-2019-12897</a> MISC
exacq -- enterprise_system_manager	A vulnerability in the exacqVision Enterprise System Manager (ESM) v5.12.2 application whereby unauthorized privilege escalation can potentially be achieved. This vulnerability impacts exacqVision ESM v5.12.2 and all prior versions of ESM running on a Windows operating system. This issue does not impact any Windows Server OSs, or Linux deployments with permissions that are not inherited from the root directory. Authorized Users have ?modify? permission to the ESM folders, which allows a low privilege account to modify files located in these directories. An executable can be	2019-06-18	6.9	<a href="#">CVE-2019-7588</a> CONFIRM MISC



	renamed and replaced by a malicious file that could connect back to a bad actor providing system level privileges. A low privileged user is not able to restart the service, but a restart of the system would trigger the execution of the malicious file. This issue affects: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) Version 5.12.2 and prior versions; This issue does not affect: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) 19.03 and above.			<a href="#">MISC</a> <a href="#">CONFIRM</a>
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.	2019-06-18	5.0	<a href="#">CVE-2019-11478</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.	2019-06-18	5.0	<a href="#">CVE-2019-11479</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x through 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has JDOM 1.x or 2.x jar in the classpath, an attacker can send a specifically crafted JSON message that allows them to read arbitrary local files on the server.	2019-06-19	4.3	<a href="#">CVE-2019-12814</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
foxitsoftware -- foxit_pdf_sdk_activex	A use after free in the TextBox field Validate action in IReader_ContentProvider can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031. An attacker can leverage this to gain remote code execution. Relative to CVE-2018-19452, this has a different free location and requires different JavaScript code for exploitation.	2019-06-17	6.8	<a href="#">CVE-2018-19444</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API app.launchURL is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19445</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A File Write can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API Doc.createObject is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19446</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A stack-based buffer overflow can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) 5.4.0.1031 when parsing the URI string. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19447</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	In Foxit Reader SDK (ActiveX) Professional 5.4.0.1031, an uninitialized object in IReader_ContentProvider::GetDocEventHandler occurs when embedding the control into Office documents. By opening a specially crafted document, an attacker can trigger an out of bounds write condition, possibly leveraging this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19448</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A File Write can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API Doc.exportAsPDF is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19449</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) 5.4.0.1031 when parsing a launch action. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19450</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 suffers from an information disclosure vulnerability due to excessive debug information, which allows authenticated administrative attackers to obtain credentials and other sensitive information.	2019-06-17	4.0	<a href="#">CVE-2019-11407</a> <a href="#">MISC</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	XSS in app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 allows remote unauthenticated attackers to inject arbitrary JavaScript characters by placing a phone call using a specially crafted caller ID number. This can further lead to remote code execution by chaining this vulnerability with a command injection vulnerability also present in FusionPBX.	2019-06-17	4.3	<a href="#">CVE-2019-11408</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	app/operator_panel/exec.php in the Operator Panel module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation that allows authenticated non-administrative attackers to execute commands on the host. This can further lead to remote code execution when combined with an XSS vulnerability also present in the FusionPBX Operator Panel module.	2019-06-17	6.5	<a href="#">CVE-2019-11409</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
genieaccess -- wip3bvaf_firmware	Genie Access WIP3BVAf WISH IP 3MP IR Auto Focus Bullet Camera devices through 3.x are vulnerable to directory traversal via the web interface, as demonstrated by reading /etc/shadow. NOTE: this product is discontinued, and its final firmware version has this vulnerability (4.x	2019-06-17	5.0	<a href="#">CVE-2019-7315</a> <a href="#">MISC</a>

	versions exist only for other Genie Access products).			
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a user with the capability of installing or deleting apps on the device using the web management interface. It seems that the device does not implement any cross-site request forgery protection mechanism which allows an attacker to trick a user who navigates to an attacker controlled page to install or delete an application on the device. Note: The cross-site request forgery is a systemic issue across all other functionalities of the device.	2019-06-17	6.8	<a href="#">CVE-2017-9381</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "file" as one of the service actions for a normal user to read a file that is stored under the /etc/cmh-lu folder. It retrieves the value from the "parameters" query string variable and then passes it to an internal function "FileUtils: ReadFileIntoBuffer" which is a library function that does not perform any sanitization on the value submitted and this allows an attacker to use directory traversal characters ". /" and read files from other folders within the device.	2019-06-17	4.0	<a href="#">CVE-2017-9382</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "wget" as one of the service actions for a normal user to connect the device to an external website. It retrieves the parameter "URL" from the query string and then passes it to an internal function that uses the curl module on the device to retrieve the contents of the website.	2019-06-17	6.5	<a href="#">CVE-2017-9383</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera Veralite 1.7.481 devices. The device has an additional OpenWRT interface in addition to the standard web interface which allows the highest privileges a user can obtain on the device. This web interface uses root as the username and the password in the /etc/cmh/cmh conf file which can be extracted by an attacker using a directory traversal attack, and then log in to the device with the highest privileges.	2019-06-17	5.0	<a href="#">CVE-2017-9385</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a script file called "get_file.sh" which allows a user to retrieve any file stored in the "cmh-ext" folder on the device. However, the "filename" parameter is not validated correctly and this allows an attacker to directory traverse outside the /cmh-ext folder and read any file on the device. It is necessary to create the folder "cmh-ext" on the device which can be executed by an attacker first in an unauthenticated fashion and then execute a directory traversal attack.	2019-06-17	4.0	<a href="#">CVE-2017-9386</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a shell script called connect.sh which is supposed to return a specific cookie for the user when the user is authenticated to https://home.getvera.com. One of the parameters retrieved by this script is "RedirectURL". However, the application lacks strict input validation of this parameter and this allows an attacker to execute the client-side code on this application.	2019-06-17	4.3	<a href="#">CVE-2017-9390</a> MISC MISC BUGTRAQ
gnu -- bash	A heap-based buffer overflow exists in GNU Bash before 4.3 when wide characters, not supported by the current locale set in the LC_CTYPE environment variable, are printed through the echo built-in function. A local attacker, who can provide data to print through the "echo -e" built-in function, may use this flaw to crash a script or execute code with the privileges of the bash process. This occurs because ansicstr() in lib/sh/strtrans.c mishandles u32conv().	2019-06-18	4.6	<a href="#">CVE-2012-6711</a> MISC BID MISC
google -- android	In publishKeyEvent, publishMotionEvent and sendUnchainedFinishedSignal of InputTransport.cpp, there are uninitialized data leading to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android ID: A-115739809	2019-06-19	4.9	<a href="#">CVE-2019-2004</a> MISC
google -- android	In onPermissionGrantResult of GrantPermissionsActivity.java, there is a possible incorrectly granted permission due to a missing permission check. This could lead to local escalation of privilege on a locked device with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-8.0 Android-8.1 Android-9 Android ID: A-68777217	2019-06-19	6.8	<a href="#">CVE-2019-2005</a> MISC
i-doit -- i-doit	An XSS issue was discovered in i-doit Open 1.12 via the src/tools/php/qr/qr.php url parameter.	2019-06-18	4.3	<a href="#">CVE-2019-6965</a> MISC
ibm -- campaign	IBM Campaign 9.1.2 and 10.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (./.) to view arbitrary files on the system. IBM X-Force ID: 162172.	2019-06-19	4.0	<a href="#">CVE-2019-4384</a> XF CONFIRM
ibm -- cloud_private	IBM Cloud Private 2.1.0, 3.1.0, 3.1.1, and 3.1.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 158338.	2019-06-18	6.8	<a href="#">CVE-2019-4142</a> XF CONFIRM
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to obtain sensitive information, caused by a flaw in the HTTP OPTIONS method, aka Optionsbleed. By sending an OPTIONS HTTP request, a remote attacker could exploit this vulnerability to read secret data from process memory and obtain sensitive information. IBM X-Force ID: 158878.	2019-06-17	4.0	<a href="#">CVE-2019-4173</a> CONFIRM XF

ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to bypass security restrictions, caused by an error related to insecure HTTP Methods. An attacker could exploit this vulnerability to gain access to the system. IBM X-Force ID: 158881.	2019-06-17	5.0	<a href="#">CVE-2019-4176</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- infosphere_governance_catalog	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 150905.	2019-06-17	5.5	<a href="#">CVE-2018-1845</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- marketing_platform	IBM Marketing Platform 9.1.0, 9.1.2, 10.0, and 10.1 exposes sensitive information in the headers that could be used by an authenticated attacker in further attacks against the system. IBM X-Force ID: 120906.	2019-06-19	4.0	<a href="#">CVE-2017-1107</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that any malicious user connecting to the device can change the default SSID and password thereby denying the owner an access to his/her own device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	<a href="#">CVE-2017-10718</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has default Wi-Fi credentials that are exactly the same for every device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	<a href="#">CVE-2017-10719</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wi-Fi name. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too. The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangenname" which allows a user to change the Wi-Fi name on the device. This function calls a sub function "sub_75876EA0" at address 0x758784F8. The function determines which action to execute based on the parameters sent to it. The "sendchangenname" passes the datastring as the second argument which is the name we enter in the textbox and integer 1 as first argument. The rest of the 3 arguments are set to 0. The function "sub_75876EA0" at address 0x75876F19 uses the first argument received and to determine which block to jump to. Since the argument passed is 1, it jumps to 0x75876F20 and proceeds from there to address 0x75876F56 which calculates the length of the data string passed as the first parameter. This length and the first argument are then passed to the address 0x75877001 which calls the memmove function which uses a stack address as the destination where the password typed by us is passed as the source and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.	2019-06-17	4.6	<a href="#">CVE-2017-10720</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has Telnet functionality enabled by default. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	<a href="#">CVE-2017-10721</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wi-Fi password. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too. The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangepass" which allows a user to change the Wi-Fi password on the device. This function calls a sub function "sub_75876EA0" at address 0x7587857C. The function determines which action to execute based on the parameters sent to it. The "sendchangepass" passes the datastring as the second argument which is the password we enter in the textbox and integer 2 as first argument. The rest of the 3 arguments are set to 0. The function "sub_75876EA0" at address 0x75876F19 uses the first argument received and to determine which block to jump to. Since the argument passed is 2, it jumps to 0x7587718C and proceeds from there to address 0x758771C2 which calculates the length of	2019-06-17	4.6	<a href="#">CVE-2017-10722</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>

	the data string passed as the first parameter. This length and the first argument are then passed to the address 0x7587726F which calls a memmove function which uses a stack address as the destination where the password typed by us is passed as the source and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.			
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device Wi-Fi SSID can exploit a memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries. The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the Wi-Fi name which contains the following format: "SETCMD0001+0001+[2 byte length of wifiname]+[Wifiname]". This request is handled by "control_dev_thread" function which at address "0x00409AE0" compares the incoming request and determines if the 10th byte is 01 and if it is then it redirects to 0x0040A74C which calls the function "setwifiname". The function "setwifiname" uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the \$PC value.	2019-06-17	6.5	<a href="#">CVE-2017-10723</a> MISC MISC BUGTRAQ
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device Wi-Fi SSID can exploit a memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries. The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the Wi-Fi name which contains the following format: "SETCMD0001+0002+[2 byte length of wifipassword]+[Wifipassword]". This request is handled by "control_dev_thread" function which at address "0x00409AE4" compares the incoming request and determines if the 10th byte is 02 and if it is then it redirects to 0x0040A7D8, which calls the function "setwifipassword". The function "setwifipassword" uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the \$PC value.	2019-06-17	6.5	<a href="#">CVE-2017-10724</a> MISC MISC BUGTRAQ
jspxcms -- jspxcms	In jspxcms 9.0.0, a vulnerable URL routing implementation allows remote code execution after logging in as web admin.	2019-06-20	6.5	<a href="#">CVE-2018-16553</a> MISC MISC
kcodes -- netusb.ko	An exploitable arbitrary memory read vulnerability exists in the KCodes NetUSB ko kernel module which enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. A specially crafted index value can cause an invalid memory read, resulting in a denial of service or remote information disclosure. An unauthenticated attacker can send a crafted packet on the local network to trigger this vulnerability.	2019-06-17	6.4	<a href="#">CVE-2019-5016</a> BID MISC
kcodes -- netusb.ko	An exploitable information disclosure vulnerability exists in the KCodes NetUSB ko kernel module that enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. An unauthenticated, remote attacker can craft and send a packet containing an opcode that will trigger the kernel module to return several addresses. One of which can be used to calculate the dynamic base address of the module for further exploitation.	2019-06-17	5.0	<a href="#">CVE-2019-5017</a> BID MISC
linksys -- wrt1900acs_firmware	An issue was discovered on Linksys WRT1900ACS 1.0.3.187766 devices. An ability exists for an unauthenticated user to browse a confidential ui/1.0.99.187766/dynamic/js/setup.js.localized file on the router's webserver, allowing for an attacker to identify possible passwords that the system uses to set the default guest network password. An attacker can use this list of 30 words along with a random 2 digit number to brute force their access onto a router's guest network.	2019-06-17	5.0	<a href="#">CVE-2019-7579</a> MISC MISC
linux -- linux_kernel	915_gem_userptr_get_pages in drivers/gpu/drm/i915/i915_gem_userptr.c in the Linux kernel 4.15.0 on Ubuntu 18.04.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact via crafted ioctl calls to /dev/dri/card0.	2019-06-18	4.6	<a href="#">CVE-2019-12881</a> MISC
misp -- misp	app/Model/Server.php in MISP 2.4.109 allows remote command execution by a super administrator because the PHP file_exists function is used with user-controlled entries, and phar // URLs trigger deserialization.	2019-06-17	6.5	<a href="#">CVE-2019-12868</a> MISC
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. JSON injection exists via the api/v1/data/tqx parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	2019-06-18	4.3	<a href="#">CVE-2018-18836</a> MISC MISC MISC

				<a href="#">CONFIRM</a> <a href="#">MISC</a>
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. HTTP Header Injection exists via the api/v1/data filename parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	2019-06-18	<a href="#">5.8</a>	<a href="#">CVE-2018-18837</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. Log Injection (or Log Forgery) exists via a %0a sequence in the url parameter to api/v1/registry.	2019-06-18	<a href="#">5.0</a>	<a href="#">CVE-2018-18838</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
my-netdata -- netdata	<b>** DISPUTED **</b> An issue was discovered in Netdata 1.10.0. Full Path Disclosure (FPD) exists via api/v1/alarms. NOTE: the vendor says "is intentional."	2019-06-18	<a href="#">5.0</a>	<a href="#">CVE-2018-18839</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nagios -- nagios_xi	An Insufficient Access Control vulnerability (leading to credential disclosure) in coreconfigsnapshot.php (aka configuration snapshot page) in Nagios XI before 5.5.4 allows remote attackers to gain access to configuration files containing confidential credentials.	2019-06-19	<a href="#">5.0</a>	<a href="#">CVE-2018-17148</a> <a href="#">MISC</a>
ngahr -- resourceLink	NGA ResourceLink 20 0.2.1 allows local file inclusion.	2019-06-19	<a href="#">4.0</a>	<a href="#">CVE-2018-18863</a> <a href="#">MISC</a>
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.1 and earlier allows Information Exposure.	2019-06-18	<a href="#">5.0</a>	<a href="#">CVE-2019-7159</a> <a href="#">MISC</a> <a href="#">MISC</a>
openfind -- mail2000	An issue was discovered in Openfind Mail2000 v6 Webmail. XSS can occur via an 'object data="data:text/html' substring in an e-mail message (The vendor subsequently patched this).	2019-06-19	<a href="#">4.3</a>	<a href="#">CVE-2019-9763</a> <a href="#">MISC</a>
otrs -- otrs	An issue was discovered in Open Ticket Request System (OTRS) 7.0 x through 7.0.8, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. In the customer or external frontend, personal information of agents (e.g., Name and mail address) can be disclosed in external notes.	2019-06-17	<a href="#">5.0</a>	<a href="#">CVE-2019-12497</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
php -- php	When using gdImageCreateFromXbm() function of PHP gd extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.	2019-06-18	<a href="#">5.0</a>	<a href="#">CVE-2019-11038</a> <a href="#">CONFIRM</a>
php -- php	Function iconv_mime_decode_headers() in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.	2019-06-18	<a href="#">6.4</a>	<a href="#">CVE-2019-11039</a> <a href="#">CONFIRM</a>
php -- php	When PHP EXIF extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	2019-06-18	<a href="#">6.4</a>	<a href="#">CVE-2019-11040</a> <a href="#">CONFIRM</a>
radare -- radare2	In radare2 through 3.5.1, cmd_mount in libr/core/cmd_mount.c has a double free for the ms command.	2019-06-17	<a href="#">4.3</a>	<a href="#">CVE-2019-12865</a> <a href="#">MISC</a>
ranksol -- live_call_support	CSRF exists in server.php in Live Call Support Application 1.5 for adding an admin account.	2019-06-19	<a href="#">6.8</a>	<a href="#">CVE-2018-17389</a> <a href="#">MISC</a> <a href="#">MISC</a>
ranksol -- nimble_professional	CSRF exists in Nimble Messaging Bulk SMS Marketing Application 1.0 for adding an admin account.	2019-06-19	<a href="#">6.8</a>	<a href="#">CVE-2018-17387</a> <a href="#">MISC</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::UserInteraction#verbose calls say without escaping, escape sequence injection is possible.	2019-06-17	<a href="#">5.0</a>	<a href="#">CVE-2019-8321</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. The gem owner command outputs the contents of the API response directly to stdout. Therefore, if the response is crafted, escape sequence injection may occur.	2019-06-17	<a href="#">5.0</a>	<a href="#">CVE-2019-8322</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Gem::GemcutterUtilities#with_response may output the API response to stdout as it is. Therefore, if the API side modifies the response, escape sequence injection may occur.	2019-06-17	<a href="#">5.0</a>	<a href="#">CVE-2019-8323</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. A crafted gem with a multi-line name is not handled correctly. Therefore, an attacker could inject arbitrary code to the stub line of gemspec, which is eval-ed by code in ensure_loadable_spec during the preinstall check.	2019-06-17	<a href="#">6.8</a>	<a href="#">CVE-2019-8324</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::CommandManager#run calls alert_error without escaping, escape sequence injection is possible. (There are many ways to cause an error.)	2019-06-17	<a href="#">5.0</a>	<a href="#">CVE-2019-8325</a> <a href="#">MISC</a>
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. A web reports module has "export to excel features" that are vulnerable to CSV injection. An attacker can embed Excel formulas inside an automation script that, when exported after execution, results in code execution.	2019-06-17	<a href="#">6.8</a>	<a href="#">CVE-2018-20468</a> <a href="#">MISC</a>



sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. The logs web interface is vulnerable to stored XSS.	2019-06-17	4.3	<a href="#">CVE-2018-20472</a> MISC MISC
samba -- samba	Samba 4.9.x before 4.9.9 and 4.10.x before 4.10.5 has a NULL pointer dereference, leading to Denial of Service. This is related to the AD DC DNS management server (dnsserver) RPC server process.	2019-06-19	4.0	<a href="#">CVE-2019-12435</a> BID UBUNTU CONFIRM
samba -- samba	Samba 4.10.x before 4.10.5 has a NULL pointer dereference, leading to an AD DC LDAP server Denial of Service. This is related to an attacker using the paged search control. The attacker must have directory read access in order to attempt an exploit.	2019-06-19	4.0	<a href="#">CVE-2019-12436</a> BID UBUNTU CONFIRM
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of setting a name for the wireless network. These values are stored by the device in NVRAM (Non-volatile RAM). It seems that the POST parameters passed in this request to set up names on the device do not have a string length check on them. This allows an attacker to send a large payload in the "mssid_1" POST parameter. The device also allows a user to view the name of the Wifi Network set by the user. While processing this request, the device calls a function at address 0x00412CE4 (routerSummary) in the binary "webServer" located in Almond folder, which retrieves the value set earlier by "mssid_1" parameter as SSID2 and this value then results in overflowing the stack set up for this function and allows an attacker to control \$ra register value on the stack which allows an attacker to control the device by executing a payload of an attacker's choice. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in DA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST parameter "mssid_1" at address 0x0042BA00 and then sets in the NVRAM at address 0x0042C314. The value is later retrieved in the function at address 0x00412EAC and this results in overflowing the buffer as the function copies the value directly on the stack.	2019-06-18	4.6	<a href="#">CVE-2017-8329</a> MISC MISC BUGTRAQ
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new port forwarding rules to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in passing commands to a "system" API in the function and thus result in command injection on the device. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in DA-pro we will notice that this follows a MIPS little endian format. The function sub_43C280 in DA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "ip_address" is extracted at address 0x0043C2F0. The POST parameter "ipaddress" is concatenated at address 0x0043C958 and this is passed to a "system" function at address 0x00437284. This allows an attacker to provide the payload of his/her choice and finally take control of the device.	2019-06-18	6.5	<a href="#">CVE-2017-8331</a> MISC MISC BUGTRAQ
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of blocking key words passing in the web traffic to prevent kids from watching content that might be deemed unsafe using the web management interface. It seems that the device does not implement any cross-site scripting protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a stored cross-site scripting payload on the user's browser and execute any action on the device provided by the web management interface.	2019-06-18	6.5	<a href="#">CVE-2017-8332</a> MISC MISC BUGTRAQ
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of blocking IP addresses using the web management interface. It seems that the device does not implement any cross-site scripting forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a cross-site scripting payload on the user's browser and execute any action on the device provided by the web management interface.	2019-06-18	6.0	<a href="#">CVE-2017-8334</a> MISC MISC BUGTRAQ
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of setting name for wireless network. These values are stored by the device in NVRAM (Non-volatile RAM). It seems that the POST parameters passed in this request to set up names on the device do not have a string length check on them. This allows an attacker to send a large payload in the "mssid_1" POST parameter. The device also allows a user to view the name of the Wifi Network set by the user. While processing this request, the device calls a function named "getCfgToHTML" at address 0x004268A8 which retrieves the value set earlier by "mssid_1" parameter as SSID2 and this value then results in overflowing the stack set up for this function and allows an attacker to control \$ra register value on the stack	2019-06-18	6.0	<a href="#">CVE-2017-8335</a> MISC

	which allows an attacker to control the device by executing a payload of an attacker's choice. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST parameter "mssid_1" at address 0x0042BA00 and then sets in the NVRAM at address 0x0042C314. The value is later retrieved in the function "getCfgToHTML" at address 0x00426924 and this results in overflowing the buffer due to "strcat" function that is utilized by this function.			<a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new routes to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in overflowing the stack set up and allow an attacker to control the \$ra register stored on the stack. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST request. The POST parameter "gateway" allows to overflow the stack and control the \$ra register after 1546 characters. The value from this post parameter is then copied on the stack at address 0x00421348 as shown below. This allows an attacker to provide the payload of his/her choice and finally take control of the device.	2019-06-18	<a href="#">6.5</a>	<a href="#">CVE-2017-8336</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of executing various actions on the web management interface. It seems that the device does not implement any Origin header check which allows an attacker who can trick a user to navigate to an attacker's webpage to exploit this issue and brute force the password for the web management interface. It also allows an attacker to then execute any other actions which include management of rules, sensors attached to the devices using the websocket requests.	2019-06-18	<a href="#">6.8</a>	<a href="#">CVE-2017-8337</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
seeddms -- seeddms	SeedDMS before 5.1.11 allows Remote Command Execution (RCE) because of unvalidated file upload of PHP scripts, a different vulnerability than CVE-2018-12940.	2019-06-20	<a href="#">6.0</a>	<a href="#">CVE-2019-12744</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
seeddms -- seeddms	out/out.GroupMgr.php in SeedDMS 5.1.11 has Stored XSS by making a new group with a JavaScript payload as the "GROUP" Name.	2019-06-17	<a href="#">4.3</a>	<a href="#">CVE-2019-12801</a> <a href="#">MISC</a>
teltonika -- rut950_firmware	An issue was discovered on Teltonika RTU950 R_31.04.89 devices. The application allows a user to login without limitation. For every successful login request, the application saves a session. A user can re-login without logging out, causing the application to store the session in memory. Exploitation of this vulnerability will increase memory use and consume free space.	2019-06-19	<a href="#">6.8</a>	<a href="#">CVE-2018-19878</a> <a href="#">MISC</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_firmware	An issue was discovered on TP-Link TL-WR1043ND V2 devices. The credentials can be easily decoded and cracked by brute-force, WordList, or Rainbow Table attacks. Specifically, credentials in the "Authorization" cookie are encoded with URL encoding and base64, leading to easy decoding. Also, the username is cleartext, and the password is hashed with the MD5 algorithm (after decoding of the URL encoded string with base64).	2019-06-19	<a href="#">5.0</a>	<a href="#">CVE-2019-6972</a> <a href="#">MISC</a> <a href="#">MISC</a>
tubigan -- welcome_to_our_resort	The Tubigan "Welcome to our Resort" 1.0 software allows CSRF via admin/mod_users/controller.php?action=edit.	2019-06-18	<a href="#">6.8</a>	<a href="#">CVE-2018-18802</a> <a href="#">MISC</a> <a href="#">MISC</a>
twistedmatrix -- twisted	In words protocols.jabber.xmlstream in Twisted through 19.2.1, XMPP support did not verify certificates when used with TLS, allowing an attacker to MITM connections.	2019-06-16	<a href="#">5.8</a>	<a href="#">CVE-2019-12855</a> <a href="#">MISC</a> <a href="#">MISC</a>
urbackup -- urbackup	In UrBackup 2.2.6, an attacker can send a malformed request to the client over the network, and trigger a fileservplugin/CClientThread.cpp CClientThread::ProcessPacket metadata_id!=0 assertion, leading to shutting down the client application.	2019-06-18	<a href="#">5.0</a>	<a href="#">CVE-2018-20013</a> <a href="#">MISC</a> <a href="#">MISC</a>
znc -- znc	Modules.cpp in ZNC before 1.7.4-rc1 allows remote authenticated non-admin users to escalate privileges and execute arbitrary code by loading a module with a crafted name.	2019-06-15	<a href="#">6.5</a>	<a href="#">CVE-2019-12816</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">BUGTRAQ</a>
zrlog -- zrlog	An issue was discovered in ZRLOG 2.0.1. There is a Stored XSS vulnerability in the nickname field of the comment area.	2019-06-19	<a href="#">4.3</a>	<a href="#">CVE-2018-17079</a> <a href="#">MISC</a> <a href="#">MISC</a>
zucchetti -- hr_portal	Zucchetti HR Portal through 2019-03-15 allows Directory Traversal. Unauthenticated users can escape outside of the restricted location (dot-dot-slash notation) to access files or directories that are elsewhere on the system. Through this vulnerability it is possible to read the application's java sources from /WEB-INF/classes/*.class	2019-06-19	<a href="#">5.0</a>	<a href="#">CVE-2019-10257</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
b3log -- symphony	In Symphony before 3.3.0, there is XSS in the Title under Post. The ID "articleTitle" of this is stored in the "articleTitle" JSON field, and executes a payload when accessing the /member/test/points URI, allowing remote attacks. Any Web script or HTML can be inserted by an admin-authenticated user via a crafted web site name.	2019-06-20	3.5	<a href="#">CVE-2018-16249</a> <a href="#">MISC</a>
cisco -- prime_service_catalog	A vulnerability in the web-based management interface of Cisco Prime Service Catalog could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by adding specific strings to multiple configuration fields. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.	2019-06-19	3.5	<a href="#">CVE-2019-1875</a> <a href="#">BID</a> <a href="#">CISCO</a>
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, a stored Cross-site scripting (XSS) vulnerability allows remote authenticated users to inject arbitrary web script via changestationname.php.	2019-06-18	3.5	<a href="#">CVE-2018-18875</a> <a href="#">MISC</a> <a href="#">MISC</a>
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, a networkdiags.php reflected Cross-site scripting (XSS) vulnerability allows remote authenticated users to inject arbitrary web script.	2019-06-18	3.5	<a href="#">CVE-2018-18880</a> <a href="#">MISC</a> <a href="#">MISC</a>
concrete5 -- concrete5	Concrete5 8.4.3 has XSS because config/concrete.php allows uploads (by administrators) of SVG files that may contain HTML data with a SCRIPT element.	2019-06-17	3.5	<a href="#">CVE-2018-19146</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
creativity -- witycms	The "utilisateur" menu in Creativity wityCMS 0.6.2 modifies the presence of XSS at two input points for user information, with the "first name" and "last name" parameters.	2019-06-20	3.5	<a href="#">CVE-2018-16250</a> <a href="#">MISC</a>
e107 -- e107	An issue was discovered in e107 v2.1.9. There is a XSS attack on e107_admin/comment.php.	2019-06-19	3.5	<a href="#">CVE-2018-17423</a> <a href="#">MISC</a> <a href="#">MISC</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a shell script called relay.sh which is used for creating new SSH relays for the device so that the device connects to Vera servers. All the parameters passed in this specific script are logged to a log file called log_relay in the /tmp folder. The user can also read all the log files from the device using a script called log.sh. However, when the script loads the log files it displays them with content-type text/html and passes all the logs through the ansi2html binary which converts all the character text including HTML meta-characters correctly to be displayed in the browser. This allows an attacker to use the log files as a storing mechanism for the XSS payload and thus whenever a user navigates to that log.sh script, it enables the XSS payload and allows an attacker to execute his malicious payload on the user's browser.	2019-06-17	3.5	<a href="#">CVE-2017-9387</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158332.	2019-06-17	3.5	<a href="#">CVE-2019-4136</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158879.	2019-06-17	2.1	<a href="#">CVE-2019-4174</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158882.	2019-06-17	2.1	<a href="#">CVE-2019-4177</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- control_desk	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160949.	2019-06-19	3.5	<a href="#">CVE-2019-4303</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- i	IBM i 7.27.3 Clustering could allow a local attacker to obtain sensitive information, caused by the use of advanced node failure detection using the REST API to interface with the HMC. An attacker could exploit this vulnerability to obtain HMC credentials. IBM X-Force ID: 162159.	2019-06-14	2.1	<a href="#">CVE-2019-4381</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the View Filters page (view_filters_page.php) and Edit Filter page (manage_filter_edit_page.php) in MantisBT 2.1.0 through 2.17.0 allows remote attackers to inject arbitrary code (if CSP settings permit it) through a crafted PATH_INFO. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-13055.	2019-06-20	2.6	<a href="#">CVE-2018-16514</a> <a href="#">MISC</a>
microfocus --	Cross-Site Scripting vulnerability in Micro Focus Fortify Software Security Center Server, versions 17.2, 18.1, 18.2, has been identified in Micro Focus Software Security Center. The vulnerability could be exploited to execute	2019-06-19	3.5	<a href="#">CVE-2019-11649</a>

fortify_software_security_center	JavaScript code in user's browser. The vulnerability could be exploited to execute JavaScript code in user's browser.			MISC
nagios -- nagios_xi	A cross-site scripting vulnerability exists in Nagios XI before 5.5.4 via the 'name' parameter within the Account Information page. Exploitation of this vulnerability allows an attacker to execute arbitrary JavaScript code within the auto login admin management page.	2019-06-19	3.5	<a href="#">CVE-2018-17146</a> MISC
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a UPnP functionality for devices to interface with the router and interact with the device. It seems that the "NewInMessage" SOAP parameter passed with a huge payload results in crashing the process. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "miniupnpd" is the one that has the vulnerable function that receives the values sent by the SOAP request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function WscDevPutMessage at address 0x0041DBB8 in IDA pro is identified to be receiving the values sent in the SOAP request. The SOAP parameter "NewInMessage" received at address 0x0041DC30 causes the miniupnpd process to finally crash when a second request is sent to the same process.	2019-06-18	3.3	<a href="#">CVE-2017-8330</a> MISC MISC BUGTRAQ
seeddms -- seeddms	out/out.UsrMgr.php in SeedDMS before 5.1.11 allows Stored Cross-Site Scripting (XSS) via the name field.	2019-06-20	3.5	<a href="#">CVE-2019-12745</a> MISC CONFIRM
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x8000204B.	2019-06-21	2.1	<a href="#">CVE-2018-15729</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x80002067.	2019-06-21	2.1	<a href="#">CVE-2018-15730</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x8000205B.	2019-06-21	2.1	<a href="#">CVE-2018-15731</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x80002063.	2019-06-21	2.1	<a href="#">CVE-2018-15732</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a NULL Pointer Dereference vulnerability due to not validating the size of the output buffer value from IOCTL 0x80002028.	2019-06-21	2.1	<a href="#">CVE-2018-15733</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x8000206B.	2019-06-21	2.1	<a href="#">CVE-2018-15734</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x8000206F.	2019-06-21	2.1	<a href="#">CVE-2018-15735</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x8000204F.	2019-06-21	2.1	<a href="#">CVE-2018-15736</a> MISC MISC
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x80002043.	2019-06-21	2.1	<a href="#">CVE-2018-15737</a> MISC MISC
symantec -- data_loss_prevention	DLP 15.5 MP1 and all prior versions may be susceptible to a cross-site scripting (XSS) vulnerability, a type of issue that can enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.	2019-06-19	3.5	<a href="#">CVE-2019-9701</a> MISC
yzmcms -- yzmcms	YzmCMS 5.1 has XSS via the admin/system_manage/user_config_add.html title parameter.	2019-06-20	3.5	<a href="#">CVE-2018-16247</a> MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
akamai -- cloudtest	Akamai CloudTest before 58.30 allows remote code execution.	2019-06-21	not yet calculated	<a href="#">CVE-2019-11011</a> CONFIRM
	When an Apache Geode server versions 1.0.0 to 1.8.0 is			

apache -- geode	operating in secure mode, a user with write permissions for specific data regions can modify internal cluster metadata. A malicious user could modify this data in a way that affects the operation of the cluster.	2019-06-21	not yet calculated	<a href="#">CVE-2017-15694</a> <a href="#">MISC</a>
apache -- tomcat	The fix for CVE-2019-0199 was incomplete and did not address HTTP/2 connection window exhaustion on write in Apache Tomcat versions 9.0.0.M1 to 9.0.19 and 8.5.0 to 8.5.40. By not sending WINDOW_UPDATE messages for the connection window (stream 0) clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS.	2019-06-21	not yet calculated	<a href="#">CVE-2019-10072</a> <a href="#">MISC</a>
asus -- vivobaby_for_android	The ASUS Vivobaby application before 1.1.09 for Android has Missing SSL Certificate Validation.	2019-06-20	not yet calculated	<a href="#">CVE-2017-17944</a> <a href="#">MISC</a>
axentra -- hipserv	/api/2.0/rest/aggregator/xml in Axentra firmware, used by NETGEAR Stora, Seagate GoFlex Home, and MEDION LifeCloud, has an XXE vulnerability that can be chained with an SSRF bug to gain remote command execution as root. It can be triggered by anyone who knows the IP address of the affected device.	2019-06-19	not yet calculated	<a href="#">CVE-2018-18471</a> <a href="#">MISC</a> <a href="#">MISC</a>
bobronix -- jeditor_for_jira	The Bobronix JEditor editor before 3.0.6 for Jira allows an attacker to add a URL/Link (to an existing issue) that can cause forgery of a request to an out-of-origin domain. This in turn may allow for a forged request that can be invoked in the context of an authenticated user, leading to stealing of session tokens and account takeover.	2019-06-21	not yet calculated	<a href="#">CVE-2019-12836</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cerio -- dt-300n_devices	Cerio DT-300N 1.1.6 through 1.1.12 devices allow OS command injection because of improper input validation of the web-interface PNG feature's use of Save.cgi to execute a ping command, as exploited in the wild in October 2018.	2019-06-18	not yet calculated	<a href="#">CVE-2018-18852</a> <a href="#">MISC</a>
check_point_software_technologies -- endpoint_security_client_for_windows	Check Point Endpoint Security Client for Windows, with Anti-Malware blade installed, before version E81.00, tries to load a non-existent DLL during an update initiated by the UI. An attacker with administrator privileges can leverage this to gain code execution within a Check Point Software Technologies signed binary, where under certain circumstances may cause the client to terminate.	2019-06-20	not yet calculated	<a href="#">CVE-2019-8458</a> <a href="#">CONFIRM</a>
check_point_software_technologies -- endpoint_security_client_for_windows	Check Point Endpoint Security Client for Windows, with the VPN blade, before version E80.83, starts a process without using quotes in the path. This can cause loading of a previously placed executable with a name similar to the parts of the path, instead of the intended one.	2019-06-20	not yet calculated	<a href="#">CVE-2019-8459</a> <a href="#">CONFIRM</a>
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to disconnect clients that are connected to the guest network on an affected router. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for device disconnection and providing the connected device information. A successful exploit could allow the attacker to deny service to specific clients that are connected to the guest network.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1897</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to acquire the list of devices that are connected to the guest network. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web interface of the router.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1899</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to access the syslog file on an affected device. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for the syslog file. A successful exploit could allow the attacker to access the information contained in the file.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1898</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- staros	A vulnerability in the internal packet-processing functionality of the Cisco StarOS operating system running on virtual platforms could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error that may occur under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to prevent the targeted service interface from receiving any traffic, which would lead to a DoS condition on the affected interface. The device may have to be manually reloaded to recover from exploitation of this vulnerability.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1869</a> <a href="#">BID</a> <a href="#">CISCO</a>
	A vulnerability in Cisco Digital Network Architecture (DNA) Center could allow an unauthenticated, adjacent attacker to bypass authentication and access critical internal services.			<a href="#">CVE-</a>



cisco -- dna_center	The vulnerability is due to insufficient access restriction to ports necessary for system operation. An attacker could exploit this vulnerability by connecting an unauthorized network device to the subnet designated for cluster services. A successful exploit could allow an attacker to reach internal services that are not hardened for external access.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1848</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- email_security_appliance	A vulnerability in the GZIP decompression engine of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper validation of GZIP-formatted files. An attacker could exploit this vulnerability by sending a malicious file inside a crafted GZIP-compressed file. A successful exploit could allow the attacker to bypass configured content filters that would normally drop the email.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1905</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on the affected device.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1632</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the CLI of Cisco Integrated Management Controller (MC) could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient validation of user-supplied input at the CLI. An attacker could exploit this vulnerability by authenticating with the administrator password via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute arbitrary commands on the device with root privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1879</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the Server Utilities of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to gain unauthorized access to sensitive user information from the configuration data that is stored on the affected system. The vulnerability is due to insufficient protection of data in the configuration file. An attacker could exploit this vulnerability by downloading the configuration file. An exploit could allow the attacker to use the sensitive information from the file to elevate privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1627</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the firmware signature checking program of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient checking of an input buffer. An attacker could exploit this vulnerability by passing a crafted file to the affected system. A successful exploit could inhibit an administrator's ability to access the system.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1630</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect bounds checking. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. An exploit could allow the attacker to cause a buffer overflow, resulting in a process crash and DoS condition on the device.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1628</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the configuration import utility of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to have write access and upload arbitrary data to the filesystem. The vulnerability is due to a failure to delete temporarily uploaded files. An attacker could exploit this vulnerability by crafting a malicious file and uploading it to the affected device. An exploit could allow the attacker to fill up the filesystem or upload malicious scripts.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1629</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web-based UI (web UI) of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web UI on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or reload an affected device. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software with the HTTP Server feature enabled. The default state of the HTTP Server feature is version dependent.	2019-06-20	not yet calculated	<a href="#">CVE-2019-1904</a> <a href="#">MISC</a>

cisco -- multiple_products	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to reload the device and causing a DoS condition.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1843</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- prime_infrastructure	A vulnerability in the Virtual Domain system of Cisco Prime Infrastructure (PI) could allow an authenticated, remote attacker to change the virtual domain configuration, which could lead to privilege escalation. The vulnerability is due to improper validation of API requests. An attacker could exploit this vulnerability by manipulating requests sent to an affected PI server. A successful exploit could allow the attacker to change the virtual domain configuration and possibly elevate privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1906</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- sd_wan_solution	A vulnerability in the vManage web-based UI (Web UI) of the Cisco SD-WAN Solution could allow an authenticated, remote attacker to gain elevated privileges on an affected vManage device. The vulnerability is due to a failure to properly authorize certain user actions in the device configuration. An attacker could exploit this vulnerability by logging in to the vManage Web UI and sending crafted HTTP requests to vManage. A successful exploit could allow attackers to gain elevated privileges and make changes to the configuration that they would not normally be authorized to make.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1626</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- sd_wan_solution	A vulnerability in the CLI of Cisco SD-WAN Solution could allow an authenticated, local attacker to elevate lower-level privileges to the root user on an affected device. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow the attacker to make configuration changes to the system as the root user.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1625</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- sd_wan_solution	A vulnerability in the vManage web-based UI (Web UI) in the Cisco SD-WAN Solution could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the vManage Web UI. A successful exploit could allow the attacker to execute commands with root privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1624</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- security_manager	A vulnerability in Cisco Security Manager could allow an unauthenticated, remote attacker to access sensitive information or cause a denial of service (DoS) condition. The vulnerability is due to improper restrictions on XML entities. An attacker could exploit this vulnerability by sending malicious requests to a targeted system that contain references within XML entities. An exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a DoS condition.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1903</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- telepresence_codec_and_collaboration_endpoint_software	A vulnerability in the Cisco Discovery Protocol (CDP) implementation for the Cisco TelePresence Codec (TC) and Collaboration Endpoint (CE) Software could allow an unauthenticated, adjacent attacker to inject arbitrary shell commands that are executed by the device. The vulnerability is due to insufficient input validation of received CDP packets. An attacker could exploit this vulnerability by sending crafted CDP packets to an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts on the targeted device.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1878</a> <a href="#">CISCO</a>
cisco -- wide_area_application_services_software	A vulnerability in the HTTPS proxy feature of Cisco Wide Area Application Services (WAAS) Software could allow an unauthenticated, remote attacker to use the Central Manager as an HTTPS proxy. The vulnerability is due to insufficient authentication of proxy connection requests. An attacker could exploit this vulnerability by sending a malicious HTTPS CONNECT message to the Central Manager. A successful exploit could allow the attacker to access public internet resources that would normally be blocked by corporate policies.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1876</a> <a href="#">BID</a> <a href="#">CISCO</a>
cloud_foundry_foundation -- bosh	Cloud Foundry BOSH 270.x versions prior to v270.1.1, contain a BOSH Director that does not properly redact credentials when configured to use a MySQL database. A local authenticated malicious user may read any credentials that are contained in a BOSH manifest.	2019-06-18	not yet calculated	<a href="#">CVE-2019-11271</a> <a href="#">CONFIRM</a>
	Cloud Foundry UAA, versions prior to 73.0 0, falls back to appending ?unknown.org? to a user's email address when one is not provided and the user name does not contain an @	2019-06-	not yet	<a href="#">CVE-2019-</a>

cloud_foundry_foundation -- uua_release	character. This domain is held by a private company, which leads to attack vectors including password recovery emails sent to a potentially fraudulent address. This would allow the attacker to gain complete control of the user's account.	19	calculated	<a href="#">3787</a> <a href="#">CONFIRM</a>
cloudera -- manager	An issue was discovered in Cloudera Manager 5.x through 5.15.0. One type of page in Cloudera Manager uses a 'returnUrl' parameter to redirect the user to another page in Cloudera Manager once a wizard is completed. The validity of this parameter was not checked. As a result, the user could be automatically redirected to an attacker's external site or perform a malicious JavaScript function that results in cross-site scripting (XSS). This was fixed by not allowing any value in the returnUrl parameter with patterns such as http://, https://, //, or javascript. The only exceptions to this rule are the SAML Login/Logout URLs, which remain supported since they are explicitly configured and they are not passed via the returnUrl parameter.	2019-06-20	not yet calculated	<a href="#">CVE-2018-15913</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
dell_emc -- avamar_adme_web_interface	Dell EMC Avamar ADMe Web Interface 1 0.50 and 1.0 51 are affected by an LFI vulnerability which may allow a malicious user to download arbitrary files from the affected system by sending a specially crafted request to the Web Interface application.	2019-06-19	not yet calculated	<a href="#">CVE-2019-3737</a> <a href="#">MISC</a>
dell_emc -- supportassist_for_business_and_supportassist_for_home_pcs	Dell SupportAssist for Business PCs version 2.0 and Dell SupportAssist for Home PCs version 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, and 3.2.1 contain an Improper Privilege Management Vulnerability. A malicious local user can exploit this vulnerability by inheriting a system thread using a leaked thread handle to gain system privileges on the affected machine.	2019-06-20	not yet calculated	<a href="#">CVE-2019-3735</a> <a href="#">MISC</a>
ethereum -- primeo_token	The doAirdrop function of a smart contract implementation for Primeo (PEO), an Ethereum token, does not check the numerical relationship between the amount of the air drop and the token's total supply, which lets the owner of the contract issue an arbitrary amount of currency. (Increasing the total supply by using 'doAirdrop' ignores the hard cap written in the contract and devalues the token.)	2019-06-19	not yet calculated	<a href="#">CVE-2018-18425</a> <a href="#">MISC</a> <a href="#">MISC</a>
evernote_corporation -- evernote	A universal Cross-site scripting (UXSS) vulnerability in the Evernote Web Clipper extension before 7.11.1 for Chrome allows remote attackers to run arbitrary web script or HTML in the context of any loaded 3rd-party Frame.	2019-06-18	not yet calculated	<a href="#">CVE-2019-12592</a> <a href="#">MISC</a> <a href="#">MISC</a>
excellent_infotec_corporation -- biyan	EXCELLENT INFOTEK BiYan v1.57 ~ v2.8 allows an attacker to leak user information without being authenticated, by sending a LOGIN_ID element to the auth/main/asp/check_user_login_info.aspx URI, and then reading the response, as demonstrated by the KW_EMAIL or KW_TEL field.	2019-06-19	not yet calculated	<a href="#">CVE-2019-11233</a> <a href="#">MISC</a>
excellent_infotec_corporation -- biyan	EXCELLENT INFOTEK BiYan v1.57 ~ v2.8 allows an attacker to leak user information (Password) without being authenticated, by sending an EMP_NO element to the kws_login/asp/query_user.asp URI, and then reading the PWD element.	2019-06-19	not yet calculated	<a href="#">CVE-2019-11232</a> <a href="#">MISC</a>
forgerock -- openam_and_am	OAuth 2.0 Authorization Server of ForgeRock Access Management (OpenAM) 13.5 0-13.5.1 and Access Management (AM) 5.0.0-5.1.1 does not correctly validate redirect_uri for some invalid requests, which allows attackers to perform phishing via an unvalidated redirect.	2019-06-19	not yet calculated	<a href="#">CVE-2017-14394</a> <a href="#">MISC</a>
forgerock -- openam_and_am	Auth 2.0 Authorization Server of ForgeRock Access Management (OpenAM) 13.5 0-13.5.1 and Access Management (AM) 5.0.0-5.1.1 does not correctly validate redirect_uri for some invalid requests, which allows attackers to execute a script in the user's browser via reflected XSS.	2019-06-19	not yet calculated	<a href="#">CVE-2017-14395</a> <a href="#">MISC</a>
freepbx -- freepbx	FreePBX 13 and 14 has SQL Injection in the DISA module via the hangup variable on the /admin/config.php?display=disa&view=form page.	2019-06-20	not yet calculated	<a href="#">CVE-2018-15892</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
freepbx -- freepbx	An issue was discovered in FreePBX core before 3.0.122.43, 14.0.18.34, and 5.0.1beta4. By crafting a request for adding Asterisk modules, an attacker is able to store JavaScript commands in a module name.	2019-06-20	not yet calculated	<a href="#">CVE-2018-15891</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
glot.io -- glot-www	The default configuration of glot-www through 2018-05-19 allows remote attackers to execute arbitrary code because glot-code-runner supports os system within a "python" "files" "content" JSON file.	2019-06-21	not yet calculated	<a href="#">CVE-2018-15747</a> <a href="#">MISC</a>
helpy -- helpy	Helpy v2.1.0 has Stored XSS via the Ticket title.	2019-06-18	not yet calculated	<a href="#">CVE-2018-18886</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web	2019-06-	not yet	<a href="#">CVE-2019-</a>

m31_printer	server potentially vulnerable to stored XSS in wireless configuration page	17	calculated	<a href="#">CVE-2019-6324</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web server potentially vulnerable to reflected XSS in wireless configuration page.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6323</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web server that is potentially vulnerable to Cross-site Request Forgery.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6325</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an IPP Parser potentially vulnerable to Buffer Overflow.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6327</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have embedded web server attributes which may be potentially vulnerable to Buffer Overflow.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6326</a> <a href="#">MISC</a>
ibm -- sprectrum_protect_plus	BM Spectrum Protect Plus 10.1.2 may display the vSnap CIFS password in the IBM Spectrum Protect Plus Joblog. This can result in an attacker gaining access to sensitive information as well as vSnap. IBM X-Force ID: 162173.	2019-06-19	not yet calculated	<a href="#">CVE-2019-4385</a> <a href="#">CONFIRM</a>
libgcrypt -- libgcrypt	In Libgcrypt 1.8.4, the C implementation of AES is vulnerable to a flush-and-reload side-channel attack because physical addresses are available to other processes. (The C implementation is used on platforms where an assembly-language implementation is unavailable.)	2019-06-19	not yet calculated	<a href="#">CVE-2019-12904</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_windows	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client 1.0.2 (build 02363) for Windows could allow an authenticated, local attacker to run arbitrary code with elevated privileges. On startup, the PIA Windows service (pia-service.exe) loads the OpenSSL library from %PROGRAMFILES%\Private Internet Access\libeay32.dll. This library attempts to load the C:\etc\ssl\openssl.cnf configuration file which does not exist. By default on Windows systems, authenticated users can create directories under C:\. A low privileged user can create a C:\etc\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine library resulting in arbitrary code execution as SYSTEM when the service starts.	2019-06-21	not yet calculated	<a href="#">CVE-2019-12572</a> <a href="#">MISC</a> <a href="#">MISC</a>
netflix -- dial	Denial of Service (DOS) in Dial Reference Source Code Used before June 18th, 2019.	2019-06-21	not yet calculated	<a href="#">CVE-2019-10028</a> <a href="#">CONFIRM</a>
openstack -- magnum	OpenStack Magnum passes OpenStack credentials into the Heat templates creating its instances. While these should just be used for retrieving the instances' SSL certificates, they allow full API access, though and can be used to perform any API operation the user is authorized to perform.	2019-06-21	not yet calculated	<a href="#">CVE-2016-7404</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
opnsense -- opnsense	OPNsense 18.7.x before 18.7.7 has Incorrect Access Control.	2019-06-17	not yet calculated	<a href="#">CVE-2018-18958</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phoenix_contact -- axc_f_2152_and_axc_f_2152_starterkit_devices	An issue was discovered on Phoenix Contact AXC F 2152 (No.2404267) before 2019.0 LTS and AXC F 2152 STARTERKIT (No.1046568) before 2019.0 LTS devices. Unlimited physical access to the PLC may lead to a manipulation of SD cards data. SD card manipulation may lead to an authentication bypass opportunity.	2019-06-18	not yet calculated	<a href="#">CVE-2019-10998</a> <a href="#">CONFIRM</a>
phoenix_contact -- axc_f_2152_and_axc_f_2152_starterkit_devices	An issue was discovered on Phoenix Contact AXC F 2152 (No.2404267) before 2019.0 LTS and AXC F 2152 STARTERKIT (No.1046568) before 2019.0 LTS devices. Protocol Fuzzing on PC WORX Engineer by a man in the middle attacker stops the PLC service. The device must be rebooted, or the PLC service must be restarted manually via a Linux shell.	2019-06-17	not yet calculated	<a href="#">CVE-2019-10997</a> <a href="#">CONFIRM</a>
pix-link -- repeater/router_lv-wr09	An XSS issue on the PIX-Link Repeater/Router LV-WR09 with firmware v28K.MiniRouter.20180616 allows attackers to steal credentials without being connected to the network. The attack vector is a crafted ESS D.	2019-06-22	not yet calculated	<a href="#">CVE-2019-12933</a> <a href="#">MISC</a>
pydio -- pydio	Pydio Cells before 1.5.0 fails to neutralize './' elements, allowing an attacker with minimum privilege to Upload files to, and Delete files/folders from, an unprivileged directory, leading to Privilege escalation.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12901</a> <a href="#">MISC</a> <a href="#">MISC</a>

pydio -- pydio	Pydio Cells before 1 5.0, when supplied with a Name field in an unexpected Unicode format, fails to handle this and includes the database column/table name as part of the error message, exposing sensitive information.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12903</a> MISC MISC
pydio -- pydio	Pydio Cells before 1 5.0 does incomplete cleanup of a user's data upon deletion. This allows a new user, holding the same User ID as a deleted user, to restore the deleted user's data.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12902</a> MISC MISC
rdk_management -- rdkb-20181217-1	A heap-based buffer overflow in cosa_dhcpv4_dml.c in the RDK RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve remote code execution by crafting a long buffer in the "Comment" field of an P reservation form in the admin panel. This is related to the CcspCommonLibrary module.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6963</a> MISC
rdk_management -- rdkb-20181217-1	A shell injection issue in cosa_wifi_apis.c in the RDK RDKB-20181217-1 CcspWifiAgent module allows attackers with login credentials to execute arbitrary shell commands under the CcspWifiSsp process (running as root) if the platform was compiled with the ENABLE_FEATURE_MESHFI macro. The attack is conducted by changing the Wi-Fi network password to include crafted escape characters. This is related to the WebUI module.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6962</a> MISC
rdk_management -- rdkb-20181217-1	Incorrect access control in actionHandlerUtility.php in the RDK RDKB-20181217-1 WebUI module allows a logged in user to control DDNS, QoS, RIP, and other privileged configurations (intended only for the network operator) by sending an HTTP POST to the PHP backend, because the page filtering for non-superuser (in header.php) is done only for GET requests and not for direct AJAX calls.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6961</a> MISC
rdk_management -- rdkb-20181217-1	A heap-based buffer over-read in Service_SetParamStringValue in cosa_x_cisco_com_ddns_dml.c of the RDK RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve information disclosure and code execution by crafting an AJAX call responsible for DDNS configuration with an exactly 64-byte username, password, or domain, for which the buffer size is insufficient for the final ' ' character. This is related to the CcspCommonLibrary and WebUI modules.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6964</a> MISC
redwoodhq -- redwoodhq	RedwoodHQ 2.5 5 does not require any authentication for database operations, which allows remote attackers to create admin users via a con automationframework users insert_one call.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12890</a> MISC MISC
shenzhen_cylan_technology -- clever_dog_smart_camera_dog-2w_and_dog-2w-v4	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the local network has unauthenticated access to the internal SD card via the HTTP service on port 8000. The HTTP web server on the camera allows anyone to view or download the video archive recorded and saved on the external memory card attached to the device.	2019-06-20	not yet calculated	<a href="#">CVE-2019-12919</a> MISC
shenzhen_cylan_technology -- clever_dog_smart_camera_dog-2w_and_dog-2w-v4	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the network can login remotely to the camera and gain root access. The device ships with a hardcoded 12345678 password for the root account, accessible from a TELNET login prompt.	2019-06-20	not yet calculated	<a href="#">CVE-2019-12920</a> MISC
solarwinds -- serv-u_ftp_server	A privilege escalation vulnerability exists in SolarWinds Serv-U before 15.1.7 for Linux.	2019-06-17	not yet calculated	<a href="#">CVE-2019-12181</a> MISC MISC CONFIRM CONFIRM
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices has a Buffer Overflow.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16595</a> MISC MISC
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices allows Directory Traversal.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16594</a> MISC MISC
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices allows Shell Metacharacter Injection.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16593</a> MISC MISC
sophos -- xg_firewall	A shell escape vulnerability in /webconsole/APIController in the API Configuration component of Sophos XG firewall 17.0.8 MR-8 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the "X-Forwarded-for"	2019-06-20	not yet calculated	<a href="#">CVE-2018-16118</a> CONFIRM



	HTTP header.			<a href="#">MISC</a> <a href="#">MISC</a>
sophos -- xg_firewall	SQL injection vulnerability in AccountStatus.jsp in Admin Portal of Sophos XG firewall 17.0.8 MR-8 allow remote authenticated attackers to execute arbitrary SQL commands via the "username" GET parameter.	2019-06-20	not yet calculated	<a href="#">CVE-2018-16116</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
tp_link -- wr1043nd_devices	Stack-based buffer overflow in the httpd server of TP-Link WR1043nd (Firmware Version 3) allows remote attackers to execute arbitrary code via a malicious MediaServer request to /userRpm/MediaServerFoldersCfgRpm.htm.	2019-06-20	not yet calculated	<a href="#">CVE-2018-16119</a> <a href="#">MISC</a> <a href="#">MISC</a>
tufin -- securetrack	An issue was discovered in Tufin SecureTrack 18.1 with TufinOS 2.16 build 1179(Final). The Audit Report module is affected by a blind XXE vulnerability when a new Best Practices Report is saved using a special payload inside the xml input field. The XXE vulnerability is blind since the response doesn't directly display a requested file, but rather returns it inside the name data field when the report is saved. An attacker is able to view restricted operating system files. This issue affects all types of users: administrators or normal users.	2019-06-19	not yet calculated	<a href="#">CVE-2018-18406</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
tyto_software -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. A directory traversal (arbitrary file access) vulnerability exists in the web reports module. This allows an outside attacker to view contents of sensitive files.	2019-06-17	not yet calculated	<a href="#">CVE-2018-20470</a> <a href="#">MISC</a> <a href="#">MISC</a>
vtch -- storio_max_devices	VTech Storio Max before 56.D3JM6 allows remote command execution via shell metacharacters in an Android activity name. It exposes the storeintenttranslate.x service on port 1668 listening for requests on localhost. Requests submitted to this service are checked for a string of random characters followed by the name of an Android activity to start. Activities are started by inserting their name into a string that is executed in a shell command. By inserting metacharacters this can be exploited to run arbitrary commands as root. The requests also match those of the HTTP protocol and can be triggered on any web page rendered on the device by requesting resources stored at an http://127.0.0.1:1668/ URI, as demonstrated by the http://127.0.0.1:1668/dacdb70556479813fab2d92896596eef?";{ping,example.org}' URL.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16618</a> <a href="#">MISC</a> <a href="#">MISC</a>
wago -- multiple_devices	WAGO 852-303 before FW06, 852-1305 before FW06, and 852-1505 before FW03 devices contain hardcoded users and passwords that can be used to login via SSH and TELNET.	2019-06-17	not yet calculated	<a href="#">CVE-2019-12550</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wago -- multiple_devices	WAGO 852-303 before FW06, 852-1305 before FW06, and 852-1505 before FW03 devices contain hardcoded private keys for the SSH daemon. The fingerprint of the SSH host key from the corresponding SSH daemon matches the embedded private key.	2019-06-17	not yet calculated	<a href="#">CVE-2019-12549</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
whatsapp -- whatsapp	When receiving calls using WhatsApp for Android, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for Android prior to 2.18.248 and WhatsApp Business for Android prior to 2.18.132.	2019-06-14	not yet calculated	<a href="#">CVE-2018-6349</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An issue was discovered in the update function in the wpForo Forum plugin before 1.5.2 for WordPress. A registered forum is able to escalate privilege to the forum administrator without any form of user interaction.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16613</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	An arbitrary password reset issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It is possible (due to lack of verification and correlation between the reset password key sent by mail and the user_id parameter) to reset the password of another user. One only needs to know the user_id, which is publicly available. One just has to intercept the password modification request and modify user_id. It is possible to modify the passwords for any users or admin WordPress Ultimate Members. This could lead to account compromise and privilege escalation.	2019-06-21	not yet calculated	<a href="#">CVE-2019-10270</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

---

This email was sent to [tmcinnis@sunnyvale.ca.gov](mailto:tmcinnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** US-CERT  
**To:** [wgularte@ci.sumnysale.ca.us](mailto:wgularte@ci.sumnysale.ca.us)  
**Subject:** SB19-175: Vulnerability Summary for the Week of June 17, 2019  
**Date:** Monday, June 24, 2019 12:52:03 PM



National Cyber Awareness System:

## SB19-175: Vulnerability Summary for the Week of June 17, 2019

06/24/2019 06:54 AM EDT

Original release date: June 24, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
actiontec -- t2200h_firmware	An issue was discovered on Actiontec T2200H T2200H-31.128L.08 devices, as distributed by Telus. By attaching a UART adapter to the UART pins on the system board, an attacker can use a special key sequence (Ctrl-I) to obtain a shell with root privileges. After gaining root access, the attacker can mount the filesystem read-write and make permanent modifications to the device including bricking of the device, disabling vendor management of the device, preventing automatic upgrades, and permanently installing malicious code on the device.	2019-06-17	7.2	<a href="#">CVE-2019-12789</a> <a href="#">MISC</a> <a href="#">MISC</a>
advantech -- webaccess	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 10012 RPC call.	2019-06-18	7.5	<a href="#">CVE-2019-3953</a> <a href="#">MISC</a>
advantech -- webaccess	Stack-based buffer overflow in Advantech WebAccess/SCADA 8.4.0 allows a remote, unauthenticated attacker to execute arbitrary code by sending a crafted IOCTL 81024 RPC call.	2019-06-18	7.5	<a href="#">CVE-2019-3954</a> <a href="#">MISC</a>
arenam -- amgallery	SQL Injection exists in the AMGallery 1.2.3 component for Joomla! via the filter_category_id parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17398</a> <a href="#">MISC</a> <a href="#">MISC</a>
bubblesoftapps -- bubbleupnp	In BubbleUPnP 0.9 update 30, the XML parsing engine for SSDP/UPnP functionality is vulnerable to an XML External Entity Processing (XXE) attack. Remote, unauthenticated attackers can use this vulnerability to: (1) Access arbitrary files from the filesystem with the same permission as the user account running BubbleUPnP, (2) Initiate SMB connections to capture a NetNTLM challenge/response and crack the cleartext password, or (3) Initiate SMB connections to relay a NetNTLM challenge/response and achieve Remote Command Execution in Windows domains.	2019-06-19	7.5	<a href="#">CVE-2018-15506</a> <a href="#">CONFIRM</a>
bzip -- bzip2	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.	2019-06-19	7.5	<a href="#">CVE-2019-12900</a> <a href="#">MISC</a>
chronoscan -- chronoscan	SQL injection vulnerability in ChronoScan version 1.5.4.3 and earlier allows an unauthenticated attacker to execute arbitrary SQL commands via the wcr_machineid cookie.	2019-06-21	7.5	<a href="#">CVE-2018-15868</a> <a href="#">MISC</a> <a href="#">MISC</a>
	A vulnerability in the CLI configuration shell of Cisco Meeting Server could allow an authenticated, local attacker to inject arbitrary commands as the root user. The vulnerability is due to insufficient			<a href="#">CVE-2019-</a>

cisco -- meeting_server	input validation during the execution of a vulnerable CLI command. An attacker with administrator-level credentials could exploit this vulnerability by injecting crafted arguments during command execution. A successful exploit could allow the attacker to perform arbitrary code execution as root on an affected product.	2019-06-19	<a href="#">7.2</a>	<a href="#">1623</a> <a href="#">BID</a> <a href="#">CISCO</a>
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, the BACnet daemon does not properly validate input, which could allow a remote attacker to send specially crafted packets causing the device to become unavailable.	2019-06-18	<a href="#">7.8</a>	<a href="#">CVE-2018-18878</a> <a href="#">MISC</a> <a href="#">MISC</a>
deltaww -- devicenet_builder	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at image00400000+0x0000000000017a45e.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2019-12898</a> <a href="#">MISC</a>
deltaww -- devicenet_builder	Delta Electronics DeviceNet Builder 2.04 has a User Mode Write AV starting at ntdll!RtlQueueWorkItem+0x00000000000005e3.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2019-12899</a> <a href="#">MISC</a>
education_website_project -- education_website	SQL injection exists in Scriptzee Education Website 1.0 via the college_list.html subject, city, or country parameter.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17840</a> <a href="#">MISC</a> <a href="#">MISC</a>
ethereum -- ethereumj	An issue was discovered in EthereumJ 1.8.2. There is Unsafe Deserialization in ois.readObject in mine/Ethash.java and decoder.readObject in crypto/ECKey.java. When a node syncs and mines a new block, arbitrary OS commands can be run on the server.	2019-06-20	<a href="#">10.0</a>	<a href="#">CVE-2018-15890</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.	2019-06-18	<a href="#">7.8</a>	<a href="#">CVE-2019-11477</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
flippa_marketplace_clone_project -- flippa_marketplace_clone	SQL injection exists in Scriptzee Flippa Marketplace Clone 1.0 via the site-search sortBy or sortDir parameter.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17841</a> <a href="#">MISC</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	app/backup/index.php in the Backup Module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation, which allows authenticated administrative attackers to execute commands on the host.	2019-06-17	<a href="#">9.0</a>	<a href="#">CVE-2019-11410</a> <a href="#">MISC</a> <a href="#">MISC</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device firmware file contains a file known as relay.sh which allows the device to create relay ports and connect the device to Vera servers. This is primarily used as a method of communication between the device and Vera servers so the devices can be communicated with even when the user is not at home. One of the parameters retrieved by this specific script is "remote_host". This parameter is not sanitized by the script correctly and is passed in a call to "eval" to execute another script where remote_host is concatenated to be passed a parameter to the second script. This allows an attacker to escape from the executed command and then execute any commands of his/her choice.	2019-06-17	<a href="#">9.0</a>	<a href="#">CVE-2017-9384</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device firmware file contains a file known as proxy.sh which allows the device to proxy a specific request to and from another website. This is primarily used as a method of communication between the device and Vera website when the user is logged in to the https://home.getvera.com and allows the device to communicate between the device and website. One of the parameters retrieved by this specific script is "url". This parameter is not sanitized by the script correctly and is passed in a call to "eval" to execute "curl" functionality. This allows an attacker to escape from the executed command and then execute any commands of his/her choice.	2019-06-17	<a href="#">9.0</a>	<a href="#">CVE-2017-9388</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a web user interface that allows a user to manage the device. As a part of the functionality the device allows a user to install applications written in the Lua programming language. Also the interface allows any user to write his/her application in the Lua language. However, this functionality is not protected by authentication and this allows an attacker to run arbitrary Lua code on the device. The POST request is forwarded to LuaUPnP daemon on the device. This binary handles the received Lua code in the function "LU::JobHandler_LuaUPnP::RunLua(LU::JobHandler_LuaUPnP * __hidden this, LU::UPnPActionWrapper *)". The value in the "code" parameter is then passed to the function "LU::LuaInterface::RunCode(char const*)" which actually loads the Lua engine and runs the code.	2019-06-17	<a href="#">9.0</a>	<a href="#">CVE-2017-9389</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>

getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "request_image" as one of the service actions for a normal user to retrieve an image from a camera that is controlled by the controller. It seems that the "URL" parameter passed in the query string is not sanitized and is stored on the stack which allows an attacker to overflow the buffer. The function "LU::Generic_IP_Camera_Manager::REQ_Image" is activated when the lu_request_image is passed as the "id" parameter in query string. This function then calls "LU::Generic_IP_Camera_Manager::GetUrlFromArguments" and passes a "pointer" to the function where it will be allowed to store the value from the URL parameter. This pointer is passed as the second parameter \$a2 to the function "LU::Generic_IP_Camera_Manager::GetUrlFromArguments". However, neither the callee or the caller in this case performs a simple length check and as a result an attacker who is able to send more than 1336 characters can easily overflow the values stored on the stack including the \$RA value and thus execute code on the device.	2019-06-17	9.0	<a href="#">CVE-2017-9391</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "request_image" as one of the service actions for a normal user to retrieve an image from a camera that is controlled by the controller. It seems that the "res" (resolution) parameter passed in the query string is not sanitized and is stored on the stack which allows an attacker to overflow the buffer. The function "LU::Generic_IP_Camera_Manager::REQ_Image" is activated when the lu_request_image is passed as the "id" parameter in the query string. This function then calls "LU::Generic_IP_Camera_Manager::GetUrlFromArguments". This function retrieves all the parameters passed in the query string including "res" and then uses the value passed in it to fill up buffer using the sprintf function. However, the function in this case lacks a simple length check and as a result an attacker who is able to send more than 184 characters can easily overflow the values stored on the stack including the \$RA value and thus execute code on the device.	2019-06-17	9.0	<a href="#">CVE-2017-9392</a> MISC MISC BUGTRAQ
google -- android	In llcp_util_parse_connect of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-111660010	2019-06-19	7.1	<a href="#">CVE-2018-9561</a> MISC
google -- android	In llcp_util_parse_cc of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-114237888	2019-06-19	7.1	<a href="#">CVE-2018-9563</a> MISC
google -- android	In llcp_util_parse_link_params of llcp_util.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-114238578	2019-06-19	7.1	<a href="#">CVE-2018-9564</a> MISC
google -- android	In findAvailSpellCheckerLocked of TextServicesManagerService.java, there is a possible way to bypass the warning dialog when selecting an untrusted spell checker due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0Android ID: A-118694079	2019-06-19	7.2	<a href="#">CVE-2019-1985</a> MISC
google -- android	In ih264d_fmt_conv_420sp_to_420p of ih264d_format_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118399205	2019-06-19	9.3	<a href="#">CVE-2019-1989</a> MISC
google -- android	In ihevcd_fmt_conv_420sp_to_420p of ihevcd_fmt_conv.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118453553	2019-06-19	9.3	<a href="#">CVE-2019-1990</a> MISC
google -- android	In addLinks of Linkify java, there is a possible phishing vector due to an unusual root cause. This could lead to remote code execution or misdirection of clicks with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116321860	2019-06-19	9.3	<a href="#">CVE-2019-2003</a> MISC



google -- android	In serviceDied of HalDeathHandlerHidl.cpp, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9Android ID: A-116665972	2019-06-19	<a href="#">10.0</a>	<a href="#">CVE-2019-2006 MISC</a>
google -- android	In getReadIndex and getWriteIndex of FifoControllerBase.cpp, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the audio server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-120789744	2019-06-19	<a href="#">10.0</a>	<a href="#">CVE-2019-2007 MISC</a>
google -- android	In createEffect of AudioFlinger.cpp, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-122309228	2019-06-19	<a href="#">7.6</a>	<a href="#">CVE-2019-2008 MISC</a>
google -- android	In l2c_lcc_proc_pdu of l2c_for.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120665616	2019-06-19	<a href="#">8.3</a>	<a href="#">CVE-2019-2009 MISC</a>
google -- android	In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-118152591	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2010 MISC</a>
google -- android	In readNullableNativeHandleNoDup of Parcel.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-120084106	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2011 MISC</a>
google -- android	In rw_t3t_act_handle_fmt_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497437	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2012 MISC</a>
google -- android	In rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120497583	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2013 MISC</a>
google -- android	In rw_t3t_handle_get_sc_poll_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120499324	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2014 MISC</a>
google -- android	In rw_t3t_act_handle_check_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120503926	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2015 MISC</a>
google -- android	In NFA_SendRawFrame of nfa_dm_api.cc, there is a possible out-of-bound write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120664978	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2016 MISC</a>
google -- android	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-121035711	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2017 MISC</a>
google -- android	In resetPasswordInternal of DevicePolicyManagerService.java, there is a possible bypass of password reset protection due to an unusual root cause. Remote user interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-110172241	2019-06-19	<a href="#">9.3</a>	<a href="#">CVE-2019-2018 MISC</a>
google -- android	In ce_t4t_data_cback of ce_t4t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-115635871	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2019 MISC</a>
	In llcp_dlc_proc_rr_mr_pdu of llcp_dlc.cc, there is a possible out-of-			

google -- android	bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-116788646	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2020</a> <a href="#">MISC</a>
google -- android	In rw_t3t_act_handle_ndef_detect_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120428041	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2021</a> <a href="#">MISC</a>
google -- android	In rw_t3t_act_handle_fmt_rsp and rw_t3t_act_handle_sro_rsp of rw_t3t.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9Android ID: A-120506143	2019-06-19	<a href="#">7.1</a>	<a href="#">CVE-2019-2022</a> <a href="#">MISC</a>
google -- android	In ServiceManager::add function in the hardware service manager, there is an insecure permissions check based on the PID of the caller. This could allow an app to add or replace a HAL service with its own service, gaining code execution in a privileged process.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9Android ID: A-121035042Upstream kernel	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2023</a> <a href="#">MISC</a>
google -- android	In em28xx_unregister_dvb of em28xx-dvb.c, there is a possible use after free issue. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-111761954References: Upstream kernel	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2024</a> <a href="#">MISC</a>
google -- android	In binder_thread_read of binder.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-116855682References: Upstream kernel	2019-06-19	<a href="#">7.2</a>	<a href="#">CVE-2019-2025</a> <a href="#">MISC</a>
healthnode_hospital_management_system_project -- healthnode_hospital_management_system	SQL Injection exists in HealthNode Hospital Management System 1.0 via the id parameter to dashboard/Patient/info.php or dashboard/Patient/patientdetails.php.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17393</a> <a href="#">MISC</a> <a href="#">MISC</a>
hotel_booking_engine_project -- hotel_booking_engine	SQL injection exists in Scriptzee Hotel Booking Engine 1.0 via the hotels h_room_type parameter.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17842</a> <a href="#">MISC</a> <a href="#">MISC</a>
ibm -- control_desk	IBM Maximo Asset Management 7.6 is vulnerable to CSV injection, which could allow a remote authenticated attacker to execute arbitrary commands on the system. IBM X-Force ID: 161680.	2019-06-19	<a href="#">8.5</a>	<a href="#">CVE-2019-4364</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- tivoli_netcool/impact	IBM Tivoli Netcool/Impact 7.1.0 allows for remote execution of command by low privileged User. Remote code execution allow to execute arbitrary code on system which lead to take control over the system. IBM X-Force ID: 158094.	2019-06-17	<a href="#">7.7</a>	<a href="#">CVE-2019-4103</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
infoblox -- nios	A privilege escalation vulnerability in the "support access" feature on Infoblox NIOS 6.8 through 8.4.1 could allow a locally authenticated administrator to temporarily gain additional privileges on an affected device and perform actions within the super user scope. The vulnerability is due to a weakness in the "support access" password generation algorithm. A locally authenticated administrative user may be able to exploit this vulnerability if the "support access" feature is enabled, they know the support access code for the current session, and they know the algorithm to generate the support access password from the support access code. "Support access" is disabled by default. When enabled, the access will be automatically disabled (and support access code will expire) after the 24 hours.	2019-06-17	<a href="#">7.2</a>	<a href="#">CVE-2018-10239</a> <a href="#">CONFIRM</a>
jimtlawl_project -- jimtlawl	SQL Injection exists in the Jimtlawl 2.2.7 component for Joomla! via the id parameter.	2019-06-19	<a href="#">7.5</a>	<a href="#">CVE-2018-17399</a> <a href="#">MISC</a> <a href="#">MISC</a>
libgd -- libgd	The GD Graphics Library (aka libgd) through 2.2.5 has a Double Free Vulnerability in the gdImageBmpPtr function.	2019-06-20	<a href="#">7.5</a>	<a href="#">CVE-2018-15878</a> <a href="#">MISC</a>
libgd -- libgd	The GD Graphics Library (aka libgd) through 2.2.5 has a Double Free Vulnerability in the gdImageBmpPt function.	2019-06-20	<a href="#">7.5</a>	<a href="#">CVE-2018-15879</a> <a href="#">MISC</a>
linux -- linux_kernel	A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.	2019-06-14	<a href="#">7.5</a>	<a href="#">CVE-2019-10126</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">BUGTRAQ</a> <a href="#">DEBIAN</a>
linux -- linux_kernel	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service	2019-06-18	<a href="#">7.2</a>	<a href="#">CVE-2019-3896</a> <a href="#">BID</a>

	(DoS).			<a href="#">CONFIRM</a>
onapp -- onapp	OnApp before 5.0.0-88, 5.5 0-93, and 6.0 0-196 allows an attacker to run arbitrary commands with root privileges on servers managed by OnApp for XEN/KVM hypervisors. To exploit the vulnerability an attacker has to have control of a single server on a given cloud (e.g. by renting one). From the source server, the attacker can craft any command and trigger the OnApp platform to execute that command with root privileges on a target server.	2019-06-19	8.5	<a href="#">CVE-2019-12491</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
open-xchange -- open-xchange_appsuite	OX App Suite 7.10 0 and earlier has Incorrect Access Control.	2019-06-17	7.5	<a href="#">CVE-2019-7158</a> <a href="#">MISC</a>
open_faculty_evaluation_system_project -- open_faculty_evaluation_system	Open Faculty Evaluation System 5.6 for PHP 5.6 allows submit_feedback.php SQL Injection, a different vulnerability than CVE-2018-18758.	2019-06-19	7.5	<a href="#">CVE-2018-18757</a> <a href="#">MISC</a> <a href="#">MISC</a>
open_faculty_evaluation_system_project -- open_faculty_evaluation_system	Open Faculty Evaluation System 7 for PHP 7 allows submit_feedback.php SQL Injection, a different vulnerability than CVE-2018-18757.	2019-06-19	7.5	<a href="#">CVE-2018-18758</a> <a href="#">MISC</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-06-19	7.5	<a href="#">CVE-2019-2729</a> <a href="#">MISC</a>
ranksol -- twilio_web_to_fax_machine_system	SQL Injection exists in Twilio WEB To Fax Machine System 1.0 via the email or password parameter to login_check.php, or the id parameter to add_email.php or edit_content.php.	2019-06-19	7.5	<a href="#">CVE-2018-17388</a> <a href="#">MISC</a> <a href="#">MISC</a>
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7 x x and 8.0.0. A parameter in the web reports module is vulnerable to h2 SQL injection. This can be exploited to inject SQL queries and run standard h2 system functions.	2019-06-17	7.5	<a href="#">CVE-2018-20469</a> <a href="#">MISC</a> <a href="#">MISC</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of changing the administrative password for the web management interface. It seems that the device does not implement any cross site request forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface to change a user's password. Also this is a systemic issue.	2019-06-18	9.3	<a href="#">CVE-2017-8328</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new routes to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in passing commands to a "popen" API in the function and thus result in command injection on the device. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a M PS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "dest" is extracted at address 0x00420FC4. The POST parameter "dest" is concatenated in a route add command and this is passed to a "popen" function at address 0x00421220. This allows an attacker to provide the payload of his/her choice and finally take control of the device.	2019-06-18	9.0	<a href="#">CVE-2017-8333</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
sophos -- sfos	A shell escape vulnerability in /webconsole/Controller in Admin Portal of Sophos XG firewall 17.0.8 MR-8 allow remote authenticated attackers to execute arbitrary OS commands via shell metacharacters in the "dbName" POST parameter.	2019-06-20	9.0	<a href="#">CVE-2018-16117</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
thephpfactory -- auction_factory	SQL Injection exists in the Auction Factory 4.5.5 component for Joomla! via the filter_order_Dir or filter_order parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17374</a> <a href="#">MISC</a> <a href="#">MISC</a>
thephpfactory -- dutch_auction_factory	SQL Injection exists in the Dutch Auction Factory 2.0.2 component for Joomla! via the filter_order_Dir or filter_order parameter.	2019-06-19	7.5	<a href="#">CVE-2018-17381</a> <a href="#">MISC</a> <a href="#">MISC</a>
thephpfactory -- micro_deal_factory	SQL Injection exists in the Micro Deal Factory 2.4.0 component for Joomla! via the id parameter, or the PATH_INFO to mydeals/ or listdeals/.	2019-06-19	7.5	<a href="#">CVE-2018-17386</a> <a href="#">MISC</a> <a href="#">MISC</a>
tp-link -- tl-wr1043nd_firmware	An issue was discovered on TP-Link TL-WR1043ND V2 devices. An attacker can send a cookie in an HTTP authentication packet to the router management web interface, and fully control the router without knowledge of the credentials.	2019-06-19	10.0	<a href="#">CVE-2019-6971</a> <a href="#">MISC</a> <a href="#">MISC</a>

videolan -- vlc_media_player	An issue was discovered in zlib_decompress_extra in modules/demux/mkv/util.cpp in VideoLAN VLC media player 3.x through 3.0.7. The Matroska demuxer, while parsing a malformed MKV file type, has a double free.	2019-06-18	7.5	<a href="#">CVE-2019-12874</a> MISC
webmin -- webmin	In Webmin through 1.910, any user authorized to the "Package Updates" module can execute arbitrary commands with root privileges via the data parameter to update.cgi.	2019-06-15	9.0	<a href="#">CVE-2019-12840</a> MISC BID MISC MISC
westerndigital -- my_book_live_firmware	Western Digital WD My Book Live (all versions) has a root Remote Command Execution bug via shell metacharacters in the /api/1.0/rest/language_configuration language parameter. It can be triggered by anyone who knows the IP address of the affected device.	2019-06-19	10.0	<a href="#">CVE-2018-18472</a> MISC MISC
whatsapp -- whatsapp	When receiving calls using WhatsApp for iOS, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for iOS prior to v2.18.90.24 and WhatsApp Business for iOS prior to v2.18.90.24.	2019-06-14	7.5	<a href="#">CVE-2018-20655</a> BID MISC
whatsapp -- whatsapp	An out-of-bounds read was possible in WhatsApp due to incorrect parsing of RTP extension headers. This issue affects WhatsApp for Android prior to 2.18.276, WhatsApp Business for Android prior to 2.18.99, WhatsApp for iOS prior to 2.18.100.6, WhatsApp Business for iOS prior to 2.18.100.2, and WhatsApp for Windows Phone prior to 2.18.224.	2019-06-14	7.5	<a href="#">CVE-2018-6350</a> BID MISC
zohocorp -- manageengine_adselfservice_plus	An authentication bypass vulnerability in the password reset functionality in Zoho ManageEngine ADSelfService Plus before 5.0.6 allows an attacker with physical access to gain a shell with SYSTEM privileges via the restricted thick client browser. The attack uses a long sequence of crafted keyboard input.	2019-06-17	7.2	<a href="#">CVE-2019-12476</a> BID MISC MISC
zohocorp -- manageengine_analytics_plus	Multiple Zoho ManageEngine products suffer from local privilege escalation due to improper permissions for the %SYSTEMDRIVE%\ManageEngine directory and its sub-folders. Moreover, the services associated with said products try to execute binaries such as sc.exe from the current directory upon system start. This will effectively allow non-privileged users to escalate privileges to NT AUTHORITY\SYSTEM. This affects Desktop Central 10.0.380, EventLog Analyzer 12.0.2, ServiceDesk Plus 10.0.0, SupportCenter Plus 8.1, O365 Manager Plus 4.0, Mobile Device Manager Plus 9.0.0, Patch Connect Plus 9.0.0, Vulnerability Manager Plus 9.0.0, Patch Manager Plus 9.0.0, OpManager 12.3, NetFlow Analyzer 11.0, OpUtils 11.0, Network Configuration Manager 11.0, FireWall 12.0, Key Manager Plus 5.6, Password Manager Pro 9.9, Analytics Plus 1.0, and Browser Security Plus.	2019-06-18	7.2	<a href="#">CVE-2019-12133</a> MISC CONFIRM

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
afian -- filerun	FileRun 2019.05.21 allows XSS via the filename to the ? module=fileman&section=do&page=up URI.	2019-06-20	4.3	<a href="#">CVE-2019-12905</a> MISC
alpinelinux -- abuild	Alpine Linux abuild through 3.4.0 allows an unprivileged member of the abuild group to add an untrusted package via a --keys-dir option that causes acceptance of an untrusted signing key.	2019-06-18	4.0	<a href="#">CVE-2019-12875</a> MISC MISC
alternate-tools -- alternate_pic_view	Alternate Pic View 2.600 has a User Mode Write AV starting at PicViewer!PerfgrapFinalize+0x000000000000a8868.	2019-06-19	5.0	<a href="#">CVE-2019-12893</a> MISC
alternate-tools -- alternate_pic_view	Alternate Pic View 2.600 has a Read Access Violation at the Instruction Pointer after a call from PicViewer!PerfgrapFinalize+0x000000000000a9a1b.	2019-06-19	5.0	<a href="#">CVE-2019-12894</a> MISC
alternate-tools -- alternate_pic_view	In Alternate Pic View 2.600, the Exception Handler is Corrupted starting at PicViewer!PerfgrapFinalize+0x000000000000b916d.	2019-06-19	5.0	<a href="#">CVE-2019-12895</a> MISC
apache -- allura	In Apache Allura prior to 1.11.0, a vulnerability exists for stored XSS on the user dropdown selector when creating or editing tickets. The XSS executes when a user engages with that dropdown on that page.	2019-06-18	4.3	<a href="#">CVE-2019-10085</a> BID MISC MLIST
artha_project -- artha	Artha ~ The Open Thesaurus 1.0.3.0 has a Buffer Overflow.	2019-06-18	5.0	<a href="#">CVE-2018-18944</a> MISC MISC
b3log -- solo	b3log Solo 2.9.3 has XSS in the Input page under the "Publish Articles" menu with an ID of "articleTags" stored in the "tag" JSON field, which allows remote attackers to inject arbitrary Web scripts or HTML via a carefully crafted site name in an admin-authenticated HTTP request.	2019-06-20	4.3	<a href="#">CVE-2018-16248</a> MISC
	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to access potentially sensitive system usage information. The			<a href="#">CVE-2019-1631</a>

cisco -- integrated_management_controller	vulnerability is due to a lack of proper data protection mechanisms. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow an attacker to view sensitive system data.	2019-06-19	5.0	<a href="#">BID</a> <a href="#">CISCO</a>
cisco -- prime_service_catalog	A vulnerability in the web-based management interface of Cisco Prime Service Catalog Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protection mechanisms on the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user.	2019-06-19	6.8	<a href="#">CVE-2019-1874</a> <a href="#">BID</a> <a href="#">CISCO</a>
cloudera -- data_science_workbench	An issue was discovered in Cloudera Data Science Workbench (CDSW) 1.2.x through 1.4.0. Unauthenticated users can get a list of user accounts.	2019-06-21	5.0	<a href="#">CVE-2018-15665</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, a readouts_rd.php directory traversal issue makes it possible to read any file present on the underlying operating system.	2019-06-18	5.0	<a href="#">CVE-2018-18876</a> <a href="#">MISC</a> <a href="#">MISC</a>
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, an authenticated web user can access an alternative configuration page config_main.php that allows manipulation of the device.	2019-06-18	6.5	<a href="#">CVE-2018-18877</a> <a href="#">MISC</a> <a href="#">MISC</a>
columbiaweather -- weather_microserver_firmware	In firmware version MS_2.6.9900 of Columbia Weather MicroServer, an authenticated web user can pipe commands directly to the underlying operating system as user input is not sanitized in networkdiags.php.	2019-06-18	6.5	<a href="#">CVE-2018-18879</a> <a href="#">MISC</a> <a href="#">MISC</a>
corel -- paintshop_pro_2019	An issue was discovered in Corel PaintShop Pro 2019 21.0.0.119. An integer overflow in the jp2 parsing library allows an attacker to overwrite memory and to execute arbitrary code.	2019-06-19	6.8	<a href="#">CVE-2019-6114</a> <a href="#">MISC</a>
craftcms -- craft_cms	Craft CMS 3.1.30 has XSS.	2019-06-18	4.3	<a href="#">CVE-2019-12823</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
creativity -- witycms	A "search for user discovery" injection issue exists in Creativity wityCMS 0.6.2 via the "Utilisateur" menu. No input parameters are filtered, e.g., the /admin/user/users Nickname, email, firstname, lastname, and groupe parameters.	2019-06-20	4.0	<a href="#">CVE-2018-16251</a> <a href="#">MISC</a>
debian -- debian_linux	An issue was discovered in Open Ticket Request System (OTRS) 7.0.x through 7.0.7, Community Edition 6.0.x through 6.0.19, and Community Edition 5.0.x through 5.0.36. An attacker could send a malicious email to an OTRS system. If a logged-in agent user quotes it, the email could cause the browser to load external image resources.	2019-06-17	4.3	<a href="#">CVE-2019-12248</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.1.6 is vulnerable to a SQL injection that can be exploited by an attacker of the role Publisher via view_unpushed_bundles.jsp.	2019-06-18	6.5	<a href="#">CVE-2019-12872</a> <a href="#">MISC</a> <a href="#">MISC</a>
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows XML External Entity Blind Injection, related to pingback.axd and BlogEngine.Core/Web/HttpHandlers/PingbackHandler.cs.	2019-06-21	5.0	<a href="#">CVE-2019-10718</a> <a href="#">MISC</a> <a href="#">MISC</a>
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution because file creation is mishandled, related to /api/upload and BlogEngine.NET/AppCode/Api/UploadController.cs. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714.	2019-06-21	6.5	<a href="#">CVE-2019-10719</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7.0 and earlier allows Directory Traversal and Remote Code Execution via the theme cookie to the File Manager. NOTE: this issue exists because of an incomplete fix for CVE-2019-6714.	2019-06-21	6.5	<a href="#">CVE-2019-10720</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MISC</a>
dotnetblogengine -- blogengine.net	BlogEngine.NET 3.3.7 and earlier allows XXE via an apml file to syndication.axd.	2019-06-21	5.0	<a href="#">CVE-2019-11392</a> <a href="#">MISC</a>
edrawsoft -- edraw_max	Edraw Max 7.9.3 has Heap Corruption starting at ntdll!RtlpNtMakeTemporaryKey+0x0000000000001a77.	2019-06-19	5.0	<a href="#">CVE-2019-12896</a> <a href="#">MISC</a>
edrawsoft -- edraw_max	Edraw Max 7.9.3 has a Read Access Violation at the Instruction Pointer after a call from ObjectModule!Paint::Clear+0x0000000000000074.	2019-06-19	5.0	<a href="#">CVE-2019-12897</a> <a href="#">MISC</a>
exacq -- enterprise_system_manager	A vulnerability in the exacqVision Enterprise System Manager (ESM) v5.12.2 application whereby unauthorized privilege escalation can potentially be achieved. This vulnerability impacts exacqVision ESM v5.12.2 and all prior versions of ESM running on a Windows operating system. This issue does not impact any Windows Server OSs, or Linux deployments with permissions that are not inherited from the root directory. Authorized Users have ?modify? permission to the ESM folders, which allows a low privilege account to modify files located in these directories. An executable can be renamed and replaced by a malicious file that could connect back to a bad actor providing system level privileges. A low privileged user is not able to restart the service, but a restart of the system would trigger the execution of	2019-06-18	6.9	<a href="#">CVE-2019-7588</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>



	the malicious file. This issue affects: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) Version 5.12.2 and prior versions; This issue does not affect: Exacq Technologies, Inc. exacqVision Enterprise System Manager (ESM) 19.03 and above.			
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.	2019-06-18	5.0	<a href="#">CVE-2019-11478</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
f5 -- big-ip_access_policy_manager	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.	2019-06-18	5.0	<a href="#">CVE-2019-11479</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CERT-VN</a>
fasterxml -- jackson-databind	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x through 2.9.9. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has JDOM 1.x or 2.x jar in the classpath, an attacker can send a specifically crafted JSON message that allows them to read arbitrary local files on the server.	2019-06-19	4.3	<a href="#">CVE-2019-12814</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a>
foxitsoftware -- foxit_pdf_sdk_activex	A use after free in the TextBox field Validate action in IReader_ContentProvider can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031. An attacker can leverage this to gain remote code execution. Relative to CVE-2018-19452, this has a different free location and requires different JavaScript code for exploitation.	2019-06-17	6.8	<a href="#">CVE-2018-19444</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API app.launchURL is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19445</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A File Write can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API Doc createDataObject is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19446</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A stack-based buffer overflow can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) 5.4.0.1031 when parsing the URI string. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19447</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	In Foxit Reader SDK (ActiveX) Professional 5.4.0.1031, an uninitialized object in IReader_ContentProvider::GetDocEventHandler occurs when embedding the control into Office documents. By opening a specially crafted document, an attacker can trigger an out of bounds write condition, possibly leveraging this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19448</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A File Write can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) Professional 5.4.0.1031 when the JavaScript API Doc exportAsFDF is used. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19449</a> <a href="#">MISC</a>
foxitsoftware -- foxit_pdf_sdk_activex	A command injection can occur for specially crafted PDF files in Foxit Reader SDK (ActiveX) 5.4.0.1031 when parsing a launch action. An attacker can leverage this to gain remote code execution.	2019-06-17	6.8	<a href="#">CVE-2018-19450</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 suffers from an information disclosure vulnerability due to excessive debug information, which allows authenticated administrative attackers to obtain credentials and other sensitive information.	2019-06-17	4.0	<a href="#">CVE-2019-11407</a> <a href="#">MISC</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	XSS in app/operator_panel/index_inc.php in the Operator Panel module in FusionPBX 4.4.3 allows remote unauthenticated attackers to inject arbitrary JavaScript characters by placing a phone call using a specially crafted caller ID number. This can further lead to remote code execution by chaining this vulnerability with a command injection vulnerability also present in FusionPBX.	2019-06-17	4.3	<a href="#">CVE-2019-11408</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
fusionpbx -- fusionpbx	app/operator_panel/exec.php in the Operator Panel module in FusionPBX 4.4.3 suffers from a command injection vulnerability due to a lack of input validation that allows authenticated non-administrative attackers to execute commands on the host. This can further lead to remote code execution when combined with an XSS vulnerability also present in the FusionPBX Operator Panel module.	2019-06-17	6.5	<a href="#">CVE-2019-11409</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
genieaccess -- wip3bvaf_firmware	Genie Access WIP3BVAf WISH IP 3MP IR Auto Focus Bullet Camera devices through 3.x are vulnerable to directory traversal via the web interface, as demonstrated by reading /etc/shadow. NOTE: this product is discontinued, and its final firmware version has this vulnerability (4.x versions exist only for other Genie Access products).	2019-06-17	5.0	<a href="#">CVE-2019-7315</a> <a href="#">MISC</a>
	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a user with the capability of installing or			

getvera -- veraedge_firmware	deleting apps on the device using the web management interface. It seems that the device does not implement any cross-site request forgery protection mechanism which allows an attacker to trick a user who navigates to an attacker controlled page to install or delete an application on the device. Note: The cross-site request forgery is a systemic issue across all other functionalities of the device.	2019-06-17	6.8	<a href="#">CVE-2017-9381</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "file" as one of the service actions for a normal user to read a file that is stored under the /etc/cmh-lu folder. It retrieves the value from the "parameters" query string variable and then passes it to an internal function "FileUtils: ReadFileIntoBuffer" which is a library function that does not perform any sanitization on the value submitted and this allows an attacker to use directory traversal characters ". /" and read files from other folders within the device.	2019-06-17	4.0	<a href="#">CVE-2017-9382</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides UPnP services that are available on port 3480 and can also be accessed via port 80 using the url "/port_3480". It seems that the UPnP services provide "wget" as one of the service actions for a normal user to connect the device to an external website. It retrieves the parameter "URL" from the query string and then passes it to an internal function that uses the curl module on the device to retrieve the contents of the website.	2019-06-17	6.5	<a href="#">CVE-2017-9383</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera Veralite 1.7.481 devices. The device has an additional OpenWRT interface in addition to the standard web interface which allows the highest privileges a user can obtain on the device. This web interface uses root as the username and the password in the /etc/cmh/cmh conf file which can be extracted by an attacker using a directory traversal attack, and then log in to the device with the highest privileges.	2019-06-17	5.0	<a href="#">CVE-2017-9385</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a script file called "get_file.sh" which allows a user to retrieve any file stored in the "cmh-ext" folder on the device. However, the "filename" parameter is not validated correctly and this allows an attacker to directory traverse outside the /cmh-ext folder and read any file on the device. It is necessary to create the folder "cmh-ext" on the device which can be executed by an attacker first in an unauthenticated fashion and then execute a directory traversal attack.	2019-06-17	4.0	<a href="#">CVE-2017-9386</a> MISC MISC BUGTRAQ
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a shell script called connect.sh which is supposed to return a specific cookie for the user when the user is authenticated to https://home.getvera.com. One of the parameters retrieved by this script is "RedirectURL". However, the application lacks strict input validation of this parameter and this allows an attacker to execute the client-side code on this application.	2019-06-17	4.3	<a href="#">CVE-2017-9390</a> MISC MISC BUGTRAQ
gnu -- bash	A heap-based buffer overflow exists in GNU Bash before 4.3 when wide characters, not supported by the current locale set in the LC_CTYPE environment variable, are printed through the echo built-in function. A local attacker, who can provide data to print through the "echo -e" built-in function, may use this flaw to crash a script or execute code with the privileges of the bash process. This occurs because ansicstr() in lib/sh/strtrans.c mishandles u32cconv().	2019-06-18	4.6	<a href="#">CVE-2012-6711</a> MISC BID MISC
google -- android	In publishKeyEvent, publishMotionEvent and sendUnchainedFinishedSignal of InputTransport.cpp, there are uninitialized data leading to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9 Android ID: A-115739809	2019-06-19	4.9	<a href="#">CVE-2019-2004</a> MISC
google -- android	In onPermissionGrantResult of GrantPermissionsActivity.java, there is a possible incorrectly granted permission due to a missing permission check. This could lead to local escalation of privilege on a locked device with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android-8.0 Android-8.1 Android-9 Android ID: A-68777217	2019-06-19	6.8	<a href="#">CVE-2019-2005</a> MISC
i-doit -- i-doit	An XSS issue was discovered in i-doit Open 1.12 via the src/tools/php/qr/qr.php url parameter.	2019-06-18	4.3	<a href="#">CVE-2019-6965</a> MISC
ibm -- campaign	IBM Campaign 9.1.2 and 10.1 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request containing "dot dot" sequences (./..) to view arbitrary files on the system. IBM X-Force ID: 162172.	2019-06-19	4.0	<a href="#">CVE-2019-4384</a> XF CONFIRM
ibm -- cloud_private	IBM Cloud Private 2.1.0, 3.1.0, 3.1.1, and 3.1.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 158338.	2019-06-18	6.8	<a href="#">CVE-2019-4142</a> XF CONFIRM
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to obtain sensitive information, caused by a flaw in the HTTP OPTIONS method, aka Optionsbleed. By sending an OPTIONS HTTP request, a remote attacker could exploit this vulnerability to read secret data from process memory and obtain sensitive information. IBM X-Force ID: 158878.	2019-06-17	4.0	<a href="#">CVE-2019-4173</a> CONFIRM XF
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3.0, 10.3.1, and 10.4.0 could allow a remote attacker to bypass security restrictions, caused by an error related to insecure HTTP Methods. An attacker could exploit this vulnerability to	2019-06-17	5.0	<a href="#">CVE-2019-4176</a> CONFIRM XF

	gain access to the system. IBM X-Force D: 158881.			
ibm -- infosphere_governance_catalog	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 150905.	2019-06-17	5.5	<a href="#">CVE-2018-1845</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- marketing_platform	IBM Marketing Platform 9.1.0, 9.1.2, 10.0, and 10.1 exposes sensitive information in the headers that could be used by an authenticated attacker in further attacks against the system. IBM X-Force ID: 120906.	2019-06-19	4.0	<a href="#">CVE-2017-1107</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that any malicious user connecting to the device can change the default SSID and password thereby denying the owner an access to his/her own device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	<a href="#">CVE-2017-10718</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has default Wi-Fi credentials that are exactly the same for every device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	<a href="#">CVE-2017-10719</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wi-Fi name. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too. The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangenam" which allows a user to change the Wi-Fi name on the device. This function calls a sub function "sub_75876EA0" at address 0x758784F8. The function determines which action to execute based on the parameters sent to it. The "sendchangenam" passes the datastring as the second argument which is the name we enter in the textbox and integer 1 as first argument. The rest of the 3 arguments are set to 0. The function "sub_75876EA0" at address 0x75876F19 uses the first argument received and to determine which block to jump to. Since the argument passed is 1, it jumps to 0x75876F20 and proceeds from there to address 0x75876F56 which calculates the length of the data string passed as the first parameter. This length and the first argument are then passed to the address 0x75877001 which calls the memmove function which uses a stack address as the destination where the password typed by us is passed as the source and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.	2019-06-17	4.6	<a href="#">CVE-2017-10720</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the device has Telnet functionality enabled by default. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries.	2019-06-17	4.0	<a href="#">CVE-2017-10721</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that the desktop application used to connect to the device suffers from a stack overflow if more than 26 characters are passed to it as the Wi-Fi password. This application is installed on the device and an attacker who can provide the right payload can execute code on the user's system directly. Any breach of this system can allow an attacker to get access to all the data that the user has access too. The application uses a dynamic link library(DLL) called "avilib.dll" which is used by the application to send binary packets to the device that allow to control the device. One such action that the DLL provides is change password in the function "sendchangepass" which allows a user to change the Wi-Fi password on the device. This function calls a sub function "sub_75876EA0" at address 0x7587857C. The function determines which action to execute based on the parameters sent to it. The "sendchangepass" passes the datastring as the second argument which is the password we enter in the textbox and integer 2 as first argument. The rest of the 3 arguments are set to 0. The function "sub_75876EA0" at address 0x75876F19 uses the first argument received and to determine which block to jump to. Since the argument passed is 2, it jumps to 0x7587718C and proceeds from there to address 0x758771C2 which calculates the length of the data string passed as the first parameter. This length and the first argument are then passed to the address 0x7587726F which calls a memmove function which uses a stack address as the destination where the	2019-06-17	4.6	<a href="#">CVE-2017-10722</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>

	password typed by us is passed as the source and length calculated above is passed as the number of bytes to copy which leads to a stack overflow.			
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device Wi-Fi SSID can exploit a memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries. The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the Wi-Fi name which contains the following format: "SETCMD0001+0001+[2 byte length of wifiname]+[Wifiname]". This request is handled by "control_dev_thread" function which at address "0x00409AE0" compares the incoming request and determines if the 10th byte is 01 and if it is then it redirects to 0x0040A74C which calls the function "setwifiname". The function "setwifiname" uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the \$PC value.	2019-06-17	6.5	<a href="#">CVE-2017-10723</a> MISC MISC BUGTRAQ
ishekar -- endoscope_camera_firmware	Recently it was discovered as a part of the research on IoT devices in the most recent firmware for Shekar Endoscope that an attacker connected to the device Wi-Fi SSID can exploit a memory corruption issue and execute remote code on the device. This device acts as an Endoscope camera that allows its users to use it in various industrial systems and settings, car garages, and also in some cases in the medical clinics to get access to areas that are difficult for a human being to reach. Any breach of this system can allow an attacker to get access to video feed and pictures viewed by that user and might allow them to get a foot hold in air gapped networks especially in case of nation critical infrastructure/industries. The firmware contains binary uvc_stream that is the UDP daemon which is responsible for handling all the UDP requests that the device receives. The client application sends a UDP request to change the Wi-Fi name which contains the following format: "SETCMD0001+0002+[2 byte length of wifipassword]+[Wifipassword]". This request is handled by "control_dev_thread" function which at address "0x00409AE4" compares the incoming request and determines if the 10th byte is 02 and if it is then it redirects to 0x0040A7D8, which calls the function "setwifipassword". The function "setwifipassword" uses a memcpy function but uses the length of the payload obtained by using strlen function as the third parameter which is the number of bytes to copy and this allows an attacker to overflow the function and control the \$PC value.	2019-06-17	6.5	<a href="#">CVE-2017-10724</a> MISC MISC BUGTRAQ
jspxcms -- jspxcms	In Jspxcms 9.0.0, a vulnerable URL routing implementation allows remote code execution after logging in as web admin.	2019-06-20	6.5	<a href="#">CVE-2018-16553</a> MISC MISC
kcodes -- netusb.ko	An exploitable arbitrary memory read vulnerability exists in the KCodes NetUSB ko kernel module which enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. A specially crafted index value can cause an invalid memory read, resulting in a denial of service or remote information disclosure. An unauthenticated attacker can send a crafted packet on the local network to trigger this vulnerability.	2019-06-17	6.4	<a href="#">CVE-2019-5016</a> BID MISC
kcodes -- netusb.ko	An exploitable information disclosure vulnerability exists in the KCodes NetUSB ko kernel module that enables the ReadySHARE Printer functionality of at least two NETGEAR Nighthawk Routers and potentially several other vendors/products. An unauthenticated, remote attacker can craft and send a packet containing an opcode that will trigger the kernel module to return several addresses. One of which can be used to calculate the dynamic base address of the module for further exploitation.	2019-06-17	5.0	<a href="#">CVE-2019-5017</a> BID MISC
linksys -- wrt1900acs_firmware	An issue was discovered on Linksys WRT1900ACS 1.0.3.187766 devices. An ability exists for an unauthenticated user to browse a confidential ui/1.0.99.187766/dynamic/js/setup.js.localized file on the router's webserver, allowing for an attacker to identify possible passwords that the system uses to set the default guest network password. An attacker can use this list of 30 words along with a random 2 digit number to brute force their access onto a router's guest network.	2019-06-17	5.0	<a href="#">CVE-2019-7579</a> MISC MISC
linux -- linux_kernel	i915_gem_userptr_get_pages in drivers/gpu/drm/i915/i915_gem_userptr.c in the Linux kernel 4.15.0 on Ubuntu 18.04.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) or possibly have unspecified other impact via crafted ioctl calls to /dev/dri/card0.	2019-06-18	4.6	<a href="#">CVE-2019-12881</a> MISC
misp -- misp	app/Model/Server.php in MISP 2.4.109 allows remote command execution by a super administrator because the PHP file_exists function is used with user-controlled entries, and phar // URLs trigger deserialization.	2019-06-17	6.5	<a href="#">CVE-2019-12868</a> MISC
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. JSON injection exists via the api/v1/data txq parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	2019-06-18	4.3	<a href="#">CVE-2018-18836</a> MISC MISC MISC CONFIRM MISC
				<a href="#">CVE-2018-</a>

my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. HTTP Header Injection exists via the api/v1/data filename parameter because of web_client_api_request_v1_data in web/api/web_api_v1.c.	2019-06-18	5.8	<a href="#">18837</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
my-netdata -- netdata	An issue was discovered in Netdata 1.10.0. Log Injection (or Log Forgery) exists via a %0a sequence in the url parameter to api/v1/registry.	2019-06-18	5.0	<a href="#">CVE-2018-18838</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
my-netdata -- netdata	<b>** DISPUTED **</b> An issue was discovered in Netdata 1.10.0. Full Path Disclosure (FPD) exists via api/v1/alarms. NOTE: the vendor says "is intentional."	2019-06-18	5.0	<a href="#">CVE-2018-18839</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nagios -- nagios_xi	An Insufficient Access Control vulnerability (leading to credential disclosure) in coreconfigsnapshot.php (aka configuration snapshot page) in Nagios XI before 5.5.4 allows remote attackers to gain access to configuration files containing confidential credentials.	2019-06-19	5.0	<a href="#">CVE-2018-17148</a> <a href="#">MISC</a>
ngahr -- resourcelink	NGA ResourceLink 20 0.2.1 allows local file inclusion.	2019-06-19	4.0	<a href="#">CVE-2018-18863</a> <a href="#">MISC</a>
open-xchange -- open-xchange_appsuite	OX App Suite 7.10.1 and earlier allows Information Exposure.	2019-06-18	5.0	<a href="#">CVE-2019-7159</a> <a href="#">MISC</a> <a href="#">MISC</a>
openfind -- mail2000	An issue was discovered in Openfind Mail2000 v6 Webmail. XSS can occur via an '<object data="data:text/html" substrin in an e-mail message (The vendor subsequently patched this).	2019-06-19	4.3	<a href="#">CVE-2019-9763</a> <a href="#">MISC</a>
otrs -- otrs	An issue was discovered in Open Ticket Request System (OTRS) 7.0 x through 7.0.8, Community Edition 6.0.x through 6 0.19, and Community Edition 5.0.x through 5.0.36. In the customer or external frontend, personal information of agents (e.g., Name and mail address) can be disclosed in external notes.	2019-06-17	5.0	<a href="#">CVE-2019-12497</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
php -- php	When using gdImageCreateFromXbm() function of PHP gd extension in PHP versions 7.1.x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6, it is possible to supply data that will cause the function to use the value of uninitialized variable. This may lead to disclosing contents of the stack that has been left there by previous code.	2019-06-18	5.0	<a href="#">CVE-2019-11038</a> <a href="#">CONFIRM</a>
php -- php	Function iconv_mime_decode_headers() in PHP versions 7.1 x below 7.1.30, 7.2.x below 7.2.19 and 7.3.x below 7.3.6 may perform out-of-buffer read due to integer overflow when parsing MIME headers. This may lead to information disclosure or crash.	2019-06-18	6.4	<a href="#">CVE-2019-11039</a> <a href="#">CONFIRM</a>
php -- php	When PHP EX F extension is parsing EXIF information from an image, e.g. via exif_read_data() function, in PHP versions 7.1 x below 7.1.30, 7 2.x below 7.2.19 and 7.3.x below 7 3.6 it is possible to supply it with data what will cause it to read past the allocated buffer. This may lead to information disclosure or crash.	2019-06-18	6.4	<a href="#">CVE-2019-11040</a> <a href="#">CONFIRM</a>
radare -- radare2	In radare2 through 3.5.1, cmd_mount in libr/core/cmd_mount.c has a double free for the ms command.	2019-06-17	4.3	<a href="#">CVE-2019-12865</a> <a href="#">MISC</a>
ranksol -- live_call_support	CSRF exists in server.php in Live Call Support Application 1 5 for adding an admin account.	2019-06-19	6.8	<a href="#">CVE-2018-17389</a> <a href="#">MISC</a> <a href="#">MISC</a>
ranksol -- nimble_professional	CSRF exists in Nimble Messaging Bulk SMS Marketing Application 1.0 for adding an admin account.	2019-06-19	6.8	<a href="#">CVE-2018-17387</a> <a href="#">MISC</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::UserInteraction#verbose calls say without escaping, escape sequence injection is possible.	2019-06-17	5.0	<a href="#">CVE-2019-8321</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. The gem owner command outputs the contents of the API response directly to stdout. Therefore, if the response is crafted, escape sequence injection may occur.	2019-06-17	5.0	<a href="#">CVE-2019-8322</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Gem::GemcutterUtilities#with_response may output the API response to stdout as it is. Therefore, if the API side modifies the response, escape sequence injection may occur.	2019-06-17	5.0	<a href="#">CVE-2019-8323</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. A crafted gem with a multi-line name is not handled correctly. Therefore, an attacker could inject arbitrary code to the stub line of gemspec, which is eval-ed by code in ensure_loadable_spec during the preinstall check.	2019-06-17	6.8	<a href="#">CVE-2019-8324</a> <a href="#">MISC</a>
rubygems -- rubygems	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::CommandManager#run calls alert_error without escaping, escape sequence injection is possible. (There are many ways to cause an error.)	2019-06-17	5.0	<a href="#">CVE-2019-8325</a> <a href="#">MISC</a>
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. A web reports module has "export to excel features" that are vulnerable to CSV injection. An attacker can embed Excel formulas inside an automation script that, when exported after execution, results in code execution.	2019-06-17	6.8	<a href="#">CVE-2018-20468</a> <a href="#">MISC</a>
sahipro -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. The logs web interface is vulnerable to stored XSS.	2019-06-17	4.3	<a href="#">CVE-2018-20472</a> <a href="#">MISC</a>



				MISC
samba -- samba	Samba 4.9.x before 4.9.9 and 4.10.x before 4.10.5 has a NULL pointer dereference, leading to Denial of Service. This is related to the AD DC DNS management server (dnsserver) RPC server process.	2019-06-19	4.0	<a href="#">CVE-2019-12435</a> <a href="#">BID</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a>
samba -- samba	Samba 4.10.x before 4.10.5 has a NULL pointer dereference, leading to an AD DC LDAP server Denial of Service. This is related to an attacker using the paged search control. The attacker must have directory read access in order to attempt an exploit.	2019-06-19	4.0	<a href="#">CVE-2019-12436</a> <a href="#">BID</a> <a href="#">UBUNTU</a> <a href="#">CONFIRM</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of setting a name for the wireless network. These values are stored by the device in NVRAM (Non-volatile RAM). It seems that the POST parameters passed in this request to set up names on the device do not have a string length check on them. This allows an attacker to send a large payload in the "mssid_1" POST parameter. The device also allows a user to view the name of the Wifi Network set by the user. While processing this request, the device calls a function at address 0x00412CE4 (routerSummary) in the binary "webServer" located in Almond folder, which retrieves the value set earlier by "mssid_1" parameter as SSID2 and this value then results in overflowing the stack set up for this function and allows an attacker to control \$ra register value on the stack which allows an attacker to control the device by executing a payload of an attacker's choice. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in DA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST parameter "mssid_1" at address 0x0042BA00 and then sets in the NVRAM at address 0x0042C314. The value is later retrieved in the function at address 0x00412EAC and this results in overflowing the buffer as the function copies the value directly on the stack.	2019-06-18	4.6	<a href="#">CVE-2017-8329</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new port forwarding rules to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in passing commands to a "system" API in the function and thus result in command injection on the device. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in DA-pro we will notice that this follows a MIPS little endian format. The function sub_43C280in DA pro is identified to be receiving the values sent in the POST request and the value set in POST parameter "ip_address" is extracted at address 0x0043C2F0. The POST parameter "ipaddress" is concatenated at address 0x0043C958 and this is passed to a "system" function at address 0x00437284. This allows an attacker to provide the payload of his/her choice and finally take control of the device.	2019-06-18	6.5	<a href="#">CVE-2017-8331</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of blocking key words passing in the web traffic to prevent kids from watching content that might be deemed unsafe using the web management interface. It seems that the device does not implement any cross-site scripting protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a stored cross-site scripting payload on the user's browser and execute any action on the device provided by the web management interface.	2019-06-18	6.5	<a href="#">CVE-2017-8332</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of blocking IP addresses using the web management interface. It seems that the device does not implement any cross-site scripting forgery protection mechanism which allows an attacker to trick a user who is logged in to the web management interface into executing a cross-site scripting payload on the user's browser and execute any action on the device provided by the web management interface.	2019-06-18	6.0	<a href="#">CVE-2017-8334</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of setting name for wireless network. These values are stored by the device in NVRAM (Non-volatile RAM). It seems that the POST parameters passed in this request to set up names on the device do not have a string length check on them. This allows an attacker to send a large payload in the "mssid_1" POST parameter. The device also allows a user to view the name of the Wifi Network set by the user. While processing this request, the device calls a function named "getCfgToHTML" at address 0x004268A8 which retrieves the value set earlier by "mssid_1" parameter as SSID2 and this value then results in overflowing the stack set up for this function and allows an attacker to control \$ra register value on the stack which allows an attacker to control the device by executing a payload of an attacker's choice. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on	2019-06-18	6.0	<a href="#">CVE-2017-8335</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>

	the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST parameter "mssid_1" at address 0x0042BA00 and then sets in the NVRAM at address 0x0042C314. The value is later retrieved in the function "getCfgToHTML" at address 0x00426924 and this results in overflowing the buffer due to "strcpy" function that is utilized by this function.			
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of adding new routes to the device. It seems that the POST parameters passed in this request to set up routes on the device can be set in such a way that would result in overflowing the stack set up and allow an attacker to control the \$ra register stored on the stack. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "goahead" is the one that has the vulnerable function that receives the values sent by the POST request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function sub_00420F38 in IDA pro is identified to be receiving the values sent in the POST request. The POST parameter "gateway" allows to overflow the stack and control the \$ra register after 1546 characters. The value from this post parameter is then copied on the stack at address 0x00421348 as shown below. This allows an attacker to provide the payload of his/her choice and finally take control of the device.	2019-06-18	6.5	<a href="#">CVE-2017-8336</a> MISC MISC BUGTRAQ
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a user with the capability of executing various actions on the web management interface. It seems that the device does not implement any Origin header check which allows an attacker who can trick a user to navigate to an attacker's webpage to exploit this issue and brute force the password for the web management interface. It also allows an attacker to then execute any other actions which include management of rules, sensors attached to the devices using the websocket requests.	2019-06-18	6.8	<a href="#">CVE-2017-8337</a> MISC MISC BUGTRAQ
seeddms -- seeddms	SeedDMS before 5.1.11 allows Remote Command Execution (RCE) because of unvalidated file upload of PHP scripts, a different vulnerability than CVE-2018-12940.	2019-06-20	6.0	<a href="#">CVE-2019-12744</a> MISC CONFIRM
seeddms -- seeddms	out/out.GroupMgr.php in SeedDMS 5.1.11 has Stored XSS by making a new group with a JavaScript payload as the "GROUP" Name.	2019-06-17	4.3	<a href="#">CVE-2019-12801</a> MISC
teltonika -- rut950_firmware	An issue was discovered on Teltonika RTU950 R_31.04.89 devices. The application allows a user to login without limitation. For every successful login request, the application saves a session. A user can re-login without logging out, causing the application to store the session in memory. Exploitation of this vulnerability will increase memory use and consume free space.	2019-06-19	6.8	<a href="#">CVE-2018-19878</a> MISC MISC
tp-link -- tl-wr1043nd_firmware	An issue was discovered on TP-Link TL-WR1043ND V2 devices. The credentials can be easily decoded and cracked by brute-force, WordList, or Rainbow Table attacks. Specifically, credentials in the "Authorization" cookie are encoded with URL encoding and base64, leading to easy decoding. Also, the username is cleartext, and the password is hashed with the MD5 algorithm (after decoding of the URL encoded string with base64).	2019-06-19	5.0	<a href="#">CVE-2019-6972</a> MISC MISC
tubigan -- welcome_to_our_resort	The Tubigan "Welcome to our Resort" 1.0 software allows CSRF via admin/mod_users/controller.php?action=edit.	2019-06-18	6.8	<a href="#">CVE-2018-18802</a> MISC MISC
twistedmatrix -- twisted	In words protocols.jabber.xmlstream in Twisted through 19.2.1, XMPP support did not verify certificates when used with TLS, allowing an attacker to MITM connections.	2019-06-16	5.8	<a href="#">CVE-2019-12855</a> MISC MISC
urbackup -- urbackup	In UrBackup 2.2.6, an attacker can send a malformed request to the client over the network, and trigger a fileservplugin/CClientThread.cpp CClientThread::ProcessPacket metadata_id!=0 assertion, leading to shutting down the client application.	2019-06-18	5.0	<a href="#">CVE-2018-20013</a> MISC MISC
znc -- znc	Modules.cpp in ZNC before 1.7.4-rc1 allows remote authenticated non-admin users to escalate privileges and execute arbitrary code by loading a module with a crafted name.	2019-06-15	6.5	<a href="#">CVE-2019-12816</a> CONFIRM CONFIRM MLIST BUGTRAQ
zrlog -- zrlog	An issue was discovered in ZRLOG 2.0.1. There is a Stored XSS vulnerability in the nickname field of the comment area.	2019-06-19	4.3	<a href="#">CVE-2018-17079</a> MISC MISC
zucchetti -- hr_portal	Zucchetti HR Portal through 2019-03-15 allows Directory Traversal. Unauthenticated users can escape outside of the restricted location (dot-dot-slash notation) to access files or directories that are elsewhere on the system. Through this vulnerability it is possible to read the application's java sources from /WEB-INF/classes/*.class	2019-06-19	5.0	<a href="#">CVE-2019-10257</a> MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
b3log -- symphony	In Symphony before 3 3.0, there is XSS in the Title under Post. The ID "articleTitle" of this is stored in the "articleTitle" JSON field, and executes a payload when accessing the /member/test/points URI, allowing remote attacks. Any Web script or HTML can be inserted by an admin-authenticated user via a crafted web site name.	2019-06-20	3.5	<a href="#">CVE-2018-16249</a> MISC
cisco -- prime_service_catalog	A vulnerability in the web-based management interface of Cisco Prime Service Catalog could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by adding specific strings to multiple configuration fields. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.	2019-06-19	3.5	<a href="#">CVE-2019-1875</a> BID CISCO
columbiaweather -- weather_microserver_firmware	In firmware version MS_2 6.9900 of Columbia Weather MicroServer, a stored Cross-site scripting (XSS) vulnerability allows remote authenticated users to inject arbitrary web script via changestationname.php.	2019-06-18	3.5	<a href="#">CVE-2018-18875</a> MISC MISC
columbiaweather -- weather_microserver_firmware	In firmware version MS_2 6.9900 of Columbia Weather MicroServer, a networkdiags.php reflected Cross-site scripting (XSS) vulnerability allows remote authenticated users to inject arbitrary web script.	2019-06-18	3.5	<a href="#">CVE-2018-18880</a> MISC MISC
concrete5 -- concrete5	Concrete5 8.4.3 has XSS because config/concrete.php allows uploads (by administrators) of SVG files that may contain HTML data with a SCRIPT element.	2019-06-17	3.5	<a href="#">CVE-2018-19146</a> MISC MISC MISC MISC
creativity -- witycms	The "utilisateur" menu in Creativity wityCMS 0.6.2 modifies the presence of XSS at two input points for user information, with the "first name" and "last name" parameters.	2019-06-20	3.5	<a href="#">CVE-2018-16250</a> MISC
e107 -- e107	An issue was discovered in e107 v2.1.9. There is a XSS attack on e107_admin/comment.php.	2019-06-19	3.5	<a href="#">CVE-2018-17423</a> MISC MISC
getvera -- veraedge_firmware	An issue was discovered on Vera VeraEdge 1.7.19 and Veralite 1.7.481 devices. The device provides a shell script called relay.sh which is used for creating new SSH relays for the device so that the device connects to Vera servers. All the parameters passed in this specific script are logged to a log file called log relay in the /tmp folder. The user can also read all the log files from the device using a script called log.sh. However, when the script loads the log files it displays them with content-type text/html and passes all the logs through the ansi2html binary which converts all the character text including HTML meta-characters correctly to be displayed in the browser. This allows an attacker to use the log files as a storing mechanism for the XSS payload and thus whenever a user navigates to that log.sh script, it enables the XSS payload and allows an attacker to execute his malicious payload on the user's browser.	2019-06-17	3.5	<a href="#">CVE-2017-9387</a> MISC BUGTRAQ
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3 0, 10.3.1, and 10.4.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 158332.	2019-06-17	3.5	<a href="#">CVE-2019-4136</a> CONFIRM XF
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3 0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158879.	2019-06-17	2.1	<a href="#">CVE-2019-4174</a> CONFIRM XF
ibm -- cognos_controller	IBM Cognos Controller 10.2.0, 10.2.1, 10.3 0, 10.3.1, and 10.4.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 158882.	2019-06-17	2.1	<a href="#">CVE-2019-4177</a> CONFIRM XF
ibm -- control_desk	IBM Maximo Asset Management 7.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force D: 160949.	2019-06-19	3.5	<a href="#">CVE-2019-4303</a> XF CONFIRM
ibm -- i	IBM i 7.27.3 Clustering could allow a local attacker to obtain sensitive information, caused by the use of advanced node failure detection using the REST API to interface with the HMC. An attacker could exploit this vulnerability to obtain HMC credentials. IBM X-Force ID: 162159.	2019-06-14	2.1	<a href="#">CVE-2019-4381</a> BID XF CONFIRM
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in the View Filters page (view_filters_page.php) and Edit Filter page (manage_filter_edit_page.php) in MantisBT 2.1.0 through 2.17.0 allows remote attackers to inject arbitrary code (if CSP settings permit it) through a crafted PATH_INFO. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-13055.	2019-06-20	2.6	<a href="#">CVE-2018-16514</a> MISC
microfocus -- fortify_software_security_center	Cross-Site Scripting vulnerability in Micro Focus Fortify Software Security Center Server, versions 17.2, 18.1, 18.2, has been identified in Micro Focus Software Security Center. The vulnerability could be exploited to execute JavaScript code in user's browser. The vulnerability could be exploited to execute JavaScript code in user's browser.	2019-06-19	3.5	<a href="#">CVE-2019-11649</a> MISC
	A cross-site scripting vulnerability exists in Nagios XI before 5.5.4 via the			<a href="#">CVE-2018-</a>

nagios -- nagios_xi	'name' parameter within the Account Information page. Exploitation of this vulnerability allows an attacker to execute arbitrary JavaScript code within the auto login admin management page.	2019-06-19	3.5	<a href="#">17146</a> <a href="#">MISC</a>
securifi -- almond+firmware	An issue was discovered on Securifi Almond, Almond+, and Almond 2015 devices with firmware AL-R096. The device provides a UPnP functionality for devices to interface with the router and interact with the device. It seems that the "NewInMessage" SOAP parameter passed with a huge payload results in crashing the process. If the firmware version AL-R096 is dissected using binwalk tool, we obtain a cpio-root archive which contains the filesystem set up on the device that contains all the binaries. The binary "miniupnpd" is the one that has the vulnerable function that receives the values sent by the SOAP request. If we open this binary in IDA-pro we will notice that this follows a MIPS little endian format. The function WscDevPutMessage at address 0x0041DBB8 in IDA pro is identified to be receiving the values sent in the SOAP request. The SOAP parameter "NewInMessage" received at address 0x0041DC30 causes the miniupnpd process to finally crash when a second request is sent to the same process.	2019-06-18	3.3	<a href="#">CVE-2017-8330</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
seeddms -- seeddms	out/out.UsrMgr.php in SeedDMS before 5.1.11 allows Stored Cross-Site Scripting (XSS) via the name field.	2019-06-20	3.5	<a href="#">CVE-2019-12745</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x8000204B.	2019-06-21	2.1	<a href="#">CVE-2018-15729</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x80002067.	2019-06-21	2.1	<a href="#">CVE-2018-15730</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x8000205B.	2019-06-21	2.1	<a href="#">CVE-2018-15731</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x80002063.	2019-06-21	2.1	<a href="#">CVE-2018-15732</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a NULL Pointer Dereference vulnerability due to not validating the size of the output buffer value from IOCTL 0x80002028.	2019-06-21	2.1	<a href="#">CVE-2018-15733</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x8000206B.	2019-06-21	2.1	<a href="#">CVE-2018-15734</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains an Arbitrary Write vulnerability due to not validating the output buffer address value from IOCTL 0x8000206F.	2019-06-21	2.1	<a href="#">CVE-2018-15735</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x8000204F.	2019-06-21	2.1	<a href="#">CVE-2018-15736</a> <a href="#">MISC</a> <a href="#">MISC</a>
stopzilla -- antimalware	An issue was discovered in STOPzilla AntiMalware 6.5.2.59. The driver file szkg64.sys contains a Denial of Service vulnerability due to not validating the output buffer address value from IOCTL 0x80002043.	2019-06-21	2.1	<a href="#">CVE-2018-15737</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- data_loss_prevention	DLP 15.5 MP1 and all prior versions may be susceptible to a cross-site scripting (XSS) vulnerability, a type of issue that can enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.	2019-06-19	3.5	<a href="#">CVE-2019-9701</a> <a href="#">MISC</a>
yzmcms -- yzmcms	YzmCMS 5.1 has XSS via the admin/system_manage/user_config_add.html title parameter.	2019-06-20	3.5	<a href="#">CVE-2018-16247</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
akamai -- cloudtest	Akamai CloudTest before 58.30 allows remote code execution.	2019-06-21	not yet calculated	<a href="#">CVE-2019-11011</a> <a href="#">CONFIRM</a>
apache -- geode	When an Apache Geode server versions 1.0.0 to 1.8.0 is operating in secure mode, a user with write permissions for specific data regions can modify internal cluster metadata. A malicious user could modify this data in a way that affects the operation of the cluster.	2019-06-21	not yet calculated	<a href="#">CVE-2017-15694</a> <a href="#">MISC</a>

apache -- tomcat	The fix for CVE-2019-0199 was incomplete and did not address HTTP/2 connection window exhaustion on write in Apache Tomcat versions 9.0.0.M1 to 9.0.19 and 8.5.0 to 8.5.40 . By not sending WINDOW_UPDATE messages for the connection window (stream 0) clients were able to cause server-side threads to block eventually leading to thread exhaustion and a DoS.	2019-06-21	not yet calculated	<a href="#">CVE-2019-10072</a> <a href="#">MISC</a>
asus -- vivobaby_for_android	The ASUS Vivobaby application before 1.1.09 for Android has Missing SSL Certificate Validation.	2019-06-20	not yet calculated	<a href="#">CVE-2017-17944</a> <a href="#">MISC</a>
axentra -- hipserv	/api/2.0/rest/aggregator/xml in Axentra firmware, used by NETGEAR Stora, Seagate GoFlex Home, and MEDION LifeCloud, has an XXE vulnerability that can be chained with an SSRF bug to gain remote command execution as root. It can be triggered by anyone who knows the IP address of the affected device.	2019-06-19	not yet calculated	<a href="#">CVE-2018-18471</a> <a href="#">MISC</a> <a href="#">MISC</a>
bobronix -- jeditor_for_jira	The Bobronix JEditor editor before 3.0.6 for Jira allows an attacker to add a URL/Link (to an existing issue) that can cause forgery of a request to an out-of-origin domain. This in turn may allow for a forged request that can be invoked in the context of an authenticated user, leading to stealing of session tokens and account takeover.	2019-06-21	not yet calculated	<a href="#">CVE-2019-12836</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
cerio -- dt-300n_devices	Cerio DT-300N 1.1.6 through 1.1.12 devices allow OS command injection because of improper input validation of the web-interface P NG feature's use of Save.cgi to execute a ping command, as exploited in the wild in October 2018.	2019-06-18	not yet calculated	<a href="#">CVE-2018-18852</a> <a href="#">MISC</a>
check_point_software_technologies -- endpoint_security_client_for_windows	Check Point Endpoint Security Client for Windows, with Anti-Malware blade installed, before version E81.00, tries to load a non-existent DLL during an update initiated by the UI. An attacker with administrator privileges can leverage this to gain code execution within a Check Point Software Technologies signed binary, where under certain circumstances may cause the client to terminate.	2019-06-20	not yet calculated	<a href="#">CVE-2019-8458</a> <a href="#">CONFIRM</a>
check_point_software_technologies -- endpoint_security_client_for_windows	Check Point Endpoint Security Client for Windows, with the VPN blade, before version E80.83, starts a process without using quotes in the path. This can cause loading of a previously placed executable with a name similar to the parts of the path, instead of the intended one.	2019-06-20	not yet calculated	<a href="#">CVE-2019-8459</a> <a href="#">CONFIRM</a>
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to disconnect clients that are connected to the guest network on an affected router. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for device disconnection and providing the connected device information. A successful exploit could allow the attacker to deny service to specific clients that are connected to the guest network.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1897</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to acquire the list of devices that are connected to the guest network. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web interface of the router.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1899</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- rv110w_and_rv130w_and_rv215w_routers	A vulnerability in the web-based management interface of Cisco RV110W, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to access the syslog file on an affected device. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing the URL for the syslog file. A successful exploit could allow the attacker to access the information contained in the file.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1898</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- staros	A vulnerability in the internal packet-processing functionality of the Cisco StarOS operating system running on virtual platforms could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error that may occur under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to prevent the targeted service interface from receiving any traffic, which would lead to a DoS condition on the affected interface. The device may have to be manually reloaded to recover from exploitation of this vulnerability.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1869</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- dna_center	A vulnerability in Cisco Digital Network Architecture (DNA) Center could allow an unauthenticated, adjacent attacker to bypass authentication and access critical internal services. The vulnerability is due to insufficient access restriction to ports necessary for system operation. An attacker could exploit this vulnerability by connecting an unauthorized network device to the subnet designated for cluster services.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1848</a> <a href="#">BID</a> <a href="#">CISCO</a>



	A successful exploit could allow an attacker to reach internal services that are not hardened for external access.			
cisco -- email_security_appliance	A vulnerability in the GZIP decompression engine of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass configured content filters on the device. The vulnerability is due to improper validation of GZIP-formatted files. An attacker could exploit this vulnerability by sending a malicious file inside a crafted GZIP-compressed file. A successful exploit could allow the attacker to bypass configured content filters that would normally drop the email.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1905</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the web-based management interface of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected device. An attacker could exploit this vulnerability by persuading a user to follow a malicious link. A successful exploit could allow the attacker to use a web browser and the privileges of the user to perform arbitrary actions on the affected device.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1632</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the CLI of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient validation of user-supplied input at the CLI. An attacker could exploit this vulnerability by authenticating with the administrator password via the CLI of an affected device and submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute arbitrary commands on the device with root privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1879</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the Server Utilities of Cisco Integrated Management Controller (IMC) could allow an authenticated, remote attacker to gain unauthorized access to sensitive user information from the configuration data that is stored on the affected system. The vulnerability is due to insufficient protection of data in the configuration file. An attacker could exploit this vulnerability by downloading the configuration file. An exploit could allow the attacker to use the sensitive information from the file to elevate privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1627</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the firmware signature checking program of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient checking of an input buffer. An attacker could exploit this vulnerability by passing a crafted file to the affected system. A successful exploit could inhibit an administrator's ability to access the system.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1630</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the web server of Cisco Integrated Management Controller (IMC) could allow an authenticated, local attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition on an affected device. The vulnerability is due to incorrect bounds checking. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected system. An exploit could allow the attacker to cause a buffer overflow, resulting in a process crash and DoS condition on the device.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1628</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- integrated_management_controller	A vulnerability in the configuration import utility of Cisco Integrated Management Controller (IMC) could allow an unauthenticated, remote attacker to have write access and upload arbitrary data to the filesystem. The vulnerability is due to a failure to delete temporarily uploaded files. An attacker could exploit this vulnerability by crafting a malicious file and uploading it to the affected device. An exploit could allow the attacker to fill up the filesystem or upload malicious scripts.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1629</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- ios_xe_software	A vulnerability in the web-based UI (web UI) of Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web UI on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the user has administrative privileges, the attacker could alter the configuration, execute commands, or reload an affected device. This vulnerability affects Cisco devices that are running a vulnerable release of Cisco IOS XE Software with the HTTP Server feature enabled. The default state of the HTTP Server feature is version dependent.	2019-06-20	not yet calculated	<a href="#">CVE-2019-1904</a> <a href="#">MISC</a>
	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated,			<a href="#">CVE-</a>

cisco -- multiple_products	remote attacker to cause a reload of an affected device, resulting in a denial of service (DoS) condition. This vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to reload the device and causing a DoS condition.	2019-06-19	not yet calculated	<a href="#">2019-1843 BID CISCO</a>
cisco -- prime_infrastructure	A vulnerability in the Virtual Domain system of Cisco Prime Infrastructure (PI) could allow an authenticated, remote attacker to change the virtual domain configuration, which could lead to privilege escalation. The vulnerability is due to improper validation of API requests. An attacker could exploit this vulnerability by manipulating requests sent to an affected PI server. A successful exploit could allow the attacker to change the virtual domain configuration and possibly elevate privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1906 BID CISCO</a>
cisco -- sd_wan_solution	A vulnerability in the vManage web-based UI (Web UI) of the Cisco SD-WAN Solution could allow an authenticated, remote attacker to gain elevated privileges on an affected vManage device. The vulnerability is due to a failure to properly authorize certain user actions in the device configuration. An attacker could exploit this vulnerability by logging in to the vManage Web UI and sending crafted HTTP requests to vManage. A successful exploit could allow attackers to gain elevated privileges and make changes to the configuration that they would not normally be authorized to make.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1626 BID CISCO</a>
cisco -- sd_wan_solution	A vulnerability in the CLI of Cisco SD-WAN Solution could allow an authenticated, local attacker to elevate lower-level privileges to the root user on an affected device. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow the attacker to make configuration changes to the system as the root user.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1625 BID CISCO</a>
cisco -- sd_wan_solution	A vulnerability in the vManage web-based UI (Web UI) in the Cisco SD-WAN Solution could allow an authenticated, remote attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the vManage Web UI. A successful exploit could allow the attacker to execute commands with root privileges.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1624 BID CISCO</a>
cisco -- security_manager	A vulnerability in Cisco Security Manager could allow an unauthenticated, remote attacker to access sensitive information or cause a denial of service (DoS) condition. The vulnerability is due to improper restrictions on XML entities. An attacker could exploit this vulnerability by sending malicious requests to a targeted system that contain references within XML entities. An exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the application to consume available resources, resulting in a DoS condition.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1903 BID CISCO</a>
cisco -- telepresence_codec_and_collaboration_endpoint_software	A vulnerability in the Cisco Discovery Protocol (CDP) implementation for the Cisco TelePresence Codec (TC) and Collaboration Endpoint (CE) Software could allow an unauthenticated, adjacent attacker to inject arbitrary shell commands that are executed by the device. The vulnerability is due to insufficient input validation of received CDP packets. An attacker could exploit this vulnerability by sending crafted CDP packets to an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts on the targeted device.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1878 CISCO</a>
cisco -- wide_area_application_services_software	A vulnerability in the HTTPS proxy feature of Cisco Wide Area Application Services (WAAS) Software could allow an unauthenticated, remote attacker to use the Central Manager as an HTTPS proxy. The vulnerability is due to insufficient authentication of proxy connection requests. An attacker could exploit this vulnerability by sending a malicious HTTPS CONNECT message to the Central Manager. A successful exploit could allow the attacker to access public internet resources that would normally be blocked by corporate policies.	2019-06-19	not yet calculated	<a href="#">CVE-2019-1876 BID CISCO</a>
cloud_foundry_foundation -- bosh	Cloud Foundry BOSH 270.x versions prior to v270.1.1, contain a BOSH Director that does not properly redact credentials when configured to use a MySQL database. A local authenticated malicious user may read any credentials that are contained in a BOSH manifest.	2019-06-18	not yet calculated	<a href="#">CVE-2019-11271 CONFIRM</a>
cloud_foundry_foundation -- uua_release	Cloud Foundry UAA, versions prior to 73.0 0, falls back to appending ?unknown.org? to a user's email address when one is not provided and the user name does not contain an @ character. This domain is held by a private company, which leads to attack vectors including password recovery emails sent to a potentially fraudulent address. This would allow the attacker to gain complete control of the user's account.	2019-06-19	not yet calculated	<a href="#">CVE-2019-3787 CONFIRM</a>

cloudera -- manager	An issue was discovered in Cloudera Manager 5.x through 5.15.0. One type of page in Cloudera Manager uses a 'returnUrl' parameter to redirect the user to another page in Cloudera Manager once a wizard is completed. The validity of this parameter was not checked. As a result, the user could be automatically redirected to an attacker's external site or perform a malicious JavaScript function that results in cross-site scripting (XSS). This was fixed by not allowing any value in the returnUrl parameter with patterns such as http://, https://, //, or javascript. The only exceptions to this rule are the SAML Login/Logout URLs, which remain supported since they are explicitly configured and they are not passed via the returnUrl parameter.	2019-06-20	not yet calculated	<a href="#">CVE-2018-15913</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
dell_emc -- avamar_adme_web_interface	Dell EMC Avamar ADMe Web Interface 1.0.50 and 1.0.51 are affected by an LFI vulnerability which may allow a malicious user to download arbitrary files from the affected system by sending a specially crafted request to the Web Interface application.	2019-06-19	not yet calculated	<a href="#">CVE-2019-3737</a> <a href="#">MISC</a>
dell_emc -- supportassist_for_business_and_supportassist_for_home_pcs	Dell SupportAssist for Business PCs version 2.0 and Dell SupportAssist for Home PCs version 2.2, 2.2.1, 2.2.2, 2.2.3, 3.0, 3.0.1, 3.0.2, 3.1, 3.2, and 3.2.1 contain an Improper Privilege Management Vulnerability. A malicious local user can exploit this vulnerability by inheriting a system thread using a leaked thread handle to gain system privileges on the affected machine.	2019-06-20	not yet calculated	<a href="#">CVE-2019-3735</a> <a href="#">MISC</a>
ethereum -- primeo_token	The doAirdrop function of a smart contract implementation for Primeo (PEO), an Ethereum token, does not check the numerical relationship between the amount of the air drop and the token's total supply, which lets the owner of the contract issue an arbitrary amount of currency. (Increasing the total supply by using 'doAirdrop' ignores the hard cap written in the contract and devalues the token.)	2019-06-19	not yet calculated	<a href="#">CVE-2018-18425</a> <a href="#">MISC</a> <a href="#">MISC</a>
evernote_corporation -- evernote	A universal Cross-site scripting (UXSS) vulnerability in the Evernote Web Clipper extension before 7.11.1 for Chrome allows remote attackers to run arbitrary web script or HTML in the context of any loaded 3rd-party Frame.	2019-06-18	not yet calculated	<a href="#">CVE-2019-12592</a> <a href="#">MISC</a> <a href="#">MISC</a>
excellent_infotec_corporation -- biyan	EXCELLENT INFOTEK BiYan v1.57 ~ v2.8 allows an attacker to leak user information without being authenticated, by sending a LOGIN_ID element to the auth/main/asp/check_user_login_info.aspx URI, and then reading the response, as demonstrated by the KW_EMAIL or KW_TEL field.	2019-06-19	not yet calculated	<a href="#">CVE-2019-11233</a> <a href="#">MISC</a>
excellent_infotec_corporation -- biyan	EXCELLENT INFOTEK BiYan v1.57 ~ v2.8 allows an attacker to leak user information (Password) without being authenticated, by sending an EMP_NO element to the kws_login/asp/query_user.asp URI, and then reading the PWD element.	2019-06-19	not yet calculated	<a href="#">CVE-2019-11232</a> <a href="#">MISC</a>
forgerock -- openam_and_am	OAuth 2.0 Authorization Server of ForgeRock Access Management (OpenAM) 13.5 0-13.5.1 and Access Management (AM) 5.0.0-5.1.1 does not correctly validate redirect_uri for some invalid requests, which allows attackers to perform phishing via an unvalidated redirect.	2019-06-19	not yet calculated	<a href="#">CVE-2017-14394</a> <a href="#">MISC</a>
forgerock -- openam_and_am	Auth 2.0 Authorization Server of ForgeRock Access Management (OpenAM) 13.5 0-13.5.1 and Access Management (AM) 5.0.0-5.1.1 does not correctly validate redirect_uri for some invalid requests, which allows attackers to execute a script in the user's browser via reflected XSS.	2019-06-19	not yet calculated	<a href="#">CVE-2017-14395</a> <a href="#">MISC</a>
freepbx -- freepbx	FreePBX 13 and 14 has SQL Injection in the DISA module via the hangup variable on the /admin/config.php?display=disa&view=form page.	2019-06-20	not yet calculated	<a href="#">CVE-2018-15892</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
freepbx -- freepbx	An issue was discovered in FreePBX core before 3.0.122.43, 14.0.18.34, and 5.0.1beta4. By crafting a request for adding Asterisk modules, an attacker is able to store JavaScript commands in a module name.	2019-06-20	not yet calculated	<a href="#">CVE-2018-15891</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
glot.io -- glot-www	The default configuration of glot-www through 2018-05-19 allows remote attackers to execute arbitrary code because glot-code-runner supports os system within a "python" "files" "content" JSON file.	2019-06-21	not yet calculated	<a href="#">CVE-2018-15747</a> <a href="#">MISC</a>
helpy -- helpy	Helpy v2.1.0 has Stored XSS via the Ticket title.	2019-06-18	not yet calculated	<a href="#">CVE-2018-18886</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web server potentially vulnerable to stored XSS in wireless configuration page	2019-06-17	not yet calculated	<a href="#">CVE-2019-6324</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer			<a href="#">CVE-</a>

m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	series (before v. 20190426) may have an embedded web server potentially vulnerable to reflected XSS in wireless configuration page.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6323</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an embedded web server that is potentially vulnerable to Cross-site Request Forgery.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6325</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have an IPP Parser potentially vulnerable to Buffer Overflow.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6327</a> <a href="#">MISC</a>
hp -- color_laserjet_pro_m280-m281_multifunction_printer_and_laserjet_pro_mfp_m28-m31_printer	HP Color LaserJet Pro M280-M281 Multifunction Printer series (before v. 20190419), HP LaserJet Pro MFP M28-M31 Printer series (before v. 20190426) may have embedded web server attributes which may be potentially vulnerable to Buffer Overflow.	2019-06-17	not yet calculated	<a href="#">CVE-2019-6326</a> <a href="#">MISC</a>
ibm -- spspectrum_protect_plus	BM Spectrum Protect Plus 10.1.2 may display the vSnap CIFS password in the IBM Spectrum Protect Plus Joblog. This can result in an attacker gaining access to sensitive information as well as vSnap. IBM X-Force ID: 162173.	2019-06-19	not yet calculated	<a href="#">CVE-2019-4385</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
libgcrypt -- libgcrypt	In Libgcrypt 1.8.4, the C implementation of AES is vulnerable to a flush-and-reload side-channel attack because physical addresses are available to other processes. (The C implementation is used on platforms where an assembly-language implementation is unavailable.)	2019-06-19	not yet calculated	<a href="#">CVE-2019-12904</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
london_trust_media -- private_internet_access_vpn_client_for_windows	A vulnerability in the London Trust Media Private Internet Access (PIA) VPN Client 1.0.2 (build 02363) for Windows could allow an authenticated, local attacker to run arbitrary code with elevated privileges. On startup, the PIA Windows service (pia-service.exe) loads the OpenSSL library from %PROGRAMFILES%\Private Internet Access\libeay32.dll. This library attempts to load the C:\etc\ssl\openssl.cnf configuration file which does not exist. By default on Windows systems, authenticated users can create directories under C:\. A low privileged user can create a C:\etc\ssl\openssl.cnf configuration file to load a malicious OpenSSL engine library resulting in arbitrary code execution as SYSTEM when the service starts.	2019-06-21	not yet calculated	<a href="#">CVE-2019-12572</a> <a href="#">MISC</a> <a href="#">MISC</a>
netflix -- dial	Denial of Service (DOS) in Dial Reference Source Code Used before June 18th, 2019.	2019-06-21	not yet calculated	<a href="#">CVE-2019-10028</a> <a href="#">CONFIRM</a>
openstack -- magnum	OpenStack Magnum passes OpenStack credentials into the Heat templates creating its instances. While these should just be used for retrieving the instances' SSL certificates, they allow full API access, though and can be used to perform any API operation the user is authorized to perform.	2019-06-21	not yet calculated	<a href="#">CVE-2016-7404</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
opnsense -- opnsense	OPNsense 18.7.x before 18.7.7 has Incorrect Access Control.	2019-06-17	not yet calculated	<a href="#">CVE-2018-18958</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
phoenix_contact -- axc_f_2152_and_axc_f_2152_starterkit_devices	An issue was discovered on Phoenix Contact AXC F 2152 (No.2404267) before 2019.0 LTS and AXC F 2152 STARTERKIT (No.1046568) before 2019.0 LTS devices. Unlimited physical access to the PLC may lead to a manipulation of SD cards data. SD card manipulation may lead to an authentication bypass opportunity.	2019-06-18	not yet calculated	<a href="#">CVE-2019-10998</a> <a href="#">CONFIRM</a>
phoenix_contact -- axc_f_2152_and_axc_f_2152_starterkit_devices	An issue was discovered on Phoenix Contact AXC F 2152 (No.2404267) before 2019.0 LTS and AXC F 2152 STARTERKIT (No.1046568) before 2019.0 LTS devices. Protocol Fuzzing on PC WORX Engineer by a man in the middle attacker stops the PLC service. The device must be rebooted, or the PLC service must be restarted manually via a Linux shell.	2019-06-17	not yet calculated	<a href="#">CVE-2019-10997</a> <a href="#">CONFIRM</a>
pix-link -- repeater/router_lv-wr09	An XSS issue on the PIX-Link Repeater/Router LV-WR09 with firmware v28K.MiniRouter.20180616 allows attackers to steal credentials without being connected to the network. The attack vector is a crafted ESS D.	2019-06-22	not yet calculated	<a href="#">CVE-2019-12933</a> <a href="#">MISC</a>
pydio -- pydio	Pydio Cells before 1.5.0 fails to neutralize '..\' elements, allowing an attacker with minimum privilege to Upload files to, and Delete files/folders from, an unprivileged directory, leading to Privilege escalation.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12901</a> <a href="#">MISC</a> <a href="#">MISC</a>
pydio -- pydio	Pydio Cells before 1.5.0, when supplied with a Name field in an unexpected Unicode format, fails to handle this and includes the database column/table name as part of the error message, exposing sensitive information.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12903</a> <a href="#">MISC</a>

				<a href="#">MISC</a>
pydio -- pydio	Pydio Cells before 1 5.0 does incomplete cleanup of a user's data upon deletion. This allows a new user, holding the same User ID as a deleted user, to restore the deleted user's data.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12902</a> <a href="#">MISC</a> <a href="#">MISC</a>
rdk_management -- rdkb-20181217-1	A heap-based buffer overflow in cosa_dhcpv4_dml.c in the RDK RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve remote code execution by crafting a long buffer in the "Comment" field of an P reservation form in the admin panel. This is related to the CcspCommonLibrary module.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6963</a> <a href="#">MISC</a>
rdk_management -- rdkb-20181217-1	A shell injection issue in cosa_wifi_apis.c in the RDK RDKB-20181217-1 CcspWifiAgent module allows attackers with login credentials to execute arbitrary shell commands under the CcspWifiSsp process (running as root) if the platform was compiled with the ENABLE_FEATURE_MESH_WI macro. The attack is conducted by changing the Wi-Fi network password to include crafted escape characters. This is related to the WebUI module.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6962</a> <a href="#">MISC</a>
rdk_management -- rdkb-20181217-1	Incorrect access control in actionHandlerUtility.php in the RDK RDKB-20181217-1 WebUI module allows a logged in user to control DDNS, QoS, RIP, and other privileged configurations (intended only for the network operator) by sending an HTTP POST to the PHP backend, because the page filtering for non-superuser (in header.php) is done only for GET requests and not for direct AJAX calls.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6961</a> <a href="#">MISC</a>
rdk_management -- rdkb-20181217-1	A heap-based buffer over-read in Service_SetParamStringValue in cosa_x_cisco_com_ddns_dml.c of the RDK RDKB-20181217-1 CcspPandM module may allow attackers with login credentials to achieve information disclosure and code execution by crafting an AJAX call responsible for DDNS configuration with an exactly 64-byte username, password, or domain, for which the buffer size is insufficient for the final ' ' character. This is related to the CcspCommonLibrary and WebUI modules.	2019-06-20	not yet calculated	<a href="#">CVE-2019-6964</a> <a href="#">MISC</a>
redwoodhq -- redwoodhq	RedwoodHQ 2.5.5 does not require any authentication for database operations, which allows remote attackers to create admin users via a con automationframework users insert_one call.	2019-06-19	not yet calculated	<a href="#">CVE-2019-12890</a> <a href="#">MISC</a> <a href="#">MISC</a>
shenzhen_cylan_technology -- clever_dog_smart_camera_dog-2w_and_dog-2w-v4	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the local network has unauthenticated access to the internal SD card via the HTTP service on port 8000. The HTTP web server on the camera allows anyone to view or download the video archive recorded and saved on the external memory card attached to the device.	2019-06-20	not yet calculated	<a href="#">CVE-2019-12919</a> <a href="#">MISC</a>
shenzhen_cylan_technology -- clever_dog_smart_camera_dog-2w_and_dog-2w-v4	On Shenzhen Cylan Clever Dog Smart Camera DOG-2W and DOG-2W-V4 devices, an attacker on the network can login remotely to the camera and gain root access. The device ships with a hardcoded 12345678 password for the root account, accessible from a TELNET login prompt.	2019-06-20	not yet calculated	<a href="#">CVE-2019-12920</a> <a href="#">MISC</a>
solarwinds -- serv-u_ftp_server	A privilege escalation vulnerability exists in SolarWinds Serv-U before 15.1.7 for Linux.	2019-06-17	not yet calculated	<a href="#">CVE-2019-12181</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices has a Buffer Overflow.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16595</a> <a href="#">MISC</a> <a href="#">MISC</a>
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices allows Directory Traversal.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16594</a> <a href="#">MISC</a> <a href="#">MISC</a>
sony -- bravia_smart_tv_devices	The Photo Sharing Plus component on Sony Bravia TV through 8.587 devices allows Shell Metacharacter Injection.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16593</a> <a href="#">MISC</a> <a href="#">MISC</a>
sophos -- xg_firewall	A shell escape vulnerability in /webconsole/APIController in the API Configuration component of Sophos XG firewall 17.0.8 MR-8 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the "X-Forwarded-for" HTTP header.	2019-06-20	not yet calculated	<a href="#">CVE-2018-16118</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a>
	SQL injection vulnerability in AccountStatus.jsp in Admin			<a href="#">CVE-2018-</a>



sophos -- xg_firewall	Portal of Sophos XG firewall 17.0.8 MR-8 allow remote authenticated attackers to execute arbitrary SQL commands via the "username" GET parameter.	2019-06-20	not yet calculated	<a href="#">16116 CONFIRM MISC</a>
tp_link -- wr1043nd_devices	Stack-based buffer overflow in the httpd server of TP-Link WR1043nd (Firmware Version 3) allows remote attackers to execute arbitrary code via a malicious MediaServer request to /userRpm/MediaServerFoldersCfgRpm.htm.	2019-06-20	not yet calculated	<a href="#">CVE-2018-16119 MISC</a>
tufin -- securetrack	An issue was discovered in Tufin SecureTrack 18.1 with TufinOS 2.16 build 1179(Final). The Audit Report module is affected by a blind XXE vulnerability when a new Best Practices Report is saved using a special payload inside the xml input field. The XXE vulnerability is blind since the response doesn't directly display a requested file, but rather returns it inside the name data field when the report is saved. An attacker is able to view restricted operating system files. This issue affects all types of users: administrators or normal users.	2019-06-19	not yet calculated	<a href="#">CVE-2018-18406 MISC</a>
tyto_software -- sahi_pro	An issue was discovered in Tyto Sahi Pro through 7.x.x and 8.0.0. A directory traversal (arbitrary file access) vulnerability exists in the web reports module. This allows an outside attacker to view contents of sensitive files.	2019-06-17	not yet calculated	<a href="#">CVE-2018-20470 MISC</a>
vtech -- storio_max_devices	VTech Storio Max before 56.D3JM6 allows remote command execution via shell metacharacters in an Android activity name. It exposes the storeintenttranslate.x service on port 1668 listening for requests on localhost. Requests submitted to this service are checked for a string of random characters followed by the name of an Android activity to start. Activities are started by inserting their name into a string that is executed in a shell command. By inserting metacharacters this can be exploited to run arbitrary commands as root. The requests also match those of the HTTP protocol and can be triggered on any web page rendered on the device by requesting resources stored at an http://127.0.0.1:1668/ URI, as demonstrated by the http://127.0.0.1:1668/dacdb70556479813fab2d92896596eef?';(ping,example.org)' URL.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16618 MISC</a>
wago -- multiple_devices	WAGO 852-303 before FW06, 852-1305 before FW06, and 852-1505 before FW03 devices contain hardcoded users and passwords that can be used to login via SSH and TELNET.	2019-06-17	not yet calculated	<a href="#">CVE-2019-12550 MISC</a>
wago -- multiple_devices	WAGO 852-303 before FW06, 852-1305 before FW06, and 852-1505 before FW03 devices contain hardcoded private keys for the SSH daemon. The fingerprint of the SSH host key from the corresponding SSH daemon matches the embedded private key.	2019-06-17	not yet calculated	<a href="#">CVE-2019-12549 MISC</a>
whatsapp -- whatsapp	When receiving calls using WhatsApp for Android, a missing size check when parsing a sender-provided packet allowed for a stack-based overflow. This issue affects WhatsApp for Android prior to 2.18.248 and WhatsApp Business for Android prior to 2.18.132.	2019-06-14	not yet calculated	<a href="#">CVE-2018-6349 BID</a>
wordpress -- wordpress	An issue was discovered in the update function in the wpForo Forum plugin before 1.5.2 for WordPress. A registered forum is able to escalate privilege to the forum administrator without any form of user interaction.	2019-06-19	not yet calculated	<a href="#">CVE-2018-16613 MISC</a>
wordpress -- wordpress	An arbitrary password reset issue was discovered in the Ultimate Member plugin 2.39 for WordPress. It is possible (due to lack of verification and correlation between the reset password key sent by mail and the user_id parameter) to reset the password of another user. One only needs to know the user_id, which is publicly available. One just has to intercept the password modification request and modify user_id. It is possible to modify the passwords for any users or admin WordPress Ultimate Members. This could lead to account compromise and privilege escalation.	2019-06-21	not yet calculated	<a href="#">CVE-2019-10270 MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add [ncas.us-cert.gov](mailto:ncas.us-cert.gov) to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED:



SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to wguitarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fgrgurina@sunnyvale.ca.gov](mailto:fgrgurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for June 17, 2019  
**Date:** Monday, June 17, 2019 5:03:44 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Click here [Having trouble viewing this email?](#)



### **California prisoners can possess pot but not consume it, appeals court rules**

California inmates can now possess marijuana without facing legal consequences from the state as long as they don't consume it, thanks to a new appeals court ruling. The 3rd District Court of Appeal overturned criminal convictions of five Sacramento defendants who had been caught with marijuana in their prison cells. The 20-page ruling says, "Consumption, not possession, is the act voters determined should remain criminalized if the user is in prison."

[Bay Area News Group](#)

### **California court says convicts must pay restitution, even if crime is minor**

Convicted criminals in California must repay their victims for financial losses even for the minor crimes classified as infractions, like a mauling that killed a disabled person's service dog, an appellate court has ruled. The state Constitution, under a provision added by a 2008 ballot initiative, specifies that "restitution shall be ordered from the convicted wrongdoer in every case ... in which a crime victim suffers a loss," said the Los Angeles County Superior Court's Appellate Division.

[San Francisco Chronicle](#)

### **Assessment: Kern County in need of 19 new judges to address high caseload**

Kern County is in need of 19 additional judges to address the Superior Court's rising caseloads, according to a new state assessment. During a meeting on May 29, the Workload Assessment Advisory Committee, as part of the Judicial Council of California, approved a draft ranking of the state's needs for additional judges. Kern County was ranked fourth in need and is the first Valley county to be listed. The county currently has 43 judges, according to Kern County Superior Court.

[The Record](#)

### **Denial of §1538.5 motion didn't bar bid under §995**

One judge's denial of a suppression motion pursuant to Penal Code §1538.5, based on the alleged illegality of a search and seizure, does not bar another judge from granting a motion under Penal Code §995 to dismiss the information on the identical ground, Div. Two of the Fourth District Court of Appeal held in an opinion certified for publication yesterday. Justice Michael J. Raphael was the author of what was initially an unpublished opinion, filed May 16.

[Metropolitan News-Enterprise](#)

### **Reforms of Proposition 47 extend to Oxnard gang-related theft case, high court says**

A Ventura County case prompted the California Supreme Court to find that the reforms of Proposition 47 can extend to a gang-related theft offense. The 5-2 decision issued Monday means Luis Donicio

Valenzuela's conviction of the gang crime of street terrorism is expected to be dismissed. William Quest, of the Ventura County Public Defender's Office, said Valenzuela was found guilty of street terrorism and felony grand theft in connection with a 2013 Oxnard incident.

[Ventura County Star](#)

### **High Court shuts Patent Office door on government challenges**

The U.S. Supreme Court has blocked federal agencies from challenging patents at the Patent and Trademark Office, in a decision that attorneys say will have a far-reaching impact. The justices overturned a U.S. Court of Appeals for the Federal Circuit decision that the U.S. Postal Service could challenge a patent at the agency. The ruling sets a precedent by clarifying that the government isn't a "person" eligible to use administrative patent challenge proceedings under the America Invents Act (AIA).

[Bloomberg Law](#)

### **Supreme Court rejects challenge to gun-silencer registration law**

The U.S. Supreme Court turned away challenges to a federal law that requires registration of gun silencers, the accessory that has drawn new scrutiny after it was used in a mass shooting in Virginia. The justices, without comment Monday, left intact the conviction of Jeremy Kettler, a Kansas man sentenced to one year of probation after a jury found him guilty of possessing an unregistered silencer.

[Bloomberg](#)

### **Case remanded with order that it not be returned to Judge Real**

The Ninth U.S. Circuit Court of Appeals on Friday directed that a case, on remand, be assigned to a judge of the U.S. District Court for the Central District of California other than Senior Judge Manuel Real, marking the 24th time in the past 10 years it has issued an anyone-but-Real order. In a memorandum opinion, a three-judge panel reversed an order by Real, 95, dismissing with prejudice an action under the Individuals with Disabilities Education Act brought on behalf of a youth, "E.B.," against the Baldwin Park Unified School District.

[Metropolitan News-Enterprise](#)

### **Ninth Circuit rips ICE, stops man's deportation**

The Ninth Circuit ruled Thursday that a Mexican man who was arrested during an immigration sting at a Los Angeles manufacturing plant should not be deported, a rebuke that may influence how immigration authorities target factories and offices. U.S. Immigration and Customs Enforcement agents stormed the premises of Micro Solutions Enterprises, a maker of printer cartridges, after getting a search warrant in February 2008 for employment-related documents and arrest warrants for eight employees.

[AP](#)



---

### **Soros spends \$1 million on VA prosecutor races**

Liberal billionaire George Soros has continued his bid to "overhaul" the criminal justice system in the United States by pouring nearly \$1 million into local Virginia prosecutor races to prop up far-left candidates. Soros's most recent round of donations include \$580,000 to Parisa Dehghani-Tafti, a candidate for Arlington County commonwealth's attorney, and almost \$400,000 to Steve Descana, a Fairfax County commonwealth's attorney candidate, for their June 11 primaries.

[The Washington Free Beacon](#)

### **Black people are charged at a higher rate than whites. What if prosecutors didn't know their race?**

While riding the train in San Francisco three years ago, a white man told an African-American man that he smelled bad and should move away from him. An argument followed, and the African-American man, Michael Smith, was eventually tackled by police officers and accused of assaulting them. The San Francisco District Attorney's Office charged Mr. Smith with seven counts, including battery on a police officer and resisting arrest.

[New York Times](#)

### **Lacey asks public's help to combat opioid addiction**

Los Angeles County District Attorney Jackie Lacey is seeking the public's help in saving lives and reducing opioid addiction in all areas of the county, the DA's Office said Tuesday. At a May 7 news conference, Lacey asked members of the public to report non-emergency information about the illegal trafficking or overprescription of opioids to her office for possible criminal prosecution.

[SCV News](#)

### **UCLA faces 'rigorous review' over handling of gynecologist abuse allegations, Napolitano says**

University of California President Janet Napolitano vowed to get to the bottom of how UCLA handled allegations of sexual misconduct by a university gynecologist, saying "there were lessons learned" in the case. "What UCLA is doing is making sure ... those kinds of issues don't happen again," she said in an interview Tuesday. "We just don't want this happening again. We just don't."

[Los Angeles Times](#)

### **Aspiring rapper charged with climbing atop freeway sign**

An aspiring rapper who snarled traffic during the morning commute for nearly two hours last summer by climbing atop a sign to drape banners over the southbound Harbor (110) Freeway in downtown Los Angeles is set to be arraigned July 1 on five misdemeanor charges, Los Angeles City Attorney Mike Feuer announced today. Alexander Dunn - who goes by the stage name Dephree - was charged last week with trespassing, resisting an officer, causing a public nuisance and failing to abide by a

peace officer's instructions, according to the City Attorney's Office.  
[City News Service](#)

### **Exclusive: Santa Clara County DA will stop filing charges in most minor drug cases**

In a pivotal policy shift that could go a long way toward unclogging court dockets and jail cells in the South Bay, the Santa Clara County District Attorney's Office no longer will file charges against most people arrested or cited solely for possessing small amounts of illegal drugs. Prosecutors say the aim of the change is to keep one- and two-time offenders out of the court system, diverting them instead to drug treatment programs and reserving bandwidth for more serious addiction cases that cross over to become community nuisances or public-safety concerns.

[Bay Area News Group](#)

### **Prop. 57, Prop 47 & AB 109**

#### **MET team arrests probationer in stolen vehicle**

On Wednesday, June 5, sheriff's deputies assigned to Highland's Multiple Enforcement Team (MET) arrested Nathan Wendale Waite Clark, a documented gang member, for possession of a stolen vehicle, in Highland. According to a sheriff's department press release, at 10:39 p.m., deputies assigned to the MET deputies were in the area of Sterling Avenue and Base Line when they observed a silver 2004 Toyota Camry that was reported stolen during a carjacking in the city of Victorville on June 4, 2019.

[Highland Community News](#)

#### **Opinion: All signs point to crime making a comeback in California**

California was once known for being tough on criminals. We're not talking about frontier days, but much more recently. It was only five years ago when the Washington Post's Max Ehrenfreund wrote that "California's criminal justice system has long been among the most punitive." At one time, Newsweek said, the state's three-strikes law was "the toughest in the nation."

[Times of San Diego](#)

### **Criminal Justice/Public Safety**

#### **Garcetti turns to young people to combat gun violence**

Earlier this year, the slaying of Nipsey Hussle, the rapper and Crenshaw neighborhood champion, came as a harsh reminder that although crime has declined in the city in recent decades, gun violence is still a daily reality for many Angelenos. Sarah Robinson said she was among those who mourned Hussle's loss. She graduated from Washington Preparatory High School in South Los Angeles this month, and said she saw him as a role model in the community.

[New York Times](#)

### **What's behind Aryan Brotherhood California prison plot?**

Leaders of the Aryan Brotherhood prison gang have been charged with directing killings and drug smuggling from within California's most secure prisons, U.S. prosecutors said. The charges filed Thursday detail five slayings and accuse an attorney of helping smuggle drugs and cellphones to aid the white supremacist gang.

[Ventura County Star](#)

### **Bodycam video shows deadly LAPD shooting in southeast L.A.**

New body camera video shows Los Angeles police officers' deadly confrontation with an armed man in southeast Los Angeles. The man, later identified as David Flores, 36, can be seen firing at responding officers as they pull up to the intersection where he is standing. Officers shooting back, striking him. He goes down and is later pronounced dead at the scene.

[ABC7](#)

### **Police know the mentally ill need more than handcuffs. Their response is shifting**

The first time that Bob Hung had to handcuff his sister, in 2010, he was afraid. He was just two years into his career as a patrol officer for the Monterey Park Police Department when his father called and told him that his older sister, diagnosed with schizophrenia, had run away from home. He called his supervisor and quickly shed his uniform.

[Los Angeles Times](#)

### **Charged with a felony in California? Odds are you'll wind up guilty.**

If you have been charged with a felony in California, the overwhelming odds are you're guilty. Or you'll be found guilty, at least. An analysis of a year's worth of felony cases in the Golden State showed that 82% wind up in some type of conviction or guilty plea. When just looking at Los Angeles County, it's even higher: 87%. You are innocent, you say? And you want to take your case to trial? The odds are even worse.

[Witness LA](#)

### **DNA site that helps cold-case sleuths curbs access for cops**

The genealogy database that helped authorities track down the alleged Golden State Killer and dozens of other suspects has changed a key policy over privacy concerns, a move that could hamper future criminal investigations. GEDmatch, which has more than 1 million genetic profiles in its database, is now asking users whether they want to allow police to access their DNA information.

[Bloomberg](#)

### **LAPD officer dies following surgery related to on-duty crash in 2015**

An LAPD officer has died after surgery related to a 2015 traffic collision that occurred while she was on duty, police said Tuesday. Officer

Esmeralda Ramirez passed away over the weekend, according to a Los Angeles Police Department news release. "Officer Esmeralda Ramirez served the city of Los Angeles with honor, integrity, and pride," LAPD Chief Michel Moore said in a tweet.

[KTLA](#)

### **There's a real-life Michael Connelly character in the LAPD, and she's gunning for Harry Bosch's job**

A Los Angeles bartender and diner manager, Roberts was used to seeing cops stagger into her establishments, seeking a bite or a beer after their shift. Conversation between the investigators and Roberts, a self-described true-crime "fanatic," came easily. She told them of her desire to chase predators. At some point, one of them suggested a career change.

[Los Angeles Times](#)

## **Policy & Legal Issues**

### **Disguising a public safety crisis as a housing crisis.**

The newest homeless camp emerged by the very upscale Sunkist Park neighborhood of Culver City, Los Angeles. First a couple of tents, then more, then it becomes a city in its own right - entitled to services such as sanitation clean up. Finally, we have a permanent camp with property rights. These camps are a breeding ground for petty crime, drugs, and disease such as scabies and staphylococcus.

[Human Events](#)

### **Keeping an eye on sheriffs: California Democrats want to empower investigators**

A dispute between Sacramento County Sheriff Scott Jones and the inspector general who investigated a deputy-involved shooting is shaping a statewide proposal to create powerful law enforcement oversight bodies. Within months of the dispute, Assemblyman Kevin McCarty, D-Sacramento, wrote a bill that would be a new check on California's 58 elected sheriffs, enabling counties to create oversight boards with authority to issue subpoenas.

[Sacramento Bee](#)

### **The road to Ferguson: This 1980 bank robbery changed how American police are armed**

When the images of heavily-armed city cops mounted atop a fleet of armored personnel carriers facing down a crowd of protesters in the streets of Ferguson, Missouri flickered across our television sets in August of 2014, many Americans wondered how we had gotten to this point. It is indeed a long and winding road to what is termed as "the militarization" of local police forces, and one that brings us back to an unlikely beginning: a single gun in the hands of a single sheriff's deputy high on a mountainside above Los Angeles in the spring of 1980.

[Salon](#)

### **Santana: OC Deputy union pays out \$50K in failed bid to seal misconduct records**

Orange County's Deputy Sheriff's union paid out nearly \$50,000 in attorney fees this past month to a Voice of OC-led media coalition that successfully challenged the deputies' bid earlier this year to seal misconduct records made available for public review by recent state legislation.

[Voice of OC](#)

### **Homelessness and the limits of enforcement**

Martin v. City of Boise and Prohibitions on Camping, Sleeping, or Lying in Public - We get frequent questions about this Ninth Circuit case, what it means, and how it impacts local governments. The case found that the City of Boise's enforcement of ordinances prohibiting camping, sleeping, or lying in public violated the Eighth Amendment ban on cruel and unusual punishment if an individual does not have a meaningful alternative (such as space in a shelter or a legal place to camp).

[MRSC Blog](#)

### **LAPD officer who shot Trader Joe's manager complied with policy, Police Commission rules**

A police officer who killed a bystander in a gun battle outside a Trader Joe's in Silver Lake did not violate department policy by shooting toward a crowded store, the Los Angeles Police Commission ruled Tuesday. A gunman had begun shooting at two LAPD officers as they pursued him in their patrol car July 21. The man crashed his car and ran towards the Trader Joe's store, firing more rounds at the officers.

[Los Angeles Times](#)

### **Kim Goldman's crusade: Make O.J. Simpson pay and never forget**

Kim Goldman wrote to O.J. Simpson a few years ago, asking to visit him in the Nevada prison where he was being held for robbery and kidnapping. She wanted to see the man she says killed her brother, Ron Goldman, and Simpson's wife 25 years ago Wednesday outside Nicole Brown Simpson's Brentwood townhouse. It would become known as "the crime of the century."

[Los Angeles Times](#)

### **LA leaders opposed a law that would make it harder to tow cars - even if people are living in them**

The juxtaposition was striking. One week to the day that L.A.'s leaders got officials word homelessness had risen 16% over the last year, they voted on an issue that directly affects many homeless people: impounding cars. At least 16,500 people live in vehicles in L.A. County according to the latest homeless count, though officials concede privately the actual number may be much higher.

[LAist](#)



## **Why are homicide rates spiking in California's County Jails?**

Deadly violence has surged in county jails across California since the state began sending thousands of inmates to local lock-ups instead of prisons, the result of a dramatic criminal justice transformation that left many sheriffs ill-equipped to handle a new and dangerous population.

[Pacific Standard](#)

## **Public Health**

### **L.A. County public officials announce efforts to improve sanitation, conditions for homeless people**

Los Angeles County Public Health officials on Wednesday detailed their continuing efforts to improve sanitation and conditions for homeless people. Data released last week showed the number of homeless people across Los Angeles County jumped by 12%, with the majority living within the city of Los Angeles.

[KTLA](#)

### **\$339,000 for a restroom? L.A. politicians balk at the cost of toilets for homeless people**

It seems like an obvious fix to the squalor and stench as homelessness surges on Los Angeles streets: more restrooms. But L.A. has estimated that staffing and operating a mobile bathroom can cost more than \$300,000 annually - a price tag that has galled some politicians. During budget talks this spring, city officials estimated that providing toilets and showers for every homeless encampment in need would cost more than \$57 million a year.

[Los Angeles Times](#)

## **Crime**

### **Man accused in deputy's killing charged with murder, other counts**

A Utah man accused of fatally shooting an off-duty sheriff's deputy inside an Alhambra fast-food restaurant and gunning down another man in downtown Los Angeles was charged Thursday with two counts of murder and loved ones and supporters of the fallen deputy later held a vigil at the shooting scene.

[My News LA](#)

### **Truck's 'Califas' license plate draws unwanted attention from Moorpark deputy**

A truck driver's fake license plate caught the eye of law enforcement in Moorpark and led to his arrest on DUI, meth possession and other charges. So what gave it away? The first clue that the plate was not genuine was probably the word "Califas" where it should have read "California." Califas is a Spanish slang term or nickname for California.

[ABC7](#)

### **California woman impersonated social worker to try and kidnap newborn, police say**

Police have arrested a woman who allegedly impersonated a social worker in an apparent effort to kidnap a California woman's newborn child. Officers arrested the woman on suspicion of kidnapping after a mom said she showed up to her home in Santa Ana, California, on Friday morning and claimed she was there to take her 1-week-old child into protective custody, authorities said.

[ABC News](#)

### **24-year-old father charged in beating death of 4-year-old son at their South L.A. home**

A 24-year-old man was charged with murder in the death of his 4-year-old son at their South Los Angeles home, the Los Angeles County District Attorney's Office announced Monday. Hirwin Calderon-Ordenez, of Los Angeles, is facing one felony count each of murder and assault on a child causing death, officials said in a news release.

[KTLA](#)

### **Get tough: Pot industry wants LA crackdown on rogue shops**

The legal marijuana industry urged Los Angeles City Hall on Monday to get tougher with illegal shops that are gouging their businesses in open sight. Illegal pot shops are widespread throughout Los Angeles and typically look like the real thing. And they're thriving - they sell cheaper products than their legal rivals because they don't charge hefty state and local taxes.

[AP](#)

## **Los Angeles County**

### **Sheriff supervisor says public should have been warned about shootings before Malibu campground slaying**

A Los Angeles County Sheriff's Department lieutenant says he wanted to warn the public about a series of mysterious shootings around Malibu Creek State Park in the months before a camper was killed, but was told to keep quiet by his superiors. James Royal, who until January was in charge of detectives at the Sheriff's Lost Hills Station, says he became the target of workplace retaliation after the widow of the dead camper filed a lawsuit that accused the County of failing to warn the public of that very danger.

[NBC4](#)

### **'Care first, jail last': Mental health plea to LA County**

If Los Angeles County hopes to create a "care first, jail last" system of justice, it will need to make a major investment in mental health and community-based services, a county working group told the Board of Supervisors Tuesday. Supervisor Sheila Kuehl said the county was aiming to reshape its approach to criminal justice. "If not `no more jails,' then fewer and fewer people in jails," Kuehl said of the board's

goal.

[My News LA](#)

### **As homeless crisis worsens in L.A, the county leans on city officials to act**

Amid a deepening homelessness crisis, top Los Angeles County officials are grappling with how best to collaborate with City Hall as it struggles to deal with sanitation issues arising from thousands living on the streets. On Friday, the county's health officer, Dr. Muntu Davis, sent a letter to the city expressing concern about simmering health issues that will worsen in homeless encampments where bathrooms are scarce and on city streets buried in heaps of dumped trash.

[Los Angeles Times](#)

### **A look at the data - Jail bookings in LA County**

A new white paper from Million Dollar Hoods dives into LA County data detailing jail bookings occurring between 2010 and 2016. The number of people booked into the LA County Sheriff's Department's jail dropped from 150,948 in 2010 to 119,821 in 2016. Yet, disparities remain embedded in the system, and the county has ramped up its enforcement efforts against homeless individuals during that time.

[Witness LA](#)

### **Welcome to Garcetti's L.A.: Heaps of trash, hordes of rats and very little leadership**

Whewww, what a week. I could give you a hundred breakdowns of what happened and what it all means, but it comes down to this: We're in troubled waters on a ship without a captain, and though there might be a few pretenders on the bridge, nobody trusts them. We found out on Tuesday that although the city and county spent \$600 million last year to chip away at the number of homeless people, the total increased by 16% to nearly 60,000.

[Los Angeles Times](#)

### **L.A. County supervisors hope cameras will make juvenile halls safer. Officers are wary**

In a damning report on the excessive use of pepper spray in Los Angeles County's juvenile detention facilities, an internal watchdog in March made numerous recommendations to improve the department's use-of-force policies. One key idea: adding scores of closed-circuit video cameras to keep digital eyes on the youths held there - and on the overwhelmed officers charged with guarding them.

[Los Angeles Times](#)

### **New probation commission must have subpoena power says important new report detailing the "dire need" for oversight**

After ten months of public meetings, which were often intensely emotional, the special panel created to come up with a plan for a new Probation Oversight Commission is about to release its report to the

board of supervisors on Thursday morning at 10 a.m.

[Witness LA](#)

## California/National

### **Jon Stewart lashes out at hearing on 9/11 responders bill: "You should be ashamed of yourselves"**

Former "Daily Show" host Jon Stewart's demeanor on Capitol Hill Tuesday was vastly different from the one his fans were accustomed to seeing on Comedy Central. He was there to call for the reauthorization of the 9/11 Victim Compensation Fund, which was established nine years ago to provide health care benefits to first responders and others in the community with illnesses related to the 2001 terror attacks.

[CBS News](#)

### **The hunt for the Golden State Killer**

The California sun caught the light in Bonnie Colwell's long, honey-blond hair as she stood in the gravel commons of Sierra College. It was her sophomore year. She worked as a lab assistant in the science department, responsible for a small menagerie of rats, rattlesnakes and orphaned birds. She had brought two of her charges, a young great horned owl and a starling, to practice flying.

[Los Angeles Times](#)

### **Sales of ammo surge as California's ID law nears**

California ammo buyers are making a run on gun shops ahead of a new state law, which on July 1 will require buyers of bullets to show identification and undergo a background check to screen out felons and people with illegal firearms. In a state with the toughest gun laws in the nation, Gov. Gavin Newsom and some other leaders see restricting ammunition sales as a necessary next step in reducing gun tragedies.

[Los Angeles Times](#)

### **Change California taxpayers can't believe in**

As Katy Grimes noted, SB 132 by San Francisco Senator Scott Wiener "would allow prison inmates to decide their own sex, how they want to be addressed (Mr., Miss, Mrs., Ms.), and would require California Department of Corrections and Rehabilitation officials to refer to them by that chosen sex and, and house them with other inmates of the same sex." SB 132 enjoys support from the ACLU, the National Center for Lesbian Rights and other groups.

[California Globe](#)

### **Confessed serial killer now linked to 60 deaths in 14 states: Report**

A confessed serial killer who claims to have left a trail of women's bodies in a decades-long, cross-country killing spree from Florida to California has now been linked to 60 deaths, a Texas prosecutor said on Friday,

according to The Associated Press. Samuel Little, 79, is serving life sentences for killing three women in Los Angeles, and has been cooperating with federal officials and authorities in a sprawling series of investigations in multiple states for some time now.

[ABC News](#)

### **California moves to let felons serve on juries**

The state of California has made no secret that it wants to let as many people out of prison as possible. From the early release of inmates through AB 109, to filling parole boards with felon friendly commissioners, to decriminalizing a litany of felonies and drug offenses with Props 47 and 57, Sacramento lawmakers are bending over backwards to dramatically reduce the state's inmate population.

[Orange County Register](#)

### **Judge cuts penalty facing Navy SEAL, cites email intrusion**

A military judge on Friday refused to dismiss the murder case of a decorated Navy SEAL, but found the prosecution's meddling in defense lawyer emails troubling enough to reduce the maximum penalty he faces. Capt. Aaron Rugh said an effort to track emails sent to lawyers for Special Operations Chief Edward Gallagher violated constitutional rights against illegal searches and the right to counsel by interfering with attorney-client privilege.

[KETK](#)

### **Bail reform poster boy Pedro Hernandez arrested for reckless driving, no license**

Bail reform poster boy Pedro Hernandez found himself in trouble with the law after he allegedly blew through stop signs and traffic lights and switched cars to get away from cops who were after another man for urinating on the street. Police said that at around 5 a.m. Saturday cops spotted a man relieving himself near a bus stop at E. 135th St. and Walnut Ave. in the Bronx.

[New York Daily News](#)

### **California may automatically expunge 1 million convictions**

California has already moved to automatically expunge the records of those convicted of qualifying marijuana crimes. Now, Democratic lawmakers and advocates want to erase the records of those who have served their time for other crimes. The lawmakers and dozens of supporters rallied in sweltering heat Tuesday supporting two Assembly-approved bills that would automatically expunge arrest and conviction records for an estimated 1 million residents who are already entitled under existing law because they have completed their sentences and supervision.

[AP](#)

### **Oakland decriminalizes hallucinogenic 'magic mushrooms' and peyote**



The Oakland City Council unanimously passed a resolution last week effectively decriminalizing the adult use of hallucinogens derived from plants or fungi, including entheogenic mushrooms and the psychoactive alkaloids found in the peyote cactus. The lawmakers agreed to prohibit city money from being used "to assist in the enforcement of laws imposing criminal penalties" against individuals who possess, cultivate, or ingest several plant-based mind-altering substances, which are still illegal under federal and state law.

[The Daily Wire](#)

## Consumer

### **Amazon is flooded with fakes, fraud, and scams**

Consumers face a real challenge when shopping Amazon's manipulative e-commerce marketplace - dodging the fakes, fraud, and scams that plague the e-commerce giant. Amazon is a free-flowing conduit that enables Amazon, and facilitates third-party global sellers, to flood the consumer market with an inexhaustible supply counterfeit, fraudulent, pirated, and replica items.

[The Counterfeit Report](#)

## Sentences/Convictions

### **East L.A. gang member who firebombed African-American residences sentenced to years in federal prison**

A member of the Big Hazard street gang was sentenced Monday to 156 months in federal prison for orchestrating and executing the nighttime firebombing of African-American families at the Ramona Gardens Housing Development in Boyle Heights in 2014 in order to force the residents out of their homes.

[Imperial Valley News](#)

### **Bellflower man sentenced for fatally shooting convenience store clerk to prevent testimony about previous robbery**

A Bellflower man received a sentence of life in prison Friday for shooting and killing a 23-year-old 7-Eleven store clerk to prevent the victim from testifying about being robbed at gunpoint by the same attacker six months earlier, officials said. Los Angeles Superior Court Judge Raul D. Sahagun sentenced Jahmal Lydel Frazier, 29, to life in prison without the possibility of parole, Los Angeles County District Attorney's officials said in a written statement.

[KTLA](#)

### **Man who murdered Elsinore store clerk during robbery sentenced**

A man who gunned down a 47-year-old Lake Elsinore store clerk and tried to shoot the victim's co-worker was sentenced Friday to life in prison without the possibility of parole. A Murrieta jury in February convicted 28-year-old James Curtis Coon of first-degree murder for the

2017 slaying of Eric Whitecomb of Wildomar.

[City News Service](#)

### **Hesperia man sentenced to 26 years for murdering girlfriend**

Timothy Aguilar Andrade, 32, of Hesperia, was sentenced to 26 years to life for fatally stabbing his girlfriend. On Aug. 23, 2015, Andrade killed Brandi Carrasco, 35, by stabbing her in the neck inside a bedroom of a house located in the 1900 block of Richard Street where they were both staying, prosecutors said. Deputy District Attorney Fernanda Barreto said Andrade was found guilty last month of one count of first-degree murder with a knife-use allegation.

[Victor Valley News](#)

### **Charles 'Chase' Merritt found guilty of killing 4 members of McStay family**

Jurors on Monday found Charles "Chase" Merritt guilty in the February 2010 bludgeoning deaths of the four-member McStay family of Fallbrook, whose bodies were found nearly four years later in two shallow graves near Victorville. Merritt now faces a possible death sentence. The verdicts, from a circumstantial-evidence case, drew gasps in the courtroom.

[Riverside Press-Enterprise](#)

### **Mistrial declared on remaining counts against ex-NFL player**

A California jury that convicted former NFL player Kellen Winslow Jr. of raping a 58-year-old homeless woman was unable to break a deadlock on eight other counts Tuesday and a judge declared a mistrial on those charges. The judge earlier denied a defense motion to dismiss the undecided charges involving the alleged rapes of a 54-year-old hitchhiker and an unconscious teen.

[AP](#)

### **Former College of The Canyons professor convicted of sexual battery**

A former College of the Canyons professor has been convicted of sexual battery Tuesday, after an alleged assault on the campus of Moorpark College, officials said. McKale Antonious, 51, of Sylmar, was found guilty of misdemeanor sexual battery by a jury, according to Ventura County District Attorney Gregory D. Totten. The crime occurred March 2, 2017 on the campus of Moorpark Community College.

[KHTS](#)

## **Homeless**

### **Even local officials are fighting on Facebook about homelessness**

Last week, Los Angeles City Councilmembers Mike Bonin and Joe Buscaino accused neighboring cities of enforcing "unconstitutional laws... to push people experiencing homelessness out of a town and across the border into Los Angeles." The councilmen filed a motion

calling on the L.A. Homeless Services Authority, city attorney's office and other relevant offices to investigate fellow cities' compliance with a 9th Circuit Court of Appeals ruling out of Boise, Idaho last September.

[LAist](#)

### **16,000 people in L.A. now live in cars, vans and RVs. But safe parking remains elusive**

Two years ago, Los Angeles began testing an alternative to homeless shelters called safe parking, giving people living in their cars a secure spot to sleep at night. The first site was quickly deemed a success, so the Los Angeles Homeless Services Authority agreed to fund nine more lots in the pilot program, with promises to expand.

[Los Angeles Times](#)

### **LA County Supervisor Janice Hahn calls for 'urgency,' prevention as homeless numbers surge**

L.A. County Supervisor Janice Hahn says prevention may be key to tackling the region's growing homeless crisis. The number of homeless people in Los Angeles County surged by 12 percent over the last year to nearly 59,000 living on the streets, according to data released Tuesday. Of that number, almost three-fourths of those people are sleeping in cars, tents and other makeshift shelters, according to the county's 2019 Biennial Homeless Count.

[CBS LA](#)

## **Corrections**

### **Lawsuit filed over prison mental health facility**

The City of Chino has been joined by three agencies in a lawsuit filed Friday against the California Department of Corrections and Rehabilitation over a 50-bed mental health crisis facility proposed at the men's prison. The men's prison, called the California Institution for Men built in 1941, is located at 14901 Central Ave. at the end of Chino Hills Parkway.

[Champion Newspapers](#)

## **Guns**

### **Attorney General William P. Barr announces the creation of a working group on prosecuting gun crimes to stop and reduce domestic violence**

Attorney General William P. Barr today announced the formation of a Domestic Violence Working Group aimed at keeping guns out of the hands of convicted domestic abusers, using the tools of federal prosecution to stop and prevent domestic violence. The group will operate under the auspices of the Attorney General's Advisory Committee (AGAC) and be comprised of nine U.S. Attorneys across the country, chaired by U.S. Attorney for the Northern District of Texas Erin Nealy Cox.

## Pensions

### **California retirees' pensions restored - at least partially - after CalPERS cuts**

The Sierra County town of Loyalton has reached a settlement agreement with three retired city workers who sued the town and CalPERS after CalPERS reduced the retirees' pension checks. The terms of the agreement are confidential, including when it was reached, but the 706-person town will pay at least a portion of what it owes the retirees, their attorney said.

[Sacramento Bee](#)

### **Did CalPERS mislead policyholders on long-term care insurance? Trial begins on a \$1.2 billion lawsuit**

A \$1.2 billion lawsuit that could affect up to about 100,000 seniors who had CalPERS long-term care insurance plans goes to trial Monday. The class-action lawsuit claims the California Public Employees' Retirement System violated insurance policy terms when it increased premiums by 85 percent in 2015 and 2016 after promising policyholders stability.

[Sacramento Bee](#)

### **Gavin Newsom's budget aims to spare California schools from some pension pain**

Gov. Gavin Newsom's first state budget frees up hundreds of millions of dollars for financially strapped schools by easing pressure on their pension rates and steering some additional money to them for special education programs. The agreement won't necessarily spare distressed school districts like Sacramento City Unified from cuts, but it could help them stave off some hard decisions.

[Sacramento Bee](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [SQLServerCentral](#)  
**To:** [Arthur Pham](#)  
**Subject:** Managing SQL Server containers using Docker SDK for Python (SQLServerCentral 2019-06-13)  
**Date:** Thursday, June 13, 2019 4:18:10 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Problems displaying this newsletter? [View online.](#)



### Featured Contents

- **Managing SQL Server containers using Docker SDK for Python - Part 1**
- **How to Copy a Table in SQL Server to Another Database**
- **From the SQL Server Central Blogs - What is a distributed transaction?**
- **From the SQL Server Central Blogs - 12 Ways To Rewrite SQL Queries for Better Performance**

### Question of the Day

- **Service Broker Undelivered Messages**

## The Voice of the DBA

### Upgrading Your OS

I loved Windows 7. I haven't felt that way about many of the Windows systems. I tolerated 3.1, preferring DOS and Solaris at the time. Windows 95 was great, with me skipping Windows 98 after installing it on a few PCs at work. I thought Windows 2000 was OK, and did really like XP. I avoided Vista, running XP until I got a beta of Win 7. Then I thought Microsoft had made a great move, slimming down the OS and making it faster on the same hardware.

I skipped Windows 8 and moved to Windows 10, so I guess I like every other version of Windows. That makes sense. I've often felt every other version of SQL Server was really good, with some slim, not quite sure I like this, not quite sure this is worth the money, in-between versions. That might be changing as I liked SQL Server 2016, 2017, and 2019 is looking good.



I ran across [an article on the move to Windows 10](#), which Microsoft has been pushing and which has proceeded very well. Many people upgraded, especially with the free offer to upgrade. However, the pace of change has leveled off, with Windows 10 at 44% recently and Windows 7 at nearly 37%. The disconcerting issue is that the latter number has barely changed from the end of 2018. With Windows 7 expected to EOL in Jan of 2020, Microsoft is trying to push people forward.

There are all sorts of reasons people are loathe to update their OS. Compatibility issues, the comfortable feeling of knowing how a system works, and certainly resource concerns. I wish security was a higher level of concern for more people. When Win7 EOLs, enterprises can pay \$200/yr/machine to get patches, but there is no option for Home users. I think this is a little short sighted as many Home users might not see value in upgrading, but they (and the rest of us) need secure machines on the Internet. Why wouldn't a \$50/yr charge for security patches make sense?

Modern hardware is powerful and lasts longer, so I could understand an individual that started running the OS in 2011 not seeing a need to change. They are happy with a PC that runs email, browses the web, plays solitaire, and manages money. Do these people need to upgrade to Win 10? I don't know that they do, and the vast majority of the world are consumers, not creators, so the much of the work done in Win10 isn't useful for them.

There isn't a right answer here, and certainly there are security concerns from an older OS, but at some point the OS and hardware will be good enough for most people to stick around a long time. Microsoft ought to be prepared in those cases to enable very long term support, perhaps with some yearly charge, to provide patches to the OS. I don't know if Win7 is the place to do that, but I do think that Win10 ought to be around for a long, long time with paid support.

**Steve Jones - SSC Editor**

[Join the debate, and respond to today's editorial on the forums](#)



## Featured Contents

### Managing SQL Server containers using Docker SDK for Python - Part 1

carlos10robles from [SQLServerCentral](#)



There are multiple ways to interact with the Docke...



## How to Copy a Table in SQL Server to Another Database

Additional Articles from [MSSQLTips.com](https://www.mssqltips.com)

Learn about options to copy a table from one SQL Server database to another including Linked Servers, PowerShell, Integration Services, backup and restore along with the associated performance metrics and completion time.



## From the SQL Server Central Blogs - What is a distributed transaction?

Kenneth.Fisher from [SQLStudies](https://www.sqlstudies.com)

A while back I did a post defining a transaction. Basically, a transaction is a unit of work. The example ... Continue reading



## From the SQL Server Central Blogs - 12 Ways To Rewrite SQL Queries for Better Performance

Bert Wagner from [Bert Wagner](https://www.bertwagner.com)

Watch this week's video on YouTube. Thanks to you, we just crossed the 2k subscriber mark! Over the past several week's I've been exploring ways to rewrite queries to improve...

## Question of the Day

Today's question (by mkdm):

### Service Broker Undelivered Messages

Service Broker is enabled on my database, but messages are not arriving in my TargetQueue. I have confirmed that the initiator and target services have been configured correctly, and that my queues are enabled. Where could I look for the undelivered messages?

Think you know the answer? [Click here](#), and find out if you are right.



## Yesterday's Question of the Day (by Steve Jones - SSC Editor)

No More Denial

I decide to prevent the Sales role from accessing the dbo.SalesArchive table. I run this:

```
DENY SELECT ON dbo.SalesArchive TO Sales
```

Later I realize that this is breaking our application and need to remove the deny. What code should I run?

**Answer:** REVOKE SELECT ON dbo.SalesArchive FROM Sales

**Explanation:** The DENY is a permission added to the user. The REVOKE statement on that permission will remove this, the same as it does for a GRANT. Ref: REVOKE - <https://docs.microsoft.com/en-us/sql/t-sql/statements/revoke-transact-sql?view=sql-server->



[2017](#)

[Discuss this question and answer on the forums](#)

## Database Pros Who Need Your Help

Here's a few of the new posts today on the forums. To see more, [visit the forums](#).

---

### SQL Server 2017 - Development

[Import XML into a sql table](#) - Hey guys! How do I upload a file with the structure as in the picture? The XML has a structure like this ??? ???????????555.00.111-33?? "??????????  
?????????????????????????????????"80000055639-182018-12-23333-33-33/12018-12-  
23586?????9,10x7,73x4005?110?? 001.392-200617333-33-33/182234-18?? 95 166-  
9832407.00.01378????????? ?????? ? ???????? ???????? ?????????? ?????????? [...]

[Count of entries & grouped by month - extracted from a date](#) - hiya amazing people I need some help with the query below. I need to see the breakdown of entries by month but the [RecvdDate] has a datatype of (varchar,null) & the date appears something like 2019-05-31 for example. What should I add in my SELECT statement to get the monthly breakdown? SELECT COUNT(ID) AS 'Total [...]

### SQL Server 2016 - Administration

[Audit login's permission change](#) - Is there a way to keep track of who is changing permission for one of the login our web is using? That login has owner rights and time to time, we run into issues where that login no longer has owner rights. But who is causing it? I created a user, granted that user with [...]

[Database is in emergency mode or is damaged and must be restarted](#) - When connecting to SSMS, the database shows online and I am able to run queries against it. But, while trying to backup the database it is giving me this error message "Could not run BEGIN TRANSACTION in database because the database is in emergency mode or is damaged and must be restarted". Thanks.

[Disable Read-intent mode only availability Group](#) - Hello everyone I have an Alwayson cluster in Availability Group AG mode the secondary replica is configured in "Read-intent only" mode I configured read request routing to the second node to ease the load on the primary node Currently following a license problem it asked me to make the second passive node not accessible in [...]

## **Administration - SQL Server 2014**

[\[HELP\] I did a DROP and CREATE blank records on a production database](#) - Hi there, My name is Kay and I work as a data analyst in Indonesia. I made a terrible mistake when I (intent to) copy the query from an old database to the live production database. Instead of copying the query, I was unaware that I did not remove the check-mark in the checkbox on [...]

[Restore SSIS without backup and only from MDF and LDF files](#) - I am needing to restore / rebuild an SSIS Catalog on a new SQL Server. Problem is, I don't have a backup and only have the MDF and LDF file. I am unfamiliar with SSIS so I have tried attaching the DB but it doesn't re-create the catalog and the jobs. I know the password [...]

## **Development - SQL Server 2014**

[Exclude records with column value starting with '836'](#) - Hi All, So my latest issue is I need to be able to exclude records with claim numbers that start with '836'. This seems pretty straight forward, but nothing I've tried seems to be working, as I'm still getting back claim numbers starting with '836'. I've tried using NOT LIKE and NOT IN. Could I [...]

## **SQL Server 2012 - T-SQL**

[Need some help with inserting text](#) - Hi, I am in a scenario where I need to manipulate some text. For example: p11034 - If the first letter is 'p' and the count of characters to the right of the 'p' is 5, then insert 4 zeros between the p and 11034. The end result is 'P000011034' Any assistance would be great. [...]

## **SQL Server 2008 - General**

[View crashes SQL Studio](#) - Hi all, I have a query which is working fine. However, when I attempt to put it into a view SQL always crashes. There is no error message when I run the view other than the crash window: SSMS - SQL Server Management has stopped working. However, if I try save the view, the error [...]



## SQL Azure - Administration

[Backup retention upto 10 years in PAAS](#) - Hi Experts, Do I have to pay additional amount to retain my PAAS SQL database backup for 10 years in Azure? Thanks Brijesh

[Azure elastic database jobs](#) - Hi, I am trying to use this approach to automate some tasks: <https://docs.microsoft.com/en-us/azure/sql-database/elastic-jobs-tsql> It mentions: "The credential needs appropriate permissions, on the databases specified by the target group, to successfully execute the script. " CREATE MASTER KEY ENCRYPTION BY PASSWORD='password'; CREATE DATABASE SCOPED CREDENTIAL myjobcred WITH IDENTITY = 'jobcred', SECRET = 'password'; GO CREATE DATABASE SCOPED [...]

## SSRS 2016

[Different extensions for view report and generate subscription](#) - Hi all, i need to hide for all reports MHTML extension (I know how to do it: but i need this extension in subscription, and after above change i dont see it Any ideas?

## Integration Services

[Extract dates from the file name in SSIS](#) - Hi, I have a requirement to extract the 2 dates from the file name in SSIS (2010) as a derived column in the data flow task. The filename is as follows: Abdr\_FC\_BHYUK\_Weekly\_Physical\_SAVERSHP\_IBLUPGE\_All Links Roll up\_050519\_110519.xlsx Can someone please help on this ? Thanks.

## SQLServerCentral.com Website Issues

[Keep getting Subscribed to Topics I've Unsubscribed from](#) - This has happened to me a couple times with long running topics like Today's Random Word and Are the posted questions getting? Despite Unsubscribing from email notifications they'll randomly just turn back on which is somewhat annoying.



you have any problems leaving the list, please contact the [webmaster@sqlservercentral.com](mailto:webmaster@sqlservercentral.com). This newsletter was sent to you because you signed up at [SQLServerCentral.com](http://SQLServerCentral.com).

**From:** [SQLServerCentral](#)  
**To:** [Lan Le](#)  
**Subject:** Managing SQL Server containers using Docker SDK for Python (SQLServerCentral 2019-06-13)  
**Date:** Thursday, June 13, 2019 2:31:02 AM

---

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

Problems displaying this newsletter? [View online.](#)



### Featured Contents

- [Managing SQL Server containers using Docker SDK for Python - Part 1](#)
- [How to Copy a Table in SQL Server to Another Database](#)
- [From the SQL Server Central Blogs - What is a distributed transaction?](#)
- [From the SQL Server Central Blogs - 12 Ways To Rewrite SQL Queries for Better Performance](#)

### Question of the Day

- [Service Broker Undelivered Messages](#)

## The Voice of the DBA

### Upgrading Your OS

I loved Windows 7. I haven't felt that way about many of the Windows systems. I tolerated 3.1, preferring DOS and Solaris at the time. Windows 95 was great, with me skipping Windows 98 after installing it on a few PCs at work. I thought Windows 2000 was OK, and did really like XP. I avoided Vista, running XP until I got a beta of Win 7. Then I thought Microsoft had made a great move, slimming down the OS and making it faster on the same hardware.

I skipped Windows 8 and moved to Windows 10, so I guess I like every other version of Windows. That makes sense. I've often felt every other version of SQL Server was really good, with some slim, not quite sure I like this, not quite sure this is worth the money, in-between versions. That might be changing as I liked SQL Server 2016, 2017, and 2019 is looking good.

I ran across [an article on the move to Windows 10](#), which Microsoft has been pushing and which has proceeded very well. Many people upgraded, especially with the free offer to upgrade. However, the pace of change has leveled off, with Windows 10 at 44% recently and Windows 7 at nearly 37%. The disconcerting issue is that the latter number has barely changed from the end of 2018. With Windows 7 expected to EOL in Jan of 2020, Microsoft is trying to push people forward.

There are all sorts of reasons people are loathe to update their OS. Compatibility issues, the comfortable feeling of knowing how a system works, and certainly resource concerns. I wish security was a higher level of concern for more people. When Win7 EOLs, enterprises can pay \$200/yr/machine to get patches, but there is no option for Home users. I think this is a little short sighted as many Home users might not see value in upgrading, but they (and the rest of us) need secure machines on the Internet. Why wouldn't a \$50/yr charge for security patches make sense?

Modern hardware is powerful and lasts longer, so I could understand an individual that started running the OS in 2011 not seeing a need to change. They are happy with a PC that runs email, browses the web, plays solitaire, and manages money. Do these people need to upgrade to Win 10? I don't know that they do, and the vast majority of the world are consumers, not creators, so the much of the work done in Win10 isn't useful for them.

There isn't a right answer here, and certainly there are security concerns from an older OS, but at some point the OS and hardware will be good enough for most people to stick around a long time. Microsoft ought to be prepared in those cases to enable very long term support, perhaps with some yearly charge, to provide patches to the OS. I don't know if Win7 is the place to do that, but I do think that Win10 ought to be around for a long, long time with paid support.

**Steve Jones - SSC Editor**

[Join the debate, and respond to today's editorial on the forums](#)



## Featured Contents

### Managing SQL Server containers using Docker SDK for Python - Part 1

carlos10robles from [SQLServerCentral](#)



There are multiple ways to interact with the Docke...



## How to Copy a Table in SQL Server to Another Database

Additional Articles from [MSSQLTips.com](https://mssqltips.com)

Learn about options to copy a table from one SQL Server database to another including Linked Servers, PowerShell, Integration Services, backup and restore along with the associated performance metrics and completion time.



## From the SQL Server Central Blogs - What is a distributed transaction?

Kenneth.Fisher from [SQLStudies](https://sqlstudies.com)

A while back I did a post defining a transaction. Basically, a transaction is a unit of work. The example ... Continue reading



## From the SQL Server Central Blogs - 12 Ways To Rewrite SQL Queries for Better Performance

Bert Wagner from [Bert Wagner](https://bertwagner.com)

Watch this week's video on YouTube. Thanks to you, we just crossed the 2k subscriber mark! Over the past several week's I've been exploring ways to rewrite queries to improve...



## Question of the Day

Today's question (by mkdm):

### Service Broker Undelivered Messages

Service Broker is enabled on my database, but messages are not arriving in my TargetQueue. I have confirmed that the initiator and target services have been configured correctly, and that my queues are enabled. Where could I look for the undelivered messages?

Think you know the answer? [Click here](#), and find out if you are right.



## Yesterday's Question of the Day (by Steve Jones - SSC Editor)

No More Denial

I decide to prevent the Sales role from accessing the dbo.SalesArchive table. I run this:

```
DENY SELECT ON dbo.SalesArchive TO Sales
```

Later I realize that this is breaking our application and need to remove the deny. What code should I run?

**Answer:** REVOKE SELECT ON dbo.SalesArchive FROM Sales

**Explanation:** The DENY is a permission added to the user. The REVOKE statement on that permission will remove this, the same as it does for a GRANT. Ref: REVOKE - <https://docs.microsoft.com/en-us/sql/t-sql/statements/revoke-transact-sql?view=sql-server->

[2017](#)

[Discuss this question and answer on the forums](#)

## Database Pros Who Need Your Help

Here's a few of the new posts today on the forums. To see more, [visit the forums](#).

---

### SQL Server 2017 - Development

[Import XML into a sql table](#) - Hey guys! How do I upload a file with the structure as in the picture? The XML has a structure like this ??? ?????????????555.00.111-33?? "??????????  
?????????????????????????????????"80000055639-182018-12-23333-33-33/12018-12-  
23586?????9,10x7,73x4005?110?? 001.392-200617333-33-33/182234-18?? 95 166-  
9832407.00.01378????????? ?????? ? ???????? ???????? ???????? ???????? [...]

[Count of entries & grouped by month - extracted from a date](#) - hiya amazing people I need some help with the query below. I need to see the breakdown of entries by month but the [RecvdDate] has a datatype of (varchar,null) & the date appears something like 2019-05-31 for example. What should I add in my SELECT statement to get the monthly breakdown? SELECT COUNT(ID) AS 'Total [...]

### SQL Server 2016 - Administration

[Audit login's permission change](#) - Is there a way to keep track of who is changing permission for one of the login our web is using? That login has owner rights and time to time, we run into issues where that login no longer has owner rights. But who is causing it? I created a user, granted that user with [...]

[Database is in emergency mode or is damaged and must be restarted](#) - When connecting to SSMS, the database shows online and I am able to run queries against it. But, while trying to backup the database it is giving me this error message "Could not run BEGIN TRANSACTION in database because the database is in emergency mode or is damaged and must be restarted". Thanks.

[Disable Read-intent mode only availability Group](#) - Hello everyone I have an Alwayson cluster in Availability Group AG mode the secondary replica is configured in "Read-intent only" mode I configured read request routing to the second node to ease the load on the primary node Currently following a license problem it asked me to make the second passive node not accessible in [...]

## **Administration - SQL Server 2014**

[\[HELP\] I did a DROP and CREATE blank records on a production database](#) - Hi there, My name is Kay and I work as a data analyst in Indonesia. I made a terrible mistake when I (intent to) copy the query from an old database to the live production database. Instead of copying the query, I was unaware that I did not remove the check-mark in the checkbox on [...]

[Restore SSIS without backup and only from MDF and LDF files](#) - I am needing to restore / rebuild an SSIS Catalog on a new SQL Server. Problem is, I don't have a backup and only have the MDF and LDF file. I am unfamiliar with SSIS so I have tried attaching the DB but it doesn't re-create the catalog and the jobs. I know the password [...]

## **Development - SQL Server 2014**

[Exclude records with column value starting with '836'](#) - Hi All, So my latest issue is I need to be able to exclude records with claim numbers that start with '836'. This seems pretty straight forward, but nothing I've tried seems to be working, as I'm still getting back claim numbers starting with '836'. I've tried using NOT LIKE and NOT IN. Could I [...]

## **SQL Server 2012 - T-SQL**

[Need some help with inserting text](#) - Hi, I am in a scenario where I need to manipulate some text. For example: p11034 - If the first letter is 'p' and the count of characters to the right of the 'p' is 5, then insert 4 zeros between the p and 11034. The end result is 'P000011034' Any assistance would be great. [...]

## **SQL Server 2008 - General**

[View crashes SQL Studio](#) - Hi all, I have a query which is working fine. However, when I attempt to put it into a view SQL always crashes. There is no error message when I run the view other than the crash window: SSMS - SQL Server Management has stopped working. However, if I try save the view, the error [...]

## SQL Azure - Administration

[Backup retention upto 10 years in PAAS](#) - Hi Experts, Do I have to pay additional amount to retain my PAAS SQL database backup for 10 years in Azure? Thanks Brijesh

[Azure elastic database jobs](#) - Hi, I am trying to use this approach to automate some tasks: <https://docs.microsoft.com/en-us/azure/sql-database/elastic-jobs-tsql> It mentions: "The credential needs appropriate permissions, on the databases specified by the target group, to successfully execute the script. " CREATE MASTER KEY ENCRYPTION BY PASSWORD='password'; CREATE DATABASE SCOPED CREDENTIAL myjobcred WITH IDENTITY = 'jobcred', SECRET = 'password'; GO CREATE DATABASE SCOPED [...]

## SSRS 2016

[Different extensions for view report and generate subscription](#) - Hi all, i need to hide for all reports MHTML extension (I know how to do it: but i need this extension in subscription, and after above change i dont see it Any ideas?

## Integration Services

[Extract dates from the file name in SSIS](#) - Hi, I have a requirement to extract the 2 dates from the file name in SSIS (2010) as a derived column in the data flow task. The filename is as follows: Abdr\_FC\_BHYUK\_Weekly\_Physical\_SAVERSHP\_IBLUPGE\_All Links Roll up\_050519\_110519.xlsx Can someone please help on this ? Thanks.

## SQLServerCentral.com Website Issues

[Keep getting Subscribed to Topics I've Unsubscribed from](#) - This has happened to me a couple times with long running topics like Today's Random Word and Are the posted questions getting? Despite Unsubscribing from email notifications they'll randomly just turn back on which is somewhat annoying.



have any problems leaving the list, please contact the webmaster@sqlservercentral.com. This newsletter was sent to you because you signed up at SQLServerCentral.com.



**From:** [CLA Public Section](#)  
**To:** [Melissa Tronquet](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, May 31, 2019 3:02:24 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive](#) (850,187 articles)



[North America](#) | [Global](#)

**USA**

[North America](#)

[Employee Benefits & Pensions](#)



### **Not So Fast...the (Unexpected) Consequences of Allowing Your Employees to Early Exercise Options**

**Wilmer Cutler Pickering Hale and Dorr LLP**

From time to time, and primarily when the economy is booming, allowing to be “early exercised”—that is...

### **IRS Adds 2019 Updates to Operational Compliance List**

**Holland & Knight LLP**

The Internal Revenue Service (IRS) has updated its Operational Compliance List for retirement plans with a number of changes that take...

### **RMDs and the “Still Working” Exception: Planning Strategies**

**Hall Benefits Law**

In general, qualified retirement plans require participants to begin taking the required minimum distribution (RMD) by April 1st of the year they...

### **Projet de loi 30 : La Colombie Britannique propose de modifier le Labour Relations Code à l'avantage des travailleurs**

[District of Columbia](#)

**Stikeman Elliott LLP**

Le 30 avril 2019, le gouvernement de la Colombie-Britannique a annoncé une importante révision du Labour Relations Code...

---

**Practice Tip: Warning Signs Your Plan May Have a Missing Participants Problem**  
**Haynes and Boone LLP**

When participants in a qualified retirement plan terminate employment with the plan sponsor, it can be challenging to ensure that their contact...

---

**Economic, Executive Tenure, and Compensation Trends for the Board**  
**McDermott Will & Emery**

Economic trends and indicators have significant implications for health care boards. In the latest episode of the Governing Health podcast, Michael...

---

**Let the Planning Begin: IRS Releases HSA and HDHP Limits for 2020**  
**Graydon Head & Ritchey LLP**

While it may be early to be thinking about next year for some, others are already knee deep in making health plan changes for 2020. For those that...

---

**The Importance of Proactive ERISA Legal Compliance Reviews**  
**Hall Benefits Law**

Periodically, the IRS will audit qualified retirement plans to ensure compliance with ERISA and federal regulations. Having taken the time to be...

---

**Mitigating the Tax Impact on Employee Equity Compensation**  
**Hall Benefits Law**

Businesses of all sizes, from brand new startups to large blue-chip enterprises, like to use equity compensation for key employees. This ties the...

---

**COBRA Coverage Considerations for Terminated Employees**  
**Hall Benefits Law**

The Consolidated Omnibus Budget Reconciliation Act of 1985's continuation of coverage requirements, now commonly known as COBRA, is the option...

---

**Surprise! A QDRO Can Apply to a Welfare Benefit Plan**  
**Dickinson Wright**

Most plan administrators are familiar with a qualified domestic relations order or "QDRO," which is used to split retirement plan benefits between a...

---

**Ohio Federal Court Rejects Attempt to Certify Class Against Third-Party Plan Administrator Under ERISA § 502(a)(3)** [Ohio](#)

**Baker & Hostetler LLP**

Employee Retirement Income Security Act (ERISA) claims can potentially involve significant amounts in controversy, and in an effort to broaden the...

---

**Washington Healthcare Update- May 24, 2019** [District of Columbia](#)

**McGuireWoods Consulting LLC**

House Ways & Means Committee: Hearing on Single-Payer Issue The House



Ways & Means Committee will hold a hearing on the single-payer issue, marking...

---

### **Documentation of ERISA Authorized Representative Procedures**

#### **Haynes and Boone LLP**

Under ERISA, a participant in an ERISA-covered plan has the right to designate an authorized representative to act on his or her behalf in connection...

---

### **IRS Announces Limited Expansion of the Determination Letter Program for Individually Designed Plans**

#### **Drinker Biddle & Reath LLP**

Since the end of the IRS's cyclical determination letter program for individually designed retirement plans in 2017, plan sponsors have been able to...

---

### **Eastern District of New York refuses to enforce an ERISA anti-assignment provision**

New York

#### **Jackson Lewis PC**

The list of the federal courts of appeals enforcing unambiguous anti-assignment provisions in ERISA health benefit plans continues to grow: almost...

---

### **Participant Loans: A Fiduciary Storm Brewing?**

#### **Drinker Biddle & Reath LLP**

The article discusses the fiduciary risk that defined contribution plan sponsors could face when participants default on plan loans.

---

### **NRECA Praises House Bill Lowering Coop Pension Premiums**

#### **Eversheds Sutherland (US) LLP**

The National Rural Electric Cooperative Association (NRECA) came out last week in support of the House of Representatives passing a bill to reduce...

---

### **House Bill Makes Significant Changes to Retirement Plans**

#### **Bradley Arant Boult Cummings LLP**

Last week, the House of Representatives overwhelmingly passed the "Setting Every Community Up for Retirement Enhancement (SECURE) Act of 2019...

---

## **Employment & Labor**



---

### **Employee termination law in Arizona**

Arizona

#### **Ogletree Deakins**

A structured guide to employee termination law in Arizona

---

### **Hiring and wage & hour law in Vermont**

Vermont

#### **Downs Rachlin Martin PLLC**

A structured guide to background checks, hiring and wage & hour law in Vermont

---

### **Employee termination law in Ohio**

Ohio

#### **Taft Stettinius & Hollister LLP**

A structured guide to employee termination law in Ohio

---

### **Employee termination law in Nevada** Nevada

#### **Holland & Hart LLP**

A structured guide to employee termination law in Nevada...

---

### **Governor Hogan Vetoes the Ban the Box Bill** Maryland

#### **Shawe Rosenthal LLP**

Governor Hogan announced on May 24, 2019 that he was vetoing HB994, the “Ban the Box” bill, as our partner Liz Torphy-Donzella predicted he would do...

---

### **New York City Council Advances Legislation Expanding Earned Safe and Sick Time Law** New York

#### **Cozen O'Connor**

The New York City Council has scheduled a hearing on Int. 800-A, legislation that would expand NYC's Earned Safe and Sick Time law by adding up to 80...

---

### **Connecticut Likely To Become Latest State to Adopt \$15 Minimum Wage**

Connecticut

#### **Epstein Becker Green**

Connecticut appears poised to become the next state to raise its minimum wage to \$15 per hour, following the trend set by California, Illinois...

---

### **The Intersection of Workers' Compensation and OSHA: Look Both Ways Before Crossing**

#### **Goldberg Segalla LLP**

In many ways, workers' compensation (WC) and the OSHA are very different. WC is a statutory compensation scheme designed to limit an employer's...

---

### **The City of Kansas City, Missouri Bans Salary History Inquiries** Kansas Missouri

#### **Stinson LLP**

Kansas City employers soon will be prohibited from asking job applicants about their salary history information, including prior compensation and...

---

### **Nevada Expands Remedies Available for Employment Discrimination Claims**

Nevada

#### **Littler Mendelson PC**

The Nevada Legislature recently passed Senate Bill No. 177, which greatly expands the remedies available under Nevada's anti-discrimination statute...

---

### **Say My Name**

#### **Graydon Head & Ritchey LLP**

In 2012, actress Quvenzhané Wallis made history as the youngest actress to be nominated for an Academy Award. She was just five years old when she...

---

### **Denial of Workers' Compensation Claim Affirmed After Incorrect Standard of Review Applied by Lower Court** Georgia



### **Goldberg Segalla LLP**

Kevin Sinyard worked as a union pipefitter since 1978; from 1986-1989, the plaintiff worked for the defendant, McKenney's Inc. at Piedmont...

---

### **The State AG Report Weekly Update May 23, 2019**

#### **Cozen O'Connor**

2019 AG Elections Republican Daniel Cameron and Democrat Greg Stumbo Secure Party Nominations for Kentucky Attorney General Daniel Cameron defeated...

---

### **Solar Company's Amended Complaint Prompts Court to Dismiss Trade Secrets Claims Against LG Electronics as Untimely**

#### **Winston & Strawn LLP**

After finding that a solar technology company's claim under California's Unfair Competition Law was preempted by its theft of trade secret claim under...

---

### **Oregon Modifies Noncompete Law for 2020**

Oregon

#### **Ogletree Deakins**

On May 14, 2019, Oregon Governor Kate Brown signed House Bill (HB) 2992, which imposes a new burden on employers that want to have enforceable...

---

### **Regulatory Spring: Rulemaking by the Wage & Hour Division - May 23, 2019**

#### **Seyfarth Shaw LLP**

Earlier this week, the comment period ended for the U.S. Department of Labor, Wage & Hour Division's proposed rule increasing the salary threshold...

---

### **Connecticut Charts Path to Increase Minimum Wage to \$15**

#### **Fox Rothschild LLP**

Joining a trend sweeping the country, Connecticut lawmakers passed a bill that introduces a schedule to increase the minimum wage to \$15 per hour by...

---

### **Georgia Supreme Court: The State Is Not Its Citizens' Data Keeper**

Georgia

#### **Womble Bond Dickinson (US) LLP**

According to the highest court in the state, Georgia state government does not have an inherent obligation to protect citizens' personal or sensitive...

---

### **Don't Fuggedaboutit: Keeping up with the ever-changing New York State and City employment law landscape**

New York

#### **Reed Smith LLP**

New York State and City legislators have enacted a flurry of new workplace-related regulations in the past few years. The new laws touch upon...

---

### **Law Now Protects Employees' Sexual and Reproductive Health Decisions**

New

York

#### **Manatt Phelps & Phillips LLP**

The New York City Human Rights Law now prohibits employment-related



discrimination and retaliation on the basis of an employee's "sexual and...

---

### **Retaliation Prevention Requires a Robust Policy and Proactive Process**

#### **Investigations Law Group**

The E.E.O.C. reports that retaliation is the most frequently raised claim in federal sector cases and the most common finding in such cases. Beyond...

---

### **New DC Circuit Case Raises the Bar for Employment Discrimination Defendants**

[District of Columbia](#)

#### **Arent Fox LLP**

The Supreme Court's, *McDonnell Douglas Corp. v. Green*, 411 US 792 (1973), burden-shifting framework is all too familiar to employment discrimination...

---

### **Legal Documents Don't Have to be in Legalese. Stick to Plain Language.**

#### **Barnes & Thornburg LLP**

Recently a client came to me and asked me to simplify its employment documents. I read through the company's standard employment agreement...

---

### **District Court Finds no CFAA Violation where Employee Shares Confidential Company Information with Competitor**

#### **Jackson Lewis PC**

A district court in Tennessee recently concluded in *Wachter Inc. v. Cabling Innovations LLC* that two former employees who allegedly shared...

---

### **New York City Enacts Law Prohibiting Pre-Employment Testing for Marijuana Use**

[New York](#)

#### **Goldberg Segalla LLP**

New York City is not shy about enacting laws governing the workplace. One of NYC's newest employment related laws will prohibit employers from...

---

### **A Whistleblower Speaks Up at Your Company — Now What? 5 Key Considerations**

#### **Vinson & Elkins LLP**

At first blush, news that an employee has filed an internal report detailing illegal or unethical behavior at your company may seem like a terrible...

---

### **Texas Service Center Now Accepting Form I-129 for Certain H-1B Petitions**

[California](#)

[Nebraska](#)

[Texas](#)

[Vermont](#)

#### **Pierce Atwood LLP**

The Texas Service Center has begun processing Form I-129, Petition for a Nonimmigrant Worker, for H-1B petitions where the beneficiary has already...

---

### **National Backlash Builds Against Non-Compete Agreements**

[Video](#)

#### **Epstein Becker Green**

Several states have passed legislation restricting non-compete agreements that temporarily prohibit departing employees from taking jobs with...

---

## **Substantial Justice is Driving Factor in Decision to Transfer Mesothelioma Case to Colorado** New York

### **Goldberg Segalla LLP**

The plaintiff, Carl Lanz, filed suit in New York against the defendants alleging he developed mesothelioma as a result of his occupational...

---

## **Required OSHA and Safety Training in NYC Extended ... Again** New York

### **Goldberg Segalla LLP**

New York City takes its approach to safety for its construction workers seriously. At least that's the idea. In 2017, New York City Council members...

---

## **NLRB General Counsel Concludes That Drivers Using the Uber App Are Independent Contractors, Not Employees**

### **Epstein Becker Green**

The Division of Advice of the National Labor Relations Board ("NLRB" or "Board"), in an Advice Memorandum, dated April 16, 2019 ("Advice Memo"),[1]...

---

## **USCIS Completes Data Entry for FY 2020 H-1B Cap Subject Petitions** California

Vermont

### **Pierce Atwood LLP**

USCIS has announced that data entry is now complete for FY 2020 H-1B Cap Subject Petitions selected in the USCIS computer-generated random selection...

---

## **Low Hanging Fruit: Take 967**

### **FisherBroyles LLP**

This particular health care provider which the EEOC nailed for \$950,000 provides such care nationwide for jails and corrections facilities, not the...

---

## **How to Properly Structure an Unpaid Internship Program in New York** New York

### **Law Office of Kristine A Sova**

A variation of this post appeared on my website a number of years ago following the initial wave of unpaid intern lawsuits that were filed in New York...

---

## **Changes to WA Laws on Noncompetition Agreements** Washington

### **Davis Wright Tremaine LLP**

On May 8, 2019, Washington Governor Jay Inslee signed new legislation (referred to as the "Washington noncompete law") that puts tighter restrictions...

---

## **What Can Employers Do About the Measles Outbreak?** California New York

### **Fox Rothschild LLP**

As measles outbreaks affect New York City and major California counties, employers should understand the best practices for ensuring the health and...

---

## **EEOC Sets September 30th Deadline for Employers to Submit Pay Data... at Least, for Now** District of Columbia

### **Nelson Mullins Riley & Scarborough LLP**



In addition to their normal filing due on May 31, 2019, EEO-1 filers must now also file information containing employee pay data by September 30, 2019...

---

**BIPA After Rosenbach — A Broad Interpretation By Illinois Courts** Illinois

**Baker McKenzie**

As we previously reported, in January, in *Rosenbach v. Six Flags Entertainment Corp.*, the Illinois Supreme Court held that a plaintiff need not plead...

---

**US Supreme Court Restricts Counterclaim Defendants' Rights to Remove Class Actions**

**Baker McKenzie**

In a 5-4 decision issued on 28 May 2019, the United States Supreme Court held that the federal removal statute does not permit a third-party...

---

**La Colombie Britannique propose des changements importants à l'Employment Standards Act** District of Columbia

**Stikeman Elliott LLP**

Le projet de loi 8, l'Employment Standards Amendment Act, 2019 (le «projet de loi 8») a été présenté; le 29...

---

**New Tripartite Guidelines on Wrongful Dismissal Offer Much-Needed Guidance**

**Duane Morris LLP**

Employees often bring claims against previous employers for wrongful dismissal without a clear idea of the merits of their claims. Likewise...

---

**Changes Coming: NLRB Considers Rulemaking on Ambush Elections and More**  
**Barnes & Thornburg LLP**

More significant changes appear to be on the way at the National Labor Relations Board (NLRB). On May 22, the agency announced it is considering...

---

**HHS Proposes Changes to 2016 Regulations for ACA Non-Discrimination Rule**  
**McDermott Will & Emery**

On Friday, March 24, 2019, the US Department of Health and Human Services issued a proposed rule (along with a related fact sheet) under Section 1557...

---

**Texas Paid Sick Leave: Dallas and San Antonio Employers Should be Prepared for Paid Sick Leave Laws by August 1 Absent Prompt Legislative or Court Intervention** Texas

**Jackson Lewis PC**

Although there is no Texas state-wide law that requires paid sick leave in Texas, the cities of Austin, Dallas, and San Antonio have adopted paid...

---

**Key Legislation Emerging from Maryland and Local Ordinances to Remember**  
**Littler Mendelson PC**

In Maryland this year, spring brings warm weather and new employment laws. The General Assembly passed, and Governor Larry Hogan signed, several new...

---

## **Recession Planning Edition**

### **Winston & Strawn LLP**

Readers may be seeing a lot of talk about the possibility of a recession in the near future. Some articles, of course, reflect the writers' political...

---

## **Supreme Court Holds That Third-Party Counterclaim Defendants May Not Remove State-Court Cases To Federal Court Under The Class Action Fairness Act**

### **Mayer Brown**

Today, the Supreme Court held in a 5-4 decision that a third-party counterclaim defendant may not remove a state-court case to federal court under the...

---

## **The Westeros Citizens Participation Act (Yeah, Right)** Texas

### **Vinson & Elkins LLP**

My disappointment with the Game of Thrones' finale on Sunday night was greatly alleviated by the news on Monday morning that a bill amending the...

---

## **Office of the General Counsel of the National Labor Relations Board says that Uber Drivers are not Employees**

### **Hogan Lovells**

In an Opinion Letter released on Tuesday, May 14, the Office of the National Labor Relations Board's General Counsel opined that Uber drivers are not...

---

## **Nevada Expands Mandatory Occupational Safety Training to Conventions and Trade Shows** Nevada

### **Littler Mendelson PC**

In 2009, Nevada implemented mandatory safety training for employees performing work on construction sites. In 2017, Nevada expanded that mandatory...

---

## **Agencies Update Regulatory Agenda for 2019 and Beyond**

### **Littler Mendelson PC**

The federal Government's Spring 2019 Unified Agenda of Regulatory and Deregulatory Actions (regulatory agenda), which provides insight into federal...

---

## **The Essential Question Of The Gig Economy**

### **Baker McKenzie**

Trying to track the employment status of gig workers will make your head spin. Contractors? Employees? Super heroes? In the last few weeks, four...

---

## **Connecticut Paid Family and Medical Leave: Senate Passes Bill, which Governor Vows to Veto in Current Form** Connecticut

### **Jackson Lewis PC**

Connecticut employers and employees are focused on Hartford, where last night the Senate passed a paid family and medical leave bill. Governor Ned...

---

## **Mile-High Expectations for Employers As Colorado Governor Signs Into Law One**



## of Nation's Toughest Pay Equity Law to Date

### **Seyfarth Shaw LLP**

Seyfarth Synopsis: Yesterday, May 22, 2019, Colorado Governor Polis signed the "Equal Pay for Equal Work Act" which is the latest—and one of the most...

---

## Oregon Enacts Pregnancy Accommodations Law Oregon

### **Jackson Lewis PC**

Beginning January 1, 2020, Oregon employers must provide reasonable accommodations to employees and job applicants who have limitations related to...

---

## New Unlawful Workplace Practices in California California

### **Masuda Funai Eifert & Mitchell Ltd**

California's Fair Employment and Housing Act ("FEHA") prohibits workplace discrimination and provides California businesses and...

---

## Colorado Passes Comprehensive Equal Pay Law Colorado

### **Jackson Lewis PC**

Colorado Governor Jared Polis has signed what is one of the toughest enhanced state pay equity laws to date. Colorado has become the ninth state in...

---

## DOL Says Some Gig Workers Are Not Employees Video

### **Epstein Becker Green**

The Department of Labor (DOL) recently issued an opinion letter that said workers providing services to customers referred to them through an...

---

## EEOC on Target to Open Pay Data Collection Portal In July

### **Jackson Lewis PC**

In its latest progress report, submitted to the Court on May 24, 2019, the EEOC details its efforts over the past weeks to get the new EEO-1 pay data...

---

## New York City Ban on Pre-Employment Drug Testing Won't Apply to (most) Healthcare Workers New York

### **Jackson Lewis PC**

On May 10, 2019, a bill amending New York City's administrative code related to prospective employee drug-testing officially became law for New York...

---

## SEC Awards Whistleblower More Than \$4.5 Million

### **Proskauer Rose LLP**

On May 24, 2019, the SEC announced payment of more than \$4.5 million to a whistleblower who sent an anonymous tip to the company alleging significant...

---

## Additional Defendants' Motions for Summary Judgment Granted Where Plaintiff's Affidavit and Related Expert Testimony Ruled Inadmissible Washington

### **Goldberg Segalla LLP**

As reported on the Asbestos Case Tracker on May 6, 2019, in Varney v. Air &



Liquid Systems Corporation, et al., the court ruled on...

---

**Jury Verdict Upheld Against Boiler Defendant** Louisiana

**Goldberg Segalla LLP**

Lynda Berry alleged that she was exposed to asbestos through the electrical work of her husband, William, at a Louisiana paper mill...

---

**Recognizing the Importance of Employee Ownership, More States Move Forward with Pro-ESOP Initiatives**

**Morgan Lewis**

Taking cues from Colorado, Missouri, Pennsylvania, Iowa, New Jersey, and Virginia, all of which have recently enacted legislation supporting and...

---

**Westchester County Adopts Mandatory Paid Safe Leave Law**

**Fox Rothschild LLP**

The Westchester County Board of Legislators has adopted a stand-alone safe leave law that provides victims of domestic violence and human trafficking...

---

**Could You Replace All of Your Employment Agreements with a Single Severance Plan?**

**Winston & Strawn LLP**

The trend to abandon or replace executive employment agreements with a severance and/or change in control plan has been underway for several years now...

---

**DOL and NLRB Agree: Gig Economy Workers Are Contractors, Not Employees**

**Akerman LLP**

According to recent guidance issued by the DOL and NLRB, workers in the so-called "gig," "on-demand," or "sharing" economy are independent...

---

**New York City Council to Consider Expanding Earned Safe and Sick Time Act to Require "Personal Time"** New York

**Proskauer Rose LLP**

The New York City Council is considering a bill that would expand the NYC Earned Safe and Sick Time Act (ESSTA) to provide eligible employees with...

---

**Washington State's New Noncompetition Laws** Washington

**Baker & Hostetler LLP**

Washington state employers that rely on noncompetition agreements will face a dramatically different legal landscape beginning Jan. 1, 2020, when a...

---

**Updates Notification of Employee Rights Under Federal Labor Law Poster**

**Jackson Lewis PC**

The Department of Labor has announced updates to the Notification of Employee Rights Under Federal Labor Law poster, required to be posted (in 11×17...

---

**Empowering Exceptional with Mark McClain** Audio

### **Vinson & Elkins LLP**

Austin's "Best CEO" and longtime V&E client Mark McClain joins us to talk about the importance of values and culture at his company, SailPoint, and...

---

### **New Massachusetts Law Requires that Employers provide Mandatory Paid Leave**

Massachusetts

### **Nelson Mullins Riley & Scarborough LLP**

Beginning in July 2019, Massachusetts employers must be aware that employees are now entitled on an annual basis to receive medical and family leave...

---

### **In a Boost to the Gig-Economy, NLRB Says Uber Drivers are Not Employees Phelps Dunbar LLP**

The National Labor Relations Board (NLRB) has released an Advisory Opinion concluding that Uber drivers are independent contractors, restricting...

---

### **New Mexico Passes Ban-the-Box and Expungement Laws**

New Mexico

### **Ogletree Deakins**

On April 3, 2019, New Mexico governor Michelle Lujan Grisham signed into law two bills related to criminal background checks that may affect...

---

### **Delaware Chancery Court Adopts a "Narrow Approach" in Applying the CFAA, Aligning Itself with the Ninth, Second, and Fourth Circuits**

Delaware

### **Crowell & Moring LLP**

On May 10, 2019, the Delaware Chancery Court issued an opinion adopting a "narrow approach" in interpreting Section 1030(a)(2)(C) of Computer Fraud...

---

### **WSIB's Rate Framework Reform: A Third Policy Update and What Can You Do Now**

### **Dickinson Wright**

This is the third post in my series of updates and insights to assist Schedule 1 employers with the transition to the new WSIB Rate Framework ("RF")...

---

### **Plaintiffs' Claims Against Employer Barred Under Workers' Compensation Grounds; May Plead Alternative Premises Liability Claims**

Louisiana

### **Goldberg Segalla LLP**

The plaintiff, Victor Michel, filed a lawsuit in state court in July 2017, alleging that his work as a mechanic exposed him to asbestos...

---

### **Colorado Enacts Comprehensive Equal Pay Law**

Colorado

### **Jackson Lewis PC**

Enacting one of the toughest enhanced state pay equity laws to date, Colorado has become the tenth state in the country to pass an equal pay law that...

---

### **Board Upholds Enforcement of Pre-Hire Arbitration Agreement**

### **Littler Mendelson PC**

The alternative dispute resolution landscape continues to evolve for employers



with unionized workforces. Anheuser-Busch, LCC, 367 NLRB 123 (May 22...

---

**Massachusetts Consumer Data Privacy Bill Could Dramatically Expand Class Action Litigation Risk** [Massachusetts](#)

**Pierce Atwood LLP**

Earlier this year, Massachusetts state senators introduced a consumer data privacy bill with a private right of action that could become the broadest...

---

**New York City Employers Barred From Testing Prospective Employees for Marijuana Use** [New York](#)

**Akerman LLP**

Beginning on May 10, 2020, absent specific exceptions, covered New York City employers will be prohibited from testing prospective job applicants for...

---

**WARNING: Illinois 25-Year Statute of Repose No Longer Prohibits Claims Against Employers** [Illinois](#)

**Gordon Rees Scully Mansukhani**

No longer will employers be entitled to rely on the Illinois workers' compensation exclusive remedy protections to prohibit civil actions filed 25...

---

**Seyfarth Shaw Policy Matters Newsletter - May 23, 2019**

**Seyfarth Shaw LLP**

On May 21, the House Committee on Education and Labor held a hearing on the "Protecting Older Workers Against Discrimination Act" (POWADA, H.R. 1230...

---

**Legal Updates - May 2019**

**Investigations Law Group**

Department of Labor Issues Opinion Letter about Gig Workers The US Department of Labor issued a new opinion letter that concluded that gig workers for...

---

**OFCCP's broad request for comp data denied**

**Constangy Brooks Smith & Prophete LLP**

In January 2017, the Office of Federal Contract Compliance Programs filed an administrative complaint against Oracle America, Inc., alleging systemic...

---

**U.S. Women's Soccer Team Sues for Gender Discrimination** [California](#)

**Investigations Law Group**

The Equal Pay Act requires that employers pay men and women equally, for equal work. Does this apply to professional athletes? The U.S. Women's soccer...

---

**Groups Request Delayed Start For Massachusetts Paid Leave Law** [Massachusetts](#)

**Fisher Phillips**

Led by Associated Industries of Massachusetts (AIM), a nine-member coalition of the Massachusetts business community, along with employee and...

---

## **US House of Representatives Passes Far-Reaching LGBTQ Rights Bill**

### **Arent Fox LLP**

The vote was 236 for the bill and 173 against it. Generally, the vote was along party lines, but eight Republicans broke ranks with their party to...

---

## **Massachusetts Court finds Memorized Client Lists Can Constitute Confidential Information**

Massachusetts

### **Nelson Mullins Riley & Scarborough LLP**

With the advent of telecommuting and employers generally reducing paper files, it seems out of the ordinary for anyone to memorize a telephone number...

---

## **Medical Marijuana "Unity Bill" Takes Effect August 28, 2019: Steps Employers Should Consider Now**

Oklahoma

### **GableGotwals**

On June 26, 2018, Oklahoma voters passed State Question (SQ) 788 legalizing medicinal marijuana. SQ788 left many questions for employers unanswered...

---

## **NY Farmworkers Win Collective Bargaining Rights - Will Other States Follow Suit?**

New York

### **Fisher Phillips**

In a groundbreaking decision, a New York state appeals panel just extended union organizing rights to farmworkers, perhaps setting the stage for...

---

## **Insurer of Long Defunct Employer May Be Held Liable Under "Enhanced Benefits" in Worker's Compensation Statute**

Missouri

### **Goldberg Segalla LLP**

MISSOURI - The plaintiff passed from mesothelioma in 2015 as a result of alleged exposure to asbestos while working at Valley Farm Dairy Company...

---

## **Another Automatic Lunch Deduction FLSA Collective Action: How Many Times Does It Have to Happen?**

### **Fox Rothschild LLP**

I have blogged numerous times about these automatic lunch deduction cases and have suggested remedies. Yet, these cases proliferate. Another very...

---

## **NLRB Announces New Rulemaking Priorities (US)**

### **Squire Patton Boggs**

As a part of the Unified Agenda of Regulatory and Deregulatory Actions ("Unified Agenda") issued Wednesday, May 22, 2019, the National Labor Relations...

---

## **カリフォルニア州公正雇用住宅法における新たな改正**

California

### **Masuda Funai Eifert & Mitchell Ltd**

カリフォルニア州の公正雇用住宅法（Fair Employment and Housing Act）（以下、FEHA）は 職場での差別を禁じ カリフォルニア州の雇用主（企業）とその従業員を対象に差別を防止するた...

---

## **GDPR for litigators**



### **Allen & Overy LLP**

Virtually all evidence, whether in litigation or arbitration or relating to investigations carried out by regulators or enforcement authorities, will...

---

### **Inclusion Or Bust**

#### **Baker McKenzie**

Once again, Baker McKenzie attorneys, industry thought leaders and key clients from around the world convened (this time in New York) to answer this...

---

### **IRS Expands Self-Correction Program, Provides Welcome Relief for Plan Sponsors**

#### **McDermott Will & Emery**

The IRS recently released an updated version of EPCRS, the IRS's program for correcting errors that occur under tax-qualified retirement plans. The...

---

### **Can Student-Workers Unionize? NLRB to Issue New Rules on the Question**

#### **Pepper Hamilton LLP**

In a significant development for private colleges and universities, the National Labor Relations Board (NLRB) announced that it intends to propose...

---

### **Conflict Over Neutral Risk Work Injuries**

#### **Goldberg Segalla LLP**

Neutral risk injuries have become a contentious topic in Illinois Workers' Compensation law. In Illinois Senate Bill 12, the legislature attempted to...

---

### **California Rules on Meal, Rest Breaks Preempted by Decision of Federal Trucking Regulator, Court Holds**

California

#### **Jackson Lewis PC**

Ruling it lacked jurisdiction to review the Federal Motor Carrier Safety Administration's (FMCSA) decision barring enforcement of California's meal...

---

### **Some States Start To Permit Portable Benefits For Gig Workers**

#### **Fisher Phillips**

There's a great story in today's Bloomberg Law by Genevieve Douglas highlighting the recent trend of states permitting self-employed workers - such...

---

### **Get Ready for the Massachusetts Paid Family and Medical Leave Law**

#### **Sullivan & Worcester LLP**

On June 28, 2018, Massachusetts Paid Family and Medical Leave ("PFML") became law. PFML does not become available as a benefit until 2021, but...

---

### **It's Official: Connecticut Minimum Wage Will Increase to \$15.00 per Hour**

#### **Ogletree Deakins**

On May 28, 2019, Governor Ned Lamont signed House Bill No. 5004 The bill, entitled "An Act Increasing the Minimum Fair Wage," increases Connecticut's...

---

### **Paid Leave Law in Maine Passes Legislature and Waits for Governor Signature**



### **Jackson Lewis PC**

The Maine legislature recently passed An Act Authorizing Earned Employee Leave. If Governor Mills, who has been vocal in her support of the bill...

---

### **Employers Should Prepare to Submit Their Component 2 Pay Data By September 30, 2019**

#### **Breazeale Sachse & Wilson LLP**

On April 25, 2019, a U.S. District Court for the District of Columbia ruled that employers who are required to file EEO-1 reports must submit...

---

### **US - Despite DOJ appeal, employers must submit gender pay gap data by 30 September 2019**

#### **Ius Laboris**

The EEOC has confirmed that larger US employers should prepare to submit gender pay gap data by 30 September 2019, despite an appeal against these...

---

### **Employers May Have To Accommodate Off-Duty Medical Marijuana Use**

#### **Porzio Bromberg & Newman PC**

New Jersey's marijuana legislation has been in constant flux throughout the first half of 2019. In February, Governor Murphy and various legislative...

---

### **Banning the Box on those Old Job Application Forms**

#### **Vinson & Elkins LLP**

While employment lawyers like myself — and the EEOC — have long cautioned employees against automatically asking job applicants about their criminal...

---

### **Memorial Day employment law quiz!**

#### **Constangy Brooks Smith & Prophete LLP**

How's your employment law history knowledge? Happy Memorial Day weekend, everybody! In honor of the occasion, see how much you remember about these...

---

### **An Increasingly Hairy Situation: Discriminatory Employment Decisions Based on Hairstyles**

New York

#### **Proskauer Rose LLP**

Hairstyles are gaining more attention in the labor and employment context. Earlier this year, Austria's Supreme Court allowed a former employee to...

---

### **What A Difference An Election Makes: Colorado Passes Slate Of New Employment Laws**

#### **Fisher Phillips**

The 2018 Colorado state elections resulted in a Democratic House, Senate, and governor, smoothing the way for the 2019 legislature to pass six new...

---

### **Court Awards Nearly Twenty Times Damages in Illinois Wage Payment Act Case**

Illinois

#### **Baker Sterchi Cowden & Rice LLC**

On December 27, 2018 the Illinois Appellate Court for the First District affirmed an

award of attorney's fees and costs to plaintiff which was nearly...

---

### **Mixing the Melting Pot**

#### **Graydon Head & Ritchey LLP**

Corporate trainer Dana Brownlee held a seminar a few years ago, where a manager in her late 50s strongly criticized several Young employees on her...

---

### **Whistleblower receives award after internal reporting resulted in SEC case**

#### **Cooley LLP**

In February 2018, SCOTUS handed down its decision in *Digital Realty v. Somers*, holding that the Dodd-Frank whistleblower anti-retaliation protections...

---

### **How Far USDOL's "Overtime Rule" Has Come, and How Far It Has Left to Go**

#### **Fisher Phillips**

The comment period for USDOL's most recent proposal regarding the Fair Labor Standards Act's white-collar exemptions (Overtime Rule 2.0) has closed...

---

### **Arizona Supreme Court Reverses Lower Court Rulings that Would Have Outlawed Cannabis Extracts**

Arizona

#### **Greenspoon Marder LLP**

On May 28, 2019, the Arizona Supreme Court came out with a major decision with respect to the Arizona Medical Marijuana Act ("AMMA"), ruling that the...

---

### **Labor Development Impacting Developers, Contractors, and Landowners**

#### **Sheppard Mullin Richter & Hampton LLP**

It is unlawful for unions to secondarily picket construction sites or to coercively enmesh neutral parties in the disputes that a union may have with...

---

### **SEC awards \$4.5 million in first-ever internal reporting whistleblower action**

#### **Buckley LLP**

On May 24, the SEC announced a \$4.5 million award to a whistleblower who reported concerns internally to his or her company and also to the SEC...

---

### **NYC Employers Barred from Weeding Out Cannabis-Using Job Applicants**

New

York

#### **Davis Wright Tremaine LLP**

New York City recently joined Maine and the District of Columbia in passing legislation banning most employers from requiring applicants to submit to...

---

### **Ride-Share Drivers Are Independent Contractors According to NLRB's General Counsel**

#### **Holland & Knight LLP**

The National Labor Relations Board's (NLRB) General Counsel released an Advice Memorandum that concludes that drivers for a ride-sharing...

---

### **Bankruptcy Discharge of Debts for Willful and Malicious Injury**

#### **Ward and Smith, P.A.**



Can a debtor discharge a debt arising out of a deliberate or intentional act that causes injury to you?...

---

### **The Equality Act Takes Another Step Forward**

**Hunton Andrews Kurth LLP**

The House of Representatives passed the Equality Act (H.R. 5 - 116th Congress) this past Friday, May 17, mostly along party lines - the resolution...

---

### **Beltway Buzz, May 24, 2019**

**Ogletree Deakins**

On May 22, 2019, the Office of Information and Regulatory Affairs (OIRA) released the administration's Spring 2019...

---

### **Texas Legislature takes aim at Anti-SLAPP challenges**

Texas

**Reed Smith LLP**

The Texas Citizens Participation Act, Tex. Civ. Prac. & Rem. Code §§ 27.001 et seq. (the TCPA), Texas' anti-SLAPP statute, is likely to receive a...

---

### **Learn How to Avoid Religious Coercion at Night School**

**Ford & Harrison LLP**

In the film Night School, the main character experiences a workplace that mixes religion and the workplace in a way that the Equal Employment...

---

### **SEC Awards First Ever \$4.5 Million to Internal Whistleblower**

**Stinson LLP**

The SEC awarded more than \$4.5 million to a whistleblower whose tip triggered the company to review the allegations as part of an internal...

---

### **If You Read This Blog You Can Probably Make A Good Guess As To What the Racial Epithet Was**

**FisherBroyles LLP**

The EEOC just sued a large health organization for alleged racial harassment and retaliation against African American employees in its California...

---

### **Update: NYC Protections for Reproductive Health Decisions Now in Effect**

**Fox Rothschild LLP**

Effective since May 20, 2019, the New York City Human Rights Law prohibits discrimination relating to an employee's "sexual and reproductive health..."

---

### **CBCA Rules Contractor Under GWAC Task Orders Properly Submitted Claims to the Agency Ordering Contracting Officer Instead of the Procuring Contracting Officer**

**Sheppard Mullin Richter & Hampton LLP**

In a case of first impression, the Civilian Board of Contract Appeals ("CBCA") ruled that a contractor performing task orders issued against a...

---

### **Equal pay "certification": A terrible idea**

### **Constangy Brooks Smith & Prophete LLP**

Mind you, I'm not recommending that you vote for or against any particular presidential candidate...

---

### **Employment Flash - May 2019**

[California](#)

[Massachusetts](#)

[New York](#)

### **Skadden Arps Slate Meagher & Flom LLP**

This edition of Employment Flash looks at developments in labor and employment law, including regarding a DOJ appeal of the EEOC's heightened pay...

---

### **Will OSHA Bring The Heat This Summer? Groups Continue To Press For Heat Standards**

#### **Fisher Phillips**

This past Memorial Day weekend, the southeastern region of the United States experienced a historic heatwave that set all-time records. It's only...

---

### **When Can You Terminate Health Coverage During FMLA?**

#### **Graydon Head & Ritchey LLP**

When faced with this situation, the employer can continue to maintain the employee's benefits through the leave period by paying employee's share of...

---

### **Georgia Court of Appeals: Hourly Backhoe Operator is Not a "Key Employee" Under Georgia's Restrictive Covenants Act**

[Georgia](#)

#### **Nelson Mullins Riley & Scarborough LLP**

Georgia's 2011 Restrictive Covenants Act (the "Act") substantively changed Georgia law governing the enforceability of restrictive covenants. Among...

---

### **Uber Drivers Not Employees According to NLRB Advice Memo**

#### **Hunton Andrews Kurth LLP**

In a recent advice memorandum, the National Labor Relations Board (the "Board") set forth its position that drivers for the rideshare company Uber are...

---

### **US - Employers must consider accommodating workers' religious objections to flu vaccination**

#### **Ius Laboris**

Recent Equal Employment Opportunity Commission action has served as a reminder of employers' obligation to accommodate employees' religious objections...

---

### **ALERT: Chad C. Brown, Inc. and Horse Trainer Chad Brown must pay \$1.6M in Department of Labor Wage and Hour Violations Investigation**

#### **McBrayer McGinnis Leslie & Kirkland PLLC**

In a development that should make every horse operation in Kentucky stand up and take notice, trainer Chad Brown will pay \$1.6 million to cover back...

---

### **Uber: the need to drive towards greater global regulation**

#### **McCabe Curwood**

The National Labor Relations Board, a United States' equivalent of Australia's



Fair Work Commission (FWC) combined with the Fair Work Ombudsman (FWO)  
...

---

### **Drug Testing & Safety Incentive Rulemaking on Long Term Regulatory Agenda for OSHA**

**Jackson Lewis PC**

It's that time of year again...when federal agencies, including OSHA, tell us what is on the horizon for rulemaking activity. This week the spring...

---

### **The Italian Job: Fifth Circuit Confirms Pleading Standard for National Origin Discrimination Claim**

**Bradley Arant Boult Cummings LLP**

Employment law is full of burden-shifting, prima facie standards and evidentiary hurdles. Sometimes, even the courts apply the wrong standard at the...

---

### **Do's and Don'ts of Conducting Internal Investigations**

**Jackson Lewis PC**

In today's post #MeToo era, most companies, big or small, will likely need to conduct an internal investigation on an employee's claims. Knowing how...

---

### **Looking Back and Looking Forward: Retroactivity and Expansion of the California Independent Contractor Test**

California

**Jackson Lewis PC**

In April 2018, the California Supreme Court issued its ruling in *Dynamex Operations West v. Superior Court* (2018) 4 Cal. 5th 903, 916-17 and set...

---

### **Legal Pot = Storm Clouds for Manufacturers**

**Robinson & Cole LLP**

New York City's recent ban on pre-employment marijuana testing, coupled with recent decisions in New Jersey and Connecticut, could give manufacturers...

---

### **10th Circuit: Compliance employees must overcome presumption that they are doing their job to obtain FCA whistleblower retaliation protection**

**Buckley LLP**

On April 30, the U.S. Court of Appeals for the 10th Circuit affirmed the dismissal of a former employee's False Claims Act (FCA) whistleblower...

---

### **SEC to vote on Regulation Best Interest; DOL to issue a Notice of Proposed Rulemaking for its Fiduciary Rule**

**Mayer Brown**

The Securities and Exchange Commission posted an Open Meeting Agenda for June 5, 2019, when the Commission will vote on whether to adopt Regulation...

---

### **What's on the spring 2019 regulatory agenda?**

**Constangy Brooks Smith & Prophete LLP**

It's spring, and a young person's fancy turns to ... why, the federal regulatory agenda! What else? Here are the items that I think will be of...



---

## **NLRB Deals Another Blow to Gig Workers' Rights Under NLRA**

**Cozen O'Connor**

Last week, the Division of Advice of the National Labor Relations Board (Board) released a previously issued advice memorandum (memorandum) concluding...

---

## **FMLA Regs May Soon Get Revamped To Ease Employer Burdens**

**Fisher Phillips**

If the Department of Labor has anything to say about it, employers may soon get a bit of a reprieve when it comes to dealing with the administrative...

---

## **[Podcast]: Key Contractual Provisions for Employers to Incorporate in Documents with Confidentiality Covenants**

[Audio](#)

**Proskauer Rose LLP**

In this episode of The Proskauer Brief, Kate Napalkova, special employee benefits and executive compensation counsel, and associate Oleg Zakatov...

---

## **Environment & Climate Change**



## **US EPA Extends Date For Designation of Inactive Substances on the TSCA Inventory to August 5, 2019**

**Squire Patton Boggs**

US EPA has announced that the formal designation of substances as inactive on US EPA's Toxic Substances Control Act (TSCA) Inventory will become...

---

## **Congress Is Gearing Up to Address PFAS**

**Greenberg Traurig LLP**

PFAS are a class of widely used chemicals, some of which have been common since the 1940s. They are used in non-stick coatings, stain- and...

---

## **Brumadinho litigation: Advocacia Garcez secures assistance from leading international lawyers**

**Leigh Day**

On 9 April 2019, Brazilian law firm Advocacia Garcez and lawyers for the Unions Siticop MG and the Brumadinho Workers Union filed a class action...

---

## **'Sudden and Accidental' Discharges May Avoid the Pollution Exclusion**

**Barnes & Thornburg LLP**

Pollution exclusions in modern commercial general liability (CGL) policies make it difficult, and often impossible, to recover the costs of...

---

## **President Trump Signs Drought Contingency Plan for Colorado River**

[Colorado](#)

**Squire Patton Boggs**

Months ago, in the face of "unacceptably high" risk to the Colorado River's complex system of reservoirs, US Bureau of Reclamation Commissioner...

---

## **Environmental Compliance and Land Use "Special Permits" in Massachusetts**

---

Massachusetts

### **Greenberg Taurig LLP**

Does compliance with environmental regulations suffice to prove that an operation is safe? Maybe not, for purposes of land use approvals in...

---

### **Bill Introduced in U.S. Congress to Ban PFAS in Food Containers**

#### **Keller and Heckman LLP**

Legislation recently introduced in the U.S. House of Representatives seeks to amend the Federal Food, Drug, and Cosmetic Act (FD&C Act) to deem any...

---

### **Failure to Comply with New NYC Building Emission Standard Could Lead to Hefty Fines**

New York

#### **Venable LLP**

On April 18, 2019, the New York City Council approved the NYC Green New Deal, which consists of a number of measures to reduce greenhouse gas...

---

### **California to Commence Cancellation Proceedings of Chlorpyrifos**

California

#### **Bergeson & Campbell PC**

On May 8, 2019, the California Environmental Protection Agency (CalEPA) announced that the California Department of Pesticide Regulation (DPR) will...

---

### **Air rules to watch for in second half of 2019**

#### **Thompson Coburn LLP**

The United States Environmental Protection Agency issued its Spring Regulatory Agenda on May 22, 2019. The Agenda includes two air rulemakings that...

---

### **Will States' Input Clarify the Final Affordable Clean Energy Rule?**

#### **Barnes & Thornburg LLP**

As the environmental world anxiously awaits the final Affordable Clean Energy (ACE) Rule, we are taking the opportunity to look back at some of the...

---

### **LNG a Focus of Recent Executive Order**

#### **Hunton Andrews Kurth LLP**

The Trump administration's recent executive order, Promoting Energy Infrastructure and Economic Growth (April 10, 2019), signals potentially...

---

### **BLM Releases Draft Environmental Assessment for Lifting Coal Leasing Moratorium**

Montana

#### **Hunton Andrews Kurth LLP**

The Bureau of Land Management (BLM) released a draft environmental assessment (EA) evaluating the potential environmental impacts of lifting the...

---

### **Proposed Maine Bill Would Prohibit Phthalates and PFAS In Food Packaging**

#### **Keller and Heckman LLP**

On March 28, 2019, the Maine legislature introduced a bill to prohibit intentionally added phthalates and perfluoroalkyl and polyfluoroalkyl...

---



## **PFAS and Public Water Supply in Pennsylvania: Challenges & Opportunities**

Pennsylvania

### **Cozen O'Connor**

The Pennsylvania Department of Environmental Protection (DEP) is currently tracking approximately 19 sites with known contamination with PFOA and...

---

## **En Banc Watch: Fight Over Substantive Due Process Sees Court Refuse to Rehear Flint Water Case**

### **Squire Patton Boggs**

The Sixth Circuit denied Flint, Michigan's petition for en banc review of a panel decision allowing citizens exposed to contaminated water to sue city...

---

## **The 2019 Pad Site Sharing Agreement: an alternative model for defining commercial relationships between oil and gas producers**

### **Burnet Duckworth & Palmer LLP**

On September 25, 2018, the Petroleum Joint Venture Association (PJVA) and the Canadian Association of Petroleum Landmen (CAPL) released the final...

---

## **Glyphosate: a new toxic tort timebomb?**

### **Clyde & Co LLP**

The global spotlight on glyphosate continues, following a third successive US court case finding that the world's most popular pesticide is...

---

## **Los Angeles County Voters Passed a Parcel Tax to Fund Water Capture Projects - What You Should Know**

California

### **Morrison & Foerster LLP**

This past November, residents of the County of Los Angeles passed Measure W, a parcel tax of 2.5 cents per square foot of impermeable land meant to...

---

## **Exploring New Opportunities in the Hydropower Industry**

### **Troutman Sanders LLP**

Partner Chuck Sensiba recently participated in a briefing sponsored by the Environmental and Energy Study Institute (EESI) and National Hydropower...

---

## **BSEE 2019 Final Revisions to the Offshore Well Control Rule**

### **Vinson & Elkins LLP**

On May 2, 2019, the federal Bureau of Safety and Environmental Enforcement ("BSEE") announced final revisions to its Well Control Rule ("WCR"). BSEE...

---

## **FWS Proposes Listing "Madtom" and "Waterdog"**

### **Nossaman LLP**

On May 22, 2019, the U.S. Fish and Wildlife Service (FWS) announced a proposal to list two intriguing North Carolina aquatic species under the...

---

## **European Council Adopts New Rules on Single-Use Plastics**

### **Keller and Heckman LLP**

The European Council adopted the Single-Use Plastics Directive on May 21,

2019. The Directive will impact plastic food-contact articles through...

---

### **The Supreme Court Decides the United States Cannot Have Title to Running Waters**

**Beveridge & Diamond PC**

The Supreme Court determined in *Sturgeon v. Frost* that the Nation River, located near Alaska's eastern border, is not public land for purposes of...

---

### **ISS Finds Improved ESG Ratings Alongside Rise in Controversies**

**Stinson LLP**

ISS ESG, an arm of ISS, released ESG Review 2019, an annual analysis of the state of adherence by companies across the globe to environmental, social...

---

### **Animals and Politics: Traveling Exotic Animal Ban Reintroduced**

**Duane Morris LLP**

On May 21, 2019 Representatives Raul M. Grijalva (D-AZ) and David Schweikert (R-AZ) introduced the Traveling Exotic Animal and Public Safety...

---

### **Wisconsin Governor Proposes Sweeping PFAS Legislation**

**Michael Best & Friedrich LLP**

On May 23, 2019, Wisconsin Governor Tony Evers and Wisconsin Department of Natural Resources (WDNR) Secretary Preston Cole proposed far-reaching...

---

### **New York Makes It Easier to Identify Potential Environmental Justice Communities**

[New York](#)

**Beveridge & Diamond PC**

The New York State Legislature passed legislation on Tuesday, April 30, that requires the State's Department of Environmental Conservation (DEC) to...

---

### **Reopener Alert: The Erosion of Peace of Mind**

**Goldberg Segalla LLP**

While covenants not to sue purport to provide some security to settling parties, in CERCLA actions, reopener provisions, which the EPA includes in...

---

### **Fish and Wildlife Service Faces Challenge on Delay in Listing Species**

[California](#)

**Troutman Sanders LLP**

On May 23, 2019, the Center for Biological Diversity and San Francisco Baykeeper (collectively "Center") filed a lawsuit against the Fish and Wildlife...

---

### **China Offices Legal Flash May 2019**

**Cuatrecasas**

On April 2, 2019, the Department of Justice of the HKSAR and the PRC Supreme People's Court signed the Arrangement Concerning Mutual Assistance in...

---

### **Washington State Passes Climate Bill to Restrict Certain Uses of HFCs**

[Washington](#)

**Beveridge & Diamond PC**



Following California's lead, Washington State has revived, at the state level, federal limits on greenhouse gases known as hydrofluorocarbons (HFCs)...

---

### **US - GSA to prepare EIS for land ports of entry**

#### **Baker McKenzie**

On May 23, 2019, the General Services Administration (GSA), Public Building Service (PBS) published in the Federal Register a Notice of Intent To...

---

### **Nasdaq Releases Global Environmental, Social and Governance Reporting Guide**

#### **Stinson LLP**

Nasdaq has released its new global environmental, social and governance (ESG) reporting guide which it believes will support public and private...

---

## **Internet & Social Media**



---

### **Domains & Domain Names in the USA**

#### **Downing IP Law**

A structured guide to domains & domain names in the USA

---

### **FTC Toughening Stance on Data Security - Five Key Takeaways from Recent Consent Orders**

California

#### **Fenwick & West LLP**

The Federal Trade Commission is putting more teeth into the multiyear compliance obligations of consent orders it enters into with companies to...

---

### **Pennsylvania Superior Court holds county where reputational harm occurs is proper venue for Internet defamation suits, confirming 50-year-old inquiry applies to website-based claims**

Pennsylvania

#### **Reed Smith LLP**

Addressing an issue of first impression, the Pennsylvania Superior Court ruled last week that a venue analysis dating to 1967 focusing on the...

---

### **Can Employers Request Social Media Account Information?**

#### **Raymond Law Group LLC**

Job seekers have recently been warned of a new trend at job interviews; prospective employers are asking applicants for their Facebook and other...

---

### **Mending (Geo)fencing Concerns**

#### **McGuireWoods LLP**

Although not a new practice, the application of geofencing continues to increase in sophistication and expand into personal space on an unprecedented...

---

### **Dating App Maker Gets COPPA Warning Letter from the Commish**

#### **Baker & Hostetler LLP**

Wildec gets apps booted from Apple and Google platforms...

---

### **Copycat Flattened by Patent & Trade Dress Jury Verdict in Win for Tiefs Shoes**



## **Hogan Lovells**

The maker of the Tieks ballet flat Gavrieli Brands walked away with over \$2.1 million when a federal jury found Soto Massini's competing designs...

---

## **Wyoming Affords “Money” Status to Certain Virtual Currencies**

### **Fenwick & West LLP**

In yet another blockchain-friendly bill signed into law by the governor of Wyoming in February 2019, the state granted certain virtual currencies...

---

## **Consultation on Consumer Internet of Things security**

### **Boyes Turner LLP**

In recent years, an increasing number of household items such as speakers, televisions and freezers are becoming “smart” and making using of Internet...

---

## **Kentucky to Begin Taxing Video Streaming Services under Telecom Tax**

**Kentucky**

### **McDermott Will & Emery**

Legislators in Frankfort added a new “video streaming service” tax to the omnibus tax bill (HB 354) as part of a closed-door conference committee...

---

## **Should the potential for misuse stop us from embracing new tech?**

### **Slaughter and May**

Facial recognition is back in the news this week as the South Wales police force defends its use of the technology after an office worker claimed it...

---

## **Oregon Amends Data Breach Law With New Requirements, and Enacts IoT Security Law**

**Oregon**

### **Lane Powell PC**

This May, Oregon’s legislature passed a set of amendments to the state’s already relatively robust data breach notice statute (ORS §§ 646A.600 - 646A...

---

## **Health Law Group Spotlight: Counsel Ira Parghi**

### **Borden Ladner Gervais LLP**

The Health Law Group is pleased to welcome back Ira Parghi, who returns to BLG as counsel after significant roles as the first-ever corporate privacy...

---

## **Chairman Pai, Commissioner Carr Issue Formal Statements Supporting T-Mobile/Sprint Merger; Commissioner O’Rielly Also “Inclined” to Support Merger**

### **Womble Bond Dickinson (US) LLP**

FCC Chairman Ajit Pai and Commissioner Brendan Carr have both issued formal statements recommending that Sprint and T-Mobile be allowed to complete...

---

## **Payment processor settles FTC fraud allegations**

### **Buckley LLP**

On May 21, the FTC announced a payment processor, its CEO and owner, and two other officers (collectively, “defendants”) agreed to settle charges...

---

## **Children's Online Privacy Protection Act: Are You Compliant?**

### **Foster Swift Collins & Smith PC**

The Children's Online Privacy Protection Act ("COPPA") was enacted in 1998 and was created to address concerns with the online collection of...

---

## **Client Alert: In Line with Recent Trends, New Jersey Amends its Data Breach Notification Law to Expand the Definition of "Personal Information"**

New Jersey

### **Vorys Sater Seymour and Pease LLP**

Earlier this month, New Jersey joined a growing list of states which require companies to provide notification under their...

---

## **Cloud Storage and Use of Vendors for Records Management Flagged by OCIE in Alert**

### **Kilpatrick Townsend & Stockton LLP**

Regulations regarding privacy, cybersecurity and the use of technology seem to be in constant flux. Compliance consultants and vendors do their best...

---

## **Qualcomm's "No License, No Chips" Program Violates Antitrust Laws**

### **Ropes & Gray LLP**

On May 21, 2019, following a full trial on the merits, Judge Koh of the Northern District of California issued a 233-page opinion in a closely...

---

## **Client Update - May 2019 California Consumer Privacy Act of 2018**

California

### **Yigal Arnon & Co**

On June 28, 2018, the California Consumer Privacy Act of 2018 ("CCPA") was enacted, introducing restrictions with respect to the processing of...

---

## **iPhone Users have Standing to Sue Apple for Alleged Monopolization**

### **Frost Brown Todd LLC**

Avoiding harm to consumers has been the guiding principle for U.S. antitrust law for decades. But antitrust law limits who in a distribution network...

---

## **Israeli Court Rules Bitcoin is Not a Form of Currency Exempted From Tax FROM TAX**

### **Pearl Cohen Zedek Latzer Baratz**

The Israeli District Court in Lod delivered a landmark decision classifying Bitcoin as an asset subject to capital gains tax. The decision was handed...

---

## **FCC Starts Accepting ATSC 3.0 Applications - The Next Generation of TV Transmission**

### **Wilkinson Barker Knauer LLP**

Effective yesterday, May 28, the FCC is accepting applications for television stations to begin to convert to the next generation TV transmission...

---

## **What Will the California Consumer Privacy Act Actually Bring in 2020?**

California

### **Procopio Cory Hargreaves & Savitch LLP**

California's passage of a landmark data privacy and protection law, the California



Consumer Privacy Act (CCPA), has rightly drawn significant...

---

### **Anti-Money Laundering Bulletin - Spring 2019**

#### **DLA Piper**

On 26 February 2019, HM Treasury published its updated advisory notice on high-risk jurisdictions (Advisory Notice). Firms subject to the Money...

---

### **How blockchain and smart contracts will change the face of insurance in the U.S.**

#### **Hogan Lovells**

In the last several years, we have seen a new crop of digital products and services enter the lexicon of the insurance industry. And with these...

---

### **OTA & Travel Distribution Update: State attorneys general explore alleged anti-trust violations; Amazon has entered the online travel industry; TripAdvisor formally adds safety features**

#### **Garvey Schubert Barer**

The week's stories remind us how quickly things continue to change in the distribution landscape. Enjoy...

---

### **Dark Web Provider Escapes Wrongful Death Drug Case**

#### **Reed Smith LLP**

This last week of May has been a big one in the James Bond universe. It includes the birthdays of Ian Fleming, who wrote the books, of Richard Maibaum...

---

### **Zo snel kan het gaan - schikking Taylor Swift**

#### **Novagraaf**

De bekende zangeres Taylor Swift en computerconsultant Patrick Bénot hebben de rechtszaken die zij tegen elkaar hadden aangespannen door een...

---

### **Healthcare Advertising: Understanding the FTC's Role and Regulations**

#### **Manatt Phelps & Phillips LLP**

Keeping patients well informed is a core principle of American healthcare policy, and advertising plays an important role in getting important...

---

### **Filtering Actions by Anti-Malware Software Provider Protected by CDA "Good Samaritan" Immunity**

Wisconsin

#### **Proskauer Rose LLP**

Three recent court decisions affirmed the robust immunity under the Communications Decency Act (CDA), 47 U.S.C. §230(c), for online providers that...

---

### **FCC Grants E911 Waiver Requests**

#### **Womble Bond Dickinson (US) LLP**

The Policy and Licensing Division of the Federal Communications Commission's Public Safety and Homeland Security Bureau has granted a waiver of the...

---

### **Ad and Publishing Industries Confront CCPA Challenges While Congress**

## **Considers Privacy** California

### **Baker & Hostetler LLP**

The California Consumer Privacy Act (CCPA), effective Jan. 1, 2020, will require more privacy transparency and choice for consumers than they have...

---

## **Will Insurers Declare “War”? The War Exclusion, the Ransomware Attack on Baltimore, and the NSA Cyber-Tool?** Maryland

### **Hunton Andrews Kurth LLP**

The City of Baltimore is the latest victim of increasingly common ransomware attacks. On May 7, 2019, unidentified hackers infiltrated Baltimore's...

---

## **Model Rule for Securities Administrators Approved by NASAA**

### **Robinson & Cole LLP**

The North American Securities Administrators Association (NASAA) this week approved an information security model rule package aimed at improving the...

---

## **Grumpy Cat - legal lessons from the ultimate sourpuss**

### **Lexology**

New York Times bestseller, A-list celebrity, coffee entrepreneur and meme legend Grumpy Cat sadly passed away a couple of weeks ago. Grumpy Cat (aka...

---

## **Insuretech and Beyond - An Evolving Litigation Landscape**

### **Womble Bond Dickinson (US) LLP**

In recent years, the life insurance industry has greatly enhanced the speed and efficiency of its underwriting decisions. This change in the...

---

## **Law Firm Domain Names Spoofed to Launch Phishing Scams**

### **Robinson & Cole LLP**

It is not unusual for lawyers to send emails to individuals and businesses they are about to sue to engage them before they do file suit to see if a...

---

## **Google Updates Ad Policies on Abortion-Related Advertising**

### **Frankfurt Kurnit Klein & Selz PC**

Google just announced changes to its policies relating to abortion-related advertising. The changes, which only apply to advertisers in the United...

---

## **Watch for Updates to the California Consumer Privacy Act: Do You Comply?**

California

### **GrayRobinson PA**

While the EU's disruptive General Data Protection Regulation (GDPR) has garnered most of the privacy headlines over the past year, U.S.-based...

---

## **Bipartisan Senate Bill Would Fund \$700M to Replace Huawei, ZTE Network Gear**

### **Womble Bond Dickinson (US) LLP**

Five U.S. Senators have introduced a bill that would, among other things, establish U.S. policy for the commercial deployment and security for 5G...

---



## **FTC, App Stores Break Up With Dating Apps**

### **Manatt Phelps & Phillips LLP**

Apple's App Store and the Google Play Store dumped three dating apps after the Federal Trade Commission (FTC) sent a warning letter to their operator...

---

## **Social Media Companies Seek Government Content Regulation?**

### **Duane Morris LLP**

Long ago in internet time, way back in the 1990s, Congress passed the Communications Decency Act (CDA). A key feature of the CDA is Section 230 of...

---

## **Battle for the BITCOIN mark, China moves closer to Hague accession, and curry conundrum: news digest**

### **World Trademark Review**

In our latest news digest, we look at the \$110 million sale of Sports Illustrated's IP, the expansion of visual search in TMView, a dispute over a...

---

## **Nearly 50 million Instagram users' data exposed, adding to Facebook's privacy woes**

### **Newmeyer & Dillion LLP**

Massive database containing information from more than 49 million Instagram accounts has been discovered online. The cache, which contained...

---

## **Connected devices: Challenges for both technology providers and consumers**

### **White & Case LLP**

Privacy and the development of technology are competing interests that are sometimes in conflict. These considerations often present a challenging...

---

## **Legal Practice**



## **Document bloatation and a response**

### **Joshua Stein PLLC**

Shorter and simpler template documents require eternal vigilance against document bloatation. But sometimes flexibility and optionality are good.

---

## **How Can a UK Witness Be Made to Testify in US Legal Proceedings?**

### **Finnegan, Henderson, Farabow, Garrett & Dunner LLP**

Under the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters ("Hague Evidence Convention"), English Courts will assist US...

---

## **Digital Marketing Is Arguably The Most Important Skill For A Freelance Attorney**

### **GableGotwals**

It is a known fact that we live in a highly digitized world, and the legal profession like all others operates in this environment. One other...

---

## **Automate, Outsource, or Own? Insights from Legal Leaders on Resourcing Legal Work**



## Brightflag

Brightflag partnered with Stout to host a panel discussion in Chicago on March 6th, 2019 discussing the changes in how corporate legal teams are...

---

## Clients Suing Their Lawyers For Malpractice Risk A Subject Matter Waiver

### McGuireWoods LLP

Clients and lawyers asserting claims against each other can waive privilege protection without disclosing any privileged communications. But such...

---

## In Voir Dire, Create a Context for Candor

### Holland & Hart LLP

Here's the situation. A large number of strangers are gathered in a formal courtroom — a hushed atmosphere, dark-wood paneling, flags for the state...

---

## GozNym Malware Attack Hits Two Law Firms for Over \$117K in Losses

### Robinson & Cole LLP

Two law firms were among the latest victims of the GozNym malware attack that caused a combined loss of more than \$117,000. Law enforcement...

---

## PR Firm Not Covered by Privilege Umbrella in Trademark Row New York

### Finnegan, Henderson, Farabow, Garrett & Dunner LLP

On May 6, 2019, a magistrate judge in the Southern District of New York ruled that emails exchanged among a company, its attorneys, and its public...

---

## Five Facts: Congressional Testimony Dos and Don'ts

### Holland & Knight LLP

Preparing for and executing testimony during a legislative hearing or investigation can be a high-stakes, stressful affair. Understanding the rules...

---

## Taking control of legal costs in 5 steps

### Legisway by WoltersKluwer

Staying in control of legal costs is one of principle ways legal departments can demonstrate value. That said, according to Wolters Kluwer's 2019...

---

## Projects & Procurement



---

## Take Two: DoD Issues Another Proposed Rule on Performance-Based Payments

### Crowell & Moring LLP

On April 30, 2019, the Department of Defense (DOD) issued a proposed rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to...

---

## CEC Awards Funding For Clean Energy Projects California

### Bergeson & Campbell PC

On May 15, 2019, the California Energy Commission (CEC) approved approximately \$11 million for Clean Energy demonstration projects that include...

---

## Proposed Rule Offers Foreign Military Sales as a Potential Pathway to

## **Commerciality**

### **Covington & Burling LLP**

Earlier this month, the FAR Council issued a proposed rule to expand the definition of “commercial item” under the Federal Acquisition Regulation...

---

## **With Cochise Decision, Supreme Court Expands Limitations Period in Declined Qui Tam Cases**

### **Hogan Lovells**

The Supreme Court handed down its decision today in Cochise Consultancy, Inc. v. United States ex rel. Hunt, a closely-watched case about the False...

---

## **EERE Announces Grants For SBIR Innovation Projects**

[District of Columbia](#)

### **Bergeson & Campbell PC**

On May 20, 2019, U.S. Energy Secretary, Rick Perry, announced that DOE's EERE will be awarding up to \$46 million in grants to small businesses funded...

---

## **National P3 Update: Higher Education and Social Infrastructure**

### **Bilzin Sumberg**

We have written about how the public-private partnership (P3) project delivery model can and should be used to meet infrastructure needs. Because P3s...

---

## **Responding to RFPs/ITTs**

### **Squire Patton Boggs**

There are many aspects to consider as a bidder when participating in procurement procedures for public works, supplies and services, as well as...

---

## **Expedited Contract Closeouts - A Fast Track Available to Select Older Contracts**

### **Crowell & Moring LLP**

On April 30, 2019, the Department of Defense (DoD) issued a final rule, effective immediately, amending the Defense Federal Acquisition Regulation...

---

## **New DOJ Guidance Aims to Incentivize Corporate Cooperation in False Claim Act Matters**

### **Drinker Biddle & Reath LLP**

On May 7, 2019, the Department of Justice issued important guidance on the type of cooperation that is eligible for credit in False Claim Act (FCA)...

---

## **Seeking to Incentivize Self-Disclosures, DOJ Issues Guidance on Credit for Cooperation with FCA Investigations**

### **Robinson & Cole LLP**

On May 7, 2019, the U.S. Department of Justice (DOJ) provided important new guidance addressing cooperation credit that may be available to...

---

## **SCOTUS Unanimously Extends Statute of Limitations for Relators to File FCA Lawsuits**

### **Arent Fox LLP**

In a 9-0 decision authored by Justice Clarence Thomas, the US Supreme Court



held that nonintervention is irrelevant to whether the “government...

---

## **International Arbitration Newsletter - May 2019 | Regional Overview: Asia Pacific**

New York

### **Garrigues**

The US District Court for the Southern District of New York entered a default judgment worth nearly US\$14 million against Chinese national Weili Su...

---

## **U.S. Supreme Court Clarifies Scope of False Claims Act Statutes of Limitations**

### **Robinson & Cole LLP**

In a unanimous decision issued on May 13, 2019, the U.S. Supreme Court sought to resolve lingering confusion over the statute of limitations under...

---

## **ABSCA Confirms Contractors May Challenge Unfavorable CPARS Ratings**

### **Covington & Burling LLP**

While you might not be able to fight City Hall, you can fight your CPARS rating. In a short opinion published last week, the ASBCA confirmed it has...

---

## **Veterans Are First at the VA Following New Class Deviation Implementing Recent Federal Circuit Mandate**

### **Sheppard Mullin Richter & Hampton LLP**

In its most recent attempt to strike the appropriate balance between the Veterans First and AbilityOne programs, the U.S. Department of Veterans...

---

## **Mixed Messages: DOJ Releases New FCA Cooperation Guidelines, while Study Questions Whether Cooperation Actually Garner Credit**

### **Bass, Berry & Sims PLC**

The U.S. Department of Justice (DOJ) routinely encourages the subjects of False Claims Act (FCA) enforcement actions to make voluntary disclosures...

---

## **The Energizer - Volume 45**

### **K&L Gates**

There is a lot of buzz around blockchain technology, distributed energy resources (“DERs”), microgrids, and other technological innovations in the...

---

## **The Evolving And Expanding Landscape Of California’s Design-Build Project Delivery Method In The Public Works Arena**

California

### **Atkinson Andelson Loya Ruud & Romo**

Proponents of design-build typically applaud the implementation and use of this project delivery method because it allows close and continuous...

---

## **Renewables’ Next Frontier: Regional Transmission Orgs**

### **Nelson Mullins Riley & Scarborough LLP**

Renewable resources, particularly wind and solar, have experienced tremendous growth in the U.S. Spurred by a combination of improved technological...

---

## **FDA Launches Menu Labeling Social Media Toolkit**

### **Keller and Heckman LLP**

FDA has launched a social media toolkit to assist with consumer awareness of menu labeling information. The toolkit features web badges that can be...

---

### **ReNEWS Southeast Volume 1**

[North Carolina](#)

[South Carolina](#)

### **K&L Gates**

Southeastern States See Large Year-Over-Year Increase in Renewable Output...

---

### **DOJ issues new guidance regarding cooperation in False Claims Act investigations**

#### **Hogan Lovells**

Continuing its recent trend of revising and issuing new white collar enforcement guidance, the U.S. Department of Justice (DOJ) on Tuesday announced a...

---

### **Africa Business in Brief - 26 MAY 2019**

#### **ENSAfrica**

Nigerian e-health start-up iDHS HealthWise is looking to expand operations across a host of African countries among them Ghana, Kenya, Rwanda and...

---

Public



### **North Carolina Legislative Update, May 24, 2019**

[North Carolina](#)

#### **Brooks Pierce McLendon Humphrey & Leonard LLP**

Senate appropriators worked on the budget bill behind closed doors this week and both houses considered a variety of bills prior to leaving for the...

---

### **Supreme Court Rules That Third-Party Counterclaim Defendants Cannot Remove Class Actions Under the Class Action Fairness Act (CAFA)**

#### **Robinson & Cole LLP**

The U.S. Supreme Court held today that a third-party defendant could not remove a class action to federal court under the Class Action Fairness Act...

---

### **Alabama Lawmakers Pass Near-total Abortion Ban**

#### **Cozen O'Connor**

Jennifer sat down with the hosts of Fox29's Good Day Philadelphia to discuss Alabama's new abortion law and what's next. The bill, the strictest in...

---

### **NC Legislative Update: May 24, 2019**

[North Carolina](#)

#### **Nexsen Pruet**

The legislature continued a slow pace this week, with Senate leadership spending most of its time behind closed doors making the final decisions on...

---

### **Summary of Principal Changes: No-Fault Act**

#### **Foster Swift Collins & Smith PC**

On May 24, 2019, the Michigan Senate and House of Representatives voted 34-4 and 94-15, respectively, to approve a 120-page bill (House Substitute...

---



## **Law Review Article Critiques Local Government Public Nuisance Suits**

### **Reed Smith LLP**

Perhaps you recall how President Trump campaigned on behalf of “Big Luther” Strange in Alabama. Strange had been appointed by Alabama’s Governor to...

---

## **Two Additional Presidential Candidates Subject to Federal Pay-to-Play Rules**

### **Skadden Arps Slate Meagher & Flom LLP**

In a recent mailing we noted that the following Democratic presidential candidates are covered under federal pay-to-play rules (i.e., SEC 206(4)-5...

---

## **President Trump Issues Proclamation Finding National Security Threat from Automotive Imports Under Section 232; Directs USTR to Initiate Negotiations with Japan, the EU, and Other "Appropriate" Countries**

### **White & Case LLP**

On May 17, 2019, President Trump issued a Proclamation containing his determinations in the US investigation into the effects imports of automobiles...

---

## **Emerging Technologies Washington Update- May 23, 2019**

District of Columbia

### **McGuireWoods Consulting LLC**

With lawmakers scheduled to leave Washington tomorrow for a week-long Memorial Day recess, congressional leaders are still negotiating a disaster aid...

---

## **It Just Got Real: TRACED Act Barrels Across The Senate Goal Line**

### **Squire Patton Boggs**

The US Senate today approved the TRACED Act, S. 151, as reported by the Senate Committee on Commerce, Science and Transportation, by a vote of 97-1...

---

## **House Releases Draft Transportation Funding Bill**

### **Winston & Strawn LLP**

On May 22, 2019, the House Appropriations Committee released its FY 2020 draft transportation appropriations bill. Highlights include: \$1.1 billion...

---

## **Debt or No Debt? Your Employees’ Future in the Balance**

### **Shawe Rosenthal LLP**

Debt can alter one’s future trajectory for good or for ill. The latter is reflected in a recent article in the Wall Street Journal. Although they are...

---

## **Pay for Delay Passes House of Representatives for First Time**

### **McGuireWoods Consulting LLC**

As Congress focuses on how to drive down drug prices, there is bipartisan support for prohibiting reverse payment agreements, also known as...

---

## **Colorado enacts the “Colorado Student Loan Servicers Act”**

Colorado

### **Buckley LLP**

On May 13, the Colorado governor signed SB19-002, the “Colorado Student Loan Servicers Act,” which requires an entity that services a student...



---

## **Sandy Hook Massacre Gun Makers Must Face Claims Under State UDAP Statute**

[Connecticut](#)

### **Frankfurt Kurnit Klein & Selz PC**

In March, The Connecticut Supreme Court issued a ruling in *Soto v. Bushmaster Firearms International, et al.* allowing private litigants' claims...

---

## **ICE Announced Increased Fees for International Students, Exchange Visitors, and SEVP-Certified Schools**

### **Pierce Atwood LLP**

ICE announced that, effective June 24 2019, fees paid to the Student and Exchange Visitor Program (SEVP) by international students, exchange visitors...

---

## **Appropriations Committee Directs New FARA Guidance on Commercial Exemption**

### **Covington & Burling LLP**

The House Appropriations Committee has quietly directed the Department of Justice to issue new guidance on the commercial exemption to the Foreign...

---

## **State AGs request automatic discharge of disabled veterans' student loan debt**

### **Buckley LLP**

On May 24, Attorneys General from 47 states, American territories, and Washington D.C., sent a letter to Secretary Betsy DeVos of the U.S. Department...

---

## **Tribal Treaty Rights Are Supreme Again**

### **Kilpatrick Townsend & Stockton LLP**

On Monday, May 20 - for the second time during the 2018-2019 term - Justice Neil M. Gorsuch joined the four U.S. Supreme Court Democratic-appointed...

---

## **Repealing TABOR: Colorado Ballot Initiative #3**

[Colorado](#)

[Audio](#)

### **Brownstein Hyatt Farber Schreck LLP**

Colorado's Initiative #3 seeks to repeal the Tax Payer Bill of Rights, more commonly known in Colorado as TABOR. Brownstein Shareholder Sarah Mercer...

---

## **Australia: Post-election update: What's ahead for IR?**

[Audio](#)

### **Herbert Smith Freehills LLP**

In our final podcast for our Federal Election series, Partner Anthony Longland chats with Wendy Fauvel, Senior Associate about what is ahead for...

---

## **Promoting Comprehensive Healthcare Delivery for Children**

### **Manatt Phelps & Phillips LLP**

The Center for Medicare and Medicaid Innovation (CMMI) will fund a model of care, Integrated Care for Kids (InCK), that will test whether alternative...

---

## **NCGA Week in Review- May 24, 2019**

[North Carolina](#)

### **McGuireWoods Consulting LLC**

Lawmakers were eager to wrap up business early this week before the long weekend. The House held their final floor vote session Wednesday afternoon...

---

### **Income Sharing Agreements Grow Despite Regulatory Uncertainty**

#### **Troutman Sanders LLP**

Align Income Share Funding is giving consumers cash in exchange for monthly payments, but don't call it a loan. Instead, Align offers Income Sharing...

---

### **Denver First-Round Election Results Are In**

#### **Brownstein Hyatt Farber Schreck LLP**

Voters cast ballots Tuesday in the City and County of Denver to decide who will be mayor, auditor, clerk and recorder, and who will make up the...

---

### **Bill Introduced to Raise the Nationwide Minimum Legal Age for Tobacco Product Sales to 21.**

#### **Troutman Sanders LLP**

Senate Majority Leader Mitch McConnell (R-KY) announced May 20th that he and Senator Tim Kaine (D-VA) have filed a bipartisan bill to raise the...

---

### **Perspectives Key Takeaways | Asian Pacific Islander Heritage Month**

#### **Kilpatrick Townsend & Stockton LLP**

In honor of Asia-Pacific Islander American Heritage Month, Kilpatrick Townsend hosted a discussion highlighting the unique perspective of...



## **Global**

### **Employment & Labor**



#### **Labour & Employment in Luxembourg**

##### **Castegnaro**

A structured guide to labour & employment in Luxembourg

---

#### **Managing the employment relationship in Nigeria**

##### **Udo Udoma & Belo-Osagie**

A structured guide to country specific laws, misclassification, contracts and foreign workers in Nigeria

---

#### **Five ways to champion women in IP**

##### **UDL Intellectual Property**

All IP careers are suitable for any gender, but some have more of a gender bias than others. For example, the majority of paralegals are female, while...

### **Environment & Climate Change**





## **Oil and gas trading and distribution laws in Venezuela**

### **InterJuris Abogados**

A structured guide to oil and gas trading and distribution laws in Venezuela

---

## **Ship registration in the Netherlands**

### **Van Traa Advocaten**

A structured guide to ship registration laws in the Netherlands

---

## **Basel Convention Extends to Include Transboundary Movements of Plastic Waste**

### **Latham & Watkins LLP**

The significant extension aims to manage plastic waste in an environmentally sound manner and support less developed nations that import waste. On May...

---

## **LNG for 2020: IMO Sulfur Limits and the LNG Alternative**

### **Reed Smith LLP**

This blog post compares the uses of liquefied natural gas (LNG) as a marine fuel with other options for complying with the more stringent sulfur...

---

## **Internet & Social Media**



## **Telecoms spectrum allocation in Germany**

### **Heuking Kühn Lüer Wojtek**

A structured guide to telecoms spectrum allocation in Germany

---

## **Collection, storage and transfer of data in Brazil**

### **Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados**

A structured guide to the collection, storage and transfer of data in Brazil

---

## **Domains & Domain Names in Japan**

### **YUASA and HARA**

A structured guide to domains & domain names in Japan

---

## **Telecoms spectrum allocation in Russia**

### **King & Spalding LLP**

A structured guide to telecoms spectrum allocation in Russia

---

## **Governments hit back over ICANN's '.amazon' TLD resolution as near-decade battle nears end**

### **World Trademark Review**

The presidents of Bolivia, Colombia, Ecuador and Peru have signed a declaration hitting out at ICANN's recent resolution to proceed with Amazon's...

---

## **Cybersquatting in 2019 Series: New Challenges for Business**

### **Taylor Vinters Via LLC**

Cybersquatting has been a problem for businesses since the nineties but, following a number of recent events, companies (and their customers)...



### **Project managing cross-border disputes**

#### **Latin Lawyer & LACCA**

Given the significant costs and challenges associated with cross-border litigation, it is critical for companies to implement a strategic plan to...



### **TBT jurisprudence: on track or off the rails?**

#### **Linklaters LLP**

The WTO's recent Panel report in Russia - Railway Equipment is the latest development in a series of WTO disputes between Russia and Ukraine. It...



### **Loi favorisant la surveillance des contrats des organismes publics et instituant l'autorité des marchés publics**

#### **Gowling WLG**

Pour faire suite à notre article portant sur l'entrée en vigueur de certaines dispositions de la (la « Loi »), de nouvelles dispositions mettant en...

### **Managing risk: A disputes perspective (2019)**

#### **Herbert Smith Freehills LLP**

The amount of data organisations are dealing with is ever-increasing and is taking on different forms. In the context of a dispute, the focus used to...

## **Other top stories**

**Artificial Intelligence on the move**

**The Contract Management Software Implementation Playbook**

**Standard Chartered agrees to pay a USD1.1 billion fine for Anti-Money Laundering and Sanctions violations**

**What Am I Doing Wrong?? Common FMLA Mistakes**

**"Rip-and-Tear Damages" In Construction: A Roadmap For Coverage Where None Existed?**

**How "Effective" Is Your Compliance Program?**

**77 Percent of Bank Boards Commit this Mistake**

**2019 Ethics & Compliance Hotline Benchmark Report**

**Roll Up, Roll Up: 'Cannabis Inc.' Is Open for Business, but UK Investors Must Wait Their Turn**

## International developments

**Federal Employers: Prepare for a Wave of Change in Workplace Harassment Obligations**

**Arbeit auf Abruf: Minimale gesetzliche Änderungen, maximale Auswirkungen auf geringfügig Beschäftigte** [DE](#)

**Pluses que desaparecen como consecuencia de la subida del salario mínimo interprofesional** [ES](#)

**Coeficiente de parcialidad en el trabajo a tiempo parcial. Discriminación indirecta según la justicia europea** [PT](#)

**Apariencia de negociación: nulidad del convenio negociado** [ES](#)

**¿Es el informe de vida laboral un documento «decisivo» para solicitar la revisión de una sentencia firme?** [ES](#)

**On your radar - Key employment issues across Europe and beyond**

**Asia Pacific Employment Law Guide 2019**

**How microaggressions can turn a “compliment” into discrimination and harassment**

**Construction in the Netherlands**

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law

[Contact Lexology](#)

[About Lexology](#)



© 2006-2019 Globe Business Media Group



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fggurina@sunnyvale.ca.gov](mailto:fggurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for May 13, 2019  
**Date:** Monday, May 13, 2019 5:03:43 AM

---

Having trouble viewing this email? [Click here](#)



## Courts & Rulings

### **Appeals Court: County has no duty to provide sleeping facilities for homeless**

The Sixth District Court of Appeal yesterday affirmed the denial of a

petition for a writ of mandate filed by a group of homeless persons seeking to compel Santa Clara County to provide "adequate and appropriate places" for individuals such as themselves "to sleep safely each night between the hours of 8 p.m. to 7 a.m."

[Metropolitan News-Enterprise](#)

### **Retired California judges fight to lift cap on temp work**

Three retired judges sued California Supreme Court Justice Tani Cantil-Sakauye, claiming she and the Judicial Council are putting unfair and illegal limits on the number of years they can continue working after retirement. All three currently participate in the Assigned Judges Program, which helps shorthanded California courts by filling their benches when judges get sick, take vacation, or are summoned away on judicial business.

[Courthouse News Service](#)

### **Stop near border based on more than 'hunch' in light of time, locality, tinted windows**

The Ninth U.S. Circuit Court of Appeals yesterday affirmed a man's conviction for transporting illegal aliens in the United States, rejecting the contention that the District Court erred in not suppressing the fruits of an allegedly unlawful vehicle stop near the Mexican border.

[Metropolitan News-Enterprise](#)

### **Judge must determine defendant's competency to stand trial once lawyer expresses doubt**

The Court of Appeal for this district yesterday "conditionally" reversed a conviction for first degree murder with personal use of a weapon because the trial judge did not make a finding as to the defendant's capacity to stand trial in light of his lawyer's withdrawal of a request that he do so.

[Metropolitan News-Enterprise](#)

### **Find out how a loophole could keep young terror suspects out of U.S. court**

The Justice Department's ability to charge minors for supporting terrorist groups has been hampered by a 2018 Supreme Court decision, forcing prosecutors to hand off at least one such case to local authorities in a state without anti-terrorism laws. The court's decision in a case unrelated to terrorism opened a loophole that could allow young supporters of groups like the Islamic State to skate on charges from the federal government.

[CBS Austin](#)

### **Yagman's action seeking CIA records on torture must be reinstated**

Disbarred attorney Stephen Yagman, once a prominent civil rights practitioner, yesterday prevailed in the Ninth U.S. Circuit Court of Appeal in a case in which he is self-represented, with the judges holding

that the District Court abused its discretion in dismissing with prejudice his action seeking records from the Central Intelligence Agency on use of torture.

[Metropolitan News-Enterprise](#)

### **WGA, claiming judge in suit against talent agencies is "prejudiced", boots him off the case**

The WGA, claiming that the judge assigned to its lawsuit against Hollywood's Big 4 talent agencies is "prejudiced," has used its one and only preemptory challenge and had him removed from the case. The guild had asked Los Angeles Superior Court Judge Marc Gross to voluntarily recuse himself from the case earlier this week, but when he did not, the WGA exercised its right to get a new judge.

[Deadline](#)

### **First District Panel rejects reasoning of opinions on SB 620**

Div. One of the First District Court of Appeal on Friday, in a 2-1 decision, dismissed the appeal of a sentence because the defendant had not secured a certificate of probable cause, repudiating the view of this district's Div. Two, and courts embracing its position, that a certificate is not needed where new legislation is invoked giving a judge discretion to strike a firearm enhancement.

[Metropolitan News-Enterprise](#)

### **County killer loses death penalty appeal**

A Tulare County killer will remain behind bars for the rest of his life following a recent ruling by the state's highest court. In a decision released on April 29, the California Supreme Court upheld the conviction and death sentence of Juan Sanchez, 54, for the first-degree murders of Ermanda Reyes and Lorena Martinez more than 20 years ago.

[The Sun Gazette](#)

### **No need to instruct on victim's past threats to third parties**

The Third District Court of Appeal held yesterday that a judge did not err in declining to instruct a jury in a homicide case that the victim's harming or threatening of others in the past could be taken into account in determining the reasonableness of the defendant's claimed perception of need for self defense, holding that the instruction requires knowledge on the defendant's part of those past acts.

[Metropolitan News-Enterprise](#)

### **Former Compton Mayor Omar Bradley's conviction upheld**

A state appeals court panel has upheld former Compton Mayor Omar Bradley's conviction for misappropriating and misusing taxpayer funds. In a ruling released late Monday, the three-justice panel from California's 2nd District Court of Appeal rejected Bradley's contention that insufficient evidence and incorrect jury instructions mandated reversal of his July 2017 conviction on the two felony counts.

[NBC4](#)

## **Verdict upheld in murder of mother, 4-year-old in Downtown Long Beach**

A state appeals court panel Monday upheld an Oklahoma man's conviction for gunning down a woman and her 4-year-old daughter in an unprovoked attack in Long Beach. The three-justice panel from California's 2nd District Court of Appeal cited "compelling evidence of guilt" by Brandon Ivan Colbert Jr., who was convicted of first-degree murder for the Aug. 6, 2016, murders of Carina Mancera, 26, and her daughter, Jennabel Anaya.

[City News Service](#)

## **Group asks court to block \$500 million parcel tax meant to fund LA schools**

A proposed parcel tax meant to generate \$500 million for the Los Angeles Unified School District over the next 12 years is under fire from a fiscal conservative group that says the language in the measure is ambiguous and should not be included on the ballots this June, according to a complaint filed Tuesday.

[Courthouse News Service](#)

## **Rule allowing union organizers to enter worksite, solicit workers, is valid**

The majority of a three judge panel of the Ninth U.S. Circuit Court of Appeals yesterday upheld the constitutionality of a regulation allowing union organizers to come onto worksites to talk with agricultural workers, with a dissenter maintaining that the rule is violative of the Fifth Amendment.

[Metropolitan News-Enterprise](#)

## **Prosecutions/Prosecutors**

### **Why the Golden State Killer may keep California's death penalty alive**

Gov. Gavin Newsom, a Democrat, issued a moratorium in March on executions in the state, which has more death row inmates than anywhere else in the Western Hemisphere. But that decision has not stopped local prosecutors from seeking new death sentences, underscoring the divide in the state between conservative prosecutors and liberal reformers like the governor.

[New York Times](#)

### **Trial begins for alleged gang member accused of murdering Pomona SWAT officer**

A reputed Mongols motorcycle gang member who shot and killed a Pomona SWAT officer was warned loudly and repeatedly that police were at the door, a prosecutor told jurors Monday, while a defense attorney countered that his client was convinced Mongols members had come to get him and fired to protect his family.

[My News LA](#)

**Los Angeles city attorney sues H&R Block and maker of TurboTax for allegedly misleading low-income taxpayers**

The Los Angeles city attorney filed suit Monday against the tax preparer H&R Block and Intuit, maker of the popular software TurboTax, alleging that the companies defrauded low-income taxpayers and charged them for a service that the companies are required by law to provide for free. The twin suits allege the companies "intentionally obscure[ed] and fail[ed] to disclose" differences between its commercial products and the "Free File" program.

[NBC News](#)

**Man accused of murdering Lancaster Sgt. Owen Back in court**

Trevon Lovell, 29, faces multiple charges - including murder - stemming from the 2016 shooting death of a Los Angeles County Sheriff's Department sergeant outside a Lancaster apartment complex. Lovell is accused of killing Owen, 53, on Oct. 5, 2016. Prosecutors said Lovell shot Owen, then continued to shoot him when the sergeant was already on the ground.

[Santa Clarita News](#)

**Alleged cop-killer's father cross-examined by prosecution**

The third day of defense testimony continued Monday in the trial of an ex-con accused of killing two Palm Springs police officers who responded to a domestic disturbance call at his family's home. Last week, family members of the accused took the stand again - for the defense this time around - in the trial of 28-year-old John Hernandez Felix, who is accused of firing an AR-15 rifle at veteran Officer Jose Gilbert Vega, 63, and rookie Officer Lesley Zerebny, 27, from inside the Felix family home in the 2700 block of Cypress Avenue on Oct. 8, 2016, killing both.

[City News Service](#)

**Palm Springs public corruption case back in court; new preliminary hearing date set**

The case involving Palm Springs' disgraced former mayor Steve Pougnet and his co-defendants, developers John Wessman and Richard Meaney, returned to court Friday, three months since it last appeared before a Riverside County judge. Judge James T. Latting, in a brief Friday afternoon hearing at the Larson Justice Center in Indio, approved a defense request to reschedule a pending preliminary hearing that had originally been scheduled for next month.

[Palm Spring Deset Sun](#)

**Prosecutors want tennis broadcaster Justin Gimelstob's plea in attack tossed out**

Los Angeles County prosecutors want tennis broadcaster Justin Gimelstob's no-contest plea in a Halloween attack tossed out after he denied committing the crime in court papers seeking a temporary



restraining order against the man he is accused of injuring.

[Los Angeles Times](#)

### **Suspect charged with murder in deaths of 3 men found shot in cars on remote Palmdale Road**

A suspect has been charged in the case of three men found shot dead and a fourth wounded inside two parked vehicles in Palmdale earlier this year, officials said Thursday. Jonathan Paul Misirli, 35, of Sun Valley, was identified as the gunman during months of investigation into the Jan. 16 killings near the corner of Ranch Center Drive and 40th Street West, the Los Angeles County Sheriff's Department said in a news release.

[KTLA](#)

### **Newhall woman charged in \$6 million chiropractor insurance fraud scheme**

A Newhall woman was among fifteen chiropractors who have been charged in a \$6 million insurance fraud and illegal kickback scheme involving automobile collision medical claims, the Los Angeles County District Attorney's Office announced Friday. The felony complaint lists a total of 18 felony counts, including charges against all of the defendants of insurance fraud and participating in patient referral rebates when licensed in the healing arts or as a chiropractor.

[KHST](#)

### **German nationals charged in L.A. in dark web case**

Three German nationals are facing federal drug distribution and money laundering charges in Los Angeles for their alleged roles as administrators of a hidden online marketplace for narcotics, counterfeit goods and malicious computer hacking software, the U.S. Department of Justice announced.

[My News LA](#)

### **Survivor of knife attack testifies against accused SoCal killer**

The survivor of a knife attack by a suspected serial killer described her ordeal for the first time in court on Monday. Michelle Murphy, now 37 years old, testified that she was awakened by someone on top of her and stabbing her with a knife. The defendant, 43-year-old Michael Gargiulo, is accused of a crime spree that began in 1993.

[ABC7](#)

### **Feds file hate crime charges in San Diego synagogue shooting**

The Justice Department filed 109 federal hate crime charges Thursday against a 19-year-old man accused of killing a 60-year-old woman and wounding a rabbi, a girl and others during a shooting at the Chabad of Poway Synagogue near San Diego. The federal charges come a week after suspect John Earnest pleaded not guilty to state charges of murder, attempted murder and arson filed by San Diego District Attorney Summer Stephan.

### **Two men charged with attack on autistic teen in Rolling Hills Estates**

Two young men are set to be arraigned Wednesday on charges that they beat and robbed an autistic man inside a Rolling Hills Estates mall parking structure in March. Alexander Bell-Wilson of Rolling Hills and Korey Oscar Benjamin Streeter of Long Beach, who are both 18, are charged with one count each of assault by means of force likely to produce great bodily injury and second-degree robbery, according to the Los Angeles County District Attorney's Office.

[NBC4](#)

### **District Attorney wants you to report opioid abuse after record-high overdose deaths**

Los Angeles County's top prosecutor urged the public on Tuesday to report the illegal trafficking and overprescription of opioids to her office for potential criminal prosecution. "We must do everything in our power to stop the flow of these deadly drugs into our community, whether they are bought illegally on the streets or legally with a valid prescription, District Attorney Jackie Lacey said.

[City News Service](#)

## **Criminal Justice/Public Safety**

### **Police deaths increased in 2018: FBI**

The number of law enforcement officers killed in the U.S. in the line of duty rose from 94 to 106 between 2017 and 2018, according to the Federal Bureau of Investigation (FBI). More than half of the deaths (55) occurred during felonious incidents, the FBI said in its annual report of Law Enforcement Officers Killed and Assaulted (LEOKA). The largest number of felonious deaths (28) occurred in Southern states, the report said.

[The Crime Report](#)

### **'Your son died an American hero.' Memorial honors 8 California police officers killed last year**

As uniformed officers and law enforcement family members held back tears, Newman Police Chief Randy Richardson got choked up himself while recounting the last time he saw Cpl. Ronil Singh. It was Christmas morning last year. And in the small Stanislaus County city, Richardson relieved Singh of his graveyard shift, one-on-one, at 6 a.m.

[Sacramento Bee](#)

### **Newman Police chief praises slain Officer Ronil Singh, scolds California lawmakers**

A police chief briefly scolded California lawmakers Monday for "making it more difficult for us" as he honored an officer whose slaying entered the national debate over immigration last year. Newman Police Chief Randy

Richardson spoke while praising Cpl. Ronil Singh, who immigrated from Fiji and was fatally shot early Dec. 26 after stopping a suspected drunk driver.

[AP](#)

### **Police Union: LAPD officers contracted staph infection after homeless person came into station**

Three Los Angeles Police Department officers have been infected with a highly contagious staph infection after what a union official says was an encounter with a homeless person at a police station. The outbreak started sometime within the last week at the LAPD West Valley station in Reseda when officers arrested a transient and was brought to the station, which has since undergone cleaning of all surfaces to stop the MRSA from spreading.

[CBS LA](#)

### **How does Border Patrol find \$7.8 million in counterfeit goods in a week? They look closely**

U.S. Customs and Border Protection said Tuesday that it seized \$7.8 million worth of fake high-end merchandise at a Greater Cincinnati point of entry this week. Officials at the shipping hub located at the Cincinnati-Northern Kentucky International Airport said they seize fake merchandise daily but over a three-day period, officers seized counterfeits worth millions of dollars.

[Cincinnati Enquirer](#)

### **California honors fallen law enforcement officers with vigil**

Hundreds attended the annual California Peace Officers' candlelight vigil in Sacramento on Sunday evening. Family, friends and colleagues gathered at the memorial monument by the state capitol grounds at 8 p.m. to honor the lives of the 10 law enforcement officers who died in the line of duty this past year.

[KCRA](#)

### **LAPD drones used twice in first 3 months of 2019**

The Los Angeles Police Department twice deployed drones through the first three months of 2019 under a one-year pilot program authorized by the Police Commission last July, according to a report presented to the commissioners today. After the creation of the program in 2018, the department's first deployment of a drone - officially known as an Unmanned Aerial System - was on Jan. 9 in the 300 block of Berendo Street, and then again on March 28 in the 7400 block of S. San Pedro Street, the report said.

[City News Service](#)

### **Anaheim officers won't be charged after firing 76 shots during pursuit, killing suspect (Warning: Graphic video)**

Two Anaheim police officers fired their weapons 76 times during a pursuit last year in which a man armed with an airsoft gun and under

the influence of drugs was killed after being struck by at least nine police bullets. The actions of the officers were described by prosecutors as "alarming and irresponsible" in a report released Wednesday, but the Orange County District Attorney's Office determined there was insufficient evidence to file charges against them.

[KTLA](#)

## **Props 47, 57 & AB 109**

### **Attorney: Gonzalez should be treated as juvenile**

A Santa Cruz man who was 15 when he allegedly raped and killed an 8-year-old girl four years ago - and is facing life in prison for the crime - could instead be sent to a sex offender treatment program after his lawyers on Thursday argued that a new state law requires him to be treated as a juvenile. Santa Cruz County District Attorney Jeff Rosell argued that law - SB 1391 - is unconstitutional, and asked Superior Court Judge Steven Siegel instead to base his ruling on a state proposition that gives judges discretion when trying juveniles.

[Register Pajaronian](#)

### **Amid surprise jail closure announcement, calls for Alameda sheriff accountability grow**

The Justice Reinvestment Coalition of Alameda County (JRC) along with various community members are calling for greater accountability from Alameda County Sheriff Greg Ahern. On the evening of April 26, 2019, Sheriff Greg Ahern announced the closing of its Oakland jail facility. Sheriff Ahern's plan to close Glenn E. Dyer jail without input from the community or notifying the Alameda County Board of Supervisors is only the latest example of the sheriff's department's lack of accountability and transparency.

[Independent Media Center](#)

## **Policy & Legal Issues**

### **Who's the victim when a Somali Muslim police officer shoots an innocent white woman? The NYT thinks it knows.**

Novelist, screenwriter, podcaster, and all-around sage Andrew Klavan has taken to referring to the New York Times as a "former newspaper." The Times, he says, clings to the pretense of news reporting while pursuing other ends, to wit, the advancement of the leftist ideology shared by the paper's writers, editors, and management.

[PJ Media](#)

### **A routine police stop landed him on California's gang database. Is it racial profiling?**

Brian Allen was driving home from work in July 2017 when he spotted someone from his days at Crenshaw High School. He stopped, they talked and he agreed to give the friend - an aspiring rapper with a criminal record - a ride. A passing LAPD cruiser did a U-turn and pulled

over Allen's Nissan. Officers questioned both men and let them go.  
[Los Angeles Times](#)

### **Are lawyers immune from defamation laws?**

If someone libels, slanders or defames your character, you can sue them. Of course, you'll have to be able to prove in court how the person injured your reputation or business, and you'll have to show that what was said was more than just ugly opinion. You'll have to show the offender made a false statement of fact.

[Creators](#)

### **Thieves are hitting California farmers hard. This crime bill will help solve problem**

California is the top agricultural-producing state in the nation and is recognized as the breadbasket and salad bowl of the world. Unfortunately, this blessing goes unrecognized and our hard-working farmers and agricultural workers are often taken for granted. It's important that farmers have a seat at the policy-making table.

[Visalia Times Delta](#)

### **Young people who can't pay court fees are getting trapped in the criminal justice system**

Shyara Hill's five-year struggle with the criminal justice system started because she hit a boy at school who had been bullying her little brother. Hill was 16 years old and a student at Upper Darby High School, a Philadelphia-area school with more than 3,500 students. She was sent to the office of a vice principal who never showed up.

[BuzzFeed News](#)

### **Sheriff's department finds way to communicate with ICE without violating sanctuary state law**

The Orange County Sheriff's Department has complained that California's "Sanctuary State Law," SB54, has made it difficult to enforce the law and comply with federal authorities. Among other restrictions, the law stipulates that state and local law enforcement are prohibited from holding illegal aliens on the basis of federal immigration detainers or transferring them into federal custody.

[The Epoch Times](#)

### **Morning Report: One year in, police policies don't always reflect 'sanctuary' law**

State lawmakers intended for the California Values Act - the so-called "sanctuary state" law - to create a firewall between local law enforcement and federal immigration officials. It prohibited, for instance, police departments from using immigration agents as interpreters, which could make victims of crimes fearful to come forward.

[Voice of San Diego](#)



---

**LAPD officer suspected of driving under influence of drugs**

An LAPD officer has been arrested following a monthslong internal affairs investigation, according to several law enforcement sources. Samuel Sabourin was booked on April 24 at the Van Nuys station jail and was released from custody several hours later, according to an LA County Sheriff's Department booking record.

[NBC4](#)

**Purse theft victim dies after she was run over by robbers**

A 32-year-old Westminster woman died after she was struck by an SUV driven by purse thieves being followed by a police task force at a shopping center in Garden Grove in an attack caught on surveillance camera, police said. Witnesses say they heard screaming, the sound of what they thought was a traffic crash and then a car screeching off in a parking lot at 13800 Brookhurst Blvd. about 9:45 a.m.

[NBC4](#)

**Chile crime rings threaten Southlanders**

In the last few years, the cyber invasions into the U.S. by such aggressors in Russia and China have been well documented. But now we learn that old fashioned crime rings are sending human burglars from Chile to steal from Southern California residents in their homes and businesses. The Los Angeles Times reported that traveling bands of so-called tourist burglars from the South American country have become a growing menace in the United States.

[Antelope Valley Press](#)

**Crime rate among homeless skyrockets in Los Angeles**

Serious crimes involving at least one homeless person rose 52 percent from 2017 to 2018, according to a new report from the Los Angeles Police Department, while crime decreased two percent citywide. In 2017, there were 4,400 Part 1 crimes where a homeless person was either a suspect or a victim. Just one year later, the number skyrocketed to 6,671 Part 1 crimes involving the homeless, the report said.

[Spectrum News 1](#)

**Arrest made in Northridge road rage shooting, more victims sought**

An anonymous tip led to the arrest was of man suspected of repeatedly shooting another driver in a Northridge road rage incident, and now police believe there may be additional victims. Los Angeles police announced the arrest Tuesday evening of David Phouanesavath. Detectives believe Phouanesavath is the shooter in the March road rage incident in Northridge that left a man hospitalized with a gunshot wound.

[Northridge-Chatsworth Patch](#)

**Anaheim police arrest two men in shooting death of 9-year-old**

## **girl**

Two Orange County men identified by police as documented gang members were arrested late Friday in connection with the shooting death of a 9-year-old girl as she played in front of her home two days earlier. Police Chief Raul Quezada, announcing the arrests on Saturday, said the investigation is ongoing and urged anyone with information to reach out to authorities.

[Orange County Register](#)

## **California 'sexually violent predator' arrested in cold case rape, murder of woman, 81**

A California man classified a "sexually violent predator" has been arrested in the cold case rape and murder of an 81-year-old woman decades ago. Police said Thursday they arrested Lenard Chester, 58, in the Dec. 1, 1980, murder of Leah Sarah Bullis in Oxnard through a DNA match. Cops found Bullis near death when they responded to her home for an assault.

[Fox News](#)

## **Will crime shift after Gateway Camp closes?**

They're heading for Harvey West, Pogonip, downtown or up Highway 9. But they aren't staying at the camp that closed Friday between Gateway Plaza Shopping Center and Highway 1. And, as civilian calls for service in the area of the camp have doubled the last six months compared to the same periods in preceding years, it is expected that those calls for service might decline in the area as a result of the city-ordered eviction of more than 100 people who settled the camp since November.

[Santa Cruz Sentinel](#)

## **Hit and runs involving property damage can be a challenge for law enforcement**

In the aftermath of a hit and run collision outside his home, Sun City resident Alan Rochman went right to work repairing a short cinderblock wall and salvaging what was left of his bed of plants. And while he doesn't think the fleeing driver will be found, statistics back up his belief. The Los Angeles Daily News last year reported that the Los Angeles Police Department solved only 8% of hit and runs in 2017. And those involve more than a broken wall.

[YourValley.net](#)

## **Chase suspect may have caused Chatsworth crash on purpose: LAPD**

A Domestic violence suspect, who led police on a chase through Chatsworth Monday morning causing a dramatic crash, may have caused the crash on purpose, police said. The suspect was arrested on suspicion of domestic violence and felony evasion and hit and run, according to the Los Angeles Police Department.

[Northridge-Chatsworth Patch](#)

### **Residents demand increased foot patrols in response to assaults, drugs**

Dozens of downtown Los Angeles residents on Thursday demanded lawmakers increase the police presence in the area in response to assaults, drug sales and harassment in the area. The DTLA Strong neighborhood group submitted a petition with more than 1,700 signatures to the City Council's Budget and Finance Committee requesting additional Los Angeles Police Department foot patrols on major streets and an analysis of crime downtown, the Los Angeles Times reported.

[Fox News](#)

### **Arrest made in TV director Barry Crane's 1985 murder**

A man arrested in North Carolina on suspicion of murdering a prominent television director in Studio City in 1985 was awaiting extradition to the Southland Friday. The victim, 57-year-old Barry Crane - who directed such television shows as "The Incredible Hulk," "The Love Boat," "Fantasy Island," "Police Woman," "Police Story" and "The Streets of San Francisco," among others - was found by his housekeeper on July 6, 1985.

[My News LA](#)

## **Los Angeles County**

### **Goldstein Investigates: Metro proposed spending \$200K on saunas, steam rooms**

While the L.A. County Metropolitan Transportation Authority struggles to replace buses that broke down and caught fire because of a lack of money, the agency is proposing spending hundreds of thousands of dollars on steam and sauna rooms for its employees.

[CBS LA](#)

### **Beutner's changes to ballot language spark debate over parcel tax for L.A. schools**

A dispute is roiling over a change to the ballot language of Measure EE, which would raise an estimated \$500 million a year for Los Angeles public schools if approved by voters next month. The funding infusion would provide major relief to the financially challenged L.A. Unified School District, but it would come at the cost of a substantial new obligation for local property owners.

[Los Angeles Times](#)

### **An important shift on youth justice in L.A. County**

We call ourselves million-dollar youth, because Los Angeles County spent at least that much on arresting, prosecuting, detaining and supervising us. A million dollars is a lot of money. And we think we're worth that, but taxpayers didn't get their money's worth. As teenagers, we struggled with poverty and unstable circumstances.

[Los Angeles Daily News](#)

## **Probation oversight panel delivers detailed plan to eliminate pepper spray from LA youth facilities in 12 months, but will it be followed?**

The Los Angeles County Supervisors have just received a smart, step-by-step plan describing how the county can eliminate pepper spray from its youth facilities in 12 months - as the board voted to do in February. Getting enough consensus from various interested factions to create the plan to remove the skin-blistering spray that youth advocates label torture, and some staff claim is a necessary tool was not an easy endeavor.

[Witness LA](#)

## **Los Angeles County Sheriff**

### **L.A. County Sheriff plans to revive highway drug team that stopped Latino drivers on I-5**

Los Angeles County Sheriff Alex Villanueva said Tuesday that he will revive a drug team that was sharply criticized for disproportionately stopping Latino drivers on the 5 Freeway but said the unit would follow strict constitutional guidelines to prevent racial profiling. The Domestic Highway Enforcement team was suspended in November after county Inspector General Max Huntsman said a preliminary investigation by his office found the unit was "inherently built to violate the constitutional rights of a vast number of people passing through the I-5 Freeway."

[Los Angeles Times](#)

### **LA Sheriff's Department won't help ICE arrest immigrants**

The Los Angeles County Sheriff's Department said Wednesday it will not participate in the U.S. Immigration and Customs Enforcement's Warrant Service Officer Program. The program allows for local authorities to arrest and temporarily detain immigrants in the United States illegally on behalf of the agency, regardless if the city is a so-called sanctuary city.

[City News Service](#)

## **Consumer News**

### **FCC warns of 'one ring' robocall scam**

The FCC on Friday warned consumers of a surge in robocalls known as the "One Ring" scam - but it has nothing to do with Sauron or his minions in Middle-earth. Jokes aside, the "One Ring" or "Wangiri" scam targets potential victims with a series of calls - usually from the 222 area code - often in the middle of the night. "Recent reports indicate these calls are using the '222' country code from the West African nation of Mauritania," the FCC said in a news release.

[NBC4](#)

## **How to force Google to automatically delete the information it**

## **saves about what you do online**

Google has begun rolling out a feature that allows you to configure how long it can save data from all of the Google services you use, like maps, search and everything you do online. Until now, you had to manually delete this data or turn it off entirely. Deleting it means Google doesn't always have enough information about you to make recommendations on what it thinks you'll like, or where you might want to go.

[CNBC](#)

## **Convictions**

### **Man who had prostitutes rob Valley banks heads to prison**

A Los Angeles pimp who had prostitutes robbing banks across the San Fernando Valley while he was in prison and on GPS monitoring was sentenced to five years in prison Monday. Robert Michael St. John, 49, a career criminal who already served time for orchestrating bank robberies committed by prostitutes was sent back for prison for doing it again.

[City News Service/Studio City Patch](#)

### **Mastermind who vowed to help hundreds find love using 'witchcraft' sentenced to 2 years**

The Argentine mastermind of an international "witchcraft extortion scheme" who targeted hundreds of people looking for love was sentenced to two years in federal prison Monday. Ariel Boiteux, 31, offered to help people find love using magic spells and advertised his services on Facebook and Instagram, the Office of the U.S. Attorney for the Southern District of California said in a news release.

[NBC News](#)

### **Former wrestling coach convicted of 47 sex-related counts**

A man who coached wrestling at a Sun Valley high school was convicted Tuesday of 47 sex-related counts, including lewd act on a child, involving seven boys and two girls. Jurors found Terry Terrell Gillard of Sylmar, 58, guilty of three felony counts each of lewd act on a child, lewd act on a child 14 or 15 and oral copulation of a person under 18, along with 28 felony counts of procuring a child to engage in a lewd act and 10 misdemeanor counts of child molestation, according to the Los Angeles County District Attorney's Office.

[My News LA](#)

## **Death Penalty**

### **California Focus: Will of the people? Bah...**

For Gov. Gavin Newsom, there's been an almost unprecedented mix of adulation and approbation for his bold moves granting reprieves to more than 700 inmates on California's Death Row and ordering the state's legal killing chamber dismantled. From the left came huzzahs and expressions of admiration from folks who believe that because very occasionally an innocent person has been executed, no one should be,



no matter how cruel, evil or heinous their crime, no matter how strongly the sentencing jury may have felt.

[Sonoma Index-Tribune](#)

### **'Trial by Fire' Director Edward Zwick on a 'Tipping Point' in the politics of the death penalty**

Edward Zwick's new movie, "Trial By Fire," which will screen in D.C. next week before its May 17 release, is coming out amid a potential shift in the politics surrounding the death penalty. California Governor Gavin Newsom put a moratorium on the state's death penalty in March, suspending executions for the more than 700 people on death row. Lawmakers in New Hampshire and Washington state have introduced bills repealing capital punishment.

[Variety](#)

### **Death row case stirs fears over quality of defense counsel**

Of all the many cases an attorney might handle, death penalty cases might be the most high-stakes, which is why most people expect that the attorneys who take such cases are the best of the best. But experts say that is often not the case. For some, that reality is on display in a death penalty case pending in California where a newly appointed attorney has come under scrutiny for bad conduct including an affair with a previous client's daughters during a murder trial.

[Law360](#)

## **California/National**

### **Gavin Newsom's \$209 billion budget calls for new taxes. Can he get them passed?**

Gov. Gavin Newsom has proposed new taxes and fees to fund health care subsidies, clean drinking water and tax credits for low-income families. But state revenue outpacing even his most optimistic predictions could present a challenge for him as he attempts to raise taxes. Last month, corporate taxes came in at \$3.4 billion, much higher than the Newsom administration's estimated \$2.6 billion.

[Sacramento Bee](#)

### **How powerful lawmakers are killing California bills - without a peep**

Gun control, school spending, curbs on greenhouse gases: With Democrats holding more power at the Capitol than they've had since the 19th century, California's legislative pipeline is full this year with big, blue-state ideas. In theory, no Democrat's bill should be left behind. But that's not what's happening, and the reason is roiling both sides of the aisle in Sacramento.

[Witness LA](#)

### **Text messages now remind defendants to show up**

C u in court. Courts around the country are embracing text messages as

a way to nudge people into showing up for their hearings. On any given day, up to half of defendants fail to show up for their scheduled proceedings. No-shows cost the courts time and money, and can cost defendants their freedom. Public defenders and court administrators are using text reminders in more than a dozen states, including Virginia, California, Pennsylvania, Maryland, Florida and Washington.

[AP](#)

### **ACLU sues Homeland Security to stop feds from moving immigrant detainees far from Orange County**

Ubaldo Arroyo, who has lived most of his life in Orange County, is being held as an undocumented detainee at the James A. Musick Detention Facility in Irvine, unsure where he will be sent following the Orange County Sheriff's announcement that it will no longer house detainees while their deportation cases are pending.

[Orange County Register](#)

### **Rantz: King County won't charge criminals assaulting cops while resisting arrest**

King County Prosecutor Dan Satterberg will "not file [charges] when the assault can be best described as resisting" an arrest from an officer, his office confirms. This position is deeply troubling to law enforcement officers, and King County Sheriff Mitzi Johanknecht says "we need to rethink this."

[770 KTHH](#)

### **Case of inmates assaulting guards at State Penitentiary sent to States Attorney's office**

The case involving the assault of seven correctional officers at the state penitentiary has been sent for review by the state's attorney's office. The Department of Corrections and Rehabilitation (DOCR) says the staff assaults happened on January 21 and 23. In February we asked if the inmates involved in the case were charged and the public information officer for the DOCR said it was still an active investigation.

[KFYRTV.com](#)

### **Aspiring sports agent accused of bribing NCAA coaches was 'trying to hustle' jury, prosecutor says**

He hustled his way into the basketball world through bribes - and when he got caught, he tried hustling a jury. That was the message Friday from a prosecutor delivering closing arguments in the trial of aspiring sports agent Christian Dawkins, who is accused of making secret payments to college basketball coaches in exchange for their help steering players to him as clients.

[New York Daily News](#)

### **California lawmakers again protect the loophole of unlimited political cash**

This isn't meant to be a trick question: Are there limits to the size of

campaign contributions that a California lawmaker can accept? Yes, there are - unless the money is given to a political committee that's supposed to either support or oppose a ballot measure. Then the answer is no; the politician can collect in donations of all sizes. And it's been that way for almost two decades.

[Los Angeles Times](#)

### **A plan to cover immigrants would divert public health dollars**

California Gov. Gavin Newsom wants the state to provide health coverage to low-income young adults who are in the country illegally, but his plan would siphon public health dollars from several counties battling surging rates of sexually transmitted diseases and, in some cases, measles outbreaks. Public health officials describe the proposed reallocation of state dollars as a well-meaning initiative that nonetheless would have "dire consequences" to core public health services.

[California Healthline](#)

### **Nonprofit launched by parents of addicts influences drug policy changes**

Twenty years ago, the nonprofit A New PATH was founded by three parents whose children were struggling with addiction. Sylvia Liwerant, Grethen Burns Bergman and Tom O' Donnell met during a support group for families. "We got together, three hurt people, parents like lions who are helping their cubs," said Liwerant.

[NBC7 San Diego](#)

## **Homeless**

### **Homelessness isn't huge in this part of L.A. - but it's a huge campaign issue**

In Los Angeles, the San Fernando Valley neighborhoods of Chatsworth, Porter Ranch and Granada Hills are about as far as you can get from skid row. Fewer people live without shelter in this suburban stretch of the city than in any other L.A. City Council district, according to the last available data from the homeless count.

[Los Angeles Times](#)

### **Mayor Garcetti expects homeless count increase, promises more housing**

The required 2019 Los Angeles homeless census was sent to the Department of Housing and Urban Development this week, but we won't know the results until an official announcement planned for the end of the month. With Orange County up by 40% and the Inland Empire up by 20%, an increase in LA County is expected. "I expect the homelessness to go up," said Mayor Eric Garcetti.

[ABC7](#)

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](#)

From: [US-CERT](#)  
To: [Tanner McGinnis](#)  
Subject: SB19-126: Vulnerability Summary for the Week of April 29, 2019  
Date: Monday, May 06, 2019 1:10:57 PM



National Cyber Awareness System:

## SB19-126 Vulnerability Summary for the Week of April 29, 2019

05/06/2019 06:52 AM EDT

Original release date: May 06, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology \(NIST\) National Vulnerability Database \(NVD\)](#) in the past week. The NVD is sponsored by the [Department of Homeland Security \(DHS\) National Cybersecurity and Communications Integration Center \(NCCIC\)](#) / [United States Computer Emergency Readiness Team \(US-CERT\)](#). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System \(CVSS\)](#) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database \(NVD\)](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
barco -- wepresent_wipg-1000p_firmware	The Crestron AM-100 firmware 1.6.0.2, Crestron AM-101 firmware 2.7.0.1, Barco wePresent WIPG-1000P firmware 2.3.0.10, Barco wePresent WIPG-1600W before firmware 2.4.1.19, Extron ShareLink 200/250 firmware 2.0.3.4, Teq AV IT WIPS710 firmware 1.1.0.7, SHARP PN-L703WA firmware 1.4.2.3, Optoma WPS-Pro firmware 1.0.0.5, Blackbox HD WPS firmware 1.0.0.5, InFocus LiteShow3 firmware 1.0.16, and InFocus LiteShow4 2.0.0.7 are vulnerable to command injection via the file_transfer.cgi HTTP endpoint. A remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.	2019-04-30	10.0	<a href="#">CVE-2019-3929</a> MISC <a href="#">EXPLOIT-DB</a> MISC
barco -- wepresent_wipg-1000p_firmware	The Crestron AM-100 firmware 1.6.0.2, Crestron AM-101 firmware 2.7.0.1, Barco wePresent WIPG-1000P firmware 2.3.0.10, Barco wePresent WIPG-1600W before firmware 2.4.1.19, Extron ShareLink 200/250 firmware 2.0.3.4, Teq AV IT WIPS710 firmware 1.1.0.7, SHARP PN-L703WA firmware 1.4.2.3, Optoma WPS-Pro firmware 1.0.0.5, Blackbox HD WPS firmware 1.0.0.5, InFocus LiteShow3 firmware 1.0.16, and InFocus LiteShow4 2.0.0.7 are vulnerable to a stack buffer overflow in libAwgCgi.so's PARSErtoCHAR function. A remote, unauthenticated attacker can use this vulnerability to execute arbitrary code as root via a crafted request to the return.cgi endpoint.	2019-04-30	10.0	<a href="#">CVE-2019-3930</a> MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v1 TCLinux Fw \$7.3.15.0 v001 / 3.40(ULM.0)b31 router distributed by TrueOnline has a command injection vulnerability in the Remote System Log forwarding function, which is accessible by an unauthenticated user. The vulnerability is in the ViewLog.asp page and can be exploited through the remote_host parameter.	2019-05-02	10.0	<a href="#">CVE-2017-18368</a> MISC MISC MISC MISC
billion -- 5200w-t_firmware	The Billion 5200W-T 1.02b.rc5.d49 router distributed by TrueOnline has a command injection vulnerability in the Remote System Log forwarding function, which is accessible by an unauthenticated user. The vulnerability is in the adv_remotelog.asp page and can be exploited through the syslogServerAddr parameter.	2019-05-02	10.0	<a href="#">CVE-2017-18369</a> MISC MISC MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v2 TCLinux Fw #7.3.37.6 router distributed by TrueOnline has a command injection vulnerability in the Remote System Log forwarding function, which is only accessible by an authenticated user. The vulnerability is in the logSet.asp page and can be exploited through the ServerIP parameter. Authentication can be achieved by exploiting CVE-2017-18371.	2019-05-02	9.0	<a href="#">CVE-2017-18370</a> MISC MISC MISC MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v2 TCLinux Fw #7.3.37.6 router distributed by TrueOnline has three user accounts with default passwords, including two hardcoded service accounts: one with the username true and password true, and another with the username supervisor and password ziad1234. These accounts can be used to login to the web interface, exploit authenticated command injections, and change router settings for malicious purposes.	2019-05-02	7.5	<a href="#">CVE-2017-18371</a> MISC MISC MISC MISC
billion -- 5200w-t_firmware	The Billion 5200W-T TCLinux Fw \$7.3.8.0 v008 130603 router distributed by TrueOnline has a command injection vulnerability in the Time Setting function, which is only accessible by an authenticated user. The vulnerability is in the tools_time.asp page and can be exploited through the uiViewSNTPServer parameter. Authentication can be achieved by exploiting CVE-2017-18373.	2019-05-02	9.0	<a href="#">CVE-2017-18372</a> MISC MISC MISC
billion -- 5200w-t_firmware	The Billion 5200W-T TCLinux Fw \$7.3.8.0 v008 130603 router distributed by TrueOnline has three user accounts with default passwords, including two hardcoded service accounts: one with the username true and password true, and another with the username user3 and a long password consisting of a repetition of the string 0123456789. These accounts can be used to login to the web interface, exploit authenticated command injections, and change router settings for malicious purposes.	2019-05-02	9.0	<a href="#">CVE-2017-18373</a> MISC MISC MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v1 TCLinux Fw \$7.3.15.0 v001 / 3.40(ULM.0)b31 router distributed by TrueOnline has two user accounts with default passwords, including a hardcoded service account with the username true and password true. These accounts can be used to login to the web interface, exploit authenticated command injections and change router settings for malicious purposes.	2019-05-02	9.0	<a href="#">CVE-2017-18374</a> MISC MISC MISC MISC
checkpoint -- endpoint_security	A local attacker can create a hard-link between a file to which the Check Point Endpoint Security client for Windows before E80.96 writes and another BAT file, then by impersonating the WPAD server, the attacker can write BAT commands into that file that will later be run by the user or the system.	2019-04-29	7.2	<a href="#">CVE-2019-8454</a> MISC
cisco -- nexus_93108tc-ex_firmware	A vulnerability in the SSH key management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, remote attacker to connect to the affected system with the privileges of the root user. The vulnerability is due to the presence of a default SSH key pair that is present in all devices. An attacker could	2019-05-03	10.0	<a href="#">CVE-2019-1804</a>



	exploit this vulnerability by opening an SSH connection via IPv6 to a targeted device using the extracted key materials. An exploit could allow the attacker to access the system with the privileges of the root user. This vulnerability is only exploitable over IPv6; IPv4 is not vulnerable.			<a href="#">CISCO</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to command injection via SNMP OID iso.3.6.1.4.1.3212.100.3.2.9.3. A remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.	2019-04-30	10.0	<a href="#">CVE-2019-3925 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to command injection via SNMP OID iso.3.6.1.4.1.3212.100.3.2.14.1. A remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.	2019-04-30	10.0	<a href="#">CVE-2019-3926 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to argument injection to the curl binary via crafted HTTP requests to return.cgi. A remote, authenticated attacker can use this vulnerability to upload files to the device and ultimately execute code as root.	2019-04-30	9.0	<a href="#">CVE-2019-3931 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to authentication bypass due to a hard-coded password in return.tgi. A remote, unauthenticated attacker can use this vulnerability to control external devices via the uart_bridge.	2019-04-30	7.5	<a href="#">CVE-2019-3932 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 use default credentials admin/admin and moderator/moderator for the web interface. An unauthenticated, remote attacker can use these credentials to gain privileged access to the device.	2019-04-30	7.5	<a href="#">CVE-2019-3939 MISC</a>
dell -- idrac6_firmware	Dell EMC iDRAC6 versions prior to 2.92, iDRAC7/iDRAC8 versions prior to 2.61.60.60, and DRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22 and 3.23.23.23 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may potentially exploit his vulnerability to crash the webserver or execute arbitrary code on the system with privileges of the webserver by sending specially crafted input data to the affected system.	2019-04-26	10.0	<a href="#">CVE-2019-3705 MISC</a>
dell -- idrac9_firmware	Dell EMC iDRAC9 versions prior to 3.24.24.24, 3.21.26.22, 3.22.22.22 and 3.21.25.22 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted data to the iDRAC web interface.	2019-04-26	10.0	<a href="#">CVE-2019-3706 MISC</a>
dhcpcd_project -- dhcpcd	dhcpcd before 7.2.1 contains a buffer overflow in dhcpcd_findna in dhcpc6.c when reading N/A/T addresses.	2019-04-28	7.5	<a href="#">CVE-2019-11577 BID MISC MISC</a>
dillonkane -- tidal_workload_automation	An issue was discovered in Dillon Kane Tidal Workload Automation Agent 3.2.0.5 (formerly known as Cisco Workload Automation or CWA). The Enterprise Scheduler for AIX allows local users to gain privileges via Command Injection in crafted Tidal Job Buffers (TJB) parameters. NOTE: this vulnerability exists because the CVE-2014-3272 solution did not address AIX operating systems.	2019-04-26	7.2	<a href="#">CVE-2019-6689 MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a default administrator credential vulnerability. A remote attacker can use this vulnerability to gain administrator privileges for the creation and modification of articles via an H0XZIT44FcN1j9LTdFc5XRKhlf30JaGe1g3cZY6i1K9 access_token in a uri=blog&action=index&controller=blog action to /api/index.php.	2019-04-30	7.5	<a href="#">CVE-2019-11618 MISC</a>
facebook -- hhvm	Insufficient boundary checks for the strpos and stripos functions allow access to out-of-bounds memory. This affects all supported versions of HHVM (4.0.3, 3.30.4, and 3.27.7 and below).	2019-04-29	7.5	<a href="#">CVE-2019-3561 MISC MISC</a>
fujifilm -- cr-ir_357_fcr_capsula_x_firmware	Fujifilm FCR Capsula X/ Carbon X/ FCR XC-2, model versions CR-IR 357 FCR Carbon X, CR-R 357 FCR XC-2, FCR-IR 357 FCR Capsula X are susceptible to a denial-of-service condition as a result of an overflow of TCP packets, which requires the device to be manually rebooted.	2019-04-30	7.8	<a href="#">CVE-2019-10948 MISC</a>
fujifilm -- cr-ir_357_fcr_capsula_x_firmware	Fujifilm FCR Capsula X/ Carbon X/ FCR XC-2, model versions CR-IR 357 FCR Carbon X, CR-R 357 FCR XC-2, FCR-IR 357 FCR Capsula X provide insecure telnet services that lack authentication requirements. An attacker who successfully exploits this vulnerability may be able to access the underlying operating system.	2019-04-30	10.0	<a href="#">CVE-2019-10950 BID MISC</a>
gitea -- gitea	Gitea before 1.8.0 allows 1FA for user accounts that have completed 2FA enrollment. If a user's credentials are known, then an attacker could send them to the API without requiring the 2FA one-time password.	2019-04-27	7.5	<a href="#">CVE-2019-11576 MISC MISC</a>
ionos -- 1&1_online_storage	STRATO HiDrive Desktop Client 5.0.1.0 for Windows suffers from a SYSTEM privilege escalation vulnerability through the HiDriveMaintenanceService service. This service establishes a NetNamedPipe endpoint that allows applications to connect and call publicly exposed methods. An attacker can inject and execute code by hijacking the insecure communications with the service. This vulnerability also affects Telekom MagentaCLOUD through 5.7.0.0 and 1&1 Online Storage through 6.1.0.0.	2019-04-30	9.0	<a href="#">CVE-2019-9486 MISC</a>
linux -- linux_kernel	udp_gro_receive_segment in net/ipv4/udp_offload.c in the Linux kernel 5.x before 5.0.13 allows remote attackers to cause a denial of service (slab-out-of-bounds memory corruption) or possibly have unspecified other impact via UDP packets with a 0 payload, because of mishandling of padded packets, aka the "GRO packet of death" issue.	2019-05-02	10.0	<a href="#">CVE-2019-11683 MLIST MLIST BID CONFIRM MISC MISC</a>
mozilla -- firefox	The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR). This allows for possible arbitrary reading and writing of objects during an exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9791 MISC MISC MISC MISC</a>
mozilla -- firefox	The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript to achieve memory corruption, which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9792 MISC MISC MISC MISC</a>
mozilla -- firefox	A vulnerability was discovered where specific command line arguments are not properly discarded during Firefox invocation as a shell handler for URLs. This could be used to retrieve and execute files whose location is supplied through these command line arguments if Firefox is configured as the default URI handler for a given URI scheme in third party applications and these applications insufficiently sanitize URL data. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9794 MISC MISC MISC MISC</a>
mozilla -- firefox	A vulnerability where type-confusion in the IonMonkey just-in-time (JIT) compiler could potentially be used by malicious JavaScript to trigger a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9795 MISC MISC MISC MISC</a>
mozilla -- firefox	A use-after-free vulnerability can occur when the SMIL animation controller incorrectly registers with the refresh driver twice when only a single registration is expected. When a registration is later freed with the removal of the animation controller element, the refresh driver incorrectly leaves a dangling pointer to the driver's observer array. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9796 MISC MISC MISC MISC</a>
mozilla -- firefox	In Firefox Developer Tools it is possible that pasting the result of the 'Copy as cURL' command into a command shell on macOS will cause the execution of unintended additional bash script commands if the URL was maliciously crafted. This is the result of an issue with the native version of Bash on macOS. *Note: This issue only affects macOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9804 MISC MISC</a>
mozilla -- firefox	A latent vulnerability exists in the Prio library where data may be read from uninitialized memory for some functions, leading to potential memory corruption. This vulnerability affects	2019-04-26	7.5	<a href="#">CVE-2019-9805 MISC</a>

	Firefox < 66.			MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-26	7.5	<a href="#">CVE-2019-2725</a> MISC BID CONFIRM EXPLOIT-DB
signing-party_project -- signing-party	gpg-key2ps in signing-party 1.1.x and 2.x before 2.10-1 contains an unsafe shell call enabling shell injection via a User ID.	2019-04-30	10.0	<a href="#">CVE-2019-11627</a> MISC MLIST
smartbear -- readyapi	The WSDL import functionality in SmartBear ReadyAPI 2.5.0 and 2.6.0 allows remote attackers to execute arbitrary Java code via a crafted request parameter in a WSDL file.	2019-05-03	9.3	<a href="#">CVE-2018-20580</a> MISC
tabslab -- mailcarrier	A buffer overflow in the SMTP response service in MailCarrier 2.51 allows the attacker to execute arbitrary code remotely via a long HELP command, a related issue to CVE-2019-11395.	2019-05-02	7.5	<a href="#">CVE-2019-11682</a> MISC
zohocorp -- manageengine_firewall_analyzer	The Custom Report import function in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123224 is vulnerable to XML External Entity (XXE) Injection.	2019-05-02	7.5	<a href="#">CVE-2019-11677</a> MISC
zohocorp -- manageengine_firewall_analyzer	The "default reports" feature in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123218 is vulnerable to SQL Injection.	2019-05-02	7.5	<a href="#">CVE-2019-11678</a> MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aiikcms -- aikcms	An issue was discovered in AikCms v2.0. There is a SQL Injection vulnerability via \$_GET['del'], as demonstrated by an admin/page/system/nav.php?del= URL.	2019-04-27	6.5	<a href="#">CVE-2019-11567</a> MISC
aiikcms -- aikcms	An issue was discovered in AikCms v2.0. There is a File upload vulnerability, as demonstrated by an admin/page/system/nav.php request with PHP code in a .php file with the application/octet-stream content type.	2019-04-27	6.8	<a href="#">CVE-2019-11568</a> MISC
anomali -- agave	Anomali Agave (formerly Drupt) through 1.0.0 fails to avoid fingerprinting by including predictable data and minimal variation in size within HTML templates, giving attackers the ability to detect and avoid this system.	2019-05-01	5.0	<a href="#">CVE-2019-11841</a> MISC
apache -- archiva	In Apache Archiva before 2.2.4, it is possible to write files to the archiva server at arbitrary locations by using the artifact upload mechanism. Existing files can be overwritten, if the archiva run user has appropriate permission on the filesystem for the target file.	2019-04-30	5.5	<a href="#">CVE-2019-0213</a> MISC MISC MLIST BID MLIST MLIST MLIST BUGTRAQ
apache -- archiva	In Apache Archiva 2.0.0 - 2.2.3, it is possible to write files to the archiva server at arbitrary locations by using the artifact upload mechanism. Existing files can be overwritten, if the archiva run user has appropriate permission on the filesystem for the target file.	2019-04-30	5.5	<a href="#">CVE-2019-0214</a> CONFIRM MISC MLIST BID MLIST MLIST MLIST BUGTRAQ
apache -- axis	A Server Side Request Forgery (SSRF) vulnerability affected the Apache Axis 1.4 distribution that was last released in 2006. Security and bug commits continue in the projects Axis 1.x Subversion repository, legacy users are encouraged to build from source. The successor to Axis 1.x is Axis2, the latest version is 1.7.9 and is not vulnerable to this issue.	2019-05-01	5.4	<a href="#">CVE-2019-0227</a> MISC
apache -- camel	Apache Camel's File is vulnerable to directory traversal. Camel 2.21.0 to 2.21.3, 2.22.0 to 2.22.2, 2.23.0 and the unsupported Camel 2.x (2.19 and earlier) versions may be also affected.	2019-04-30	5.0	<a href="#">CVE-2019-0194</a> MLIST MLIST MLIST MISC MLIST
apache -- pluto	The input fields of the Apache Pluto "Chat Room" demo portlet 3.0.0 and 3.0.1 are vulnerable to Cross-Site Scripting (XSS) attacks. Mitigation: * Uninstall the ChatRoomDemo war file - or - * migrate to version 3.1.0 of the chat-room-demo war file	2019-04-26	4.3	<a href="#">CVE-2019-0186</a> MLIST MISC BID MLIST MISC EXPLOIT-DB MLIST
apache -- unstructured_information_management_architecture_distributed_uima_cluster_computing	This vulnerability relates to the user's browser processing of DUCC webpage input data. The javascript comprising Apache UIMA DUCC (<= 2.2.2) which runs in the user's browser does not sufficiently filter user supplied inputs, which may result in unintended execution of user supplied javascript code.	2019-05-01	4.3	<a href="#">CVE-2018-8035</a> CONFIRM
atlassian -- jira	The WallboardServlet resource in Jira before version 7.13.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the cyclePeriod parameter.	2019-05-03	4.3	<a href="#">CVE-2018-20824</a> MISC
atlassian -- jira	The BrowseProjects.jspa resource in Jira before version 7.13.2, and from version 8.0.0 before version 8.0.2 allows remote attackers to see information for archived projects through a missing authorisation check.	2019-04-30	5.0	<a href="#">CVE-2019-3399</a> MISC
atlassian -- jira	The labels gadget in Jira before version 7.13.2, and from version 8.0.0 before version 8.0.2 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the jql parameter.	2019-05-03	4.3	<a href="#">CVE-2019-3400</a> MISC
bpcbt -- smartvista	BPC SmartVista 2 has CSRF via SVFE2/pages/admpages/roles/creatorole.jsf.	2019-04-30	6.8	<a href="#">CVE-2018-15206</a> MISC
bpcbt -- smartvista	BPC SmartVista 2 has Improper Access Control in the SVFE module, where it fails to appropriately restrict access: a normal user is able to access the SVFE2/pages/flnadmin/currcnvrate/currcnvrate.jsf functionality that should be only accessible to an admin.	2019-04-30	6.5	<a href="#">CVE-2018-15207</a> MISC
				<a href="#">CVE-2018-</a>

bpcbt -- smartvista	BPC SmartVista 2 has Session Fixation via the JSESSIONID parameter.	2019-04-30	5.1	<a href="#">15208 MISC</a>
buffalo -- open_xdmod	An issue was discovered in Open XDMod through 7.5.0. html/gui/general/login.php has Reflected XSS via the xd_user_formal_name parameter.	2019-05-02	4.3	<a href="#">CVE-2018-16960 MISC</a>
buffalo -- open_xdmod	An issue was discovered in Open XDMod through 7.5.0. html/gui/general/dl_publication.php allows Path traversal via the file parameter, allowing remote attackers to read PDF files in arbitrary directories.	2019-05-02	5.0	<a href="#">CVE-2018-16961 MISC</a>
buffalo -- open_xdmod	An issue was discovered in Open XDMod through 7.5.0. An authentication bypass (account takeover) exists due to a weak password reset mechanism. A brute-force attack against an MD5 rid value requires only 600 guesses in the plausible situation where the attacker knows that the victim has started a password-reset process (pass_reset.php, password_reset.php, XDUser.php) in the past few minutes.	2019-05-02	5.0	<a href="#">CVE-2018-16988 MISC</a>
cisco -- hx220c_af_m5_firmware	A vulnerability in the web-based management interface of Cisco HyperFlex HX-Series could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on an affected system by using a web browser and with the privileges of the user.	2019-05-03	6.8	<a href="#">CVE-2019-1857 CISCO</a>
cisco -- network_registrar	A vulnerability in the web-based management interface of Cisco Prime Network Registrar could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.	2019-05-03	4.3	<a href="#">CVE-2019-1852 CISCO</a>
cisco -- prime_collaboration_assurance	A vulnerability in the web-based management interface of Cisco Prime Collaboration Assurance (PCA) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to the insufficient validation of data supplied by external devices to the web-based management interface of an affected PCA device. An attacker in control of devices integrated with an affected PCA device could exploit this vulnerability by using crafted data in certain fields of the controlled devices. A successful exploit could allow the attacker to execute arbitrary script code in the context of the PCA web-based management interface or allow the attacker to access sensitive browser-based information.	2019-05-03	4.3	<a href="#">CVE-2019-1856 BID CISCO</a>
cisco -- telepresence_video_communication_server	A vulnerability in the management web interface of Cisco Expressway Series could allow an authenticated, remote attacker to perform a directory traversal attack against an affected device. The vulnerability is due to insufficient input validation on the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web interface. A successful exploit could allow the attacker to bypass security restrictions and access the web interface of a Cisco Unified Communications Manager associated with the affected device. Valid credentials would still be required to access the Cisco Unified Communications Manager interface.	2019-05-03	4.0	<a href="#">CVE-2019-1854 CISCO</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 anyone can change the administrator and moderator passwords via the iso.3.6.1.4.1.3212.100.3.2.8.1 and iso.3.6.1.4.1.3212.100.3.2.8.2 OIDs. A remote, unauthenticated attacker can use this vulnerability to change the admin or moderator user's password and gain access to restricted areas on the HTTP interface.	2019-04-30	5.0	<a href="#">CVE-2019-3927 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allow any user to obtain the presentation passcode via the iso.3.6.1.4.1.3212.100.3.2.7.4 OIDs. A remote, unauthenticated attacker can use this vulnerability to access a restricted presentation or to become the presenter.	2019-04-30	5.0	<a href="#">CVE-2019-3928 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allows anyone to bypass the presentation code simply by requesting /images/browserslide.jpg via HTTP. A remote, unauthenticated attacker can use this vulnerability to watch a slideshow without knowing the access code.	2019-04-30	5.0	<a href="#">CVE-2019-3933 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allows anyone to bypass the presentation code sending a crafted HTTP POST request to login.cgi. A remote, unauthenticated attacker can use this vulnerability to download the current slide image without knowing the access code.	2019-04-30	5.0	<a href="#">CVE-2019-3934 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allows anyone to act as a moderator to a slide show via crafted HTTP POST requests to conference.cgi. A remote, unauthenticated attacker can use this vulnerability to start, stop, and disconnect active slideshows.	2019-04-30	6.4	<a href="#">CVE-2019-3935 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 is vulnerable to denial of service via a crafted request to TCP port 389. The request will force the slideshow to transition into a "stopped" state. A remote, unauthenticated attacker can use this vulnerability to stop an active slideshow.	2019-04-30	5.0	<a href="#">CVE-2019-3936 MISC</a>
dhcpcd_project -- dhcpcd	auth.c in dhcpcd before 7.2.1 allowed attackers to infer secrets by performing latency attacks.	2019-04-28	4.3	<a href="#">CVE-2019-11578 BID MISC MISC MISC</a>
dhcpcd_project -- dhcpcd	dhcpc.c in dhcpcd before 7.2.1 contains a 1-byte read overflow with DHO_OPTSOVERLOADED.	2019-04-28	5.0	<a href="#">CVE-2019-11579 BID MISC MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/copyfile.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11806 MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/copydir.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11807 MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/renamefile.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information or make the server	2019-04-30	6.4	<a href="#">CVE-2019-11808 MISC</a>

	unserviceable.			
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/movefile.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information or make the server unserviceable.	2019-04-30	6.4	<a href="#">CVE-2019-11609</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/downloadaddr.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11610</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/download.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11611</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has an arbitrary file deletion vulnerability in /fileman/php/deletefile.php. A remote unauthenticated attacker can exploit this vulnerability to delete arbitrary files.	2019-04-30	6.4	<a href="#">CVE-2019-11612</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/views/ajax/contactView.php. A remote normal registered user could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11613</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/views/ajax/commentView.php. A remote unauthorized attacker could exploit the vulnerability to obtain database sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11614</a> MISC
doorgets -- doorgets_cms	/fileman/php/upload.php in doorGets 7.0 has an arbitrary file upload vulnerability. A remote normal registered user can use this vulnerability to upload backdoor files to control the server.	2019-04-30	6.5	<a href="#">CVE-2019-11615</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /setup/temp/admin.php and /setup/temp/database.php. A remote unauthenticated attacker could exploit this vulnerability to obtain the administrator password.	2019-04-30	5.0	<a href="#">CVE-2019-11616</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a CSRF vulnerability in /doorgets/app/requests/user/configurationRequest.php. A remote attacker can exploit this vulnerability for "Google Analytics code" modification.	2019-04-30	6.8	<a href="#">CVE-2019-11617</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=analytics. A remote background administrator privilege user (or a user with permission to manage configuration analytics) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11619</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/modulecategoryRequest.php. A remote background administrator privilege user (or a user with permission to manage modulecategory) could exploit the vulnerability to obtain database sensitive information via modulecategory_add_titre.	2019-04-30	4.0	<a href="#">CVE-2019-11620</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=network. A remote background administrator privilege user (or a user with permission to manage network configuration) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11621</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/modulecategoryRequest.php. A remote background administrator privilege user (or a user with permission to manage modulecategory) could exploit the vulnerability to obtain database sensitive information via modulecategory_edit_titre.	2019-04-30	4.0	<a href="#">CVE-2019-11622</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=siteweb. A remote background administrator privilege user (or a user with permission to manage configuration siteweb) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11623</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has an arbitrary file deletion vulnerability in /doorgets/app/requests/user/configurationRequest.php. A remote background administrator privilege user can exploit this vulnerability to delete arbitrary files.	2019-04-30	5.5	<a href="#">CVE-2019-11624</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/emailingRequest.php. A remote background administrator privilege user (or a user with permission to manage emailing) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11625</a> MISC
doorgets -- doorgets_cms	routers/ajaxRouter.php in doorGets 7.0 has a web site physical path leakage vulnerability, as demonstrated by an ajax/index.php?url=1234%5c request.	2019-04-30	5.0	<a href="#">CVE-2019-11626</a> MISC
esotalk -- esotalk	esoTalk 1.0.0g4 has XSS via the PATH_INFO to the conversations/ URI.	2019-04-29	4.3	<a href="#">CVE-2015-9285</a> MISC MISC
facebook -- fizz	An improperly performed length calculation on a buffer in PlaintextRecordLayer could lead to an infinite loop and denial-of-service based on user input. This issue affected versions of fizz prior to v2019.03.04.00.	2019-04-29	5.0	<a href="#">CVE-2019-3580</a> MISC
freedesktop -- systemd	It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.	2019-04-26	4.6	<a href="#">CVE-2019-3843</a> BID CONFIRM FEDORA
freedesktop -- systemd	It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.	2019-04-26	4.6	<a href="#">CVE-2019-3844</a> BID CONFIRM
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a NULL pointer dereference in the function rec_rset_get_props at rec-rset.c in librec.a, leading to a crash.	2019-05-01	4.3	<a href="#">CVE-2019-11637</a> MISC MISC
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a NULL pointer dereference in the function rec_field_name_equal_p at rec-field-name.c in librec.a, leading to a crash.	2019-05-01	4.3	<a href="#">CVE-2019-11638</a> MISC MISC
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a stack-based buffer overflow in the function rec_type_check_enum at rec-types.c in librec.a.	2019-05-01	6.8	<a href="#">CVE-2019-11639</a> MISC MISC
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a heap-based buffer overflow in the function rec_fex_parse_str_simple at rec-fex.c in librec.a.	2019-05-01	6.8	<a href="#">CVE-2019-11640</a> MISC MISC

groonga -- groonga-httpd	The groonga-httpd package 6.1.5-1 for Debian sets the /var/log/groonga ownership to the groonga account, which might let local users obtain root access because of unsafe interaction with logrotate. For example, an attacker can exploit a race condition to insert a symlink from /var/log/groonga/httpd to /etc/bash_completion.d. NOTE: this is an issue in the Debian packaging of the Groonga HTTP server.	2019-05-02	6.9	<a href="#">CVE-2019-11675</a> MISC
honeypress_project -- honeypress	HoneyPress through 2016-09-27 can be fingerprinted by attackers because of the ingrained unique www.atxsec.com and ayyimao.wengine.com hostnames within the fake WordPress templates. This allows attackers to discover and avoid this honeypot system.	2019-05-01	5.0	<a href="#">CVE-2019-11633</a> MISC
ibm -- api_connect	IBM API Connect 2018.1 and 2018.4.1.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 155078.	2019-04-29	5.0	<a href="#">CVE-2018-2007</a> CONFIRM XF
ibm -- api_connect	IBM API Connect 2018.1 and 2018.4.1.4 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 155195.	2019-05-02	4.3	<a href="#">CVE-2018-2015</a> BID XF CONFIRM
ibm -- emptoris_contract_management	IBM Emptoris Contract Management 10.0.0 and 10.1.3.0 could disclose sensitive information from detailed information from error messages. IBM X-Force ID: 153657.	2019-04-29	5.0	<a href="#">CVE-2018-1961</a> XF CONFIRM
ibm -- jazz_reporting_service	IBM Jazz Reporting Service (JRS) 6.0.6 could allow an authenticated user to access the execution log files as a guest user, and obtain the information of the server execution. IBM X-Force ID: 156243.	2019-04-29	4.0	<a href="#">CVE-2019-4047</a> BID XF CONFIRM
ibm -- rational_engineering_lifecycle_manager	IBM Rational Engineering Lifecycle Manager 6.0 through 6.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 143798.	2019-05-01	5.0	<a href="#">CVE-2018-1608</a> XF CONFIRM
ibm -- storediq	IBM StoredIQ 7.6 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 158699.	2019-04-30	5.8	<a href="#">CVE-2019-4166</a> CONFIRM BID XF
ilinkp2p_project -- ilinkp2p	The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.	2019-04-26	6.4	<a href="#">CVE-2019-11219</a> MISC
ilinkp2p_project -- ilinkp2p	An authentication flaw in Shenzhen Yunni Technology iLnkP2P allows remote attackers to actively intercept user-to-device traffic in cleartext, including video streams and device credentials.	2019-04-26	4.3	<a href="#">CVE-2019-11220</a> MISC
imagemagick -- imagemagick	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file.	2019-04-29	5.8	<a href="#">CVE-2019-11597</a> BID MISC
imagemagick -- imagemagick	In ImageMagick 7.0.8-40 Q16, there is a heap-based buffer over-read in the function WritePNMImage of coders/pnm.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file. This is related to SetGrayscaleImage in MagickCore/quantize.c.	2019-04-29	5.8	<a href="#">CVE-2019-11598</a> BID MISC
infinitemit -- directadmin	The FileManager in InfinitemIT DirectAdmin through v1.561 has XSS via CMD_FILE_MANAGER, CMD_SHOW_USER, and CMD_SHOW_RESELLER; an attacker can bypass the CSRF protection with this, and take over the administration panel.	2019-04-30	6.8	<a href="#">CVE-2019-11193</a> MISC MISC EXPLOIT-DB
iobit -- malware_fighter	IMFForceDelete.sys in IObit Malware Fighter 6.2 allows a low privileged user to send IOCTL 0x8016E000 along with a user defined string to a file; that file will be promptly deleted regardless of access controls.	2019-04-30	5.5	<a href="#">CVE-2019-6494</a> MISC
jenkins -- ansible_tower	A cross-site request forgery vulnerability in Jenkins Ansible Tower Plugin 0.9.1 and earlier in the TowerInstallation.TowerInstallationDescriptor#doTestTowerConnection form validation method allowed attackers permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins	2019-04-30	6.8	<a href="#">CVE-2019-10310</a> MLIST MISC
jenkins -- ansible_tower	A missing permission check in Jenkins Ansible Tower Plugin 0.9.1 and earlier in the TowerInstallation.TowerInstallationDescriptor#doTestTowerConnection form validation method allowed attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-04-30	4.0	<a href="#">CVE-2019-10311</a> MLIST MISC
jenkins -- ansible_tower	A missing permission check in Jenkins Ansible Tower Plugin 0.9.1 and earlier in the TowerInstallation.TowerInstallationDescriptor#doFillTowerCredentialsIdItems method allowed attackers with Overall/Read permission to enumerate credentials ID of credentials stored in Jenkins.	2019-04-30	4.0	<a href="#">CVE-2019-10312</a> MLIST MISC
jenkins -- aqua_microscanner	Jenkins Aqua MicroScanner Plugin 1.0.5 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system.	2019-04-30	4.0	<a href="#">CVE-2019-10316</a> MLIST MISC
jenkins -- azure_ad	Jenkins Azure AD Plugin 0.3.3 and earlier stored the client secret unencrypted in the global config.xml configuration file on the Jenkins master where it could be viewed by users with access to the master file system.	2019-04-30	4.0	<a href="#">CVE-2019-10318</a> MLIST MISC
jenkins -- github_authentication	Jenkins GitHub Authentication Plugin 0.31 and earlier did not use the state parameter of OAuth to prevent CSRF.	2019-04-30	6.8	<a href="#">CVE-2019-10315</a> MLIST MISC
jenkins -- koji	Jenkins Koji Plugin disables SSL/TLS and hostname verification globally for the Jenkins master JVM.	2019-04-30	4.3	<a href="#">CVE-2019-10314</a> MLIST MISC
jenkins -- self-organizing_swarm_modules	Jenkins Self-Organizing Swarm Plug-in Modules Plugin clients that use UDP broadcasts to discover Jenkins masters do not prevent XML External Entity processing when processing the responses, allowing unauthorized attackers on the same network to read arbitrary files from Swarm clients.	2019-04-30	4.8	<a href="#">CVE-2019-10309</a> MLIST MISC
jenkins -- sitemonitor	Jenkins SiteMonitor Plugin 0.5 and earlier disabled SSL/TLS and hostname verification globally for the Jenkins master JVM.	2019-04-30	4.3	<a href="#">CVE-2019-10317</a> MLIST





mozilla -- firefox	initiated, it is possible to create a modal alert message with this text as the content. This could potentially be used for social engineering attacks. This vulnerability affects Firefox < 66.	2019-04-26	4.3	<a href="#">9807</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If WebRTC permission is requested from documents with data: or blob: URLs, the permission notifications do not properly display the originating domain. The notification states "Unknown origin" as the requestee, leading to user confusion about which site is asking for this permission. This vulnerability affects Firefox < 66.	2019-04-26	5.0	<a href="#">CVE-2019-9808</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If the source for resources on a page is through an FTP connection, it is possible to trigger a series of modal alert messages for these resources through invalid credentials or locations. These messages cannot be immediately dismissed, allowing for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	5.0	<a href="#">CVE-2019-9809</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	6.8	<a href="#">CVE-2019-9810</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Incorrect handling of __proto__ mutations may lead to type confusion in IonMonkey JIT code and can be leveraged for arbitrary memory read and write. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	6.8	<a href="#">CVE-2019-9813</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- network_security_services	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-zero value instead. This results in full malleability of the ClientHello for SSLv2 used for TLS 1.2 in all versions prior to NSS 3.39. This does not impact TLS 1.3.	2019-04-29	4.3	<a href="#">CVE-2018-12384</a> <a href="#">CONFIRM</a>
mozilla -- network_security_services	A cached side channel attack during handshakes using RSA encryption could allow for the decryption of encrypted content. This is a variant of the Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) and affects all NSS versions prior to NSS 3.41.	2019-05-02	4.3	<a href="#">CVE-2018-12404</a> <a href="#">BID</a> <a href="#">MISC</a>
mozilla -- thunderbird	A flaw during verification of certain S/MIME signatures causes emails to be shown in Thunderbird as having a valid digital signature, even if the shown message contents aren't covered by the signature. The flaw allows an attacker to reuse a valid S/MIME signature to craft an email message with arbitrary content. This vulnerability affects Thunderbird < 60.5.1.	2019-04-26	5.0	<a href="#">CVE-2018-18509</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A crash can occur when processing a crafted S/MIME message or an XPI package containing a crafted signature. This can be used as a denial-of-service (DOS) attack because Thunderbird reopens the last seen message on restart, triggering the crash again. This vulnerability affects Thunderbird < 60.5.	2019-04-26	5.0	<a href="#">CVE-2018-18513</a> <a href="#">MISC</a> <a href="#">MISC</a>
netapp -- hyper_converged_infrastructure_compute_node	Element Plug-in for vCenter Server versions prior to 4.2.3 may disclose sensitive account information to an unauthenticated attacker. NetApp HCI Compute Node versions prior to 1.4P2 bundle affected versions of Element Plug-in for vCenter Server.	2019-04-29	5.0	<a href="#">CVE-2019-5492</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
nodebb -- nodebb	Controllers.outgoing in controllers/index.js in NodeBB before 0.7.3 has outgoing XSS.	2019-04-30	4.3	<a href="#">CVE-2019-9286</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
octopus -- octopus_deploy	In Octopus Deploy 2019.1.0 through 2019.3.1 and 2019.4.0 through 2019.4.5, an authenticated user with the VariableViewUnscoped or VariableEditUnscoped permission scoped to a specific project could view or edit unscoped variables from a different project. (These permissions are only used in custom User Roles and do not affect built in User Roles.)	2019-05-01	5.5	<a href="#">CVE-2019-11632</a> <a href="#">MISC</a> <a href="#">MISC</a>
omniauth_project -- omniauth	The request phase of the OmniAuth Ruby gem is vulnerable to Cross-Site Request Forgery when used as part of the Ruby on Rails framework, allowing accounts to be connected without user intent, user interaction, or feedback to the user. This permits a secondary account to be able to sign into the web application as the primary account.	2019-04-26	6.8	<a href="#">CVE-2019-9284</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
phpbb -- phpbb	The fulltext search component in phpBB before 3.2.6 allows Denial of Service.	2019-05-02	5.0	<a href="#">CVE-2019-9826</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
polarisft -- intellect_core_banking	An issue was discovered in the Armor module in Polaris FT Intellect Core Banking 9.7.1. Input passed through the code parameter in three pages as collaterals/colexe3t.jsp and /references/refsuppu.jsp and /references/refbranu.jsp is mishandled before being used in SQL queries, allowing SQL injection with an authenticated session.	2019-04-30	6.5	<a href="#">CVE-2018-14874</a> <a href="#">MISC</a>
polarisft -- intellect_core_banking	An issue was discovered in the Armor module in Polaris FT Intellect Core Banking 9.7.1. CSRF can occur via a /CollatWebApp/gcmsRefInsert?name=SUPP URI.	2019-04-30	6.8	<a href="#">CVE-2018-14930</a> <a href="#">MISC</a>
polarisft -- intellect_core_banking	An issue was discovered in the Core and Portal modules in Polaris FT Intellect Core Banking 9.7.1. An open redirect exists via a /IntellectMain.jsp?IntellectSystem= URI.	2019-04-30	5.8	<a href="#">CVE-2018-14931</a> <a href="#">MISC</a>
projectsend -- projectsend	ProjectSend before r1070 writes user passwords to the server logs.	2019-04-26	5.0	<a href="#">CVE-2019-11492</a> <a href="#">CONFIRM</a>
projectsend -- projectsend	Cross-site scripting (XSS) vulnerability in ProjectSend before r1070 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	4.3	<a href="#">CVE-2019-11533</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
rapid7 -- metasploit	Rapid7 Metasploit Framework suffers from an instance of CWE-22, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in the Zip import function of Metasploit. Exploiting this vulnerability can allow an attacker to execute arbitrary code in Metasploit at the privilege level of the user running Metasploit. This issue affects: Rapid7 Metasploit Framework version 4.14.0 and prior versions.	2019-04-30	6.5	<a href="#">CVE-2019-5624</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
solarwinds -- damewire_mini_remote_control	DWRCC in SolarWinds DameWare Mini Remote Control 10.0 x64 has a Buffer Overflow associated with the size field for the machine name.	2019-05-02	5.0	<a href="#">CVE-2019-9017</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
sonicwall -- global_management_system	A vulnerability in SonicWall Global Management System (GMS), allow a remote user to gain access to the appliance using existing SSH key. This vulnerability affects GMS versions 9.1, 9.0, 8.7, 8.6, 8.4, 8.3 and earlier.	2019-04-26	6.8	<a href="#">CVE-2019-7476</a> <a href="#">CONFIRM</a>

ublock -- ublock	In uBlock before 0.9.5.15, the \$rewrite filter option allows filter-list maintainers to run arbitrary code in a client-side session when a web service loads a script for execution using XMLHttpRequest or Fetch, and the script origin has an open redirect.	2019-04-29	6.8	<a href="#">CVE-2019-11595</a> MISC <a href="#">MISC</a>
w1.fi -- hostapd	The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not validate fragmentation reassembly state properly for a case where an unexpected fragment could be received. This could result in process termination due to a NULL pointer dereference (denial of service). This affects eap_server/eap_server_pwd.c and eap_peer/eap_pwd.c.	2019-04-26	4.3	<a href="#">CVE-2019-11555</a> MLIST MISC MISC MISC
weaver -- e-cology	An issue was discovered in Weaver e-cology 9.0. There is a CRLF Injection vulnerability via the /workflow/request/ViewRequestForwardSPA.jsp isintervenor parameter, as demonstrated by the %0aSet-cookie: substring.	2019-04-30	4.3	<a href="#">CVE-2019-10272</a> MISC CONFIRM
webidsupport -- webid	WeBid 1.2.2 has reflected XSS via the id parameter to admin/deletenews.php, admin/editbannersuser.php, admin/editfaqscategory.php, or admin/excludeuser.php, or the offset parameter to admin/edituser.php.	2019-04-29	4.3	<a href="#">CVE-2019-11592</a> MISC
z.cash -- zcash	Zcash 2.x allows an inexpensive approach to "fill all transactions of all blocks" and "prevent any real transaction from occurring" via a "Sapling Wood-Chipper" attack.	2019-05-01	5.0	<a href="#">CVE-2019-11636</a> MISC MISC
zimbra -- collaboration_server	Zimbra Collaboration Suite before 8.6 patch 13, 8.7.x before 8.7.11 patch 10, and 8.8.x before 8.8.10 patch 7 or 8.8.x before 8.8.11 patch 3 allows SSRF via the ProxyServlet component.	2019-04-30	5.0	<a href="#">CVE-2019-9621</a> MISC MISC MISC MISC MISC CONFIRM EXPLOIT-DB
zohocorp -- manageengine_admanager_plus	Zoho ManageEngine ADManager Plus 6.6 Build 6657 allows local users to gain privileges (after a reboot) by placing a Trojan horse file into the permissive bin directory.	2019-04-30	6.9	<a href="#">CVE-2018-19374</a> MISC
zohocorp -- manageengine_firewall_analyzer	The user defined DNS name in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123224 is vulnerable to stored XSS attacks.	2019-05-02	4.3	<a href="#">CVE-2019-11676</a> MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- application_links	Application Links before version 5.0.11, from version 5.1.0 before 5.2.10, from version 5.3.0 before 5.3.6, from version 5.4.0 before 5.4.12, and from version 6.0.0 before 6.0.4 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the apLinkStartingUrl parameter.	2019-04-30	3.5	<a href="#">CVE-2018-20239</a> MISC
cisco -- application_policy_infrastructure_controller	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. This vulnerability has been fixed in software version 14.1(1i).	2019-05-03	3.5	<a href="#">CVE-2019-1838</a> CISCO
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 stores usernames, passwords, slideshow passcode, and other configuration options in cleartext in the file tmp/scfgdnf. A local attacker can use this vulnerability to recover sensitive data.	2019-04-30	2.1	<a href="#">CVE-2019-3937</a> MISC
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 stores usernames, passwords, and other configuration options in the file generated via the "export configuration" feature. The configuration file is encrypted using the awenc binary. The same binary can be used to decrypt any configuration file since all the encryption logic is hard coded. A local attacker can use this vulnerability to gain access to devices username and passwords.	2019-04-30	2.1	<a href="#">CVE-2019-3938</a> MISC
ibm -- jazz_reporting_service	BM Jazz Reporting Service (JRS) 6.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155006.	2019-04-29	3.5	<a href="#">CVE-2018-2004</a> BID XF CONFIRM
ibm -- planning_analytics	BM Planning Analytics 2.0 through 2.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153177.	2019-05-01	3.5	<a href="#">CVE-2018-1933</a> CONFIRM XF
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 6.0.0.0 and 6.0.0.1 Standard Edition is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159946.	2019-05-01	3.5	<a href="#">CVE-2019-4258</a> CONFIRM XF
imagemagick -- imagemagick	An off-by-one read vulnerability was discovered in ImageMagick before version 7.0.7-28 in the format!PTCfromBuffer function in coders/meta.c. A local attacker may use this flaw to read beyond the end of the buffer or to crash the program.	2019-04-30	3.6	<a href="#">CVE-2019-10131</a> BID CONFIRM CONFIRM
linux -- linux_kernel	The print_binder_ref_olocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading "ref *desc *node" lines in a debugfs file.	2019-04-30	2.1	<a href="#">CVE-2018-20509</a> MISC MLIST
linux -- linux_kernel	The print_binder_transaction_olocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading ""*from *code flags" lines in a debugfs file.	2019-04-30	2.1	<a href="#">CVE-2018-20510</a> BID MISC
philips -- tasy_emr	n Philips Tasy EMR, Tasy EMR Versions 3.02.1744 and prior, the software incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.	2019-05-01	3.5	<a href="#">CVE-2019-6562</a> MISC
polarisft -- intellect_core_banking	An issue was discovered in the Core and Portal modules in Polaris FT Intellect Core Banking 9.7.1. Reflected XSS exists with an authenticated session via the Customerid, formName, FormId, or MODE parameter.	2019-04-30	3.5	<a href="#">CVE-2018-14875</a> MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary	Description	Published	CVSS	Source &
---------	-------------	-----------	------	----------

Vendor -- Product			Score	Patch Info
adblock_plus -- adblock	In AdBlock before 3.45.0, the \$rewrite filter option allows filter-list maintainers to run arbitrary code in a client-side session when a web service loads a script for execution using XMLHttpRequest or Fetch, and the script origin has an open redirect.	2019-04-29	not yet calculated	<a href="#">CVE-2019-11594</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
adblock_plus -- adblock_plus	In Adblock Plus before 3.5.2, the \$rewrite filter option allows filter-list maintainers to run arbitrary code in a client-side session when a web service loads a script for execution using XMLHttpRequest or Fetch, and the script origin has an open redirect.	2019-04-29	not yet calculated	<a href="#">CVE-2019-11593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the WebVPN login process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for existing WebVPN login operations. An attacker could exploit this vulnerability by sending multiple WebVPN login requests to the device. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition.	2019-05-03	not yet calculated	<a href="#">CVE-2018-15388</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the Internet Key Exchange Version 2 Mobility and Multihoming Protocol (MOBIKE) feature for the Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak or a reload of an affected device that leads to a denial of service (DoS) condition. The vulnerability is due to the incorrect processing of certain MOBIKE packets. An attacker could exploit this vulnerability by sending crafted MOBIKE packets to an affected device to be processed. A successful exploit could cause an affected device to continuously consume memory and eventually reload, resulting in a DoS condition. The MOBIKE feature is supported only for IPv4 addresses.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1708</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the Deterministic Random Bit Generator (DRBG), also known as Pseudorandom Number Generator (PRNG), used in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a cryptographic collision, enabling the attacker to discover the private key of an affected device. The vulnerability is due to insufficient entropy in the DRBG when generating cryptographic keys. An attacker could exploit this vulnerability by generating a large number of cryptographic keys on an affected device and looking for collisions with target devices. A successful exploit could allow the attacker to impersonate an affected target device or to decrypt traffic secured by an affected key that is sent to or from an affected target device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1715</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the detection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to send data directly to the kernel of an affected device. The vulnerability exists because the software improperly filters Ethernet frames sent to an affected device. An attacker could exploit this vulnerability by sending crafted packets to the management interface of an affected device. A successful exploit could allow the attacker to bypass the Layer 2 (L2) filters and send data directly to the kernel of the affected device. A malicious frame successfully delivered would make the target device generate a specific syslog entry.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1695</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the TCP processing engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to the improper handling of TCP traffic. An attacker could exploit this vulnerability by sending a specific sequence of packets at a high rate through an affected device. A successful exploit could allow the attacker to temporarily disrupt traffic through the device while it reboots.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1694</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the WebVPN service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper management of authenticated sessions in the WebVPN portal. An attacker could exploit this vulnerability by authenticating with valid credentials and accessing a specific URL in the WebVPN portal. A successful exploit could allow the attacker to cause the device to reload, resulting in a temporary DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1693</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the TCP proxy functionality for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to an error in TCP-based packet inspection, which could cause the TCP packet to have an invalid Layer 2 (L2)-formatted header. An attacker could exploit this vulnerability by sending a crafted TCP packet sequence to the targeted device. A successful exploit could allow the attacker to cause a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1687</a> <a href="#">CISCO</a>
	A vulnerability in the implementation of Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO) for Clientless SSL VPN (WebVPN) and AnyConnect Remote Access VPN in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker			

cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	to successfully establish a VPN session to an affected device. The vulnerability is due to improper credential management when using NT LAN Manager (NTLM) or basic authentication. An attacker could exploit this vulnerability by opening a VPN session to an affected device after another VPN user has successfully authenticated to the affected device via SAML SSO. A successful exploit could allow the attacker to connect to secured networks behind the affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1714</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets sent to an affected device. An attacker could exploit these vulnerabilities by sending a crafted LDAP packet, using Basic Encoding Rules (BER), to be processed by an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1697</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	Multiple vulnerabilities in the WebVPN service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the WebVPN portal of an affected device. The vulnerabilities exist because the software insufficiently validates user-supplied input on an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. An attacker would need administrator privileges on the device to exploit these vulnerabilities.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1701</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_software	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the user has administrative privileges, the attacker could alter the configuration of, extract information from, or reload an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1713</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_software	A vulnerability in the remote access VPN session manager of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the remote access VPN services. The vulnerability is due to an issue with the remote access VPN session manager. An attacker could exploit this vulnerability by requesting an excessive number of remote access VPN sessions. An exploit could allow the attacker to cause a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1705</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- adaptive_security_virtual_appliance_and_firepower_2100_series	A vulnerability in the software cryptography module of the Cisco Adaptive Security Virtual Appliance (ASAv) and Firepower 2100 Series running Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause an unexpected reload of the device that results in a denial of service (DoS) condition. The vulnerability is due to a logic error with how the software cryptography module handles IPsec sessions. An attacker could exploit this vulnerability by creating and sending traffic in a high number of IPsec sessions through the targeted device. A successful exploit could cause the device to reload and result in a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1706</a> <a href="#">CISCO</a>
cisco -- application_policy_infrastructure_controller_software	A vulnerability in the FUSE filesystem functionality for Cisco Application Policy Infrastructure Controller (APIC) software could allow an authenticated, local attacker to escalate privileges to root on an affected device. The vulnerability is due to insufficient input validation for certain command strings issued on the CLI of the affected device. An attacker with write permissions for files within a readable folder on the device could alter certain definitions in the affected file. A successful exploit could allow an attacker to cause the underlying FUSE driver to execute said crafted commands, elevating the attacker's privileges to root on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1682</a> <a href="#">CISCO</a>
cisco -- application_policy_infrastructure_controller_software	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) Software could allow an unauthenticated, remote attacker to access sensitive system usage information. The vulnerability is due to a lack of proper data protection mechanisms for certain components in the underlying Application Centric Infrastructure (ACI). An attacker could exploit this vulnerability by attempting to observe certain network traffic when accessing the APIC. A successful exploit could allow the attacker to access and collect certain tracking data and usage statistics on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1692</a> <a href="#">CISCO</a>
cisco -- application_policy_infrastructure_controller_software	A vulnerability in Cisco Application Policy Infrastructure Controller (APIC) Software could allow an unauthenticated, local attacker with physical access to obtain sensitive information from an affected device. The vulnerability is due to insecure removal of cleartext encryption keys stored on local partitions in the hard drive of an affected device. An attacker could exploit this vulnerability by retrieving data from the physical disk on the affected partition(s). A successful exploit could allow the attacker to retrieve encryption keys, possibly allowing the attacker to further decrypt other data and sensitive information on the device, which could lead to the disclosure of confidential information.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1586</a> <a href="#">BID</a> <a href="#">CISCO</a>



cisco -- email_security_appliance	A vulnerability in certain attachment detection mechanisms of the Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the filtering functionality of an affected device. The vulnerability is due to improper detection of certain content sent to an affected device. An attacker could exploit this vulnerability by sending certain file types without Content-Disposition information to an affected device. A successful exploit could allow an attacker to send messages that contain malicious content to users.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1844</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- firepower_2100_series	A vulnerability in the internal packet-processing functionality of Cisco Firepower Threat Defense (FTD) Software for the Cisco Firepower 2100 Series could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error, which may prevent ingress buffers from being replenished under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to consume all input buffers, which are shared between all interfaces, leading to a queue wedge condition in all active interfaces. This situation would cause an affected device to stop processing any incoming traffic and result in a DoS condition until the device is reloaded manually.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1793</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	Multiple vulnerabilities in the Server Message Block (SMB) Protocol preprocessor detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent or remote attacker to cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1696</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting commands into arguments for a specific command. A successful exploit could allow the attacker to execute commands with root privileges.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1709</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting commands into arguments for a specific command. A successful exploit could allow the attacker to execute commands with root privileges.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1699</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	Multiple vulnerabilities in the Server Message Block (SMB) Protocol preprocessor detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent or remote attacker to cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1704</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	A vulnerability in the TCP ingress handler for the data interfaces that are configured with management access to Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an increase in CPU and memory usage, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient ingress TCP rate limiting for TCP ports 22 (SSH) and 443 (HTTPS). An attacker could exploit this vulnerability by sending a crafted, steady stream of TCP traffic to port 22 or 443 on the data interfaces that are configured with management access to the affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2018-15462</a> <a href="#">CISCO</a>
cisco -- ip_phone_7800_series_and_8800_series_session_initiation_protocol_software	A vulnerability in the call-handling functionality of Session Initiation Protocol (SIP) Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause an affected phone to reload unexpectedly, resulting in a temporary denial of service (DoS) condition. The vulnerability is due to incomplete error handling when XML data within a SIP packet is parsed. An attacker could exploit this vulnerability by sending a SIP packet that contains a malicious XML payload to an affected phone. A successful exploit could allow the attacker to cause the affected phone to reload unexpectedly, resulting in a temporary DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1635</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_application_centric_infrastructure_mode_switch_software	A vulnerability in the filesystem management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an authenticated, local attacker with administrator rights to gain elevated privileges as the root user on an affected device. The vulnerability is due to overly permissive file permissions of specific system files. An attacker could exploit this vulnerability by authenticating to an affected device, creating a crafted command string, and writing this crafted string to a specific file location. A successful exploit could allow the attacker to execute arbitrary operating system commands as root on an affected device. The attacker would need to have valid administrator credentials for the device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1803</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches	A vulnerability in Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an authenticated, remote attacker to access sensitive information. The vulnerability occurs because the affected software does not properly validate user-supplied input. An attacker could exploit this vulnerability by issuing certain commands with filtered query results on the device. This action may cause returned messages to display confidential system information. A successful exploit could allow the attacker to read sensitive information on the device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1587</a> <a href="#">CISCO</a>
	A vulnerability in the system shell for Cisco Nexus 9000			

cisco -- nexus_9000_series_fabric_switches	Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an authenticated, local attacker to use symbolic links to overwrite system files. These system files may be sensitive and should not be overwritable by non-root users. The attacker would need valid device credentials. The vulnerability is due to incorrect symbolic link verification of directory paths when they are used in the system shell. An attacker could exploit this vulnerability by authenticating to the device and providing crafted user input to specific symbolic link CLI commands. Successful exploitation could allow the attacker to overwrite system files that should be restricted. This vulnerability has been fixed in software version 14.1(1i).	2019-05-03	not yet calculated	<a href="#">CVE-2019-1836</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches_in_application_centric_infrastructure_mode_switch_software	A vulnerability in the background operations functionality of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an authenticated, local attacker to gain elevated privileges as root on an affected device. The vulnerability is due to insufficient validation of user-supplied files on an affected device. An attacker could exploit this vulnerability by logging in to the CLI of the affected device and creating a crafted file in a specific directory on the filesystem. A successful exploit could allow the attacker to execute arbitrary operating system commands as root on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1592</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches_in_application_centric_infrastructure_mode_switch_software	A vulnerability in the Transport Layer Security (TLS) certificate validation functionality of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, remote attacker to perform insecure TLS client authentication on an affected device. The vulnerability is due to insufficient TLS client certificate validations for certificates sent between the various components of an ACI fabric. An attacker who has possession of a certificate that is trusted by the Cisco Manufacturing CA and the corresponding private key could exploit this vulnerability by presenting a valid certificate while attempting to connect to the targeted device. An exploit could allow the attacker to gain full control of all other components within the ACI fabric of an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1590</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches_software	A vulnerability in the Trusted Platform Module (TPM) functionality of software for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, local attacker with physical access to view sensitive information on an affected device. The vulnerability is due to a lack of proper data-protection mechanisms for disk encryption keys that are used within the partitions on an affected device hard drive. An attacker could exploit this vulnerability by obtaining physical access to the affected device to view certain cleartext keys. A successful exploit could allow the attacker to execute a custom boot process or conduct further attacks on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1589</a> <a href="#">CISCO</a>
cisco -- small_business_rv320_and_rv325_dual_gigabit_wan_vpn_routers	A vulnerability in the session management functionality of the web-based interface for Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to hijack a valid user session on an affected system. An attacker could use this impersonated session to create a new user account or otherwise control the device with the privileges of the hijacked session. The vulnerability is due to a lack of proper session management controls. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted device. A successful exploit could allow the attacker to take control of an existing user session on the device. Exploitation of the vulnerability requires that an authorized user session is active and that the attacker can craft an HTTP request to impersonate that session.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1724</a> <a href="#">CISCO</a>
cisco -- small_business_switches_software	A vulnerability in the Secure Shell (SSH) authentication process of Cisco Small Business Switches software could allow an attacker to bypass client-side certificate authentication and revert to password authentication. The vulnerability exists because OpenSSH mishandles the authentication process. An attacker could exploit this vulnerability by attempting to connect to the device via SSH. A successful exploit could allow the attacker to access the configuration as an administrative user if the default credentials are not changed. There are no workarounds available; however, if client-side certificate authentication is enabled, disable it and use strong password authentication. Client-side certificate authentication is disabled by default.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1859</a> <a href="#">CISCO</a>
cisco -- umbrella_dashboard	A vulnerability in the session management functionality of the web UI for the Cisco Umbrella Dashboard could allow an authenticated, remote attacker to access the Dashboard via an active, user session. The vulnerability exists due to the affected application not invalidating an existing session when a user authenticates to the application and changes the users credentials via another authenticated session. An attacker could exploit this vulnerability by using a separate, authenticated, active session to connect to the application through the web UI. A successful exploit could allow the attacker to maintain access to the dashboard via an authenticated user's browser session. Cisco has addressed this vulnerability in the Cisco Umbrella Dashboard. No user action is required.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1807</a> <a href="#">CISCO</a>
cisco -- web_security_appliance	A vulnerability in the log subscription subsystem of the Cisco Web Security Appliance (WSA) could allow an authenticated, local attacker to perform command injection and elevate privileges to root. The vulnerability is due to insufficient validation of user-supplied input on the web and command-line interface. An attacker could exploit this vulnerability by authenticating to the affected device and injecting scripting commands in the scope of the log subscription subsystem. A successful exploit could allow	2019-05-03	not yet calculated	<a href="#">CVE-2019-1816</a> <a href="#">CISCO</a>

	the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root.			
cisco -- web_security_appliance	A vulnerability in the web proxy functionality of Cisco AsyncOS Software for Cisco Web Security Appliance could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of HTTP and HTTPS requests. An attacker could exploit this vulnerability by sending a malformed HTTP or HTTPS request to an affected device. An exploit could allow the attacker to cause a restart of the web proxy process, resulting in a temporary DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1817</a> <a href="#">CISCO</a>
cjson -- cjson	parse_string in cJSON.c in cJSON before 2016-10-02 has a buffer over-read, as demonstrated by a string that begins with a " character and ends with a \ character.	2019-04-29	not yet calculated	<a href="#">CVE-2016-10749</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
das_u-boot -- das_u-boot	gen_rand_uuid in lib/uuid.c in Das U-Boot v2014.04 through v2019.04 lacks a srand call, which allows attackers to determine UUID values in scenarios where CONFIG_RANDOM_UUID is enabled, and Das U-Boot is relied upon for UUID values of a GUID Partition Table of a boot device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-11690</a> <a href="#">MISC</a>
dell_emc -- idrac9	Dell EMC iDRAC9 versions prior to 3.30.30.30 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted input data to the WS-MAN interface.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3707</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, internal methods used to prevent arbitrary file overwrites in Appliance Mode were not fully effective. An authenticated attacker with a high privilege level may be able to bypass protections implemented in appliance mode to overwrite arbitrary system files.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6614</a> <a href="#">CONFIRM</a>
f5 -- big-ip	When BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8 are processing certain rare data sequences occurring in PPTP VPN traffic, the BIG-IP system may execute incorrect logic. The TMM may restart and produce a core file as a result of this condition. The BIG-IP system provisioned with the CGNAT module and configured with a virtual server using a PPTP profile is exposed to this vulnerability.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6611</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, DNS query TCP connections that are aborted before receiving a response from a DNS cache may cause TMM to restart.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6612</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, SNMP may expose sensitive configuration objects over insecure transmission channels. This issue is exposed when a passphrase is used with various profile types and is accessed using SNMPv2.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6613</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, administrative users with TMSH access can overwrite critical system files on BIG-IP which can result in bypass of whitelist / blacklist restrictions enforced by appliance mode.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6616</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, Administrator and Resource Administrator roles might exploit TMSH access to bypass Appliance Mode restrictions on BIG-IP systems.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6615</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, a user with the Resource Administrator role is able to overwrite sensitive low-level files (such as /etc/passwd) using SFTP to modify user permissions, without Advanced Shell access. This is contrary to our definition for the Resource Administrator (RA) role restrictions.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6617</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, users with the Resource Administrator role can modify sensitive portions of the filesystem if provided Advanced Shell Access, such as editing /etc/passwd. This allows modifications to user objects and is contrary to our definition for the Resource Administrator (RA) role restrictions.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6618</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, the Traffic Management Microkernel (TMM) may restart when a virtual server has an HTTP/2 profile with Application Layer Protocol Negotiation (ALPN) enabled and it processes traffic where the ALPN extension size is zero.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6619</a> <a href="#">CONFIRM</a>
facebook_technologies -- oculus_browser_ui	A remote web page could inject arbitrary HTML code into the Oculus Browser UI, allowing an attacker to spoof UI and potentially execute code. This affects the Oculus Browser starting from version 5.2.7 until 5.7.11.	2019-04-29	not yet calculated	<a href="#">CVE-2019-3562</a> <a href="#">MISC</a>
filezilla_project -- filezilla	Untrusted search path in FileZilla before 3.41.0-rc1 allows an attacker to gain privileges via a malicious 'fzsfip' binary in the user's home directory.	2019-04-29	not yet calculated	<a href="#">CVE-2019-5429</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lantronix -- securelinux_spider_devices	Lantronix SecureLinux Spider (SLS) 2.2+ devices have XSS in the auth.asp login page.	2019-05-02	not yet calculated	<a href="#">CVE-2018-10383</a> <a href="#">MISC</a>
lenovo -- xclarity_administrator	An internal product security audit of Lenovo XClarity Administrator (LXCA) discovered HTTP proxy credentials being written to a log file in clear text. This only affects LXCA when HTTP proxy credentials have been configured. This affects LXCA versions 2.0.0 to 2.3.x.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6158</a> <a href="#">MISC</a>
microfocus -- open_enterprise_server	A DOM based XSS vulnerability has been identified in the Netstorage component of Open Enterprise Server (OES) allowing a remote attacker to execute javascript in the victims browser by tricking the victim into clicking on a specially crafted link. This affects OES versions OES2015SP1, OES2018, and OES2018SP1. Older versions may be affected but were not tested as they are out of support.	2019-05-02	not yet calculated	<a href="#">CVE-2019-3490</a> <a href="#">MISC</a>

mozilla -- bugzilla	A third party website can access information available to a user with access to a restricted bug entry using the image generation in report.cgi in all Bugzilla versions prior to 4.4.	2019-04-29	not yet calculated	<a href="#">CVE-2018-5123</a> <a href="#">CONFIRM</a>
national_center_for_biotechnology_information -- toolbox	A heap-based buffer overflow exists in nph-viewgif.cgi in the 2.0.7 through 2.2.26 legacy versions of the NCBI ToolBox.	2019-05-02	not yet calculated	<a href="#">CVE-2018-16717</a> <a href="#">MISC</a>
national_center_for_biotechnology_information -- toolbox	An XSS vulnerability exists in wwwblast.c in the 2.0.7 through 2.2.26 legacy versions of the NCBI ToolBox via a crafted -z1 argument.	2019-05-02	not yet calculated	<a href="#">CVE-2018-16718</a> <a href="#">MISC</a>
national_center_for_biotechnology_information -- toolbox	A path traversal vulnerability exists in viewcgi.c in the 2.0.7 through 2.2.26 legacy versions of the NCBI ToolBox, which may result in reading of arbitrary files (i.e., significant information disclosure) or file deletion via the nph-viewgif.cgi query string.	2019-05-02	not yet calculated	<a href="#">CVE-2018-16716</a> <a href="#">MISC</a>
national_electrical_manufacturers_association -- digital_imaging_and_communications_in_medicine_part_10_file_format	An issue was discovered in the DICOM Part 10 File Format in the NEMA DICOM Standard 1995 through 2019b. The preamble of a DICOM file that complies with this specification can contain the header for an executable file, such as Portable Executable (PE) malware. This space is left unspecified so that dual-purpose files can be created. (For example, dual-purpose TIFF/DICOM files are used in digital whole slide imaging for applications in medicine.) To exploit this vulnerability, someone must execute a maliciously crafted file that is encoded in the DICOM Part 10 File Format. PE/DICOM files are executable even with the .dcm file extension. Anti-malware configurations at healthcare facilities often ignore medical imagery. Also, anti-malware tools and business processes could violate regulatory frameworks (such as HIPAA) when processing suspicious DICOM files.	2019-05-02	not yet calculated	<a href="#">CVE-2019-11687</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
node-tar -- node-tar	A vulnerability was found in node-tar before version 4.4.2. An Arbitrary File Overwrite issue exists when extracting a tarball containing a hardlink to a file that already exists on the system, in conjunction with a later plain file with the same name as the hardlink. This plain file content replaces the existing file content.	2019-04-30	not yet calculated	<a href="#">CVE-2018-20834</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
php -- php	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.	2019-05-03	not yet calculated	<a href="#">CVE-2019-11036</a> <a href="#">MISC</a>
php -- php	In PHP imagick extension in versions between 3.3.0 and 3.4.4, writing to an array of values in ImagickKernel::fromMatrix() function did not check that the address will be within the allocated array. This could lead to out of bounds write to memory if the function is called with the data controlled by untrusted party.	2019-05-03	not yet calculated	<a href="#">CVE-2019-11037</a> <a href="#">MISC</a>
qliktech_international -- qlikview_server_and_qlik_sense_enterprise_and_qlik_analytics_platform	An issue was discovered in QlikView Server before 11.20 SR19, 12.00 and 12.10 before 12.10 SR11, 12.20 before SR9, and 12.30 before SR2; and Qlik Sense Enterprise and Qlik Analytics Platform installations that lack these patch levels: February 2018 Patch 4, April 2018 Patch 3, June 2018 Patch 3, September 2018 Patch 4, November 2018 Patch 4, or February 2019 Patch 2. An authenticated user may be able to bypass intended file-read restrictions via crafted Browser requests.	2019-04-30	not yet calculated	<a href="#">CVE-2019-11628</a> <a href="#">MISC</a>
rockwell_automation -- compactlogix_and_compact_guardlogix_and_armor_compact_guardlogix_controllers	An attacker could send a crafted HTTP/HTTPS request to render the web server unavailable and/or lead to remote code execution caused by a stack-based buffer overflow vulnerability. A cold restart is required for recovering CompactLogix 5370 L1, L2, and L3 Controllers, Compact GuardLogix 5370 controllers, and Armor Compact GuardLogix 5370 Controllers Versions 20 to 30.014 and earlier systems.	2019-05-01	not yet calculated	<a href="#">CVE-2019-10952</a> <a href="#">BID</a> <a href="#">MISC</a>
rockwell_automation -- compactlogix_and_compact_guardlogix_and_armor_compact_guardlogix_controllers	An attacker could send crafted SMTP packets to cause a denial-of-service condition where the controller enters a major non-recoverable faulted state (MNRF) in CompactLogix 5370 L1, L2, and L3 Controllers, Compact GuardLogix 5370 controllers, and Armor Compact GuardLogix 5370 Controllers Versions 20 to 30.014 and earlier.	2019-05-01	not yet calculated	<a href="#">CVE-2019-10954</a> <a href="#">BID</a> <a href="#">MISC</a>
tar-fs -- tar-fs	A vulnerability was found in tar-fs before 1.16.2. An Arbitrary File Overwrite issue exists when extracting a tarball containing a hardlink to a file that already exists on the system, in conjunction with a later plain file with the same name as the hardlink. This plain file content replaces the existing file content.	2019-04-30	not yet calculated	<a href="#">CVE-2018-20835</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wangle -- wangle	Wangle's LineBasedFrameDecoder contains logic for identifying newlines which incorrectly advances a buffer, leading to a potential underflow. This affects versions of Wangle prior to v2019.04.22.00	2019-04-29	not yet calculated	<a href="#">CVE-2019-3563</a> <a href="#">MISC</a>
wildfly -- wildfly	A flaw was discovered in wildfly versions up to 16.0.0.Final that would allow local users who are able to execute init.d script to terminate arbitrary processes on the system. An attacker could exploit this by modifying the PID file in /var/run/boss-eap/ allowing the init.d script to terminate any process as root.	2019-05-03	not yet calculated	<a href="#">CVE-2019-3805</a> <a href="#">CONFIRM</a>
wildfly -- wildfly	It was discovered that the ElytronManagedThread in Wildfly's Elytron subsystem in versions from 11 to 16 stores a SecurityIdentity to run the thread as. These threads do not necessarily terminate if the keep alive time has not expired. This could allow a shared thread to use the wrong security identity when executing.	2019-05-03	not yet calculated	<a href="#">CVE-2019-3894</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The WebDorado Contact Form Builder plugin before 1.0.69 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11557</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WebDorado Contact Form plugin before 1.13.5 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a	2019-04-29	not yet calculated	<a href="#">CVE-2019-11591</a> <a href="#">MISC</a>

	discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.			MISC MISC
wordpress -- wordpress	Server Side Request Forgery (SSRF) exists in the Print My Blog plugin before 1.6.7 for WordPress via the site parameter.	2019-04-27	not yet calculated	CVE-2019-11565 MISC MISC MISC MISC MISC
wordpress -- wordpress	The 10Web Form Maker plugin before 1.13.5 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.	2019-04-29	not yet calculated	CVE-2019-11590 MISC MISC MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nssa.us-cert.gov to your address book.

OTHER RESOURCES  
[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED  


SUBSCRIBER SERVICES  
[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [tmcgrinnis@sunnyvale.ca.gov](mailto:tmcgrinnis@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 25 Murray Lane SW Bldg 10 · Washington, DC 20568 · (888) 282-0870





IN THE BEGINNING...After John called the City of Santa Clara about Mister Olenak trying to poison neighborhood ducks with bleach; three Santa Clara police officers (including Gabby Seagrave and Pablo Lopez) responded even though John did not call the police. Mister Olenak was angry about being exposed; then made criminal threats that he later followed up on and admitted to in court.

View the complaint filed by John: <http://likroper.com/SCAN0027.JPG> --  
<http://likroper.com/SCAN0026.JPG> -- <http://likroper.com/SCAN0027.JPG> --  
<http://likroper.com/SCAN0029.JPG> -- <http://likroper.com/SCAN0030.JPG> --  
<http://likroper.com/SCAN0031.JPG> -- <http://likroper.com/SCAN0032.JPG> --  
<http://likroper.com/SCAN0033.JPG> -- <http://likroper.com/SCAN0034.JPG> --  
<http://likroper.com/SCAN0035.JPG> -- <http://likroper.com/SCAN0036.JPG> --  
<http://likroper.com/SCAN0037.JPG> -- <http://likroper.com/SCAN0038.JPG> --  
<http://likroper.com/SCAN0039.JPG>

In a nutshell: John was repeatedly and continually harassed for a number of years since getting involved in Santa Clara and/or Sunnyvale politics (go to: <http://addendumblog1.blogspot.com/2013/12/the-city-of-santa-clara-1333-lawrence.html>) and/or filing a complaint against the Santa Clara Police department in 2007; where it appears John was ambushed by two vehicles laying in wait for him to return home; an ambush that was ultimately foiled by the high speed John was traveling on his bicycle at the time; and a cell phone deployed during the drive-by attack -- a cell phone which took no photos but which worked as a deterrent to scatter the criminals involved in this malicious late-night vandalism and near vehicular manslaughter.

John is about 99.9 percent certain the individuals involved in the night time attack were essentially put up to it by rogue members of the Santa Clara police department (Pablo Lopez; Don Paolinetti etc) seeking revenge for John's complaint filing.

Note: Adding to this; the Rebholtz family's daughter (who was also conspiratorially involved in the harassment and/or stalking of John (GO TO: <http://addendumblog1.blogspot.com/2013/09/stalking-by-rebholtzs-daughter.html>) used what was essentially a false flag incident with segment and/or incident (GO TO: <https://www.youtube.com/watch?v=xzXCvv9g9eI>) adding on an extra layer of bullshit and/or negligence; as this false flag incident then spiraled out of control and turned into opportunistic and/or malicious false allegations by the Rebholtz's daughter; allegations she obviously made up based around this false flag incident.

Johns' neighbor Jane looked out her window one day to see a sniper in her backyard pointing a rifle towards Johns' residence FOR PICKING UP LITTER IN THE NEIGHBORHOOD!?! Let me say this again; THERE WAS A SNIPER IN JANES' BACKYARD BECAUSE JOHN WAS PICKING UP LITTER IN THE NEIGHBORHOOD; AND SUNNYVALE DPS HAD TONS OF PRIOR KNOWLEDGE ABOUT JOHNS' VOLUNTEER WEEKLY CLEANUP ACTIVITY! This kind of unnecessary "GI-JOE bullshit" is essentially what emboldened Rebholtz's daughter. > Question: Why was Steve Henson at the Peterson field only the day of the SWAT team raid just before it occurred and never again since? Did Steve Henson have anything to do with this raid? GO TO: NEIGHBORHOOD COPWATCH: RESIDENCE ALMOST STORMED AND 'SUSPECT' SHOT AT FOR PICKING UP LITTER? @ <https://www.youtube.com/watch?v=xzXCvv9g9eI>

Between a SWAT team being called for feeding ducks and cleaning up litter on two separate incidents (GO TO: <https://www.youtube.com/watch?v=xzXCvv9g9eI>); an angry and scorned Jun or High School principal with an agenda against whistle blowers trying to criminalize John for helping someone cross the street (GO TO: <http://addendumblog2.blogspot.com/2016/06/petition-to-terminate-employment-of.html>); and a slanderous, self-righteous supposed "social worker" trying to have John arrested for caring a little too much for his dying cat Buster (GO TO: <http://addendumblog2.blogspot.com/2016/09/the-first-amendment-of-united-states.html> + <http://addendumblog2.blogspot.com/2016/10/rest-in-peace-buster-cat.html>); John does not have to deal with and/or seriously acknowledge seemingly psychopathic and/or crazy fucking diots like this.

QUESTIONABLE RESTRAINING ORDER COPIES -- these are copies of the temporary restraining order issued by Mrs. Rebholtz etc; clearly showing how John made a concerted effort to bring an end to the harassment he was experiencing for a

number of years at that time. (go to: <http://likroper.com/SCAN0008.JPG> + <http://likroper.com/SCAN0006.JPG> + <http://likroper.com/SCAN0007.JPG>)  
QUESTION: How could this obvious evidence of John being harassed up to one year before this event have been overlooked? This misleading court filing is OBVIOUS evidence of the harassment John experienced; so why did the court system not act upon this at the onset and set try to the record straight? Did Judge Manoukian even read the transcripts? And if so; how could Judge Manoukian have overlooked this evidence?



THIS FLYER SHOWING PRIOR KNOWLEDGE OF EVENTS WAS ON FILE AT THE SANTA CLARA POLICE DEPARTMENT FOR ROUGHLY ONE YEAR PRIOR TO THE JUNE 2011 INCIDENT

GO TO: OBSTRUCTION OF JUSTICE AND/OR DOMESTIC TERRORISM AND/OR FELONY STALKING AND/OR UNCIVIL HARASSMENT (CONTINUED) @ <http://addendumblog1.blogspot.com/2015/08/obstruction-of-justice-and-or-domestic.html> + OBSTRUCTION OF JUSTICE: PRIOR KNOWLEDGE OF EVENTS AND/OR ILLEGALLY SUPPRESSED EVIDENCE BY THE SANTA CLARA POLICE DEPARTMENT IN JUNE 2010 AND/OR THE SUNNYVALE POLICE DEPARTMENT IN JUNE 2011 @ <http://addendumblog1.blogspot.com/2013/11/prior-knowledge-of-events-and-or.html>

Steve Henson and his son witnessed Jake Paolinetti and his friends (including at least one Rebholtz family member) yelling loudly and honking while driving by John's house at around 10 PM in early June 2010; leading to the flyer that went around the neighborhood to 40 or so houses, warning them of the attacks (note: a conversation between John and Steve Henson discussing the events in question can be heard @ <http://likroper.com/Voice0006.amr>)

SEE ALSO: CAUSE AND EFFECT AND/OR ACTION-REACTION? @ <http://addendumblog1.blogspot.com/2015/09/cause-and-effect-and-or-action-reaction.html>

It is obvious the Rebholtz family conspired and/or colluded with Officer Don Paolinetti and/or the members of the Paolinetti family to cover up and/or suppress evidence regarding what had been happening to John for over a year at that time. Mrs. Rebholtz told John "I don't think you're a criminal"; failing to realize she just made herself a conspiratorial criminal by obstructing justice with her son. Perhaps the main problem we are confronting at this moment in time is our society has a hard time criminalizing soccer mom types like Hillary Clinton and/or Mrs. Rebholtz.

NOTE: While this action is not necessarily about appealing this (sham) restraining order; if there is any appeal of sorts of the questionable June 2011 restraining order served; it would be in the bait-and-switch nature where it clearly says that John "cannot come near the house" (which John only did one time last year to tell Mrs Rebholtz of the harassment John had been experiencing over the years) conflicted by another part of the order which says John can come over to the house and talk to them if done in a civil manner (which he has no intentions of ever doing and only did to tell Mrs. Rebholtz to keep her idiot sons away from Johns' place of residence). This is a confusing dialogue that could easily turn ugly if followed by John. John had to do what he did on that June 2011 day to end the harassment; as John in a sense "shook the shit bag" until all of the shit came out -- as nothing else would have stopped this rampant abuse which continued long thereafter. (GO TO: INCIDENT ON 15 DECEMBER 2013 -- EV 133490020 @

<http://addendumblog1.blogspot.com/2014/07/various-criminal-andor-illegal-cover.html> + EX-SUNNYVALE DEPARTMENT OF PUBLIC SAFETY (DPS) OFFICER MATTHEW BENINGER & SON ETC @ <http://addendumblog2.blogspot.com/2016/10/ex-police-officer-matthew-beninger.html> + ALL OTHER RELATED LINKS CAN BE SEEN @ <http://ireblogger.blogspot.com/2016/11/all-other-related-links.html> + <http://addendumblog1.blogspot.com/> + <http://addendumblog2.blogspot.com/>

Deb Squadrito wrote: "I filed a corruption complaint against the Santa Clara Sheriffs Dept. 16 years ago!! Nothing was done. They go beyond corruption. They repeatedly covered up complaints about one of their officers sexually assaulting and harassing women. This allowed the officer to get away with it for over 10 years, till I had him arrested. But it did not end there. After he was arrested several (not all) did their best to destroy evidence. In the end I was victorious in getting a conviction. No federal investigation though. I had to give up my home (owned free and clear) and hide in another state before trial due to death threats after they told me "We cant protect you" They are like the mob..." GO TO: <https://www.facebook.com/Santa-Clara-County-Crime-Family-499882993459818/>

"I have had personal experience with this corrupt judge....this is REAL!..." "He is also in bed with slumlords...he is a bad guy..." "I will give you a name...Paul Pries." "You can also look into code enforcement, I know there is a paper trail...the aforementioned judge is complicit..." "Ah huh! Cedar Glen Apartments 2275 S Bascom Ave!!!!" "and many more...and I see now he is acquiring more property with the aid of the redevelopment agency...it's shameful. I would look for ties familial or religious (Greek orthodox). They think the people are stupid..." " You're in deep with these guys, I hope you know. Prayers sent..." -- ANONYMOUS

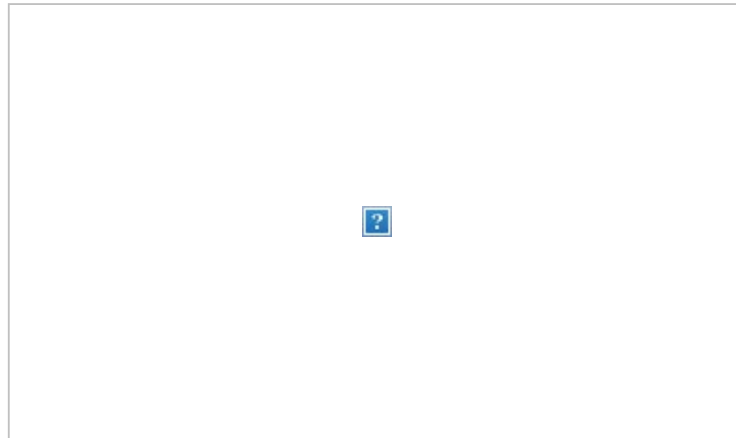
QUESTION: "And this property is being acquired with Judge Manoukian's help? Illegally?"  
-- SANTA CLARA COUNTY CRIME FAMILY

GO TO: "<http://pdfsr.com/pdf/suspicious-transactions-by-santa-clara-county-superior-court-judge-socrates-peter-manoukian-possible>" / "<http://pdfsr.com/pdf/paul-pries-transanactions-santa-clara-county-grantor-grantee-index.pdf>" / "<https://www.bizapedia.com/addresses/1845-dry-creek-rd-campbell-ca-95008.html>" / "<http://pdfsr.com/pdf/maria-pries-financial-transactions-santa-clara-county-california-possibly-in-collusion-with-judge-so>" / "<http://pdfsr.com/pdf/terry-pries-financial-transactions-santa-clara-county-grantor-grantee-index-possible-collusion-with>" -- SANTA CLARA COUNTY CRIME FAMILY + SEE ALSO: <http://likroper.com/PRIES1.jpg>

UPDATE: 29 july 2017 / THE PLOT THICKENS: Why is Santa Clara County Hiding Death and Crime? @ <http://www.uglyjudge.com/santa-clara-county-hiding-death-crime/>

On Thu, Apr 25, 2019 at 11:51 AM Johnny Roper <[jclefstad@gmail.com](mailto:jclefstad@gmail.com)> wrote:

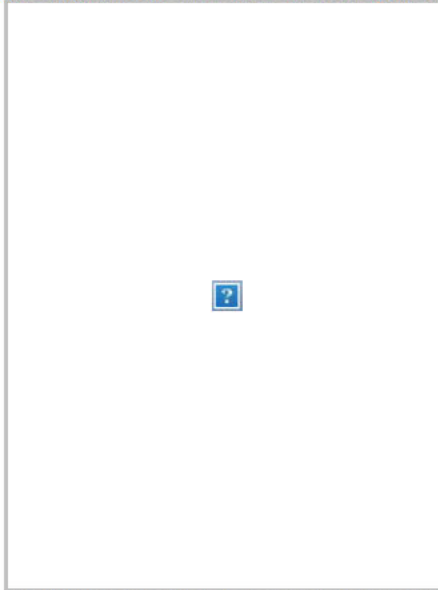
## THANKS FOR NOTHING / PART II -- MOTION FOR EXPUNGEMENT AND/OR FACTUAL INNOCENCE



Part of John's message to Mr. Struble was "You will (likely) be charged with attempted vehicular manslaughter. Merry Xmas" (the word likely was left out) Note: Johns' brother was killed roughly one year after on Christmas Eve by a man named Danny Matos; who was charged with vehicular manslaughter!?!). > **GO TO: REST IN PEACE MOM AND BROTHER CARL @ <http://addendumblog1.blogspot.com/2014/03/rest-in-peace-mom-and-brother-carl.html>**

1) The first time John called the Sunnyvale D.P.S. after being attacked in the street was back in December 1998. Three Sunnyvale D.P.S. officers responded; and Mister Struble corroborated the story when he was called at work by Officer Discher. A few days later; John was given a temporary restraining order from Officer Beninger; who never spoke to Officer Discher about the event.

When Officer Beninger was asked whether or not he spoke to Officer Discher; he responded with "Who's Discher?" The female judge in charge of the case was suspicious of Officer Beninger; suggesting that this was instead a "neighborhood matter".



John had the heavily redacted 911 readout and an email document from the City of Sunnyvale (see photos above); but never showed it to the judge due to coercion and intimidation on the part of the Strubles. Note: Even though John had actually played drums in large arenas before this event; John was still shy when it came to public speaking – but since then John has started singing karaoke; and this has made John an absolutely fearless speaker. > go to: <https://www.youtube.com/user/LIKROPER>

NOTE: Sunnyvale D.P.S. Officers Smith and Ochoa violated John's civil rights by ordering John to leave the Oasis Nightclub without pulling up surveillance footage showing John being attacked in front of the club by Doug Ward. John had attended this same nightclub and sat in the same seat for over ten years at the time; making this incident as bad and/or worse than anything Rosa Parks ever encountered. > **GO TO: OFFICERS SMITH AND OCHOA @** <http://addendumblog1.blogspot.com/2013/04/officers-smith-and-ochoa.html>

**GO TO: INCIDENT #EV-98-112345 / MISTER STRUBLE @**

<http://addendumblog1.blogspot.com/search?q=struble>

2) The second outstanding incident in question occurred when Mister Olenak was laying in wait to attack John at around 6 AM one morning. John fed the ducks across the street where he had for many years; and was then followed back to his house and attacked by Mister Olenak.

John called the police and was treated by the responding Officers as if he did something wrong; even though John had worked with both cities to install the duck crossing signs on his street; and had even gotten permission to feed ducks from now ex-Santa Clara mayor Judy Nadler. To make a long story short; an administrative hearing was scheduled where Mister Olenak admitted to attacking John in front of an entire room full of witnesses; including Officers Pablo Lopez and Gabrielle Seagrave; and Judge Louis Amadeo Junior – who took no action to bring justice to this unusual situation. Note: Tom Foley was used as a "witness to duck feeding" at this particular hearing.

**GO TO: STATE LAW CROSSWALK SIGN NEEDED ON DUNFORD WAY IN SUNNYVALE,**



From: [US-CERT](mailto:us-cert@cisecurity.com)  
To: [us-cert@cisecurity.com](mailto:us-cert@cisecurity.com)  
Subject: SB19-126: Vulnerability Summary for the Week of April 29, 2019  
Date: Monday, May 06, 2019 12:12:11 PM



National Cyber Awareness System:

## SB19-126 Vulnerability Summary for the Week of April 29, 2019

05/06/2019 06:52 AM EDT

Original release date: May 06, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology \(NIST\) National Vulnerability Database \(NVD\)](#) in the past week. The NVD is sponsored by the [Department of Homeland Security \(DHS\) National Cybersecurity and Communications Integration Center \(NCCIC\)](#) / [United States Computer Emergency Readiness Team \(US-CERT\)](#). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System \(CVSS\)](#) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database \(NVD\)](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
barco -- wepresent_wipg-1000p_firmware	The Crestron AM-100 firmware 1.6.0.2, Crestron AM-101 firmware 2.7.0.1, Barco wePresent WIPG-1000P firmware 2.3.0.10, Barco wePresent WIPG-1600W before firmware 2.4.1.19, Extron ShareLink 200/250 firmware 2.0.3.4, Teq AV IT WIPS710 firmware 1.1.0.7, SHARP PN-L703WA firmware 1.4.2.3, Optoma WPS-Pro firmware 1.0.0.5, Blackbox HD WPS firmware 1.0.0.5, InFocus LiteShow3 firmware 1.0.16, and InFocus LiteShow4 2.0.0.7 are vulnerable to command injection via the file_transfer.cgi HTTP endpoint. A remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.	2019-04-30	10.0	<a href="#">CVE-2019-3929</a> MISC <a href="#">EXPLOIT-DB</a> MISC
barco -- wepresent_wipg-1000p_firmware	The Crestron AM-100 firmware 1.6.0.2, Crestron AM-101 firmware 2.7.0.1, Barco wePresent WIPG-1000P firmware 2.3.0.10, Barco wePresent WIPG-1600W before firmware 2.4.1.19, Extron ShareLink 200/250 firmware 2.0.3.4, Teq AV IT WIPS710 firmware 1.1.0.7, SHARP PN-L703WA firmware 1.4.2.3, Optoma WPS-Pro firmware 1.0.0.5, Blackbox HD WPS firmware 1.0.0.5, InFocus LiteShow3 firmware 1.0.16, and InFocus LiteShow4 2.0.0.7 are vulnerable to a stack buffer overflow in libAwgCgi.so's PARSErtoCHAR function. A remote, unauthenticated attacker can use this vulnerability to execute arbitrary code as root via a crafted request to the return.cgi endpoint.	2019-04-30	10.0	<a href="#">CVE-2019-3930</a> MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v1 TCLinux Fw \$7.3.15.0 v001 / 3.40(ULM.0)b31 router distributed by TrueOnline has a command injection vulnerability in the Remote System Log forwarding function, which is accessible by an unauthenticated user. The vulnerability is in the ViewLog.asp page and can be exploited through the remote_host parameter.	2019-05-02	10.0	<a href="#">CVE-2017-18368</a> MISC MISC MISC MISC
billion -- 5200w-t_firmware	The Billion 5200W-T 1.02b.rc5.d49 router distributed by TrueOnline has a command injection vulnerability in the Remote System Log forwarding function, which is accessible by an unauthenticated user. The vulnerability is in the adv_remotelog.asp page and can be exploited through the syslogServerAddr parameter.	2019-05-02	10.0	<a href="#">CVE-2017-18369</a> MISC MISC MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v2 TCLinux Fw \$7.3.37.6 router distributed by TrueOnline has a command injection vulnerability in the Remote System Log forwarding function, which is only accessible by an authenticated user. The vulnerability is in the logSet.asp page and can be exploited through the ServerIP parameter. Authentication can be achieved by exploiting CVE-2017-18371.	2019-05-02	9.0	<a href="#">CVE-2017-18370</a> MISC MISC MISC MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v2 TCLinux Fw \$7.3.37.6 router distributed by TrueOnline has three user accounts with default passwords, including two hardcoded service accounts: one with the username true and password true, and another with the username supervisor and password ziad1234. These accounts can be used to login to the web interface, exploit authenticated command injections, and change router settings for malicious purposes.	2019-05-02	7.5	<a href="#">CVE-2017-18371</a> MISC MISC MISC MISC
billion -- 5200w-t_firmware	The Billion 5200W-T TCLinux Fw \$7.3.8.0 v008 130603 router distributed by TrueOnline has a command injection vulnerability in the Time Setting function, which is only accessible by an authenticated user. The vulnerability is in the tools_time.asp page and can be exploited through the uiViewSNTPServer parameter. Authentication can be achieved by exploiting CVE-2017-18373.	2019-05-02	9.0	<a href="#">CVE-2017-18372</a> MISC MISC MISC
billion -- 5200w-t_firmware	The Billion 5200W-T TCLinux Fw \$7.3.8.0 v008 130603 router distributed by TrueOnline has three user accounts with default passwords, including two hardcoded service accounts: one with the username true and password true, and another with the username user3 and a long password consisting of a repetition of the string 0123456789. These accounts can be used to login to the web interface, exploit authenticated command injections, and change router settings for malicious purposes.	2019-05-02	9.0	<a href="#">CVE-2017-18373</a> MISC MISC MISC
billion -- 5200w-t_firmware	The ZyXEL P660HN-T1A v1 TCLinux Fw \$7.3.15.0 v001 / 3.40(ULM.0)b31 router distributed by TrueOnline has two user accounts with default passwords, including a hardcoded service account with the username true and password true. These accounts can be used to login to the web interface, exploit authenticated command injections and change router settings for malicious purposes.	2019-05-02	9.0	<a href="#">CVE-2017-18374</a> MISC MISC MISC MISC
checkpoint -- endpoint_security	A local attacker can create a hard-link between a file to which the Check Point Endpoint Security client for Windows before E80.96 writes and another BAT file, then by impersonating the WPAD server, the attacker can write BAT commands into that file that will later be run by the user or the system.	2019-04-29	7.2	<a href="#">CVE-2019-8454</a> MISC
cisco -- nexus_93108tc-ex_firmware	A vulnerability in the SSH key management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, remote attacker to connect to the affected system with the privileges of the root user. The vulnerability is due to the presence of a default SSH key pair that is present in all devices. An attacker could	2019-05-03	10.0	<a href="#">CVE-2019-1804</a>



	exploit this vulnerability by opening an SSH connection via IPv6 to a targeted device using the extracted key materials. An exploit could allow the attacker to access the system with the privileges of the root user. This vulnerability is only exploitable over IPv6; IPv4 is not vulnerable.			<a href="#">CISCO</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to command injection via SNMP OID iso.3.6.1.4.1.3212.100.3.2.9.3. A remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.	2019-04-30	10.0	<a href="#">CVE-2019-3925 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to command injection via SNMP OID iso.3.6.1.4.1.3212.100.3.2.14.1. A remote, unauthenticated attacker can use this vulnerability to execute operating system commands as root.	2019-04-30	10.0	<a href="#">CVE-2019-3926 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to argument injection to the curl binary via crafted HTTP requests to return.cgi. A remote, authenticated attacker can use this vulnerability to upload files to the device and ultimately execute code as root.	2019-04-30	9.0	<a href="#">CVE-2019-3931 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 are vulnerable to authentication bypass due to a hard-coded password in return.tgi. A remote, unauthenticated attacker can use this vulnerability to control external devices via the uart_bridge.	2019-04-30	7.5	<a href="#">CVE-2019-3932 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 use default credentials admin/admin and moderator/moderator for the web interface. An unauthenticated, remote attacker can use these credentials to gain privileged access to the device.	2019-04-30	7.5	<a href="#">CVE-2019-3939 MISC</a>
dell -- idrac6_firmware	Dell EMC iDRAC6 versions prior to 2.92, iDRAC7/iDRAC8 versions prior to 2.61.60.60, and DRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22 and 3.23.23.23 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may potentially exploit his vulnerability to crash the webserver or execute arbitrary code on the system with privileges of the webserver by sending specially crafted input data to the affected system.	2019-04-26	10.0	<a href="#">CVE-2019-3705 MISC</a>
dell -- idrac9_firmware	Dell EMC iDRAC9 versions prior to 3.24.24.24, 3.21.26.22, 3.22.22.22 and 3.21.25.22 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted data to the iDRAC web interface.	2019-04-26	10.0	<a href="#">CVE-2019-3706 MISC</a>
dhcpcd_project -- dhcpcd	dhcpcd before 7.2.1 contains a buffer overflow in dhcpcd_findna in dhcpc6.c when reading N/A/T addresses.	2019-04-28	7.5	<a href="#">CVE-2019-11577 BID MISC MISC</a>
dillonkane -- tidal_workload_automation	An issue was discovered in Dillon Kane Tidal Workload Automation Agent 3.2.0.5 (formerly known as Cisco Workload Automation or CWA). The Enterprise Scheduler for AIX allows local users to gain privileges via Command Injection in crafted Tidal Job Buffers (TJB) parameters. NOTE: this vulnerability exists because the CVE-2014-3272 solution did not address AIX operating systems.	2019-04-26	7.2	<a href="#">CVE-2019-6689 MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a default administrator credential vulnerability. A remote attacker can use this vulnerability to gain administrator privileges for the creation and modification of articles via an H0XZIT44FcN1j9LTdFc5XRXhlf30JaGe1g3cZY6i1K9 access_token in a uri=blog&action=index&controller=blog action to /api/index.php.	2019-04-30	7.5	<a href="#">CVE-2019-11618 MISC</a>
facebook -- hhvm	Insufficient boundary checks for the strpos and stripos functions allow access to out-of-bounds memory. This affects all supported versions of HHVM (4.0.3, 3.30.4, and 3.27.7 and below).	2019-04-29	7.5	<a href="#">CVE-2019-3561 MISC MISC</a>
fujifilm -- cr-ir_357_fcr_capsula_x_firmware	Fujifilm FCR Capsula X/ Carbon X/ FCR XC-2, model versions CR-IR 357 FCR Carbon X, CR-R 357 FCR XC-2, FCR-IR 357 FCR Capsula X are susceptible to a denial-of-service condition as a result of an overflow of TCP packets, which requires the device to be manually rebooted.	2019-04-30	7.8	<a href="#">CVE-2019-10948 MISC</a>
fujifilm -- cr-ir_357_fcr_capsula_x_firmware	Fujifilm FCR Capsula X/ Carbon X/ FCR XC-2, model versions CR-IR 357 FCR Carbon X, CR-R 357 FCR XC-2, FCR-IR 357 FCR Capsula X provide insecure telnet services that lack authentication requirements. An attacker who successfully exploits this vulnerability may be able to access the underlying operating system.	2019-04-30	10.0	<a href="#">CVE-2019-10950 BID MISC</a>
gitea -- gitea	Gitea before 1.8.0 allows 1FA for user accounts that have completed 2FA enrollment. If a user's credentials are known, then an attacker could send them to the API without requiring the 2FA one-time password.	2019-04-27	7.5	<a href="#">CVE-2019-11576 MISC MISC</a>
ionos -- 1&1_online_storage	STRATO HiDrive Desktop Client 5.0.1.0 for Windows suffers from a SYSTEM privilege escalation vulnerability through the HiDriveMaintenanceService service. This service establishes a NetNamedPipe endpoint that allows applications to connect and call publicly exposed methods. An attacker can inject and execute code by hijacking the insecure communications with the service. This vulnerability also affects Telekom MagentaCLOUD through 5.7.0.0 and 1&1 Online Storage through 6.1.0.0.	2019-04-30	9.0	<a href="#">CVE-2019-9486 MISC</a>
linux -- linux_kernel	udp GRO receive segment in net/ipv4/udp_offload.c in the Linux kernel 5.x before 5.0.13 allows remote attackers to cause a denial of service (slab-out-of-bounds memory corruption) or possibly have unspecified other impact via UDP packets with a 0 payload, because of mishandling of padded packets, aka the "GRO packet of death" issue.	2019-05-02	10.0	<a href="#">CVE-2019-11683 MLIST MLIST BID CONFIRM MISC MISC</a>
mozilla -- firefox	The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR). This allows for possible arbitrary reading and writing of objects during an exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9791 MISC MISC MISC MISC</a>
mozilla -- firefox	The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript to achieve memory corruption, which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9792 MISC MISC MISC MISC</a>
mozilla -- firefox	A vulnerability was discovered where specific command line arguments are not properly discarded during Firefox invocation as a shell handler for URLs. This could be used to retrieve and execute files whose location is supplied through these command line arguments if Firefox is configured as the default URI handler for a given URI scheme in third party applications and these applications insufficiently sanitize URL data. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9794 MISC MISC MISC MISC</a>
mozilla -- firefox	A vulnerability where type-confusion in the IonMonkey just-in-time (JIT) compiler could potentially be used by malicious JavaScript to trigger a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9795 MISC MISC MISC MISC</a>
mozilla -- firefox	A use-after-free vulnerability can occur when the SMIL animation controller incorrectly registers with the refresh driver twice when only a single registration is expected. When a registration is later freed with the removal of the animation controller element, the refresh driver incorrectly leaves a dangling pointer to the driver's observer array. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9796 MISC MISC MISC MISC</a>
mozilla -- firefox	In Firefox Developer Tools it is possible that pasting the result of the 'Copy as cURL' command into a command shell on macOS will cause the execution of unintended additional bash script commands if the URL was maliciously crafted. This is the result of an issue with the native version of Bash on macOS. *Note: This issue only affects macOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9804 MISC MISC</a>
mozilla -- firefox	A latent vulnerability exists in the Prio library where data may be read from uninitialized memory for some functions, leading to potential memory corruption. This vulnerability affects	2019-04-26	7.5	<a href="#">CVE-2019-9805 MISC</a>

	Firefox < 66.			MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-26	7.5	<a href="#">CVE-2019-2725</a> MISC BID CONFIRM EXPLOIT-DB
signing-party_project -- signing-party	gpg-key2ps in signing-party 1.1.x and 2.x before 2.10-1 contains an unsafe shell call enabling shell injection via a User ID.	2019-04-30	10.0	<a href="#">CVE-2019-11627</a> MISC MLIST
smartbear -- readyapi	The WSDL import functionality in SmartBear ReadyAPI 2.5.0 and 2.6.0 allows remote attackers to execute arbitrary Java code via a crafted request parameter in a WSDL file.	2019-05-03	9.3	<a href="#">CVE-2018-20580</a> MISC
tabslab -- mailcarrier	A buffer overflow in the SMTP response service in MailCarrier 2.51 allows the attacker to execute arbitrary code remotely via a long HELP command, a related issue to CVE-2019-11395.	2019-05-02	7.5	<a href="#">CVE-2019-11682</a> MISC
zohocorp -- manageengine_firewall_analyzer	The Custom Report import function in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123224 is vulnerable to XML External Entity (XXE) Injection.	2019-05-02	7.5	<a href="#">CVE-2019-11677</a> MISC
zohocorp -- manageengine_firewall_analyzer	The "default reports" feature in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123218 is vulnerable to SQL Injection.	2019-05-02	7.5	<a href="#">CVE-2019-11678</a> MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aiikcms -- aikcms	An issue was discovered in AiikCms v2.0. There is a SQL Injection vulnerability via \$_GET['del'], as demonstrated by an admin/page/system/nav.php?del= URL.	2019-04-27	6.5	<a href="#">CVE-2019-11567</a> MISC
aiikcms -- aikcms	An issue was discovered in AiikCms v2.0. There is a File upload vulnerability, as demonstrated by an admin/page/system/nav.php request with PHP code in a .php file with the application/octet-stream content type.	2019-04-27	6.8	<a href="#">CVE-2019-11568</a> MISC
anomali -- agave	Anomali Agave (formerly Drupot) through 1.0.0 fails to avoid fingerprinting by including predictable data and minimal variation in size within HTML templates, giving attackers the ability to detect and avoid this system.	2019-05-01	5.0	<a href="#">CVE-2019-11841</a> MISC
apache -- archiva	In Apache Archiva before 2.2.4, it is possible to write files to the archiva server at arbitrary locations by using the artifact upload mechanism. Existing files can be overwritten, if the archiva run user has appropriate permission on the filesystem for the target file.	2019-04-30	5.5	<a href="#">CVE-2019-0213</a> MISC MISC MLIST BID MLIST MLIST MLIST BUGTRAQ
apache -- archiva	In Apache Archiva 2.0.0 - 2.2.3, it is possible to write files to the archiva server at arbitrary locations by using the artifact upload mechanism. Existing files can be overwritten, if the archiva run user has appropriate permission on the filesystem for the target file.	2019-04-30	5.5	<a href="#">CVE-2019-0214</a> CONFIRM MISC MLIST BID MLIST MLIST MLIST BUGTRAQ
apache -- axis	A Server Side Request Forgery (SSRF) vulnerability affected the Apache Axis 1.4 distribution that was last released in 2006. Security and bug commits continue in the projects Axis 1.x Subversion repository, legacy users are encouraged to build from source. The successor to Axis 1.x is Axis2, the latest version is 1.7.9 and is not vulnerable to this issue.	2019-05-01	5.4	<a href="#">CVE-2019-0227</a> MISC
apache -- camel	Apache Camel's File is vulnerable to directory traversal. Camel 2.21.0 to 2.21.3, 2.22.0 to 2.22.2, 2.23.0 and the unsupported Camel 2.x (2.19 and earlier) versions may be also affected.	2019-04-30	5.0	<a href="#">CVE-2019-0194</a> MLIST MLIST MLIST MISC MLIST
apache -- pluto	The input fields of the Apache Pluto "Chat Room" demo portlet 3.0.0 and 3.0.1 are vulnerable to Cross-Site Scripting (XSS) attacks. Mitigation: * Uninstall the ChatRoomDemo war file - or - * migrate to version 3.1.0 of the chat-room-demo war file	2019-04-26	4.3	<a href="#">CVE-2019-0186</a> MLIST MISC BID MLIST MISC EXPLOIT-DB MLIST
apache -- unstructured_information_management_architecture_distributed_uima_cluster_computing	This vulnerability relates to the user's browser processing of DUCC webpage input data. The javascript comprising Apache UIMA DUCC (<= 2.2.2) which runs in the user's browser does not sufficiently filter user supplied inputs, which may result in unintended execution of user supplied javascript code.	2019-05-01	4.3	<a href="#">CVE-2018-8035</a> CONFIRM
atlassian -- jira	The WallboardServlet resource in Jira before version 7.13.1 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the cyclePeriod parameter.	2019-05-03	4.3	<a href="#">CVE-2018-20824</a> MISC
atlassian -- jira	The BrowseProjects.jspa resource in Jira before version 7.13.2, and from version 8.0.0 before version 8.0.2 allows remote attackers to see information for archived projects through a missing authorisation check.	2019-04-30	5.0	<a href="#">CVE-2019-3399</a> MISC
atlassian -- jira	The labels gadget in Jira before version 7.13.2, and from version 8.0.0 before version 8.0.2 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the jqf parameter.	2019-05-03	4.3	<a href="#">CVE-2019-3400</a> MISC
bpcbt -- smartvista	BPC SmartVista 2 has CSRF via SVFE2/pages/admpages/roles/createrole.jsf.	2019-04-30	6.8	<a href="#">CVE-2018-15206</a> MISC
bpcbt -- smartvista	BPC SmartVista 2 has Improper Access Control in the SVFE module, where it fails to appropriately restrict access: a normal user is able to access the SVFE2/pages/flnadmin/currcnvrate/currcnvrate.jsf functionality that should be only accessible to an admin.	2019-04-30	6.5	<a href="#">CVE-2018-15207</a> MISC
				<a href="#">CVE-2018-</a>

bpcbt -- smartvista	BPC SmartVista 2 has Session Fixation via the JSESSIONID parameter.	2019-04-30	5.1	<a href="#">15208 MISC</a>
buffalo -- open_xdmod	An issue was discovered in Open XDMod through 7.5.0. html/gui/general/login.php has Reflected XSS via the xd_user_formal_name parameter.	2019-05-02	4.3	<a href="#">CVE-2018-16960 MISC</a>
buffalo -- open_xdmod	An issue was discovered in Open XDMod through 7.5.0. html/gui/general/dl_publication.php allows Path traversal via the file parameter, allowing remote attackers to read PDF files in arbitrary directories.	2019-05-02	5.0	<a href="#">CVE-2018-16961 MISC</a>
buffalo -- open_xdmod	An issue was discovered in Open XDMod through 7.5.0. An authentication bypass (account takeover) exists due to a weak password reset mechanism. A brute-force attack against an MD5 rid value requires only 600 guesses in the plausible situation where the attacker knows that the victim has started a password-reset process (pass_reset.php, password_reset.php, XDUser.php) in the past few minutes.	2019-05-02	5.0	<a href="#">CVE-2018-16988 MISC</a>
cisco -- hx220c_af_m5_firmware	A vulnerability in the web-based management interface of Cisco HyperFlex HX-Series could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on an affected system by using a web browser and with the privileges of the user.	2019-05-03	6.8	<a href="#">CVE-2019-1857 CISCO</a>
cisco -- network_registrar	A vulnerability in the web-based management interface of Cisco Prime Network Registrar could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.	2019-05-03	4.3	<a href="#">CVE-2019-1852 CISCO</a>
cisco -- prime_collaboration_assurance	A vulnerability in the web-based management interface of Cisco Prime Collaboration Assurance (PCA) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to the insufficient validation of data supplied by external devices to the web-based management interface of an affected PCA device. An attacker in control of devices integrated with an affected PCA device could exploit this vulnerability by using crafted data in certain fields of the controlled devices. A successful exploit could allow the attacker to execute arbitrary script code in the context of the PCA web-based management interface or allow the attacker to access sensitive browser-based information.	2019-05-03	4.3	<a href="#">CVE-2019-1856 BID CISCO</a>
cisco -- telepresence_video_communication_server	A vulnerability in the management web interface of Cisco Expressway Series could allow an authenticated, remote attacker to perform a directory traversal attack against an affected device. The vulnerability is due to insufficient input validation on the web interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web interface. A successful exploit could allow the attacker to bypass security restrictions and access the web interface of a Cisco Unified Communications Manager associated with the affected device. Valid credentials would still be required to access the Cisco Unified Communications Manager interface.	2019-05-03	4.0	<a href="#">CVE-2019-1854 CISCO</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 anyone can change the administrator and moderator passwords via the iso.3.6.1.4.1.3212.100.3.2.8.1 and iso.3.6.1.4.1.3212.100.3.2.8.2 OIDs. A remote, unauthenticated attacker can use this vulnerability to change the admin or moderator user's password and gain access to restricted areas on the HTTP interface.	2019-04-30	5.0	<a href="#">CVE-2019-3927 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allow any user to obtain the presentation passcode via the iso.3.6.1.4.1.3212.100.3.2.7.4 OIDs. A remote, unauthenticated attacker can use this vulnerability to access a restricted presentation or to become the presenter.	2019-04-30	5.0	<a href="#">CVE-2019-3928 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allows anyone to bypass the presentation code simply by requesting /images/browserslide.jpg via HTTP. A remote, unauthenticated attacker can use this vulnerability to watch a slideshow without knowing the access code.	2019-04-30	5.0	<a href="#">CVE-2019-3933 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allows anyone to bypass the presentation code sending a crafted HTTP POST request to login.cgi. A remote, unauthenticated attacker can use this vulnerability to download the current slide image without knowing the access code.	2019-04-30	5.0	<a href="#">CVE-2019-3934 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 allows anyone to act as a moderator to a slide show via crafted HTTP POST requests to conference.cgi. A remote, unauthenticated attacker can use this vulnerability to start, stop, and disconnect active slideshows.	2019-04-30	6.4	<a href="#">CVE-2019-3935 MISC</a>
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 is vulnerable to denial of service via a crafted request to TCP port 389. The request will force the slideshow to transition into a "stopped" state. A remote, unauthenticated attacker can use this vulnerability to stop an active slideshow.	2019-04-30	5.0	<a href="#">CVE-2019-3936 MISC</a>
dhcpcd_project -- dhcpcd	auth.c in dhcpcd before 7.2.1 allowed attackers to infer secrets by performing latency attacks.	2019-04-28	4.3	<a href="#">CVE-2019-11578 BID MISC MISC MISC</a>
dhcpcd_project -- dhcpcd	dhcpc.c in dhcpcd before 7.2.1 contains a 1-byte read overflow with DHO_OPTSOVERLOADED.	2019-04-28	5.0	<a href="#">CVE-2019-11579 BID MISC MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/copyfile.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11806 MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/copydir.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11807 MISC</a>
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/renamefile.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information or make the server	2019-04-30	6.4	<a href="#">CVE-2019-11808 MISC</a>

	unserviceable.			
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/movefile.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information or make the server unserviceable.	2019-04-30	6.4	<a href="#">CVE-2019-11609</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/downloadaddr.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11610</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /fileman/php/download.php. A remote unauthenticated attacker can exploit this vulnerability to obtain server-sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11611</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has an arbitrary file deletion vulnerability in /fileman/php/deletefile.php. A remote unauthenticated attacker can exploit this vulnerability to delete arbitrary files.	2019-04-30	6.4	<a href="#">CVE-2019-11612</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/views/ajax/contactView.php. A remote normal registered user could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11613</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/views/ajax/commentView.php. A remote unauthorized attacker could exploit the vulnerability to obtain database sensitive information.	2019-04-30	5.0	<a href="#">CVE-2019-11614</a> MISC
doorgets -- doorgets_cms	/fileman/php/upload.php in doorGets 7.0 has an arbitrary file upload vulnerability. A remote normal registered user can use this vulnerability to upload backdoor files to control the server.	2019-04-30	6.5	<a href="#">CVE-2019-11615</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a sensitive information disclosure vulnerability in /setup/temp/admin.php and /setup/temp/database.php. A remote unauthenticated attacker could exploit this vulnerability to obtain the administrator password.	2019-04-30	5.0	<a href="#">CVE-2019-11616</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a CSRF vulnerability in /doorgets/app/requests/user/configurationRequest.php. A remote attacker can exploit this vulnerability for "Google Analytics code" modification.	2019-04-30	6.8	<a href="#">CVE-2019-11617</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=analytics. A remote background administrator privilege user (or a user with permission to manage configuration analytics) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11619</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/modulecategoryRequest.php. A remote background administrator privilege user (or a user with permission to manage modulecategory) could exploit the vulnerability to obtain database sensitive information via modulecategory_add_titre.	2019-04-30	4.0	<a href="#">CVE-2019-11620</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=network. A remote background administrator privilege user (or a user with permission to manage network configuration) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11621</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/modulecategoryRequest.php. A remote background administrator privilege user (or a user with permission to manage modulecategory) could exploit the vulnerability to obtain database sensitive information via modulecategory_edit_titre.	2019-04-30	4.0	<a href="#">CVE-2019-11622</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/configurationRequest.php when action=siteweb. A remote background administrator privilege user (or a user with permission to manage configuration siteweb) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11623</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has an arbitrary file deletion vulnerability in /doorgets/app/requests/user/configurationRequest.php. A remote background administrator privilege user can exploit this vulnerability to delete arbitrary files.	2019-04-30	5.5	<a href="#">CVE-2019-11624</a> MISC
doorgets -- doorgets_cms	doorGets 7.0 has a SQL injection vulnerability in /doorgets/app/requests/user/emailingRequest.php. A remote background administrator privilege user (or a user with permission to manage emailing) could exploit the vulnerability to obtain database sensitive information.	2019-04-30	4.0	<a href="#">CVE-2019-11625</a> MISC
doorgets -- doorgets_cms	routers/ajaxRouter.php in doorGets 7.0 has a web site physical path leakage vulnerability, as demonstrated by an ajax/index.php?url=1234%5c request.	2019-04-30	5.0	<a href="#">CVE-2019-11626</a> MISC
esotalk -- esotalk	esoTalk 1.0.0g4 has XSS via the PATH_INFO to the conversations/ URI.	2019-04-29	4.3	<a href="#">CVE-2015-9285</a> MISC MISC
facebook -- fizz	An improperly performed length calculation on a buffer in PlaintextRecordLayer could lead to an infinite loop and denial-of-service based on user input. This issue affected versions of fizz prior to v2019.03.04.00.	2019-04-29	5.0	<a href="#">CVE-2019-3580</a> MISC
freedesktop -- systemd	It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.	2019-04-26	4.6	<a href="#">CVE-2019-3843</a> BID CONFIRM FEDORA
freedesktop -- systemd	It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.	2019-04-26	4.6	<a href="#">CVE-2019-3844</a> BID CONFIRM
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a NULL pointer dereference in the function rec_rset_get_props at rec-rset.c in librec.a, leading to a crash.	2019-05-01	4.3	<a href="#">CVE-2019-11637</a> MISC MISC
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a NULL pointer dereference in the function rec_field_name_equal_p at rec-field-name.c in librec.a, leading to a crash.	2019-05-01	4.3	<a href="#">CVE-2019-11638</a> MISC MISC
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a stack-based buffer overflow in the function rec_type_check_enum at rec-types.c in librec.a.	2019-05-01	6.8	<a href="#">CVE-2019-11639</a> MISC MISC
gnu -- recutils	An issue was discovered in GNU recutils 1.8. There is a heap-based buffer overflow in the function rec_fex_parse_str_simple at rec-fex.c in librec.a.	2019-05-01	6.8	<a href="#">CVE-2019-11640</a> MISC MISC

groonga -- groonga-httpd	The groonga-httpd package 6.1.5-1 for Debian sets the /var/log/groonga ownership to the groonga account, which might let local users obtain root access because of unsafe interaction with logrotate. For example, an attacker can exploit a race condition to insert a symlink from /var/log/groonga/httpd to /etc/bash_completion.d. NOTE: this is an issue in the Debian packaging of the Groonga HTTP server.	2019-05-02	6.9	<a href="#">CVE-2019-11675</a> MISC
honeypress_project -- honeypress	HoneyPress through 2016-09-27 can be fingerprinted by attackers because of the ingrained unique www.atxsec.com and ayyimao.wengine.com hostnames within the fake WordPress templates. This allows attackers to discover and avoid this honeypot system.	2019-05-01	5.0	<a href="#">CVE-2019-11633</a> MISC
ibm -- api_connect	IBM API Connect 2018.1 and 2018.4.1.2 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 155078.	2019-04-29	5.0	<a href="#">CVE-2018-2007</a> CONFIRM XF
ibm -- api_connect	IBM API Connect 2018.1 and 2018.4.1.4 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 155195.	2019-05-02	4.3	<a href="#">CVE-2018-2015</a> BID XF CONFIRM
ibm -- emptoris_contract_management	IBM Emptoris Contract Management 10.0.0 and 10.1.3.0 could disclose sensitive information from detailed information from error messages. IBM X-Force ID: 153657.	2019-04-29	5.0	<a href="#">CVE-2018-1961</a> XF CONFIRM
ibm -- jazz_reporting_service	IBM Jazz Reporting Service (JRS) 6.0.6 could allow an authenticated user to access the execution log files as a guest user, and obtain the information of the server execution. IBM X-Force ID: 156243.	2019-04-29	4.0	<a href="#">CVE-2019-4047</a> BID XF CONFIRM
ibm -- rational_engineering_lifecycle_manager	IBM Rational Engineering Lifecycle Manager 6.0 through 6.0.6 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 143798.	2019-05-01	5.0	<a href="#">CVE-2018-1608</a> XF CONFIRM
ibm -- storediq	IBM StoredIQ 7.6 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 158699.	2019-04-30	5.8	<a href="#">CVE-2019-4166</a> CONFIRM BID XF
ilinkp2p_project -- ilinkp2p	The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.	2019-04-26	6.4	<a href="#">CVE-2019-11219</a> MISC
ilinkp2p_project -- ilinkp2p	An authentication flaw in Shenzhen Yunni Technology iLnkP2P allows remote attackers to actively intercept user-to-device traffic in cleartext, including video streams and device credentials.	2019-04-26	4.3	<a href="#">CVE-2019-11220</a> MISC
imagemagick -- imagemagick	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file.	2019-04-29	5.8	<a href="#">CVE-2019-11597</a> BID MISC
imagemagick -- imagemagick	In ImageMagick 7.0.8-40 Q16, there is a heap-based buffer over-read in the function WritePNMImage of coders/pnm.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file. This is related to SetGrayscaleImage in MagickCore/quantize.c.	2019-04-29	5.8	<a href="#">CVE-2019-11598</a> BID MISC
infinitemit -- directadmin	The FileManager in InfinitemIT DirectAdmin through v1.561 has XSS via CMD_FILE_MANAGER, CMD_SHOW_USER, and CMD_SHOW_RESELLER; an attacker can bypass the CSRF protection with this, and take over the administration panel.	2019-04-30	6.8	<a href="#">CVE-2019-11193</a> MISC MISC EXPLOIT-DB
iobit -- malware_fighter	IMFForceDelete.sys in IObit Malware Fighter 6.2 allows a low privileged user to send IOCTL 0x8016E000 along with a user defined string to a file; that file will be promptly deleted regardless of access controls.	2019-04-30	5.5	<a href="#">CVE-2019-6494</a> MISC
jenkins -- ansible_tower	A cross-site request forgery vulnerability in Jenkins Ansible Tower Plugin 0.9.1 and earlier in the TowerInstallation.TowerInstallationDescriptor#doTestTowerConnection form validation method allowed attackers permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins	2019-04-30	6.8	<a href="#">CVE-2019-10310</a> MLIST MISC
jenkins -- ansible_tower	A missing permission check in Jenkins Ansible Tower Plugin 0.9.1 and earlier in the TowerInstallation.TowerInstallationDescriptor#doTestTowerConnection form validation method allowed attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-04-30	4.0	<a href="#">CVE-2019-10311</a> MLIST MISC
jenkins -- ansible_tower	A missing permission check in Jenkins Ansible Tower Plugin 0.9.1 and earlier in the TowerInstallation.TowerInstallationDescriptor#doFillTowerCredentialsIdItems method allowed attackers with Overall/Read permission to enumerate credentials ID of credentials stored in Jenkins.	2019-04-30	4.0	<a href="#">CVE-2019-10312</a> MLIST MISC
jenkins -- aqua_microscanner	Jenkins Aqua MicroScanner Plugin 1.0.5 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system.	2019-04-30	4.0	<a href="#">CVE-2019-10316</a> MLIST MISC
jenkins -- azure_ad	Jenkins Azure AD Plugin 0.3.3 and earlier stored the client secret unencrypted in the global config.xml configuration file on the Jenkins master where it could be viewed by users with access to the master file system.	2019-04-30	4.0	<a href="#">CVE-2019-10318</a> MLIST MISC
jenkins -- github_authentication	Jenkins GitHub Authentication Plugin 0.31 and earlier did not use the state parameter of OAuth to prevent CSRF.	2019-04-30	6.8	<a href="#">CVE-2019-10315</a> MLIST MISC
jenkins -- koji	Jenkins Koji Plugin disables SSL/TLS and hostname verification globally for the Jenkins master JVM.	2019-04-30	4.3	<a href="#">CVE-2019-10314</a> MLIST MISC
jenkins -- self-organizing_swarm_modules	Jenkins Self-Organizing Swarm Plug-in Modules Plugin clients that use UDP broadcasts to discover Jenkins masters do not prevent XML External Entity processing when processing the responses, allowing unauthorized attackers on the same network to read arbitrary files from Swarm clients.	2019-04-30	4.8	<a href="#">CVE-2019-10309</a> MLIST MISC
jenkins -- sitemonitor	Jenkins SiteMonitor Plugin 0.5 and earlier disabled SSL/TLS and hostname verification globally for the Jenkins master JVM.	2019-04-30	4.3	<a href="#">CVE-2019-10317</a> MLIST



				MISC
jenkins -- static_analysis_utilities	A cross-site request forgery vulnerability in Jenkins Static Analysis Utilities Plugin 1.95 and earlier in the DefaultGraphConfigurationView#doSave form handler method allowed attackers to change the per-job default graph configuration for all users.	2019-04-30	4.3	CVE-2019-10307 MLIST MISC
jenkins -- static_analysis_utilities	A missing permission check in Jenkins Static Analysis Utilities Plugin 1.95 and earlier in the DefaultGraphConfigurationView#doSave form handler method allowed attackers with Overall/Read permission to change the per-job default graph configuration for all users.	2019-04-30	4.0	CVE-2019-10308 MLIST MISC
jenkins -- twitter	Jenkins Twitter Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	2019-04-30	4.0	CVE-2019-10313 MLIST MISC
linux -- linux_kernel	The coredump implementation in the Linux kernel before 5.0.10 does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a race condition with mmget_not_zero or get_task_mm calls. This is related to fs/userfaultfd.c, mm/mmap.c, fs/proc/task_mm.c, and drivers/infiniband/core/uverbs_main.c.	2019-04-29	6.9	CVE-2019-11599 MISC MLIST MLIST MLIST BID MISC MISC MISC MISC MISC EXPLOIT-DB
memcached -- memcached	In memcached before 1.5.14, a NULL pointer dereference was found in the "lru mode" and "lru temp_ttl" commands. This causes a denial of service when parsing crafted lru command messages in process_lru_command in memcached.c.	2019-04-29	5.0	CVE-2019-11596 MISC MISC MISC UBUNTU
microfocus -- network_automation	A potential security vulnerability has been identified in Micro Focus Network Automation Software 9.20, 9.21, 10.00, 10.10, 10.20, 10.30, 10.40, 10.50, 2018.05, 2018.08, 2018.11, and Micro Focus Network Operations Management (NOM) all versions. The vulnerability could be remotely exploited to Remote Code Execution.	2019-04-29	6.5	CVE-2019-3493 CONFIRM
moodle -- moodle	Moodle 3.6.3 allows remote authenticated administrators to execute arbitrary PHP code via a ZIP archive, containing a theme_*.php file, to repository/repository_ajax.php?action=upload and admin/tool/installaddon/index.php.	2019-04-30	6.5	CVE-2019-11631 MISC BID MISC EXPLOIT-DB
mozilla -- firefox	Cross-origin images can be read from a canvas element in violation of the same-origin policy using the transferFromImageBitmap method. *Note: This only affects Firefox 65. Previous versions are unaffected.*. This vulnerability affects Firefox < 65.0.1.	2019-04-26	4.3	CVE-2018-18511 MISC MISC
mozilla -- firefox	Unsanitized output in the browser UI leaves HTML tags in place and can result in arbitrary code execution in Firefox before version 58.0.1.	2019-04-26	4.3	CVE-2018-5124 MISC
mozilla -- firefox	A service worker can send the activate event on itself periodically which allows it to run perpetually, allowing it to monitor activity by users. Affects all versions prior to Firefox 60.	2019-04-26	5.0	CVE-2018-5179 MISC
mozilla -- firefox	A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. This vulnerability could allow an attacker to create an arbitrary value in compiled JavaScript, for which the range analysis will infer a fully controlled, incorrect range in circumstances where users have explicitly disabled Spectre mitigations. *Note: Spectre mitigations are currently enabled for all users by default settings.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	4.3	CVE-2019-9793 MISC MISC MISC
mozilla -- firefox	Cross-origin images can be read in violation of the same-origin policy by exporting an image after using createImageBitmap to read the image and then rendering the resulting bitmap image within a canvas element. This vulnerability affects Firefox < 66.	2019-04-26	5.0	CVE-2019-9797 MISC MISC
mozilla -- firefox	On Android systems, Firefox can load a library from APITRACE_LIB, which is writable by all users and applications. This could allow malicious third party applications to execute a man-in-the-middle attack if a malicious code was written to that location and loaded. *Note: This issue only affects Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	5.8	CVE-2019-9798 MISC MISC
mozilla -- firefox	Insufficient bounds checking of data during inter-process communication might allow a compromised content process to be able to read memory from the parent process under certain conditions. This vulnerability affects Firefox < 66.	2019-04-26	5.0	CVE-2019-9799 MISC MISC
mozilla -- firefox	Firefox will accept any registered Program ID as an external protocol handler and offer to launch this local application when given a matching URL on Windows operating systems. This should only happen if the program has specifically registered itself as a "URL Handler" in the Windows registry. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	5.0	CVE-2019-9801 MISC MISC MISC MISC
mozilla -- firefox	If a Sandbox content process is compromised, it can initiate an FTP download which will then use a child process to render the downloaded data. The downloaded data can then be passed to the Chrome process with an arbitrary file length supplied by an attacker, bypassing sandbox protections and allow for a potential memory read of adjacent data from the privileged Chrome process, which may include sensitive data. This vulnerability affects Firefox < 66.	2019-04-26	5.0	CVE-2019-9802 MISC MISC
mozilla -- firefox	The Upgrade-Insecure-Requests (UIR) specification states that if UIR is enabled through Content Security Policy (CSP), navigation to a same-origin URL must be upgraded to HTTPS. Firefox will incorrectly navigate to an HTTP URL rather than perform the security upgrade requested by the CSP in some circumstances, allowing for potential man-in-the-middle attacks on the linked resources. This vulnerability affects Firefox < 66.	2019-04-26	5.8	CVE-2019-9803 MISC MISC MISC MISC
mozilla -- firefox	A vulnerability exists during authorization prompting for FTP transaction where successive modal prompts are displayed and cannot be immediately dismissed. This allows for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	5.0	CVE-2019-9806 MISC MISC
	When arbitrary text is sent over an FTP connection and a page reload is			CVE-2019-

mozilla -- firefox	initiated, it is possible to create a modal alert message with this text as the content. This could potentially be used for social engineering attacks. This vulnerability affects Firefox < 66.	2019-04-26	4.3	<a href="#">9807</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If WebRTC permission is requested from documents with data: or blob: URLs, the permission notifications do not properly display the originating domain. The notification states "Unknown origin" as the requestee, leading to user confusion about which site is asking for this permission. This vulnerability affects Firefox < 66.	2019-04-26	5.0	<a href="#">CVE-2019-9808</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If the source for resources on a page is through an FTP connection, it is possible to trigger a series of modal alert messages for these resources through invalid credentials or locations. These messages cannot be immediately dismissed, allowing for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	5.0	<a href="#">CVE-2019-9809</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	6.8	<a href="#">CVE-2019-9810</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Incorrect handling of __proto__ mutations may lead to type confusion in IonMonkey JIT code and can be leveraged for arbitrary memory read and write. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	6.8	<a href="#">CVE-2019-9813</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- network_security_services	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-zero value instead. This results in full malleability of the ClientHello for SSLv2 used for TLS 1.2 in all versions prior to NSS 3.39. This does not impact TLS 1.3.	2019-04-29	4.3	<a href="#">CVE-2018-12384</a> <a href="#">CONFIRM</a>
mozilla -- network_security_services	A cached side channel attack during handshakes using RSA encryption could allow for the decryption of encrypted content. This is a variant of the Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) and affects all NSS versions prior to NSS 3.41.	2019-05-02	4.3	<a href="#">CVE-2018-12404</a> <a href="#">BID</a> <a href="#">MISC</a>
mozilla -- thunderbird	A flaw during verification of certain S/MIME signatures causes emails to be shown in Thunderbird as having a valid digital signature, even if the shown message contents aren't covered by the signature. The flaw allows an attacker to reuse a valid S/MIME signature to craft an email message with arbitrary content. This vulnerability affects Thunderbird < 60.5.1.	2019-04-26	5.0	<a href="#">CVE-2018-18509</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">MLIST</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A crash can occur when processing a crafted S/MIME message or an XPI package containing a crafted signature. This can be used as a denial-of-service (DOS) attack because Thunderbird reopens the last seen message on restart, triggering the crash again. This vulnerability affects Thunderbird < 60.5.	2019-04-26	5.0	<a href="#">CVE-2018-18513</a> <a href="#">MISC</a> <a href="#">MISC</a>
netapp -- hyper_converged_infrastructure_compute_node	Element Plug-in for vCenter Server versions prior to 4.2.3 may disclose sensitive account information to an unauthenticated attacker. NetApp HCI Compute Node versions prior to 1.4P2 bundle affected versions of Element Plug-in for vCenter Server.	2019-04-29	5.0	<a href="#">CVE-2019-5492</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
nodebb -- nodebb	Controllers.outgoing in controllers/index.js in NodeBB before 0.7.3 has outgoing XSS.	2019-04-30	4.3	<a href="#">CVE-2019-9286</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
octopus -- octopus_deploy	In Octopus Deploy 2019.1.0 through 2019.3.1 and 2019.4.0 through 2019.4.5, an authenticated user with the VariableViewUnscoped or VariableEditUnscoped permission scoped to a specific project could view or edit unscoped variables from a different project. (These permissions are only used in custom User Roles and do not affect built in User Roles.)	2019-05-01	5.5	<a href="#">CVE-2019-11632</a> <a href="#">MISC</a> <a href="#">MISC</a>
omniauth_project -- omniauth	The request phase of the OmniAuth Ruby gem is vulnerable to Cross-Site Request Forgery when used as part of the Ruby on Rails framework, allowing accounts to be connected without user intent, user interaction, or feedback to the user. This permits a secondary account to be able to sign into the web application as the primary account.	2019-04-26	6.8	<a href="#">CVE-2019-9284</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
phpbb -- phpbb	The fulltext search component in phpBB before 3.2.6 allows Denial of Service.	2019-05-02	5.0	<a href="#">CVE-2019-9826</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
polarisft -- intellect_core_banking	An issue was discovered in the Armor module in Polaris FT Intellect Core Banking 9.7.1. Input passed through the code parameter in three pages as collaterals/colexe3t.jsp and /references/refsuppu.jsp and /references/refbranu.jsp is mishandled before being used in SQL queries, allowing SQL injection with an authenticated session.	2019-04-30	6.5	<a href="#">CVE-2018-14874</a> <a href="#">MISC</a>
polarisft -- intellect_core_banking	An issue was discovered in the Armor module in Polaris FT Intellect Core Banking 9.7.1. CSRF can occur via a /CollatWebApp/gcmsRefInsert?name=SUPP URI.	2019-04-30	6.8	<a href="#">CVE-2018-14930</a> <a href="#">MISC</a>
polarisft -- intellect_core_banking	An issue was discovered in the Core and Portal modules in Polaris FT Intellect Core Banking 9.7.1. An open redirect exists via a /IntellectMain.jsp?IntellectSystem= URI.	2019-04-30	5.8	<a href="#">CVE-2018-14931</a> <a href="#">MISC</a>
projectsend -- projectsend	ProjectSend before r1070 writes user passwords to the server logs.	2019-04-26	5.0	<a href="#">CVE-2019-11492</a> <a href="#">CONFIRM</a>
projectsend -- projectsend	Cross-site scripting (XSS) vulnerability in ProjectSend before r1070 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	4.3	<a href="#">CVE-2019-11533</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
rapid7 -- metasploit	Rapid7 Metasploit Framework suffers from an instance of CWE-22, Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in the Zip import function of Metasploit. Exploiting this vulnerability can allow an attacker to execute arbitrary code in Metasploit at the privilege level of the user running Metasploit. This issue affects: Rapid7 Metasploit Framework version 4.14.0 and prior versions.	2019-04-30	6.5	<a href="#">CVE-2019-5624</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
solarwinds -- damewire_mini_remote_control	DWRCC in SolarWinds DameWare Mini Remote Control 10.0 x64 has a Buffer Overflow associated with the size field for the machine name.	2019-05-02	5.0	<a href="#">CVE-2019-9017</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
sonicwall -- global_management_system	A vulnerability in SonicWall Global Management System (GMS), allow a remote user to gain access to the appliance using existing SSH key. This vulnerability affects GMS versions 9.1, 9.0, 8.7, 8.6, 8.4, 8.3 and earlier.	2019-04-26	6.8	<a href="#">CVE-2019-7476</a> <a href="#">CONFIRM</a>

ublock -- ublock	In uBlock before 0.9.5.15, the \$rewrite filter option allows filter-list maintainers to run arbitrary code in a client-side session when a web service loads a script for execution using XMLHttpRequest or Fetch, and the script origin has an open redirect.	2019-04-29	6.8	<a href="#">CVE-2019-11595</a> MISC <a href="#">MISC</a>
w1.fi -- hostapd	The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not validate fragmentation reassembly state properly for a case where an unexpected fragment could be received. This could result in process termination due to a NULL pointer dereference (denial of service). This affects eap_server/eap_server_pwd.c and eap_peer/eap_pwd.c.	2019-04-26	4.3	<a href="#">CVE-2019-11555</a> MLIST MISC MISC MISC
weaver -- e-cology	An issue was discovered in Weaver e-cology 9.0. There is a CRLF Injection vulnerability via the /workflow/request/ViewRequestForwardSPA.jsp isintervenor parameter, as demonstrated by the %0aSet-cookie: substring.	2019-04-30	4.3	<a href="#">CVE-2019-10272</a> MISC CONFIRM
webidsupport -- webid	WeBid 1.2.2 has reflected XSS via the id parameter to admin/deletenews.php, admin/editbannersuser.php, admin/editfaqscategory.php, or admin/excludeuser.php, or the offset parameter to admin/edituser.php.	2019-04-29	4.3	<a href="#">CVE-2019-11592</a> MISC
z.cash -- zcash	Zcash 2.x allows an inexpensive approach to "fill all transactions of all blocks" and "prevent any real transaction from occurring" via a "Sapling Wood-Chipper" attack.	2019-05-01	5.0	<a href="#">CVE-2019-11636</a> MISC MISC
zimbra -- collaboration_server	Zimbra Collaboration Suite before 8.6 patch 13, 8.7.x before 8.7.11 patch 10, and 8.8.x before 8.8.10 patch 7 or 8.8.x before 8.8.11 patch 3 allows SSRF via the ProxyServlet component.	2019-04-30	5.0	<a href="#">CVE-2019-9621</a> MISC MISC MISC MISC MISC CONFIRM EXPLOIT-DB
zohocorp -- manageengine_admanager_plus	Zoho ManageEngine ADManager Plus 6.6 Build 6657 allows local users to gain privileges (after a reboot) by placing a Trojan horse file into the permissive bin directory.	2019-04-30	6.9	<a href="#">CVE-2018-19374</a> MISC
zohocorp -- manageengine_firewall_analyzer	The user defined DNS name in Zoho ManageEngine Firewall Analyzer before 12.3 Build 123224 is vulnerable to stored XSS attacks.	2019-05-02	4.3	<a href="#">CVE-2019-11676</a> MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- application_links	Application Links before version 5.0.11, from version 5.1.0 before 5.2.10, from version 5.3.0 before 5.3.6, from version 5.4.0 before 5.4.12, and from version 6.0.0 before 6.0.4 allows remote attackers to inject arbitrary HTML or JavaScript via a cross site scripting (XSS) vulnerability in the apLinkStartingUrl parameter.	2019-04-30	3.5	<a href="#">CVE-2018-20239</a> MISC
cisco -- application_policy_infrastructure_controller	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. This vulnerability has been fixed in software version 14.1(1i).	2019-05-03	3.5	<a href="#">CVE-2019-1838</a> CISCO
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 stores usernames, passwords, slideshow passcode, and other configuration options in cleartext in the file tmp/scfgdnf. A local attacker can use this vulnerability to recover sensitive data.	2019-04-30	2.1	<a href="#">CVE-2019-3937</a> MISC
crestron -- am-100_firmware	Crestron AM-100 with firmware 1.6.0.2 and AM-101 with firmware 2.7.0.2 stores usernames, passwords, and other configuration options in the file generated via the "export configuration" feature. The configuration file is encrypted using the awenc binary. The same binary can be used to decrypt any configuration file since all the encryption logic is hard coded. A local attacker can use this vulnerability to gain access to devices username and passwords.	2019-04-30	2.1	<a href="#">CVE-2019-3938</a> MISC
ibm -- jazz_reporting_service	BM Jazz Reporting Service (JRS) 6.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155006.	2019-04-29	3.5	<a href="#">CVE-2018-2004</a> BID XF CONFIRM
ibm -- planning_analytics	BM Planning Analytics 2.0 through 2.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153177.	2019-05-01	3.5	<a href="#">CVE-2018-1933</a> CONFIRM XF
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 6.0.0.0 and 6.0.0.1 Standard Edition is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159946.	2019-05-01	3.5	<a href="#">CVE-2019-4258</a> CONFIRM XF
imagemagick -- imagemagick	An off-by-one read vulnerability was discovered in ImageMagick before version 7.0.7-28 in the format!PTCfromBuffer function in coders/meta.c. A local attacker may use this flaw to read beyond the end of the buffer or to crash the program.	2019-04-30	3.6	<a href="#">CVE-2019-10131</a> BID CONFIRM CONFIRM
linux -- linux_kernel	The print_binder_ref_olocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading "ref *desc *node" lines in a debugfs file.	2019-04-30	2.1	<a href="#">CVE-2018-20509</a> MISC MLIST
linux -- linux_kernel	The print_binder_transaction_olocked function in drivers/android/binder.c in the Linux kernel 4.14.90 allows local users to obtain sensitive address information by reading ""*from *code flags" lines in a debugfs file.	2019-04-30	2.1	<a href="#">CVE-2018-20510</a> BID MISC
philips -- tasy_emr	n Philips Tasy EMR, Tasy EMR Versions 3.02.1744 and prior, the software incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.	2019-05-01	3.5	<a href="#">CVE-2019-6562</a> MISC
polarisft -- intellect_core_banking	An issue was discovered in the Core and Portal modules in Polaris FT Intellect Core Banking 9.7.1. Reflected XSS exists with an authenticated session via the Customerid, formName, FormId, or MODE parameter.	2019-04-30	3.5	<a href="#">CVE-2018-14875</a> MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary	Description	Published	CVSS	Source &
---------	-------------	-----------	------	----------

Vendor -- Product			Score	Patch Info
adblock_plus -- adblock	In Adblock before 3.45.0, the \$rewrite filter option allows filter-list maintainers to run arbitrary code in a client-side session when a web service loads a script for execution using XMLHttpRequest or Fetch, and the script origin has an open redirect.	2019-04-29	not yet calculated	<a href="#">CVE-2019-11594</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
adblock_plus -- adblock_plus	In Adblock Plus before 3.5.2, the \$rewrite filter option allows filter-list maintainers to run arbitrary code in a client-side session when a web service loads a script for execution using XMLHttpRequest or Fetch, and the script origin has an open redirect.	2019-04-29	not yet calculated	<a href="#">CVE-2019-11593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the WebVPN login process of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause increased CPU utilization on an affected device. The vulnerability is due to excessive processing load for existing WebVPN login operations. An attacker could exploit this vulnerability by sending multiple WebVPN login requests to the device. A successful exploit could allow the attacker to increase CPU load on the device, resulting in a denial of service (DoS) condition.	2019-05-03	not yet calculated	<a href="#">CVE-2018-15388</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the Internet Key Exchange Version 2 Mobility and Multihoming Protocol (MOBIKE) feature for the Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a memory leak or a reload of an affected device that leads to a denial of service (DoS) condition. The vulnerability is due to the incorrect processing of certain MOBIKE packets. An attacker could exploit this vulnerability by sending crafted MOBIKE packets to an affected device to be processed. A successful exploit could cause an affected device to continuously consume memory and eventually reload, resulting in a DoS condition. The MOBIKE feature is supported only for IPv4 addresses.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1708</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the Deterministic Random Bit Generator (DRBG), also known as Pseudorandom Number Generator (PRNG), used in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a cryptographic collision, enabling the attacker to discover the private key of an affected device. The vulnerability is due to insufficient entropy in the DRBG when generating cryptographic keys. An attacker could exploit this vulnerability by generating a large number of cryptographic keys on an affected device and looking for collisions with target devices. A successful exploit could allow the attacker to impersonate an affected target device or to decrypt traffic secured by an affected key that is sent to or from an affected target device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1715</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the detection engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent attacker to send data directly to the kernel of an affected device. The vulnerability exists because the software improperly filters Ethernet frames sent to an affected device. An attacker could exploit this vulnerability by sending crafted packets to the management interface of an affected device. A successful exploit could allow the attacker to bypass the Layer 2 (L2) filters and send data directly to the kernel of the affected device. A malicious frame successfully delivered would make the target device generate a specific syslog entry.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1695</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the TCP processing engine of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerability is due to the improper handling of TCP traffic. An attacker could exploit this vulnerability by sending a specific sequence of packets at a high rate through an affected device. A successful exploit could allow the attacker to temporarily disrupt traffic through the device while it reboots.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1694</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the WebVPN service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper management of authenticated sessions in the WebVPN portal. An attacker could exploit this vulnerability by authenticating with valid credentials and accessing a specific URL in the WebVPN portal. A successful exploit could allow the attacker to cause the device to reload, resulting in a temporary DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1693</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the TCP proxy functionality for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to restart unexpectedly, resulting in a denial of service (DoS) condition. The vulnerability is due to an error in TCP-based packet inspection, which could cause the TCP packet to have an invalid Layer 2 (L2)-formatted header. An attacker could exploit this vulnerability by sending a crafted TCP packet sequence to the targeted device. A successful exploit could allow the attacker to cause a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1687</a> <a href="#">CISCO</a>
	A vulnerability in the implementation of Security Assertion Markup Language (SAML) 2.0 Single Sign-On (SSO) for Clientless SSL VPN (WebVPN) and AnyConnect Remote Access VPN in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker			

cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	to successfully establish a VPN session to an affected device. The vulnerability is due to improper credential management when using NT LAN Manager (NTLM) or basic authentication. An attacker could exploit this vulnerability by opening a VPN session to an affected device after another VPN user has successfully authenticated to the affected device via SAML SSO. A successful exploit could allow the attacker to connect to secured networks behind the affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1714</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	A vulnerability in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco Adaptive Security Appliance (ASA) Software and Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets sent to an affected device. An attacker could exploit these vulnerabilities by sending a crafted LDAP packet, using Basic Encoding Rules (BER), to be processed by an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1697</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_and_firepower_threat_defense_software	Multiple vulnerabilities in the WebVPN service of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the WebVPN portal of an affected device. The vulnerabilities exist because the software insufficiently validates user-supplied input on an affected device. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. An attacker would need administrator privileges on the device to exploit these vulnerabilities.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1701</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_software	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the user has administrative privileges, the attacker could alter the configuration of, extract information from, or reload an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1713</a> <a href="#">CISCO</a>
cisco -- adaptive_security_appliance_software	A vulnerability in the remote access VPN session manager of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the remote access VPN services. The vulnerability is due to an issue with the remote access VPN session manager. An attacker could exploit this vulnerability by requesting an excessive number of remote access VPN sessions. An exploit could allow the attacker to cause a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1705</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- adaptive_security_virtual_appliance_and_firepower_2100_series	A vulnerability in the software cryptography module of the Cisco Adaptive Security Virtual Appliance (ASAv) and Firepower 2100 Series running Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause an unexpected reload of the device that results in a denial of service (DoS) condition. The vulnerability is due to a logic error with how the software cryptography module handles IPsec sessions. An attacker could exploit this vulnerability by creating and sending traffic in a high number of IPsec sessions through the targeted device. A successful exploit could cause the device to reload and result in a DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1706</a> <a href="#">CISCO</a>
cisco -- application_policy_infrastructure_controller_software	A vulnerability in the FUSE filesystem functionality for Cisco Application Policy Infrastructure Controller (APIC) software could allow an authenticated, local attacker to escalate privileges to root on an affected device. The vulnerability is due to insufficient input validation for certain command strings issued on the CLI of the affected device. An attacker with write permissions for files within a readable folder on the device could alter certain definitions in the affected file. A successful exploit could allow an attacker to cause the underlying FUSE driver to execute said crafted commands, elevating the attacker's privileges to root on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1682</a> <a href="#">CISCO</a>
cisco -- application_policy_infrastructure_controller_software	A vulnerability in the web-based management interface of Cisco Application Policy Infrastructure Controller (APIC) Software could allow an unauthenticated, remote attacker to access sensitive system usage information. The vulnerability is due to a lack of proper data protection mechanisms for certain components in the underlying Application Centric Infrastructure (ACI). An attacker could exploit this vulnerability by attempting to observe certain network traffic when accessing the APIC. A successful exploit could allow the attacker to access and collect certain tracking data and usage statistics on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1692</a> <a href="#">CISCO</a>
cisco -- application_policy_infrastructure_controller_software	A vulnerability in Cisco Application Policy Infrastructure Controller (APIC) Software could allow an unauthenticated, local attacker with physical access to obtain sensitive information from an affected device. The vulnerability is due to insecure removal of cleartext encryption keys stored on local partitions in the hard drive of an affected device. An attacker could exploit this vulnerability by retrieving data from the physical disk on the affected partition(s). A successful exploit could allow the attacker to retrieve encryption keys, possibly allowing the attacker to further decrypt other data and sensitive information on the device, which could lead to the disclosure of confidential information.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1586</a> <a href="#">BID</a> <a href="#">CISCO</a>



cisco -- email_security_appliance	A vulnerability in certain attachment detection mechanisms of the Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the filtering functionality of an affected device. The vulnerability is due to improper detection of certain content sent to an affected device. An attacker could exploit this vulnerability by sending certain file types without Content-Disposition information to an affected device. A successful exploit could allow an attacker to send messages that contain malicious content to users.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1844</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- firepower_2100_series	A vulnerability in the internal packet-processing functionality of Cisco Firepower Threat Defense (FTD) Software for the Cisco Firepower 2100 Series could allow an unauthenticated, remote attacker to cause an affected device to stop processing traffic, resulting in a denial of service (DoS) condition. The vulnerability is due to a logic error, which may prevent ingress buffers from being replenished under specific traffic conditions. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to consume all input buffers, which are shared between all interfaces, leading to a queue wedge condition in all active interfaces. This situation would cause an affected device to stop processing any incoming traffic and result in a DoS condition until the device is reloaded manually.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1793</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	Multiple vulnerabilities in the Server Message Block (SMB) Protocol preprocessor detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent or remote attacker to cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1696</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting commands into arguments for a specific command. A successful exploit could allow the attacker to execute commands with root privileges.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1709</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	A vulnerability in the CLI of Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by injecting commands into arguments for a specific command. A successful exploit could allow the attacker to execute commands with root privileges.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1699</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	Multiple vulnerabilities in the Server Message Block (SMB) Protocol preprocessor detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, adjacent or remote attacker to cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1704</a> <a href="#">CISCO</a>
cisco -- firepower_threat_defense_software	A vulnerability in the TCP ingress handler for the data interfaces that are configured with management access to Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an increase in CPU and memory usage, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient ingress TCP rate limiting for TCP ports 22 (SSH) and 443 (HTTPS). An attacker could exploit this vulnerability by sending a crafted, steady stream of TCP traffic to port 22 or 443 on the data interfaces that are configured with management access to the affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2018-15462</a> <a href="#">CISCO</a>
cisco -- ip_phone_7800_series_and_8800_series_session_initiation_protocol_software	A vulnerability in the call-handling functionality of Session Initiation Protocol (SIP) Software for Cisco IP Phone 7800 Series and 8800 Series could allow an unauthenticated, remote attacker to cause an affected phone to reload unexpectedly, resulting in a temporary denial of service (DoS) condition. The vulnerability is due to incomplete error handling when XML data within a SIP packet is parsed. An attacker could exploit this vulnerability by sending a SIP packet that contains a malicious XML payload to an affected phone. A successful exploit could allow the attacker to cause the affected phone to reload unexpectedly, resulting in a temporary DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1635</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_application_centric_infrastructure_mode_switch_software	A vulnerability in the filesystem management for the Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an authenticated, local attacker with administrator rights to gain elevated privileges as the root user on an affected device. The vulnerability is due to overly permissive file permissions of specific system files. An attacker could exploit this vulnerability by authenticating to an affected device, creating a crafted command string, and writing this crafted string to a specific file location. A successful exploit could allow the attacker to execute arbitrary operating system commands as root on an affected device. The attacker would need to have valid administrator credentials for the device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1803</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches	A vulnerability in Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an authenticated, remote attacker to access sensitive information. The vulnerability occurs because the affected software does not properly validate user-supplied input. An attacker could exploit this vulnerability by issuing certain commands with filtered query results on the device. This action may cause returned messages to display confidential system information. A successful exploit could allow the attacker to read sensitive information on the device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1587</a> <a href="#">CISCO</a>
	A vulnerability in the system shell for Cisco Nexus 9000			

cisco -- nexus_9000_series_fabric_switches	Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an authenticated, local attacker to use symbolic links to overwrite system files. These system files may be sensitive and should not be overwritable by non-root users. The attacker would need valid device credentials. The vulnerability is due to incorrect symbolic link verification of directory paths when they are used in the system shell. An attacker could exploit this vulnerability by authenticating to the device and providing crafted user input to specific symbolic link CLI commands. Successful exploitation could allow the attacker to overwrite system files that should be restricted. This vulnerability has been fixed in software version 14.1(1i).	2019-05-03	not yet calculated	<a href="#">CVE-2019-1836</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches_in_application_centric_infrastructure_mode_switch_software	A vulnerability in the background operations functionality of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an authenticated, local attacker to gain elevated privileges as root on an affected device. The vulnerability is due to insufficient validation of user-supplied files on an affected device. An attacker could exploit this vulnerability by logging in to the CLI of the affected device and creating a crafted file in a specific directory on the filesystem. A successful exploit could allow the attacker to execute arbitrary operating system commands as root on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1592</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches_in_application_centric_infrastructure_mode_switch_software	A vulnerability in the Transport Layer Security (TLS) certificate validation functionality of Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software could allow an unauthenticated, remote attacker to perform insecure TLS client authentication on an affected device. The vulnerability is due to insufficient TLS client certificate validations for certificates sent between the various components of an ACI fabric. An attacker who has possession of a certificate that is trusted by the Cisco Manufacturing CA and the corresponding private key could exploit this vulnerability by presenting a valid certificate while attempting to connect to the targeted device. An exploit could allow the attacker to gain full control of all other components within the ACI fabric of an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1590</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_fabric_switches_software	A vulnerability in the Trusted Platform Module (TPM) functionality of software for Cisco Nexus 9000 Series Fabric Switches in Application Centric Infrastructure (ACI) mode could allow an unauthenticated, local attacker with physical access to view sensitive information on an affected device. The vulnerability is due to a lack of proper data-protection mechanisms for disk encryption keys that are used within the partitions on an affected device hard drive. An attacker could exploit this vulnerability by obtaining physical access to the affected device to view certain cleartext keys. A successful exploit could allow the attacker to execute a custom boot process or conduct further attacks on an affected device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1589</a> <a href="#">CISCO</a>
cisco -- small_business_rv320_and_rv325_dual_gigabit_wan_vpn_routers	A vulnerability in the session management functionality of the web-based interface for Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to hijack a valid user session on an affected system. An attacker could use this impersonated session to create a new user account or otherwise control the device with the privileges of the hijacked session. The vulnerability is due to a lack of proper session management controls. An attacker could exploit this vulnerability by sending a crafted HTTP request to a targeted device. A successful exploit could allow the attacker to take control of an existing user session on the device. Exploitation of the vulnerability requires that an authorized user session is active and that the attacker can craft an HTTP request to impersonate that session.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1724</a> <a href="#">CISCO</a>
cisco -- small_business_switches_software	A vulnerability in the Secure Shell (SSH) authentication process of Cisco Small Business Switches software could allow an attacker to bypass client-side certificate authentication and revert to password authentication. The vulnerability exists because OpenSSH mishandles the authentication process. An attacker could exploit this vulnerability by attempting to connect to the device via SSH. A successful exploit could allow the attacker to access the configuration as an administrative user if the default credentials are not changed. There are no workarounds available; however, if client-side certificate authentication is enabled, disable it and use strong password authentication. Client-side certificate authentication is disabled by default.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1859</a> <a href="#">CISCO</a>
cisco -- umbrella_dashboard	A vulnerability in the session management functionality of the web UI for the Cisco Umbrella Dashboard could allow an authenticated, remote attacker to access the Dashboard via an active, user session. The vulnerability exists due to the affected application not invalidating an existing session when a user authenticates to the application and changes the users credentials via another authenticated session. An attacker could exploit this vulnerability by using a separate, authenticated, active session to connect to the application through the web UI. A successful exploit could allow the attacker to maintain access to the dashboard via an authenticated user's browser session. Cisco has addressed this vulnerability in the Cisco Umbrella Dashboard. No user action is required.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1807</a> <a href="#">CISCO</a>
cisco -- web_security_appliance	A vulnerability in the log subscription subsystem of the Cisco Web Security Appliance (WSA) could allow an authenticated, local attacker to perform command injection and elevate privileges to root. The vulnerability is due to insufficient validation of user-supplied input on the web and command-line interface. An attacker could exploit this vulnerability by authenticating to the affected device and injecting scripting commands in the scope of the log subscription subsystem. A successful exploit could allow	2019-05-03	not yet calculated	<a href="#">CVE-2019-1816</a> <a href="#">CISCO</a>

	the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root.			
cisco -- web_security_appliance	A vulnerability in the web proxy functionality of Cisco AsyncOS Software for Cisco Web Security Appliance could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper validation of HTTP and HTTPS requests. An attacker could exploit this vulnerability by sending a malformed HTTP or HTTPS request to an affected device. An exploit could allow the attacker to cause a restart of the web proxy process, resulting in a temporary DoS condition.	2019-05-03	not yet calculated	<a href="#">CVE-2019-1817</a> <a href="#">CISCO</a>
cjson -- cjson	parse_string in cJSON.c in cJSON before 2016-10-02 has a buffer over-read, as demonstrated by a string that begins with a " character and ends with a \ character.	2019-04-29	not yet calculated	<a href="#">CVE-2016-10749</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
das_u-boot -- das_u-boot	gen_rand_uuid in lib/uuid.c in Das U-Boot v2014.04 through v2019.04 lacks a srand call, which allows attackers to determine UUID values in scenarios where CONFIG_RANDOM_UUID is enabled, and Das U-Boot is relied upon for UUID values of a GUID Partition Table of a boot device.	2019-05-03	not yet calculated	<a href="#">CVE-2019-11690</a> <a href="#">MISC</a>
dell_emc -- idrac9	Dell EMC iDRAC9 versions prior to 3.30.30.30 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted input data to the WS-MAN interface.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3707</a> <a href="#">MISC</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, internal methods used to prevent arbitrary file overwrites in Appliance Mode were not fully effective. An authenticated attacker with a high privilege level may be able to bypass protections implemented in appliance mode to overwrite arbitrary system files.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6614</a> <a href="#">CONFIRM</a>
f5 -- big-ip	When BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8 are processing certain rare data sequences occurring in PPTP VPN traffic, the BIG-IP system may execute incorrect logic. The TMM may restart and produce a core file as a result of this condition. The BIG-IP system provisioned with the CGNAT module and configured with a virtual server using a PPTP profile is exposed to this vulnerability.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6611</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, DNS query TCP connections that are aborted before receiving a response from a DNS cache may cause TMM to restart.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6612</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, SNMP may expose sensitive configuration objects over insecure transmission channels. This issue is exposed when a passphrase is used with various profile types and is accessed using SNMPv2.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6613</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, administrative users with TMSH access can overwrite critical system files on BIG-IP which can result in bypass of whitelist / blacklist restrictions enforced by appliance mode.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6616</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, Administrator and Resource Administrator roles might exploit TMSH access to bypass Appliance Mode restrictions on BIG-IP systems.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6615</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, a user with the Resource Administrator role is able to overwrite sensitive low-level files (such as /etc/passwd) using SFTP to modify user permissions, without Advanced Shell access. This is contrary to our definition for the Resource Administrator (RA) role restrictions.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6617</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, 12.1.0-12.1.4, 11.6.1-11.6.3.4, and 11.5.2-11.5.8, users with the Resource Administrator role can modify sensitive portions of the filesystem if provided Advanced Shell Access, such as editing /etc/passwd. This allows modifications to user objects and is contrary to our definition for the Resource Administrator (RA) role restrictions.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6618</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On BIG-IP 14.0.0-14.1.0.1, 13.0.0-13.1.1.4, and 12.1.0-12.1.4, the Traffic Management Microkernel (TMM) may restart when a virtual server has an HTTP/2 profile with Application Layer Protocol Negotiation (ALPN) enabled and it processes traffic where the ALPN extension size is zero.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6619</a> <a href="#">CONFIRM</a>
facebook_technologies -- oculus_browser_ui	A remote web page could inject arbitrary HTML code into the Oculus Browser UI, allowing an attacker to spoof UI and potentially execute code. This affects the Oculus Browser starting from version 5.2.7 until 5.7.11.	2019-04-29	not yet calculated	<a href="#">CVE-2019-3562</a> <a href="#">MISC</a>
filezilla_project -- filezilla	Untrusted search path in FileZilla before 3.41.0-rc1 allows an attacker to gain privileges via a malicious 'fzstfp' binary in the user's home directory.	2019-04-29	not yet calculated	<a href="#">CVE-2019-5429</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
lantronix -- securelinux_spider_devices	Lantronix SecureLinux Spider (SLS) 2.2+ devices have XSS in the auth.asp login page.	2019-05-02	not yet calculated	<a href="#">CVE-2018-10383</a> <a href="#">MISC</a>
lenovo -- xclarity_administrator	An internal product security audit of Lenovo XClarity Administrator (LXCA) discovered HTTP proxy credentials being written to a log file in clear text. This only affects LXCA when HTTP proxy credentials have been configured. This affects LXCA versions 2.0.0 to 2.3.x.	2019-05-03	not yet calculated	<a href="#">CVE-2019-6158</a> <a href="#">MISC</a>
microfocus -- open_enterprise_server	A DOM based XSS vulnerability has been identified in the Netstorage component of Open Enterprise Server (OES) allowing a remote attacker to execute javascript in the victims browser by tricking the victim into clicking on a specially crafted link. This affects OES versions OES2015SP1, OES2018, and OES2018SP1. Older versions may be affected but were not tested as they are out of support.	2019-05-02	not yet calculated	<a href="#">CVE-2019-3490</a> <a href="#">MISC</a>

mozilla -- bugzilla	A third party website can access information available to a user with access to a restricted bug entry using the image generation in report.cgi in all Bugzilla versions prior to 4.4.	2019-04-29	not yet calculated	<a href="#">CVE-2018-5123</a> <a href="#">CONFIRM</a>
national_center_for_biotechnology_information -- toolbox	A heap-based buffer overflow exists in nph-viewgif.cgi in the 2.0.7 through 2.2.26 legacy versions of the NCBI ToolBox.	2019-05-02	not yet calculated	<a href="#">CVE-2018-16717</a> <a href="#">MISC</a>
national_center_for_biotechnology_information -- toolbox	An XSS vulnerability exists in wwwblast.c in the 2.0.7 through 2.2.26 legacy versions of the NCBI ToolBox via a crafted -z1 argument.	2019-05-02	not yet calculated	<a href="#">CVE-2018-16718</a> <a href="#">MISC</a>
national_center_for_biotechnology_information -- toolbox	A path traversal vulnerability exists in viewcgi.c in the 2.0.7 through 2.2.26 legacy versions of the NCBI ToolBox, which may result in reading of arbitrary files (i.e., significant information disclosure) or file deletion via the nph-viewgif.cgi query string.	2019-05-02	not yet calculated	<a href="#">CVE-2018-16716</a> <a href="#">MISC</a>
national_electrical_manufacturers_association -- digital_imaging_and_communications_in_medicine_part_10_file_format	An issue was discovered in the DICOM Part 10 File Format in the NEMA DICOM Standard 1995 through 2019b. The preamble of a DICOM file that complies with this specification can contain the header for an executable file, such as Portable Executable (PE) malware. This space is left unspecified so that dual-purpose files can be created. (For example, dual-purpose TIFF/DICOM files are used in digital whole slide imaging for applications in medicine.) To exploit this vulnerability, someone must execute a maliciously crafted file that is encoded in the DICOM Part 10 File Format. PE/DICOM files are executable even with the .dcm file extension. Anti-malware configurations at healthcare facilities often ignore medical imagery. Also, anti-malware tools and business processes could violate regulatory frameworks (such as HIPAA) when processing suspicious DICOM files.	2019-05-02	not yet calculated	<a href="#">CVE-2019-11687</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
node-tar -- node-tar	A vulnerability was found in node-tar before version 4.4.2. An Arbitrary File Overwrite issue exists when extracting a tarball containing a hardlink to a file that already exists on the system, in conjunction with a later plain file with the same name as the hardlink. This plain file content replaces the existing file content.	2019-04-30	not yet calculated	<a href="#">CVE-2018-20834</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
php -- php	When processing certain files, PHP EXIF extension in versions 7.1.x below 7.1.29, 7.2.x below 7.2.18 and 7.3.x below 7.3.5 can be caused to read past allocated buffer in exif_process_IFD_TAG function. This may lead to information disclosure or crash.	2019-05-03	not yet calculated	<a href="#">CVE-2019-11036</a> <a href="#">MISC</a>
php -- php	In PHP imagick extension in versions between 3.3.0 and 3.4.4, writing to an array of values in ImagickKernel::fromMatrix() function did not check that the address will be within the allocated array. This could lead to out of bounds write to memory if the function is called with the data controlled by untrusted party.	2019-05-03	not yet calculated	<a href="#">CVE-2019-11037</a> <a href="#">MISC</a>
qliktech_international -- qlikview_server_and_qlik_sense_enterprise_and_qlik_analytics_platform	An issue was discovered in QlikView Server before 11.20 SR19, 12.00 and 12.10 before 12.10 SR11, 12.20 before SR9, and 12.30 before SR2; and Qlik Sense Enterprise and Qlik Analytics Platform installations that lack these patch levels: February 2018 Patch 4, April 2018 Patch 3, June 2018 Patch 3, September 2018 Patch 4, November 2018 Patch 4, or February 2019 Patch 2. An authenticated user may be able to bypass intended file-read restrictions via crafted Browser requests.	2019-04-30	not yet calculated	<a href="#">CVE-2019-11628</a> <a href="#">MISC</a>
rockwell_automation -- compactlogix_and_compact_guardlogix_and_armor_compact_guardlogix_controllers	An attacker could send a crafted HTTP/HTTPS request to render the web server unavailable and/or lead to remote code execution caused by a stack-based buffer overflow vulnerability. A cold restart is required for recovering CompactLogix 5370 L1, L2, and L3 Controllers, Compact GuardLogix 5370 controllers, and Armor Compact GuardLogix 5370 Controllers Versions 20 to 30.014 and earlier systems.	2019-05-01	not yet calculated	<a href="#">CVE-2019-10952</a> <a href="#">BID</a> <a href="#">MISC</a>
rockwell_automation -- compactlogix_and_compact_guardlogix_and_armor_compact_guardlogix_controllers	An attacker could send crafted SMTP packets to cause a denial-of-service condition where the controller enters a major non-recoverable faulted state (MNRF) in CompactLogix 5370 L1, L2, and L3 Controllers, Compact GuardLogix 5370 controllers, and Armor Compact GuardLogix 5370 Controllers Versions 20 to 30.014 and earlier.	2019-05-01	not yet calculated	<a href="#">CVE-2019-10954</a> <a href="#">BID</a> <a href="#">MISC</a>
tar-fs -- tar-fs	A vulnerability was found in tar-fs before 1.16.2. An Arbitrary File Overwrite issue exists when extracting a tarball containing a hardlink to a file that already exists on the system, in conjunction with a later plain file with the same name as the hardlink. This plain file content replaces the existing file content.	2019-04-30	not yet calculated	<a href="#">CVE-2018-20835</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wangle -- wangle	Wangle's LineBasedFrameDecoder contains logic for identifying newlines which incorrectly advances a buffer, leading to a potential underflow. This affects versions of Wangle prior to v2019.04.22.00	2019-04-29	not yet calculated	<a href="#">CVE-2019-3563</a> <a href="#">MISC</a>
wildfly -- wildfly	A flaw was discovered in wildfly versions up to 16.0.0.Final that would allow local users who are able to execute init.d script to terminate arbitrary processes on the system. An attacker could exploit this by modifying the PID file in /var/run/boss-eap/ allowing the init.d script to terminate any process as root.	2019-05-03	not yet calculated	<a href="#">CVE-2019-3805</a> <a href="#">CONFIRM</a>
wildfly -- wildfly	It was discovered that the ElytronManagedThread in Wildfly's Elytron subsystem in versions from 11 to 16 stores a SecurityIdentity to run the thread as. These threads do not necessarily terminate if the keep alive time has not expired. This could allow a shared thread to use the wrong security identity when executing.	2019-05-03	not yet calculated	<a href="#">CVE-2019-3894</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The WebDorado Contact Form Builder plugin before 1.0.69 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11557</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WebDorado Contact Form plugin before 1.13.5 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a	2019-04-29	not yet calculated	<a href="#">CVE-2019-11591</a> <a href="#">MISC</a>

	discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.			MISC MISC
wordpress -- wordpress	Server Side Request Forgery (SSRF) exists in the Print My Blog plugin before 1.6.7 for WordPress via the site parameter.	2019-04-27	not yet calculated	CVE-2019-11565 MISC MISC MISC MISC MISC
wordpress -- wordpress	The 10Web Form Maker plugin before 1.13.5 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.	2019-04-29	not yet calculated	CVE-2019-11590 MISC MISC MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nssa.us-cert.gov to your address book.

OTHER RESOURCES  
[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED  


SUBSCRIBER SERVICES  
[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [wguitar.e@ci.sunnyvale.ca.us](mailto:wguitar.e@ci.sunnyvale.ca.us) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 2 5 Murray Lane SW Bldg 10 · Washington, DC 20598 · (888) 282-0870





From: [US-CERT](#)  
To: [Tanner McGinnis](#)  
Subject: SB19-119: Vulnerability Summary for the Week of April 22, 2019  
Date: Monday, April 29, 2019 4:09:38 PM



National Cyber Awareness System:

## SB19-119 Vulnerability Summary for the Week of April 22, 2019

04/29/2019 09:00 AM EDT

Original release date: April 29, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology \(NIST\) National Vulnerability Database \(NVD\)](#) in the past week. The NVD is sponsored by the [Department of Homeland Security \(DHS\) National Cybersecurity and Communications Integration Center \(NCCIC\)](#) / [United States Computer Emergency Readiness Team \(US-CERT\)](#). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System \(CVSS\)](#) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database \(NVD\)](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activision -- call_of_duty:advanced_warfare	SV_SteamAuthClient in various Activision Infinity Ward Call of Duty games before 2015-08-11 is missing a size check when reading authBlob data into a buffer, which allows one to execute code on the remote target machine when sending a steam authentication request. This affects Call of Duty: Modern Warfare 2, Call of Duty: Modern Warfare 3, Call of Duty: Ghosts, Call of Duty: Advanced Warfare, Call of Duty: Black Ops 1, and Call of Duty: Black Ops 2.	2019-04-19	7.5	<a href="#">CVE-2018-20817</a> MISC MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. The NumberToFixed() and numtostr implementations in jsnumber.c have a stack-based buffer overflow.	2019-04-22	7.5	<a href="#">CVE-2019-11411</a> MISC MISC MISC
atftp_project -- atftp	An issue was discovered in atftpd in atftp 0.7.1. A remote attacker may send a crafted packet triggering a stack-based buffer overflow due to an insecurely implemented strncpy call. The vulnerability is triggered by sending an error packet of 3 bytes or fewer. There are multiple instances of this vulnerable strncpy pattern within the code base, specifically within tftpd_file.c, tftp_file.c, tftpd_mftfp.c, and tftp_mftfp.c.	2019-04-20	7.5	<a href="#">CVE-2019-11365</a> MISC MISC
burrow-wheeler_aligner_project -- burrow-wheeler_aligner	BWA (aka Burrow-Wheeler Aligner) 0.7.17 r1198 has a Buffer Overflow via a long prefix that is mishandled in bns_fasta2bntseq and bns_dump at bntseq.c.	2019-04-20	7.5	<a href="#">CVE-2019-11371</a> MISC
freeradius -- freeradius	FreeRADIUS before 3.0.19 does not prevent use of reflection for authentication spoofing, aka a "Dragonblood" issue, a similar issue to CVE-2019-9497.	2019-04-22	7.5	<a href="#">CVE-2019-11234</a> CONFIRM MISC MISC MISC UBUNTU MISC
freeradius -- freeradius	FreeRADIUS before 3.0.19 mishandles the "each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used" protection mechanism, aka a "Dragonblood" issue, a similar issue to CVE-2019-9498 and CVE-2019-9499.	2019-04-22	7.5	<a href="#">CVE-2019-11235</a> CONFIRM MISC MISC MISC UBUNTU MISC
google -- android	In floor0_inverse1 of floor0.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119120561.	2019-04-19	9.3	<a href="#">CVE-2019-2027</a> CONFIRM
google -- android	In numerous hand-crafted functions in libmpeg2, NEON registers are not preserved. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120644655.	2019-04-19	9.3	<a href="#">CVE-2019-2028</a> CONFIRM
google -- android	In removeInterfaceAddress of NetworkController.cpp, there is a possible use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-119496789.	2019-04-19	7.5	<a href="#">CVE-2019-2030</a> CONFIRM
ibm -- bladecenter_hs23_firmware	A potential vulnerability was found in an SMI handler in various BIOS versions of certain legacy IBM System x and IBM BladeCenter systems that could lead to denial of service.	2019-04-22	7.8	<a href="#">CVE-2019-6155</a> MISC
imagemagick -- imagemagick	The cineon parsing component in ImageMagick 7.0.8-26 Q16 allows attackers to cause a denial-of-service (uncontrolled resource consumption) by crafting a Cineon image with an incorrect claimed image size. This occurs because ReadCINImage in coders/cin.c lacks a check for insufficient image data in a file.	2019-04-23	7.1	<a href="#">CVE-2019-11470</a> MISC MISC
intelbras -- iwr_3000n_firmware	An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. A malformed login request allows remote attackers to cause a denial of service (reboot), as demonstrated by JSON misparsing of the {} string to v1/system/login.	2019-04-22	7.8	<a href="#">CVE-2019-11415</a> MISC
intelbras -- iwr_3000n_firmware	A CSRF issue was discovered on Intelbras IWR 3000N 1.5.0 devices, leading to complete control of the router, as demonstrated by v1/system/user.	2019-04-22	9.3	<a href="#">CVE-2019-11416</a> MISC
linux -- linux_kernel	cipso_v4_validate in include/net/cipso_ipv4.h in the Linux kernel before 3.11.7, when CONFIG_NETLABEL is disabled, allows attackers to cause a denial of service (infinite loop and crash), as demonstrated by icmpsic, a different vulnerability than CVE-2013-0310.	2019-04-22	7.1	<a href="#">CVE-2013-7470</a> MISC MISC MISC
mitel -- cmg_suite	SQL injection vulnerabilities in CMG Suite 8.4 SP2 and earlier, could allow an unauthenticated attacker to conduct an SQL injection attack due to insufficient input validation for the login interface. A successful exploit could allow an attacker to extract sensitive information from the database and execute arbitrary scripts.	2019-04-25	7.5	<a href="#">CVE-2018-18285</a> CONFIRM CONFIRM
mitel -- cmg_suite	SQL injection vulnerabilities in CMG Suite 8.4 SP2 and earlier, could allow an unauthenticated attacker to conduct an SQL injection attack due to insufficient input validation for the changepwd interface. A successful exploit could allow an attacker to extract sensitive information from the database and execute arbitrary scripts.	2019-04-25	7.5	<a href="#">CVE-2018-18286</a> CONFIRM CONFIRM
mozilla -- firefox	Mozilla developers and community members reported memory safety bugs present in Firefox 65, Firefox ESR 60.5, and Thunderbird 60.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code.	2019-04-26	7.5	<a href="#">CVE-2019-9788</a> MISC MISC MISC

	This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.			<a href="#">MISC</a>
mozilla -- firefox	Mozilla developers and community members reported memory safety bugs present in Firefox 65. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9789</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9790</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A use-after-free vulnerability can occur while playing a sound notification in Thunderbird. The memory storing the sound data is immediately freed, although the sound is still being played asynchronously, leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 60.5.	2019-04-26	7.5	<a href="#">CVE-2018-18512</a> <a href="#">MISC</a> <a href="#">MISC</a>
neatorobotics -- botvac_connected_firmware	A Buffer Overflow in Network:AuthenticationClient::VerifySignature in /bin/astro in Neato Botvac Connected 2.2.0 allows a remote attacker to execute arbitrary code with root privileges via a crafted POST request to a nucleo.neatocloud.com:4443/vendors/neato/robots/[robot_serial]/messages Neato cloud URL.	2019-04-25	10.0	<a href="#">CVE-2018-19442</a> <a href="#">MISC</a>
nice -- engage	In NICE Engage through 6.5, the default configuration binds an unauthenticated JMX/RMI interface to all network interfaces, without restricting registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol by using the JMX connector. The observed affected TCP port is 6338 but, based on the product's configuration, a different one could be vulnerable.	2019-04-23	7.5	<a href="#">CVE-2019-7727</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
nmap -- npcap	An issue was discovered in Npcap 0.992. Sending a malformed .pcap file with the loopback adapter using either pcap_sendqueue_queue() or pcap_sendqueue_transmit() results in kernel pool corruption. This could lead to arbitrary code executing inside the Windows kernel and allow escalation of privileges.	2019-04-23	9.3	<a href="#">CVE-2019-11490</a> <a href="#">MISC</a>
openkm -- openkm	OpenKM 6.3.2 through 6.3.7 allows an attacker to upload a malicious JSP file into the /okm:root directories and move that file to the home directory of the site, via frontend/FileUpload and admin/repository_export.jsp. This is achieved by interfering with the Filesystem path control in the admin's Export field. As a result, attackers can gain remote code execution through the application server with root privileges.	2019-04-22	9.0	<a href="#">CVE-2019-11445</a> <a href="#">MISC</a> <a href="#">MISC</a>
openplcproject -- openplc_v2_firmware	A buffer overflow vulnerability was discovered in the OpenPLC controller, in the OpenPLC_v2 and OpenPLC_v3 versions. It occurs in the modbus.cpp mapUnusedIO() function, which can cause a runtime crash of the PLC or possibly have unspecified other impact.	2019-04-22	7.5	<a href="#">CVE-2018-20818</a> <a href="#">MISC</a>
oracle -- database_server	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having DBFS_ROLE privilege with network access via Oracle Net to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/H/I:H/A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2517</a> <a href="#">MISC</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	<a href="#">CVE-2019-2608</a> <a href="#">MISC</a>
oracle -- retail_convenience_store_back_office	Vulnerability in the Oracle Retail Convenience Store Back Office component of Oracle Retail Applications (subcomponent: Level 3 Maintenance Functions). The supported version that is affected is 3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Convenience Store Back Office. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Convenience Store Back Office accessible data as well as unauthorized read access to a subset of Oracle Retail Convenience Store Back Office accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Convenience Store Back Office. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	<a href="#">CVE-2019-2424</a> <a href="#">MISC</a>
oracle -- retail_point-of-service	Vulnerability in the Oracle Retail Point-of-Service component of Oracle Retail Applications (subcomponent: Infrastructure). Supported versions that are affected are 13.4, 14.0 and 14.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Point-of-Service. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Point-of-Service accessible data as well as unauthorized read access to a subset of Oracle Retail Point-of-Service accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Point-of-Service. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	<a href="#">CVE-2019-2558</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2645</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: EJB Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2646</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2658</a> <a href="#">MISC</a>
pluck-cms -- pluck	data/inc/files.php in Pluck 4.7.8 allows remote attackers to execute arbitrary code by uploading a .htaccess file that specifies SetHandler x-httpd-php for a .txt file, because only certain PHP-related filename extensions are blocked.	2019-04-19	7.5	<a href="#">CVE-2019-11344</a> <a href="#">MISC</a>
rocboss -- rocboss	app/controllers/frontend/PostController.php in ROCBOS V2.2.1 has SQL injection via the Post:doReward score paramter, as demonstrated by the /do/reward/3 URI.	2019-04-20	7.5	<a href="#">CVE-2019-11362</a> <a href="#">MISC</a>
tabslab -- mailcarrier	A buffer overflow in MailCarrier 2.51 allows remote attackers to execute arbitrary code via a long string, as demonstrated by SMTP RCPT TO, POP3 USER, POP3 LIST, POP3 TOP, or POP3 RETR.	2019-04-22	7.5	<a href="#">CVE-2019-11395</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
trendnet -- tew-632brp_firmware	apply.cgi on the TRENDnet TEW-632BRP 1.010B32 router has a buffer overflow via long strings to the SOAPACTION:HNAP1 interface.	2019-04-22	7.5	<a href="#">CVE-2019-11418</a> <a href="#">MISC</a>
trendnet -- tv-ip110wn_firmware	system.cgi on TRENDnet TV-IP110WN cameras has a buffer overflow caused by an inadequate source-length check before a strcpy operation in the respondAsp function. Attackers can exploit the vulnerability by using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68.	2019-04-22	7.5	<a href="#">CVE-2019-11417</a> <a href="#">MISC</a>

whatsns -- whatsns	whatsns 4.0 allows index.php?question/ajaxadd.html title SQL injection.	2019-04-22	7.5	CVE-2019-11450 MISC
zohocorp -- manageengine_applications_manager	An issue was discovered in Zoho ManageEngine Applications Manager 11.0 through 14.0. An unauthenticated user can gain the authority of SYSTEM on the server due to a PopUp_SLA.jsp sid SQL injection vulnerability. For example, the attacker can subsequently write arbitrary text to a .vbs file.	2019-04-22	10.0	CVE-2019-11448 MISC EXPLOIT-DB CONFIRM
zohocorp -- manageengine_applications_manager	Zoho ManageEngine Applications Manager 12 through 14 allows FaultTemplateOptions.jsp resourceid SQL injection. Subsequently, an unauthenticated user can gain the authority of SYSTEM on the server by uploading a malicious file via the "Execute Program Action(s)" feature.	2019-04-23	10.0	CVE-2019-11469 MISC MISC MISC EXPLOIT-DB CONFIRM

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
74cms -- 74cms	74CMS v5.0.1 has a CSRF vulnerability to add a new admin user via the index.php?m=Admin&c=admin&a=add URL.	2019-04-20	6.8	CVE-2019-11374 MISC MISC EXPLOIT-DB
apache -- pony_mail	A vulnerability was discovered wherein a specially crafted URL could enable reflected XSS via JavaScript in the pony mail interface.	2019-04-22	4.3	CVE-2019-0218 MISC CONFIRM
apache -- zeppelin	Apache Zeppelin prior to 0.8.0 had a stored XSS issue via Note permissions. Issue reported by "Josna Joseph".	2019-04-23	4.3	CVE-2018-1328 MISC MISC MISC
aquaverde -- aquarius_cms	aquaverde Aquarius CMS through 4.3.5 allows Information Exposure through Log Files because of an error in the Log-File writer component.	2019-04-24	5.0	CVE-2019-9724 CONFIRM MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. jscompile.c can cause a denial of service (invalid stack-frame jump) because it lacks an ENDRY opcode call.	2019-04-22	5.0	CVE-2019-11412 MISC MISC MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. It has unlimited recursion because the match function in regexp.c lacks a depth check.	2019-04-22	5.0	CVE-2019-11413 MISC MISC MISC
atftp_project -- atftp	An issue was discovered in atftpd in atftp 0.7.1. It does not lock the thread_list_mutex mutex before assigning the current thread data structure. As a result, the daemon is vulnerable to a denial of service attack due to a NULL pointer dereference. If thread_data is NULL when assigned to current, and modified by another thread before a certain tftp_list.c check, there is a crash when dereferencing current->next.	2019-04-20	4.3	CVE-2019-11366 MISC MISC
atutor -- atutor	An issue was discovered in ATutor through 2.2.4. It allows the user to run commands on the server with the teacher user privilege. The Upload Files section in the File Manager field contains an arbitrary file upload vulnerability via upload.php. The \$illegalExtensions value only lists lowercase (and thus .php is a bypass), and omits .shml and .phtml.	2019-04-22	6.5	CVE-2019-11446 MISC EXPLOIT-DB
audiocodes -- 405hd_firmware	Cross Site Scripting in different input fields (domain field and personal settings) in AudioCodes 405HD VoIP phone with firmware 2.2.12 allows an attacker (local or remote) to inject JavaScript into the web interface of the device by manipulating the phone book entries or manipulating the domain name sent to the device from the domain controller.	2019-04-25	4.3	CVE-2018-16220 MISC
block -- jit-wasm	EOS.IO jit-wasm 4.1 has a heap-based buffer overflow via a crafted wast file.	2019-04-24	6.8	CVE-2018-13443 MISC MISC MISC
brassica -- soy_cms	** DISPUTED ** SOY CMS v3.0.2 allows remote attackers to execute arbitrary PHP code via a <?php substring in the second text box. NOTE: the vendor indicates that there was an assumption that the content is "made editable on its own."	2019-04-20	6.5	CVE-2019-11376 MISC MISC
cloudbees -- jenkins_operations_center	CloudBees Jenkins Operations Center 2.150.2.3, when an expired trial license exists, allows Cleartext Password Storage and Retrieval via the proxy configuration page.	2019-04-19	5.0	CVE-2019-11350 MISC
cutephp -- cutenews	An issue was discovered in CutePHP CuteNews 2.1.2. An attacker can infiltrate the server through the avatar upload process in the profile area via the avatar_file field to index.php?mod=main&opt=personal. There is no effective control of \$imgsize in /core/modules/dashboard.php. The header content of a file can be changed and the control can be bypassed for code execution. (An attacker can use the GIF header for this.)	2019-04-22	6.5	CVE-2019-11447 MISC EXPLOIT-DB
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Heap-based overflow vulnerability, triggered when the user opens a malformed DIB format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9135 MISC
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Heap-based overflow vulnerability, triggered when the user opens a malformed JPEG2000 format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9136 MISC
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed PhotoShop file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9138 MISC
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed PDF file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9139 MISC
dropbox -- lepton	read_ujpg in jpgcoder.cc in Dropbox Lepton 1.2.1 allows attackers to cause a denial-of-service (application runtime crash because of an integer overflow) via a crafted file.	2019-04-23	4.3	CVE-2018-20820 MISC MISC
drupal -- drupal	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	2019-04-19	4.3	CVE-2019-11358 MISC MISC MISC MISC MISC MISC MISC

				MLIST BUGTRAQ MISC DEBIAN MISC
ea -- origin	The client in Electronic Arts (EA) Origin 10.5.36 on Windows allows template injection in the title parameter of the Origin2 URI handler. This can be used to escape the underlying AngularJS sandbox and achieve remote code execution via an origin2://game/launch URL for QtApplication QDesktopServices communication.	2019-04-19	6.8	CVE-2019-11354 MISC MISC MISC MISC MISC MISC MISC
eclipse -- jetty	In Eclipse Jetty version 9.2.26 and older, 9.3.25 and older, and 9.4.15 and older, the server is vulnerable to XSS conditions if a remote client USES a specially formatted URL against the DefaultServlet or ResourceHandler that is configured for showing a Listing of directory contents.	2019-04-22	4.3	CVE-2019-10241 CONFIRM
fortinet -- fortimanager	A cleartext transmission of sensitive information vulnerability in Fortinet FortiManager 5.2.0 through 5.2.7, 5.4.0 and 5.4.1 may allow an unauthenticated attacker in a man in the middle position to retrieve the admin password via intercepting REST API JSON responses.	2019-04-25	4.3	CVE-2018-1360 BID CONFIRM
gilacms -- gila_cms	Gila CMS 1.10.1 allows fm/save CSRF for executing arbitrary PHP code.	2019-04-22	6.8	CVE-2019-11456 MISC
gilacms -- gila_cms	core/classes/db_backup.php in Gila CMS 1.10.1 allows admin/db_backup?download= absolute path traversal to read arbitrary files.	2019-04-25	4.0	CVE-2019-11515 MISC
gitlab -- gitlab	GitLab CE & EE 11.2 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 have Persistent XSS.	2019-04-25	4.3	CVE-2018-18643 MISC MISC MISC
gitlab -- gitlab	GitLab Community and Enterprise Edition 8.9 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 has Incorrect Access Control.	2019-04-25	6.5	CVE-2018-19359 MISC MISC MISC
gnome -- evince	The tiff_document_render() and tiff_document_get_thumbnail() functions in the TIFF document backend in GNOME Evince through 3.32.0 did not handle errors from TIFFReadRGBAImageOriented(), leading to uninitialized memory use when processing certain TIFF image files.	2019-04-22	4.3	CVE-2019-11459 MISC
gnome -- gnome-desktop	An issue was discovered in GNOME gnome-desktop 3.26, 3.28, and 3.30 prior to 3.30.2.2, and 3.32 prior to 3.32.1.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCTST ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCTST ioctl on 64-bit systems, similar to CVE-2019-10063.	2019-04-22	6.8	CVE-2019-11460 MISC
google -- android	In updateAssistMenuItems of Editor.java, there is a possible escape from the Setup Wizard due to a missing permission check. This could lead to local escalation of privilege and FRP bypass with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android ID: A-120866126	2019-04-19	4.6	CVE-2019-2026 CONFIRM
google -- android	In btm_proc_smp_cbk of tm_ble.cc, there is a possible memory corruption due to a use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120612744.	2019-04-19	6.8	CVE-2019-2029 CONFIRM
google -- android	In rw_t3t_act_handle_check_ndef_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120502559.	2019-04-19	4.6	CVE-2019-2031 CONFIRM
google -- android	In SetScanResponseData of ble_advertiser_hci_interface.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-121145627.	2019-04-19	4.6	CVE-2019-2032 CONFIRM
google -- android	In create_hdr of dnssd_clientstub.c, there is a possible use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-121327565.	2019-04-19	4.6	CVE-2019-2033 CONFIRM
google -- android	In rw_i93_sm_read_ndef of rw_i93.cc, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the NFC process with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122035770.	2019-04-19	6.8	CVE-2019-2034 CONFIRM
google -- android	In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122320256	2019-04-19	6.8	CVE-2019-2035 CONFIRM
google -- android	In I2cu_send_peer_config_rej of I2c_utils.cc, there is a possible out-of-bound read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119870451.	2019-04-19	5.0	CVE-2019-2037 CONFIRM
google -- android	In rw_i93_process_sys_info of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121259048.	2019-04-19	4.3	CVE-2019-2038 CONFIRM
google -- android	In rw_i93_sm_detect_ndef of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121260197.	2019-04-19	4.7	CVE-2019-2039 CONFIRM
google -- android	In rw_i93_process_ext_sys_info of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122316913.	2019-04-19	4.7	CVE-2019-2040 CONFIRM
google -- android	In the configuration of NFC modules on certain devices, there is a possible failure to distinguish individual devices due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-8.1 Android-9. Android ID: A-122034690.	2019-04-19	6.9	CVE-2019-2041 CONFIRM
google -- tensorflow	Google TensorFlow 1.6.x and earlier is affected by: Null Pointer Dereference. The type of exploitation is: context-dependent.	2019-04-23	4.3	CVE-2018-7576 CONFIRM
google -- tensorflow	Google TensorFlow 1.7 and below is affected by: Buffer Overflow. The impact is: execute arbitrary code (local).	2019-04-23	6.8	CVE-2018-8825 CONFIRM
google -- tensorflow	NULL pointer dereference in Google TensorFlow before 1.12.2 could cause a denial of service via an invalid GIF file.	2019-04-24	4.3	CVE-2019-9635 MISC
				CVE-2019-

gradle -- enterprise	In Gradle Enterprise before 2018.5.3, Build Cache Nodes did not store the credentials at rest in an encrypted format.	2019-04-22	5.0	11402 MISC
gradle -- enterprise	In Gradle Enterprise before 2018.5.2, Build Cache Nodes would reflect the configured password back when viewing the HTML page source of the settings page.	2019-04-22	5.0	11403 MISC
graphicsmagick -- graphicsmagick	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (out-of-bounds read and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.	2019-04-23	4.3	CVE-2019-11473 MISC MISC MISC BID
graphicsmagick -- graphicsmagick	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (floating-point exception and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.	2019-04-23	4.3	CVE-2019-11474 MISC MISC MISC BID
graphicsmagick -- graphicsmagick	In GraphicsMagick from version 1.3.8 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WritePDBImage of coders/pdb.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to MagickBitStreamMSBWrite in magick/bit_stream.c.	2019-04-24	6.8	CVE-2019-11505 MISC BID MISC
graphicsmagick -- graphicsmagick	In GraphicsMagick from version 1.3.30 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WriteMATLABImage of coders/mat.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to ExportRedQuantumType in magick/export.c.	2019-04-24	6.8	CVE-2019-11506 MISC MISC
gstreamer_project -- gstreamer	GStreamer before 1.16.0 has a heap-based buffer overflow in the RTSP connection parser via a crafted response from a server, potentially allowing remote code execution.	2019-04-24	6.8	CVE-2019-9928 CONFIRM CONFIRM MLIST MLIST
i-librarian -- i-librarian	Cross-site scripting (XSS) vulnerability in display.php in I, Librarian 4.10 allows remote attackers to inject arbitrary web script or HTML via the project parameter.	2019-04-19	4.3	CVE-2019-11359 MISC
i-librarian -- i-librarian	I, Librarian 4.10 has XSS via the export.php export_files parameter.	2019-04-22	4.3	CVE-2019-11428 MISC
i-librarian -- i-librarian	I, Librarian 4.10 has XSS via the notes.php notes parameter.	2019-04-22	4.3	CVE-2019-11449 MISC
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0CD could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 157654.	2019-04-25	5.8	CVE-2019-4092 CONFIRM XF
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 147708.	2019-04-19	5.0	CVE-2018-1729 CONFIRM BID XF
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to view process definition of a business process without permission. IBM X-Force ID: 159231.	2019-04-25	4.0	CVE-2019-4222 XF CONFIRM
idreamsoft -- icms	An XSS issue was discovered in app/admincp/template/admincp.header.php in idreamsoft iCMS 7.0.14 via the admincp.php?app=config tab parameter.	2019-04-22	4.3	CVE-2019-11426 MISC
idreamsoft -- icms	An XSS issue was discovered in app/search/search.app.php in idreamsoft iCMS 7.0.14 via the public/api.php?app=search q parameter.	2019-04-22	4.3	CVE-2019-11427 MISC
imagemagick -- imagemagick	ReadXWDImage in coders/xwd.c in the XWD image parsing component of ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (divide-by-zero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first.	2019-04-23	4.3	CVE-2019-11472 MISC MISC
intelbras -- iwr_3000n_firmware	An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. When the administrator password is changed from a certain client IP address, administrative authorization remains available to any client at that IP address, leading to complete control of the router.	2019-04-22	4.3	CVE-2019-11414 MISC
kubernetes -- kubernetes	In Kubernetes v1.12.0-v1.12.4 and v1.13.0, the rest AnonymousClientConfig() method returns a copy of the provided config, with credentials removed (bearer token, username/password, and client certificate/key data). In the affected versions, rest AnonymousClientConfig() did not effectively clear service account credentials loaded using rest.InClusterConfig()	2019-04-22	4.3	CVE-2019-11243 BID MISC
linux -- linux_kernel	The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions.	2019-04-23	6.9	CVE-2019-11486 MISC MISC MISC MISC
matrix -- sydent	util/emailutils.py in Matrix Sydent before 1.0.2 mishandles registration restrictions that are based on e-mail domain, if the allowed_local_3pids option is enabled. This occurs because of potentially unwanted behavior in Python, in which an email.utils.parseaddr call on user@bad.example.net@good.example.com returns the user@bad.example.net substring.	2019-04-19	4.3	CVE-2019-11340 MISC MISC MISC
mediaarea -- mediainfo	An out-of-bounds read in MediaInfoLib::File__Tags_Helper::Synched_Test in Tag/File__Tags.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash.	2019-04-20	4.3	CVE-2019-11372 MISC FEDORA MISC
mediaarea -- mediainfo	An out-of-bounds read in File__Analyze::Get_L8 in File__Analyze_Buffer.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash.	2019-04-20	4.3	CVE-2019-11373 MISC FEDORA MISC
meisivod -- msvod	Msvod v10 has a CSRF vulnerability to change user information via the admin/member/edit.html URI.	2019-04-20	4.3	CVE-2019-11375 MISC MISC EXPLOIT-DB
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-942-APPLICATION-ATTACK-SQLi.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators.	2019-04-20	5.0	CVE-2019-11387 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators.	2019-04-20	5.0	CVE-2019-11388 MISC
	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0.			CVE-2019-



modsecurity -- owasp_modsecurity_core_rule_set	/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with next# at the beginning and nested repetition operators.	2019-04-20	5.0	11389 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with set_error_handler# at the beginning and nested repetition operators.	2019-04-20	5.0	CVE-2019-11390 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with \$a# at the beginning and nested repetition operators.	2019-04-20	5.0	CVE-2019-11391 MISC
mozilla -- firefox	The about:crashcontent and about:crashparent pages can be triggered by web content. These pages are used to crash the loaded page or the browser for test purposes. This issue allows for a non-persistent denial of service (DOS) attack by a malicious site which links to these pages. This vulnerability affects Firefox < 64.	2019-04-26	4.3	CVE-2018-18510 MISC
openstack -- nova	Versions of nova before 2012.1 could expose hypervisor host files to a guest operating system when processing a maliciously constructed qcow filesystem.	2019-04-22	5.0	CVE-2011-3147 MISC
oracle -- advanced_outbound_telephony	Vulnerability in the Oracle Advanced Outbound Telephony component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	5.8	CVE-2019-2663 MISC
oracle -- application_object_library	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	4.3	CVE-2019-2621 MISC
oracle -- application_testing_suite	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	6.5	CVE-2019-2557 MISC
oracle -- applications_framework	Vulnerability in the Oracle Applications Framework component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	5.8	CVE-2019-2682 MISC
oracle -- autovue_3d_professional_advanced	Vulnerability in the Oracle AutoVue 3D Professional Advanced component of Oracle Supply Chain Products Suite (subcomponent: Format Handling - 2D). Supported versions that are affected are 21.0.0 and 21.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle AutoVue 3D Professional Advanced. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle AutoVue 3D Professional Advanced accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A/N).	2019-04-23	5.0	CVE-2019-2575 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A/N).	2019-04-23	4.0	CVE-2019-2588 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	5.8	CVE-2019-2595 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/H/I/L/A/N).	2019-04-23	4.9	CVE-2019-2601 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). While the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data as well as unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/H/I/L/A/N).	2019-04-23	6.4	CVE-2019-2616 MISC
oracle -- business_process_management_suite	Vulnerability in the Oracle Business Process Management Suite component of Oracle Fusion Middleware (subcomponent: BPM Foundation Services). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Process Management Suite, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Process Management Suite accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Process Management Suite accessible	2019-04-23	5.8	CVE-2019-2706 MISC BID

		data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- commerce_merchandising	Vulnerability in the Oracle Commerce Merchandising component of Oracle Commerce (subcomponent: Asset Manager). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Merchandising. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Merchandising accessible data as well as unauthorized read access to a subset of Oracle Commerce Merchandising accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	2019-04-23	6.4	<a href="#">CVE-2019-2712</a>	<a href="#">MISC</a>
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2659</a>	<a href="#">MISC</a>
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). Supported versions that are affected are 11.2.0.3 and 11.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2712</a>	<a href="#">MISC</a>
oracle -- common_applications	Vulnerability in the Oracle Common Applications component of Oracle E-Business Suite (subcomponent: CRM User Management Framework). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2665</a>	<a href="#">MISC</a>
oracle -- configurator	Vulnerability in the Oracle Configurator component of Oracle Supply Chain Products Suite (subcomponent: Active Model Generation). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2567</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2639</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	<a href="#">CVE-2019-2669</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2671</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2675</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	<a href="#">CVE-2019-2676</a>	<a href="#">MISC</a>
oracle -- database	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:A/H).	2019-04-23	4.6	<a href="#">CVE-2019-2619</a>	<a href="#">MISC</a>
oracle -- database_server	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:A/H).	2019-04-23	4.6	<a href="#">CVE-2019-2516</a>	<a href="#">MISC</a>

	(CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).			
oracle -- database_server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	<a href="#">CVE-2019-2518</a> MISC
oracle -- database_server	Vulnerability in the RDBMS DataPump component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Difficult to exploit vulnerability allows high privileged attacker having DBA role privilege with network access via Oracle Net to compromise RDBMS DataPump. Successful attacks of this vulnerability can result in takeover of RDBMS DataPump. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	<a href="#">CVE-2019-2571</a> MISC
oracle -- database_server	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2582</a> MISC
oracle -- e-business_suite	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2551</a> MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2600</a> MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2651</a> MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2661</a> MISC
oracle -- general_ledger	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Consolidation Hierarchy Viewer). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-04-23	5.5	<a href="#">CVE-2019-2638</a> MISC
oracle -- health_sciences_data_management_workbench	Vulnerability in the Oracle Health Sciences Data Management Workbench component of Oracle Health Sciences Applications (subcomponent: User Interface). The supported version that is affected is 2.4.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences Data Management Workbench accessible data as well as unauthorized read access to a subset of Oracle Health Sciences Data Management Workbench accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2019-04-23	5.5	<a href="#">CVE-2019-2629</a> MISC
oracle -- hospitality_cruise_dining_room_management	Vulnerability in the Oracle Hospitality Cruise Dining Room Management component of Oracle Hospitality Applications (subcomponent: Web Service). The supported version that is affected is 8.0.80. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Dining Room Management. While the vulnerability is in Oracle Hospitality Cruise Dining Room Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Dining Room Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Dining Room Management accessible data. CVSS 3.0 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2019-04-23	6.4	<a href="#">CVE-2019-2702</a> MISC
oracle -- interaction_center_intelligence	Vulnerability in the Oracle Interaction Center Intelligence component of Oracle E-Business Suite (subcomponent: Business Intelligence (OLTP)). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Interaction Center Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Interaction Center Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Interaction Center Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle Interaction Center Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2655</a> MISC
oracle -- istore	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2652</a> MISC
oracle -- isupplier_portal	Vulnerability in the Oracle iSupplier Portal component of Oracle E-Business Suite (subcomponent: Attachments). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupplier Portal, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	2019-04-23	5.8	<a href="#">CVE-2019-2683</a>

	unauthorized access to critical data or complete access to all Oracle iSupplier Portal accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupplier Portal accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A:N).			MISC
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	CVE-2019-2564 MISC
oracle -- jd_edwards_world_technical_foundation	Vulnerability in the JD Edwards World Technical Foundation component of Oracle JD Edwards Products (subcomponent: Service Enablement). Supported versions that are affected are A9.2, A9.3.1 and A9.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards World Technical Foundation. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards World Technical Foundation accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2565 MISC
oracle -- jdk	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	5.0	CVE-2019-2602 MISC
oracle -- jdk	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H).	2019-04-23	4.3	CVE-2019-2684 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2697 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2698 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). The supported version that is affected is Java SE: 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. While the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2699 MISC CONFIRM
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge Management component of Oracle E-Business Suite (subcomponent: Setup, Admin). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A:N).	2019-04-23	5.8	CVE-2019-2660 MISC
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge component of Oracle Siebel CRM (subcomponent: Web Applications (InfoCenter)). Supported versions that are affected are 8.5.1.0 - 8.5.1.7, 8.6.0 and 8.6.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge accessible data as well as unauthorized read access to a subset of Oracle Knowledge accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/L/I/L/A:N).	2019-04-23	5.8	CVE-2019-2719 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I/L/A:N).	2019-04-23	5.8	CVE-2019-2604 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I/L/A:N).	2019-04-23	5.8	CVE-2019-2664 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	2019-04-23	4.3	CVE-2019-2670



	Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).			MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2673 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2677 MISC
oracle -- micros_lucas	Vulnerability in the MICROS Lucas component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 2.9.5.6 and 2.9.5.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Lucas. Successful attacks of this vulnerability can result in takeover of MICROS Lucas. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	CVE-2018-3120 MISC
oracle -- micros_relate_customer_relationship_management_software	Vulnerability in the MICROS Relate CRM Software component of Oracle Retail Applications (subcomponent: Customer). The supported version that is affected is 11.4. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Relate CRM Software. While the vulnerability is in MICROS Relate CRM Software, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MICROS Relate CRM Software accessible data as well as unauthorized access to critical data or complete access to all MICROS Relate CRM Software accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2019-04-23	4.9	CVE-2018-3314 MISC
oracle -- micros_retail-j	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Back Office). The supported version that is affected is 12.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MICROS Retail-J accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2018-2880 MISC
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: libmysqld). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	4.3	CVE-2018-3123 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-In). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2566 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2580 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2581 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2584 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2585 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2587 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2589 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2592 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2593 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2596 MISC CONFIRM
	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security:			





oracle -- mysql	Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	23	4.0	MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2691 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2693 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2694 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2695 MISC CONFIRM
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I/L:A/N).	2019-04-23	5.8	CVE-2019-2603 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I/L:A/N).	2019-04-23	5.8	CVE-2019-2653 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I/L:A/N).	2019-04-23	5.8	CVE-2019-2654 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/N:I/L:A/N).	2019-04-23	4.3	CVE-2019-2674 MISC
oracle -- oracle_retail_customer_engagement	Vulnerability in the Oracle Retail Customer Engagement component of Oracle Retail Applications (subcomponent: Segment). Supported versions that are affected are 16.0 and 17.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Retail Customer Engagement. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Retail Customer Engagement accessible data as well as unauthorized read access to a subset of Oracle Retail Customer Engagement accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Customer Engagement. CVSS 3.0 Base Score 5.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L).	2019-04-23	6.0	CVE-2018-3312 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2609 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2610 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2611 MISC

	(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)	2019-04-23	6.4	<a href="#">CVE-2019-2612 MISC</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)	2019-04-23	6.4	<a href="#">CVE-2019-2613 MISC</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology as well as unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)	2019-04-23	6.4	<a href="#">CVE-2019-2705 MISC</a>
oracle -- peoplesoft_enterprise_elm_enterprise_learning_management	Vulnerability in the PeopleSoft Enterprise ELM component of Oracle PeopleSoft Products (subcomponent: Enterprise Learning Mgmt). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)	2019-04-23	4.0	<a href="#">CVE-2019-2700 MISC</a>
oracle -- peoplesoft_enterprise_human_capital_management_candidate_gateway	Vulnerability in the PeopleSoft Enterprise HRMS component of Oracle PeopleSoft Products (subcomponent: Candidate Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HRMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HRMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HRMS accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2591 MISC</a>
oracle -- peoplesoft_enterprise_human_capital_management_talent_acquisition_manager	Vulnerability in the PeopleSoft Enterprise HCM Talent Acquisition Manager component of Oracle PeopleSoft Products (subcomponent: Job Opening). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Talent Acquisition Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Talent Acquisition Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2590 MISC</a>
oracle -- peoplesoft_enterprise_learning_management	Vulnerability in the PeopleSoft Enterprise ELM Enterprise Learning Management component of Oracle PeopleSoft Products (subcomponent: Application Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM Enterprise Learning Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise ELM Enterprise Learning Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2707 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Homepage & Navigation). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)	2019-04-23	4.3	<a href="#">CVE-2019-2573 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: RemoteCall). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)	2019-04-23	4.0	<a href="#">CVE-2019-2586 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.55, 8.56 and 8.57. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N)	2019-04-23	4.9	<a href="#">CVE-2019-2594 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2597 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: SQR). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise	2019-04-23	5.5	<a href="#">CVE-2019-2598 MISC</a>

	PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).			
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2637</a> MISC
oracle -- primavera_p6_enterprise_project_portfolio_management	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). The supported version that is affected is 18.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2701</a> MISC
oracle -- service_bus	Vulnerability in the Oracle Service Bus component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Service Bus. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	5.0	<a href="#">CVE-2019-2576</a> MISC
oracle -- service_contracts	Vulnerability in the Oracle Service Contracts component of Oracle E-Business Suite (subcomponent: Renewals). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Service Contracts, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Service Contracts accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	<a href="#">CVE-2019-2622</a> MISC
oracle -- siebel_crm	Vulnerability in the Siebel Core - Server BizLogic Script component of Oracle Siebel CRM (subcomponent: Integration - Scripting). The supported version that is affected is 19.3. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Siebel Core - Server BizLogic Script. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Core - Server BizLogic Script accessible data as well as unauthorized read access to a subset of Siebel Core - Server BizLogic Script accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Siebel Core - Server BizLogic Script. CVSS 3.0 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	6.5	<a href="#">CVE-2019-2570</a> MISC
oracle -- soa_suite	Vulnerability in the Oracle SOA Suite component of Oracle Fusion Middleware (subcomponent: Fabric Layer). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle SOA Suite accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2572</a> MISC
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: IPS Package Manager). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2704</a> MISC
oracle -- territory_management	Vulnerability in the Oracle Territory Management component of Oracle E-Business Suite (subcomponent: Territory Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Territory Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Territory Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Territory Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Territory Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2662</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2640</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2641</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2642</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2643</a> MISC
	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 6.3.7, 6.4.2 and 6.4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to			



oracle -- transportation_management	compromise Oracle Transportation Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Transportation Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2709 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2656 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2657 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2680 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.4	<a href="#">CVE-2019-2690 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2696 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2703 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2721 MISC EXPLOIT: DB</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2722 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2723 MISC</a>
oracle -- webcenter_sites	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2578 MISC</a>
oracle -- webcenter_sites	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2579 MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/N/I:L/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2568 MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2615 MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS	2019-04-23	5.5	<a href="#">CVE-2019-2618 MISC</a>



	Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N).			
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2647</a> MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2648</a> MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2649</a> MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2650</a> MISC
oracle -- work_in_process	Vulnerability in the Oracle Work in Process component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-04-23	5.5	<a href="#">CVE-2019-2633</a> MISC
osticket -- osticket	In osTicket before 1.12, XSS exists via /upload/file.php, /upload/scp/users.php?do=import-users, and /upload/scp/ajax.php/users/import if an agent manager user uploads a crafted .csv file to the User Importer, because file contents can appear in an error message. The XSS can lead to local file inclusion.	2019-04-25	4.3	<a href="#">CVE-2019-11537</a> MISC MISC MISC
projectsend -- projectsend	An issue was discovered in ProjectSend r1053. upload-process-form.php allows finished_files[]=./ directory traversal. It is possible for users to read arbitrary files and (potentially) access the supporting database, delete arbitrary files, access user passwords, or run arbitrary code.	2019-04-20	6.5	<a href="#">CVE-2019-11378</a> BID MISC
projectsend -- projectsend	Cross-site scripting (XSS) vulnerability in ProjectSend before r1070 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	4.3	<a href="#">CVE-2019-11533</a> BID CONFIRM
qemu -- qemu	hw/sparc64/sun4u.c in QEMU 3.1.50 is vulnerable to a NULL pointer dereference, which allows the attacker to cause a denial of service via a device driver.	2019-04-19	5.0	<a href="#">CVE-2019-5008</a> BID MISC MISC
redhat -- keycloak	Keycloak up to version 6.0.0 allows the end user token (access or id token JWT) to be used as the session cookie for browser sessions for OIDC. As a result an attacker with access to service provider backend could hijack user's browser session.	2019-04-24	5.5	<a href="#">CVE-2019-3868</a> BID CONFIRM
redhat -- virtualization	A memory leak in archive_read_format_zip_cleanup in archive_read_support_format_zip.c in libarchive 3.3.4-dev allows remote attackers to cause a denial of service via a crafted ZIP file because of a HAVE_LZMA_H typo. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product's official releases are unaffected.	2019-04-22	4.3	<a href="#">CVE-2019-11463</a> MISC MISC
sass-lang -- libsass	The parsing component in LibSass through 3.5.5 allows attackers to cause a denial-of-service (uncontrolled recursion in Sass::Parser::parse_css_variable_value in parser.cpp).	2019-04-23	4.3	<a href="#">CVE-2018-20821</a> MISC
sass-lang -- libsass	LibSass 3.5.4 allows attackers to cause a denial-of-service (uncontrolled recursion in Sass::Complex_Selector::perform in ast.hpp and Sass::Inspect::operator in inspect.cpp).	2019-04-23	4.3	<a href="#">CVE-2018-20822</a> MISC
sem-cms -- semcms	An issue was discovered in SEMCMS 3.8. SEMCMS_Inquiry.php allows AID[] SQL Injection because the class.phpmailer.php inject_check_sql protection mechanism is incomplete.	2019-04-25	6.5	<a href="#">CVE-2019-11518</a> MISC
siteserver -- siteserver_cms	A issue was discovered in SiteServer CMS 6.9.0. It allows remote attackers to execute arbitrary code because an administrator can add the permitted file extension .aasp, which is converted to .asp because the "as" substring is deleted.	2019-04-22	6.5	<a href="#">CVE-2019-11401</a> MISC
struktur -- libheif	libheif 1.4.0 has a use-after-free in heif::HeifContext::Image::set_alpha_channel in heif_context.h because heif_context.cc mishandles references to non-existing alpha images.	2019-04-23	6.8	<a href="#">CVE-2019-11471</a> MISC MISC
veronalabs -- wp_statistics	The WP Statistics plugin through 12.6.2 for WordPress has XSS, allowing a remote attacker to inject arbitrary web script or HTML via the Referer header of a GET request.	2019-04-23	4.3	<a href="#">CVE-2019-10864</a> CONFIRM
verypdf -- verypdf	VeryPDF 4.1 has a Memory Overflow leading to Code Execution because pdfocx(CxImageTIF::operator in pdfocx.ocx (used by pdfeditor.exe and pdfcmd.exe) is mishandled.	2019-04-26	6.8	<a href="#">CVE-2019-11493</a> MISC
vestacp -- control_panel	Vesta Control Panel 0.9.8-23 allows XSS via a crafted URL.	2019-04-19	4.3	<a href="#">CVE-2019-9841</a> MISC CONFIRM CONFIRM
wavpack -- wavpack	WavpackSetConfiguration64 in pack_utils.c in libwavpack.a in WavPack through 5.1.0 has a "Conditional jump or move depends on uninitialised value" condition, which might allow attackers to cause a denial of service (application crash) via a DFF file that lacks valid sample-rate data.	2019-04-24	4.3	<a href="#">CVE-2019-11498</a> MISC MISC
wcms -- wcms	wcms/wex/finder/action.php in WCMS v0.3.2 has a Arbitrary File Upload Vulnerability via developer/finder because .php is a valid extension according to the fm_get_text_exts function.	2019-04-20	6.5	<a href="#">CVE-2019-11377</a> MISC MISC
whatsns -- whatsns	whatsns 4.0 allows index.php?inform/add.html qid SQL injection.	2019-04-22	6.5	<a href="#">CVE-2019-11451</a> MISC
whatsns -- whatsns	whatsns 4.0 allows index.php?admin_category/remove.html cid[] SQL injection.	2019-04-22	6.5	<a href="#">CVE-2019-11452</a> MISC
wifi_ftp_server_project -- wifi_ftp_server	An issue was discovered in the Medha WiFi FTP Server application 1.8.3 for Android. An attacker can read the username/password of a valid user via /data/data/com.medhaapps.wififtpserver/shared_prefs/com.medhaapps.wififtpserver_preferences.xml	2019-04-22	5.0	<a href="#">CVE-2019-11383</a> MISC
wordfence -- wordfence	The Wordfence plugin 7.2.3 for WordPress allows XSS via a unique attack vector.	2019-04-	4.3	<a href="#">CVE-2019-9669</a>

		25		MISC
zalora -- zalora	The Zalora application 6.15.1 for Android stores confidential information insecurely on the system (i.e. plain text), which allows a non-root user to find out the username/password of a valid user via /data/data/com.zalora.android/shared_prefs/login_data.xml.	2019-04-22	5.0	CVE-2019-11384 MISC
zohocorp -- servicedesk_plus	Zoho ManageEngine ServiceDesk 9.3 allows session hijacking and privilege escalation because an established guest session is automatically converted into an established administrator session when the guest user enters the administrator username, with an arbitrary incorrect password, in an mc/ login attempt within a different browser tab.	2019-04-24	6.5	CVE-2019-10008 EXPLOIT-DB CONFIRM

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
audiocodes -- 405hd_firmware	A missing password verification in the web interface in AudioCodes 405HD VoIP phone with firmware 2.2.12 allows an remote attacker (in the same network as the device) to change the admin password without authentication via a POST request.	2019-04-25	3.3	CVE-2018-16219 MISC
cmsmadesimple -- cms_made_simple	The File Manager in CMS Made Simple through 2.2.10 has Reflected XSS via the "New name" field in a Rename action.	2019-04-24	3.5	CVE-2019-11513 MISC
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155999.	2019-04-25	3.5	CVE-2019-4033 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159464.	2019-04-25	3.5	CVE-2019-4238 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157107.	2019-04-25	3.5	CVE-2019-4073 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157108.	2019-04-25	3.5	CVE-2019-4074 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157109.	2019-04-25	3.5	CVE-2019-4075 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157110.	2019-04-25	3.5	CVE-2019-4076 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157111.	2019-04-25	3.5	CVE-2019-4077 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to obtain sensitive document information under unusual circumstances. IBM X-Force ID: 158401.	2019-04-25	3.5	CVE-2019-4146 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158414.	2019-04-25	3.5	CVE-2019-4148 XF CONFIRM
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Web Catalog). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/L/I:N/A/N).	2019-04-23	2.6	CVE-2019-2605 MISC
oracle -- data_integrator	Vulnerability in the Oracle Data Integrator component of Oracle Fusion Middleware (subcomponent: ODI Tools). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Data Integrator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Data Integrator accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C/L/I:N/A/N).	2019-04-23	3.5	CVE-2019-2720 MISC
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2614 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2617 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2623 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2630 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with login to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	1.9	CVE-2019-2634 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Group Replication Plugin). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via MySQL Protocol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2636 MISC CONFIRM
	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J).			

oracle -- mysql_connector/j	Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with login to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2019-04-23	3.5	<a href="#">CVE-2019-2692</a> MISC
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: File Locking Services). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	2.1	<a href="#">CVE-2019-2577</a> MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	2.1	<a href="#">CVE-2019-2574</a> MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	2.1	<a href="#">CVE-2019-2678</a> MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:H).	2019-04-23	3.6	<a href="#">CVE-2019-2679</a> MISC
profiles_project -- profiles	XSS exists in the ProFiles 1.5 component for Joomla! via the name or path parameter when creating a new folder in the administrative panel.	2019-04-26	3.5	<a href="#">CVE-2018-18276</a> MISC
wolfcms -- wolfcms	WolfCMS 0.8.3.1 allows XSS via an SVG file to /?/admin/plugin/file_manager/browse/.	2019-04-25	3.5	<a href="#">CVE-2018-18823</a> MISC MISC MISC MISC
wolfcms -- wolfcms	WolfCMS v0.8.3.1 allows XSS via an SVG file to /?/admin/plugin/file_manager/browse/.	2019-04-25	3.5	<a href="#">CVE-2018-18824</a> MISC MISC MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aiikcms -- aiikcms	An issue was discovered in AiikCms v2.0. There is a File upload vulnerability, as demonstrated by an admin/page/system/nav.php request with PHP code in a .php file with the application/octet-stream content type.	2019-04-27	not yet calculated	<a href="#">CVE-2019-11568</a> MISC
aiikcms -- aiikcms	An issue was discovered in AiikCms v2.0. There is a SQL Injection vulnerability via \$_GET[del], as demonstrated by an admin/page/system/nav.php?del= URI.	2019-04-27	not yet calculated	<a href="#">CVE-2019-11567</a> MISC
apache -- pluto	The input fields of the Apache Pluto "Chat Room" demo portlet 3.0.0 and 3.0.1 are vulnerable to Cross-Site Scripting (XSS) attacks. Mitigation: * Uninstall the ChatRoomDemo war file - or - * migrate to version 3.1.0 of the chat-room-demo war file	2019-04-26	not yet calculated	<a href="#">CVE-2019-0186</a> MLIST MISC BID MLIST MISC EXPLOIT-DB MLIST
apache -- qpuid_proton	While investigating bug PROTON-2014, we discovered that under some circumstances Apache Qpid Proton versions 0.9 to 0.27.0 (C library and its language bindings) can connect to a peer anonymously using TLS "even when configured to verify the peer certificate" while used with OpenSSL versions before 1.1.0. This means that an undetected man in the middle attack could be constructed if an attacker can arrange to intercept TLS traffic.	2019-04-23	not yet calculated	<a href="#">CVE-2019-0223</a> MLIST BID REDHAT MISC MLIST MLIST MLIST MLIST
apache -- zeppelin	In Apache Zeppelin prior to 0.8.0 the cron scheduler was enabled by default and could allow users to run paragraphs as other users without authentication.	2019-04-23	not yet calculated	<a href="#">CVE-2018-1317</a> MLIST BID MLIST MISC
apache -- zeppelin	Apache Zeppelin prior to 0.7.3 was vulnerable to session fixation which allowed an attacker to hijack a valid user session. Issue was reported by "stone lone".	2019-04-23	not yet calculated	<a href="#">CVE-2017-12619</a> MLIST BID MLIST MISC
apparmor -- apparmor	In all versions of AppArmor mount rules are accidentally widened when compiled.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1585</a> MISC
aquaverde -- aquarius_cms	aquaverde Aquarius CMS through 4.3.5 writes POST and GET parameters (including passwords) to a log file because of incorrect if/else usage in the Log-File writer component.	2019-04-24	not yet calculated	<a href="#">CVE-2019-9734</a> MISC MISC
arrow-kt -- arrow	arrow-kt Arrow before 0.9.0 resolved Gradle build artifacts (for compiling and building the published JARs) over HTTP instead of HTTPS. Any of these dependent artifacts could have been maliciously compromised by an MITM attack.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11404</a> MISC MISC MISC MISC
asus -- zenfone_3_max_android_device	The ASUS ZenFone 3 Max Android device with a build fingerprint of asus/US_Phone/ASUS_X008_17.0/NRD90M/US_Phone-14.14.1711.92-20171208:user/release-keys contains the android framework (i.e., system_server) with a package name of android (versionCode=24, versionName=7.0) that has been modified by ASUS or another entity in the supply chain. The system_server process in the core android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage (i.e., sdcard). The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the	2019-04-25	not yet calculated	<a href="#">CVE-2018-14980</a> MISC MISC

	EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.			
asus -- zenfone_v_live_android_device	The ASUS Zenfone V Live Android device with a build fingerprint of asus/VZW_ASUS_A009/ASUS_A009:7.1.1/NMF26F/14.0610.1802.78-20180313:user/release-keys and the Asus ZenFone 3 Max Android device with a build fingerprint of asus/US_Phone/ASUS_X008_1:7.0/NRD90M/US_Phone-14.14.1711.92-20171208:user/release-keys both contain a pre-installed platform app with a package name of com.asus.splendidcommandagent (versionCode=1510200090, versionName=1.2.0.18_160928) that contains an exported service named com.asus.splendidcommandagent.SplendidCommandAgentService that allows any app co-located on the device to supply arbitrary commands to be executed as the system user. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. Executing commands as system user can allow a third-party app to video record the user's screen, factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), change the default Input Method Editor (IME) (e.g., keyboard) with one contained within the attacking app that contains keylogging functionality, obtain the user's text messages, and more.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14993</a> MISC MISC MISC
audiocodes -- audiocodes_405hd	A command injection (missing input validation, escaping) in the monitoring or memory status web interface in AudioCodes 405HD (firmware 2.2.12) VoIP phone allows an authenticated remote attacker in the same network as the device to trigger OS commands (like starting telnetd or opening a reverse shell) via a POST request to the web server. In combination with another attack (unauthenticated password change), the attacker can circumvent the authentication requirement.	2019-04-25	not yet calculated	<a href="#">CVE-2018-16216</a> MISC
c3p0 -- c3p0	c3p0 version < 0.9.5.4 may be exploited by a billion laughs attack when loading XML configuration due to missing protections against recursive entity expansion when loading configuration.	2019-04-22	not yet calculated	<a href="#">CVE-2019-5427</a> MISC
canonical -- appopt	Any Python module in sys.path can be imported if the command line of the process triggering the coredump is Python and the first argument is -m in Appopt before 2.19.2 function _python_module_path.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1341</a> MISC MISC
canonical -- oxide	A malicious webview could install long-lived unload handlers that re-use an incognito BrowserContext that is queued for destruction in versions of Oxide before 1.18.3.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1586</a> MISC
canonical -- snapd	A vulnerability in the seccomp filters of Canonical snapd before version 2.37.4 allows a strict mode snap to insert characters into a terminal on a 64-bit host. The seccomp rules were generated to match 64-bit ioctl(2) commands on a 64-bit platform; however, the Linux kernel only uses the lower 32 bits to determine which ioctl(2) commands to run. This issue affects: Canonical snapd versions prior to 2.37.4.	2019-04-23	not yet calculated	<a href="#">CVE-2019-7303</a> MISC MISC
canonical -- snapd	snap-confine as included in snapd before 2.39 did not guard against symlink races when performing the chdir() to the current working directory of the calling user, aka a "cwd restore permission bypass."	2019-04-24	not yet calculated	<a href="#">CVE-2019-11503</a> MLIST MISC MISC
canonical -- snapd	snap-confine in snapd before 2.38 incorrectly set the ownership of a snap application to the uid and gid of the first calling user. Consequently, that user had unintended access to a private /tmp directory.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11502</a> MLIST MISC MISC
canonical -- snapd	Canonical snapd before version 2.37.1 incorrectly performed socket owner validation, allowing an attacker to run arbitrary commands as root. This issue affects: Canonical snapd versions prior to 2.37.1.	2019-04-23	not yet calculated	<a href="#">CVE-2019-7304</a> MISC MISC MISC
canonical -- ubuntu_maas	A vulnerability in maasserver.api.get_file_by_name of Ubuntu MAAS allows unauthenticated network clients to download any file. This issue affects: Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2014-1426</a> MISC
canonical -- ubuntu_maas	A vulnerability in generate_filestorage_key of Ubuntu MAAS allows an attacker to brute-force filenames. This issue affects Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2014-1428</a> MISC
canonical -- ubuntu_maas	A vulnerability in the REST API of Ubuntu MAAS allows an attacker to cause a logged-in user to execute commands via cross-site scripting. This issue affects MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2014-1427</a> MISC
canonical -- ubuntu_maas	The SeaMicro provisioning of Ubuntu MAAS logs credentials, including username and password, for the management interface. This issue affects Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1320</a> MISC
canonical -- ubuntu_selinux_initscript	The Ubuntu SELinux initscript before version 1.0:10 used touch to create a lockfile in a world-writable directory. If the OS kernel does not have symlink protections then an attacker can cause a zero byte file to be allocated on any writable filesystem.	2019-04-22	not yet calculated	<a href="#">CVE-2011-3151</a> MISC
cerner -- connectivity_engine_4_devices	An issue was discovered on Cerner Connectivity Engine (CCE) 4 devices. The hostname, timezone, and NTP server configurations on the CCE device are vulnerable to command injection by sending a crafted configuration file over the network.	2019-04-25	not yet calculated	<a href="#">CVE-2018-20053</a> MISC
cerner -- connectivity_engine_4_devices	An issue was discovered on Cerner Connectivity Engine (CCE) 4 devices. The user running the main CCE firmware has NOPASSWD sudo privileges to several utilities that could be used to escalate privileges to root. One example is the "sudo ln -s /tmp/script /etc/cron.hourly/script" command.	2019-04-25	not yet calculated	<a href="#">CVE-2018-20052</a> MISC
check_point -- zonealarm_and_endpoint_security_client_for_windows	A hard-link created from log file archive of Check Point ZoneAlarm up to 15.4.062 or Check Point Endpoint Security client for Windows before E80.96 to any file on the system will get its permission changed so that all users can access that linked file. Doing this on files with limited access gains the local attacker higher privileges to the file.	2019-04-22	not yet calculated	<a href="#">CVE-2019-8452</a> MISC
cloud_foundry -- bosh_backup_and_restore_cli	Cloud Foundry BOSH Backup and Restore CLI, all versions prior to 1.5.0, does not check the authenticity of backup scripts in BOSH. A remote authenticated malicious user can modify the metadata file of a Bosh Backup and Restore job to request extra backup files from different jobs upon restore. The exploited hooks in this metadata script were only maintained in the cfr-etc-d-release, so clusters deployed with the BBR job for etcd in this release are vulnerable.	2019-04-24	not yet calculated	<a href="#">CVE-2019-3786</a> CONFIRM
cloud_foundry -- cf-deployment	Cloud Foundry cf-deployment, versions prior to 7.9.0, contain java components that are using an insecure protocol to fetch dependencies when building. A remote unauthenticated malicious attacker could hijack the DNS entry for the dependency, and inject malicious code into the component.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3801</a> CONFIRM
cloud_foundry -- routing_release	Cloud Foundry Routing Release, all versions prior to 0.188.0, contains a vulnerability that can hijack the traffic to route services hosted outside the platform. A user with space developer permissions can create a private domain that shadows the external domain of the route service, and map that route to an app. When the gorouter receives traffic destined for the external route service, this traffic will instead be directed to the internal app using the shadow route.	2019-04-24	not yet calculated	<a href="#">CVE-2019-3789</a> CONFIRM
cloud_foundry -- uaa_release	Cloud Foundry UAA Release, versions prior to 71.0, allows clients to be configured with an insecure redirect uri. Given a UAA client was configured with a wildcard in the redirect uri's subdomain, a remote malicious unauthenticated user can craft a phishing link to get a UAA access code from the victim.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3788</a> CONFIRM
contao -- contao	Contao 3.0.0 to 3.5.30 and 4.0.0 to 4.4.7 contains an SQL injection vulnerability in the back end as well as in the listing module.	2019-04-25	not yet calculated	<a href="#">CVE-2017-16558</a> CONFIRM CONFIRM
cribl -- cribl_ui	Cribl UI 1.5.0 allows remote attackers to run arbitrary commands via an unauthenticated web request.	2019-04-23	not yet calculated	<a href="#">CVE-2019-11076</a> CONFIRM MISC
daviewindy -- daviewindy	DaviewIndy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed Image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	not yet calculated	<a href="#">CVE-2019-9137</a> MISC
dell_emc -- idrac	Dell EMC iDRAC6 versions prior to 2.92, iDRAC7/iDRAC8 versions prior to 2.61.60.60, and iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22 and 3.23.23.23 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to crash the webserver or execute arbitrary code on the system with privileges of the webserver by sending specially crafted input data to the affected system.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3705</a> MISC
	Dell EMC iDRAC9 versions prior to 3.30.30.30 contain an authentication bypass vulnerability.		not yet	<a href="#">CVE-2019-3707</a>

dell_emc -- idrac9	A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted input data to the WS-MAN interface.	2019-04-26	calculated	MISC
dell_emc -- idrac9	Dell EMC iDRAC9 versions prior to 3.24.24.24, 3.21.26.22, 3.22.22.22 and 3.21.25.22 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted data to the iDRAC web interface.	2019-04-26	not yet calculated	CVE-2019-3706 MISC
dell_emc -- open_manage_system_administrator	Dell EMC Open Manage System Administrator (OMSA) versions prior to 9.3.0 contain a Directory Traversal Vulnerability. A remote authenticated malicious user with admin privileges could potentially exploit this vulnerability to gain unauthorized access to the file system by exploiting insufficient sanitization of input parameters.	2019-04-25	not yet calculated	CVE-2019-3720 MISC
dell_emc -- open_manage_system_administrator	Dell EMC Open Manage System Administrator (OMSA) versions prior to 9.3.0 contain an Improper Range Header Processing Vulnerability. A remote unauthenticated attacker may send crafted requests with overlapping ranges to cause the application to compress each of the requested bytes, resulting in a crash due to excessive memory consumption and preventing users from accessing the system.	2019-04-25	not yet calculated	CVE-2019-3721 MISC
deltek -- vision	Deltek Vision 7.x before 7.6 permits the execution of any attacker supplied SQL statement through a custom RPC over HTTP protocol. The Vision system relies on the client binary to enforce security rules and integrity of SQL statements and other content being sent to the server. Client HTTP calls can be manipulated by one of several means to execute arbitrary SQL statements (similar to SQLi) or possibly have unspecified other impact via this custom protocol. To perform these attacks an authenticated session is first required. In some cases client calls are obfuscated by encryption, which can be bypassed due to hard-coded keys and an insecure key rotation protocol. Impacts may include remote code execution in some deployments; however, the vendor states that this cannot occur when the installation documentation is heeded.	2019-04-24	not yet calculated	CVE-2018-18251 CONFIRM
dentsply_sirona -- sidexis	A default username and password in Dentsply Sirona Sidexis 4.2 and possibly others allows an attacker to gain administrative access to the application server.	2019-04-24	not yet calculated	CVE-2019-11081 MISC
dillon_kane_group -- tidal_workload_automation_agent	An issue was discovered in Dillon Kane Tidal Workload Automation Agent 3.2.0.5 (formerly known as Cisco Workload Automation or CWA). The Enterprise Scheduler for AIX allows local users to gain privileges via Command Injection in crafted Tidal Job Buffers (TJB) parameters. NOTE: this vulnerability exists because the CVE-2014-3272 solution did not address AIX operating systems.	2019-04-26	not yet calculated	CVE-2019-6689 MISC
dovecot -- dovecot	The JSON encoder in Dovecot before 2.3.5.2 allows attackers to repeatedly crash the authentication service by attempting to authenticate with an invalid UTF-8 sequence as the username.	2019-04-24	not yet calculated	CVE-2019-10691 MUST MUST
dropbox -- lepton	io/ZlibCompression.cc in the decompression component in Dropbox Lepton 1.2.1 allows attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact by crafting a jpg image file. The root cause is a missing check of header payloads that may be (incorrectly) larger than the maximum file size.	2019-04-23	not yet calculated	CVE-2018-20819 MISC
eclipse -- jetty	In Eclipse Jetty version 7.x, 8.x, 9.2.27 and older, 9.3.26 and older, and 9.4.16 and older, the server running on any OS and Jetty version combination will reveal the configured fully qualified directory base resource location on the output of the 404 error for not finding a Context that matches the requested path. The default server behavior on jetty-distribution and jetty-home will include at the end of the Handler tree a DefaultHandler, which is responsible for reporting this 404 error, it presents the various configured contexts as HTML for users to click through to. This produced HTML includes output that contains the configured fully qualified directory base resource location for each context.	2019-04-22	not yet calculated	CVE-2019-10247 CONFIRM
eclipse -- jetty	In Eclipse Jetty version 9.2.27, 9.3.26, and 9.4.16, the server running on Windows is vulnerable to exposure of the fully qualified Base Resource directory name on Windows to a remote client when it is configured for showing a Listing of directory contents. This information reveal is restricted to only the content in the configured base resource directories.	2019-04-22	not yet calculated	CVE-2019-10246 CONFIRM
eclipse -- openj9	In Eclipse OpenJ9 prior to the 0.14.0 release, the Java bytecode verifier incorrectly allows a method to execute past the end of bytecode array causing crashes. Eclipse OpenJ9 v0.14.0 correctly detects this case and rejects the attempted class load.	2019-04-19	not yet calculated	CVE-2019-10245 CONFIRM
eclipse -- vorto	Eclipse Vorto versions prior to 0.11 resolved Maven build artifacts for the Xtext project over HTTP instead of HTTPS. Any of these dependent artifacts could have been maliciously compromised by a MITM attack. Hence produced build artifacts of Vorto might be infected.	2019-04-22	not yet calculated	CVE-2019-10248 CONFIRM
ekiga -- ekiga	Ekiga versions before 3.3.0 attempted to load a module from /tmp/ekiga_test.so.	2019-04-22	not yet calculated	CVE-2011-1830 MISC
envoy_proxy -- envoy	When parsing HTTP/1.x header values, Envoy 1.9.0 and before does not reject embedded zero characters (NUL, ASCII 0x0). This allows remote attackers crafting header values containing embedded NUL characters to potentially bypass header matching rules, gaining access to unauthorized resources.	2019-04-25	not yet calculated	CVE-2019-9900 REDHAT CONFIRM CONFIRM CONFIRM
envoy_proxy -- envoy	Envoy 1.9.0 and before does not normalize HTTP URL paths. A remote attacker may craft a relative path, e.g., something/.admin, to bypass access control, e.g., a block on /admin. A backend server could then interpret the non-normalized path and provide an attacker access beyond the scope provided for by the access control policy.	2019-04-25	not yet calculated	CVE-2019-9901 CONFIRM CONFIRM CONFIRM
essential_products -- phone_android_device	The Essential Phone Android device with a build fingerprint of essential/mata/mata;8.1.0/OPM1.180104.166/297:user/release-keys contains a pre-installed platform app with a package name of com.ts.android.hiddenmenu (versionName=1.0, platformBuildVersionName=8.1.0) that contains an exported activity app component named com.ts.android.hiddenmenu.rtn.RTNResetActivity that allows any app co-located on the device to programmatically initiate a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	CVE-2018-14994 MISC MISC MISC
flarum -- flarum	User/Command/ConfirmEmailHandler.php in Flarum before 0.1.0-beta.8 mishandles invalidation of user email tokens.	2019-04-24	not yet calculated	CVE-2019-11514 MISC MISC
gitea -- gitea	Gitea before 1.8.0 allows 1FA for user accounts that have completed 2FA enrollment. If a user's credentials are known, then an attacker could send them to the API without requiring the 2FA one-time password.	2019-04-27	not yet calculated	CVE-2019-11576 MISC MISC
gnome -- nautilus	An issue was discovered in GNOME Nautilus 3.30 prior to 3.30.6 and 3.32 prior to 3.32.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCSTI ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCSTI ioctl on 64-bit systems, similar to CVE-2019-10063.	2019-04-22	not yet calculated	CVE-2019-11461 MISC
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/faqmasterformupdate.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15581 CONFIRM
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/boardgroup_form_update.php and adm/boardgroup_list_update.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15584 CONFIRM CONFIRM
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/sms_admin/num_book_write.php and adm/sms_admin/num_book_update.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15582 CONFIRM CONFIRM
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/contentformupdate.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	CVE-2018-15580 CONFIRM
google -- tensorflow	Invalid memory access and/or a heap buffer overflow in the TensorFlow XLA compiler in Google TensorFlow before 1.7.1 could cause a crash or read from other parts of process memory via a crafted configuration file.	2019-04-24	not yet calculated	CVE-2018-10055 CONFIRM
google -- tensorflow	Google TensorFlow 1.7.x and earlier is affected by a Buffer Overflow vulnerability. The type of exploitation is context-dependent.	2019-04-24	not yet calculated	CVE-2018-7575 CONFIRM
google -- tensorflow	Memcpy parameter overlap in Google Snappy library 1.1.4, as used in Google TensorFlow before 1.7.1, could result in a crash or read from other parts of process memory.	2019-04-24	not yet calculated	CVE-2018-7577 CONFIRM



google -- tensorflow	Google TensorFlow 1.6.x and earlier is affected by a Null Pointer Dereference vulnerability. The type of exploitation is: context-dependent.	2019-04-24	not yet calculated	<a href="#">CVE-2018-7574</a> CONFIRM
heketi -- heketi	It was found that default configuration of Heketi does not require any authentication potentially exposing the management interface to misuse. This issue only affects heketi as shipped with OpenShift Container Platform 3.11.	2019-04-22	not yet calculated	<a href="#">CVE-2019-3899</a> CONFIRM
hisilicon -- hi3510_firmware	Incorrect access control in the RTSP stream and web portal on all IP cameras based on Hisilicon Hi3510 firmware (until Webware version V1.0.1) allows attackers to view an RTSP stream by connecting to the stream with hidden credentials (guest or user) that are neither displayed nor configurable in the camera's CamHi or keye mobile management application. This affects certain devices labeled as Hi3510, Hi3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Uniotek, ESCAM, etc.	2019-04-23	not yet calculated	<a href="#">CVE-2019-10711</a> MISC
hisilicon -- hi3510_firmware	Insecure permissions in the Web management portal on all IP cameras based on Hisilicon Hi3510 firmware allow authenticated attackers to receive a network's cleartext WiFi credentials via a specific HTTP request. This affects certain devices labeled as Hi3510, Hi3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Uniotek, ESCAM, etc.	2019-04-23	not yet calculated	<a href="#">CVE-2019-10710</a> MISC
hostapd_and_wpa_supplicant -- hostapd_and_wpa_supplicant	The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not validate fragmentation reassembly state properly for a case where an unexpected fragment could be received. This could result in process termination due to a NULL pointer dereference (denial of service). This affects eap_server/eap_server_pwd.c and eap_peer/eap_pwd.c.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11555</a> MLIST MISC MISC MISC
hr-technologies -- easytorecruit	In EasyToRecruit (EZR) before 2.11, the upload feature and the Candidate Profile Management feature are prone to Cross Site Scripting (XSS) injection in multiple locations.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11032</a> MISC MISC
ibm -- mq	IBM MQ 8.0.0.0 through 8.0.0.10, 9.0.0.0 through 9.0.0.5, and 9.1.0.0 through 9.1.1 is vulnerable to a denial of service attack within the TLS key renegotiation function. IBM X-Force ID: 156564.	2019-04-19	not yet calculated	<a href="#">CVE-2019-4055</a> BID XF CONFIRM
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.1, 5.2.6.3, 6, 6.0.0.0, and 6.0.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 147294.	2019-04-25	not yet calculated	<a href="#">CVE-2018-1720</a> XF CONFIRM
imperva -- securesphere	A command injection vulnerability in PWS in Imperva SecureSphere 13.0.0.10 and 13.1.0.10 Gateway allows an attacker with authenticated access to execute arbitrary OS commands on a vulnerable installation.	2019-04-25	not yet calculated	<a href="#">CVE-2018-16660</a> MISC MISC
jakub_chodounskey -- bonobo_git_server	Improper handling of extra parameters in the AccountController (User Profile edit) in Jakub Chodounskey Bonobo Git Server before 6.5.0 allows authenticated users to gain application administrator privileges via additional form parameter submissions.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11218</a> CONFIRM MISC
jakub_chodounskey -- bonobo_git_server	The GitController in Jakub Chodounskey Bonobo Git Server before 6.5.0 allows execution of arbitrary commands in the context of the web server via a crafted http request.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11217</a> CONFIRM MISC
juju_core -- joyent_provider	Juju Core's Joyent provider before version 1.25.5 uploads the user's private ssh key.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1316</a> MISC
kubernetes -- kubernetes	In Kubernetes v1.8.x-v1.14.x, schema info is cached by kubectrl in the location specified by --cache-dir (defaulting to \$HOME/.kube/http-cache), written with world-writable permissions (rw-rw-rw-). If --cache-dir is specified and pointed at a different location accessible to other users/groups, the written files may be modified by other users/groups and disrupt the kubectrl invocation.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11244</a> BID MISC
leagoo -- p1_android_device	The Leagoo P1 Android device with a build fingerprint of sp7731c_1h10_32v4_bird:6.0/MRA58K/android.20170629.214736:user/release-keys contains the android framework (i.e., system_server) with a package name of android that has been modified by Leagoo or another entity in the supply chain. The system_server process in the core Android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage. The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14997</a> MISC MISC MISC
leagoo -- p1_android_device	The Leagoo P1 device with a build fingerprint of sp7731c_1h10_32v4_bird:6.0/MRA58K/android.20170629.214736:user/release-keys contains a pre-installed platform app with a package name of com.wtk.factory (versionCode=1, versionName=1.0) that contains an exported broadcast receiver named com.wtk.factory.MMTestReceiver allows any app co-located on the device to programmatically initiate a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14999</a> MISC MISC MISC
lenovo -- system_x	In various firmware versions of Lenovo System x, the integrated management module II (IMM2)'s first failure data capture (FFDC) includes the web server's private key in the generated log file for support.	2019-04-22	not yet calculated	<a href="#">CVE-2019-6157</a> MISC
librenms -- librenms	LibreNMS 1.46 allows remote attackers to execute arbitrary OS commands by using the \$_POST[community] parameter to html/pages/addhost.inc.php during creation of a new device, and then making a /ajax_output.php?id=capture&format=text&type=snmpwalk&hostname=localhost request that triggers html/includes/output/capture.inc.php command mishandling.	2019-04-24	not yet calculated	<a href="#">CVE-2018-20434</a> MISC MISC MISC
libseccomp-golang -- libseccomp-golang	libseccomp-golang 0.9.0 and earlier incorrectly generates BPFs that OR multiple arguments rather than ANDING them. A process running under a restrictive seccomp filter that specified multiple syscall arguments could bypass intended access restrictions by specifying a single matching argument.	2019-04-24	not yet calculated	<a href="#">CVE-2017-18367</a> MLIST MISC MISC
liferay -- portal_community_edition	An issue was discovered in Liferay Portal CE 7.1.2 GA3. An attacker can use Liferay's Groovy script console to execute OS commands. Commands can be executed via a [command].execute() call, as demonstrated by "def cmd =" in the ServerAdminPortlet_script value to group/control_panel/manage. Valid credentials for an application administrator user account are required.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11444</a> MISC MISC
linux -- linux_kernel	The Linux kernel before 5.1-rc5 allows page-> refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/splice.c, include/linux/mm.h, include/linux/pipe_fs_i.h, kernel/trace/trace.c, mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.	2019-04-23	not yet calculated	<a href="#">CVE-2019-11487</a> BID MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
linux -- linux_kernel	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3900</a> BID CONFIRM CONFIRM
	A flaw was found in the Linux kernel's vfoo interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfoo driver, such as vfoo-pci, and the		not yet	<a href="#">CVE-2019-3882</a>

linux -- linux_kernel	local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.	2019-04-24	calculated	<a href="#">CONFIRM</a>
linux -- linux_kernel	A race condition in perf_event_open() allows local attackers to leak sensitive data from setuid programs. As no relevant locks (in particular the cred_guard_mutex) are held during the ptrace_may_access() call, it is possible for the specified target task to perform an execve() syscall with setuid execution before perf_event_alloc() actually attaches to it, allowing an attacker to bypass the ptrace_may_access() check and the perf_event_exit_task(current) call that is performed in install_exec_creds() during privileged execve() calls. This issue affects kernel versions before 4.8.	2019-04-22	not yet calculated	<a href="#">CVE-2019-3901</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
lxd -- lxd	LXD before version 0.19-0ubuntu5 doUidshiftIntoContainer() has an unsafe Chmod() call that races against the stat in the Filepath.Walk() function. A symbolic link created in that window could cause any file on the system to have any mode of the attacker's choice.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1340</a> <a href="#">MISC</a>
mercurial -- mercurial	A flaw was found in Mercurial before 4.9. It was possible to use symlinks and subrepositories to defeat Mercurial's path-checking logic and write files outside a repository.	2019-04-22	not yet calculated	<a href="#">CVE-2019-3902</a> <a href="#">CONFIRM</a> <a href="#">LIST</a> <a href="#">MISC</a>
mount.ecryptfs_private -- mount.ecryptfs_private	When mount.ecryptfs_private before version 87-0ubuntu1.2 calls setreuid() it doesn't also set the effective group id. So when it creates the new version, mtab.tmp, it's created with the group id of the user running mount.ecryptfs_private.	2019-04-22	not yet calculated	<a href="#">CVE-2011-3145</a> <a href="#">MISC</a>
mozilla -- firefox	On Android systems, Firefox can load a library from APITRACE_LIB, which is writable by all users and applications. This could allow malicious third party applications to execute a man-in-the-middle attack if a malicious code was written to that location and loaded. *Note: This issue only affects Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9798</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A latent vulnerability exists in the Prio library where data may be read from uninitialized memory for some functions, leading to potential memory corruption. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9805</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	In Firefox Developer Tools it is possible that pasting the result of the 'Copy as cURL' command into a command shell on macOS will cause the execution of unintended additional bash script commands if the URL was maliciously crafted. This is the result of an issue with the native version of Bash on macOS. *Note: This issue only affects macOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9804</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Insufficient bounds checking of data during inter-process communication might allow a compromised content process to be able to read memory from the parent process under certain conditions. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9799</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	The Upgrade-Insecure-Requests (UIR) specification states that if UIR is enabled through Content Security Policy (CSP), navigation to a same-origin URL must be upgraded to HTTPS. Firefox will incorrectly navigate to an HTTP URL rather than perform the security upgrade requested by the CSP in some circumstances, allowing for potential man-in-the-middle attacks on the linked resources. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9803</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A service worker can send the activate event on itself periodically which allows it to run perpetually, allowing it to monitor activity by users. Affects all versions prior to Firefox 60.	2019-04-26	not yet calculated	<a href="#">CVE-2018-5179</a> <a href="#">MISC</a>
mozilla -- firefox	Unsanitized output in the browser UI leaves HTML tags in place and can result in arbitrary code execution in Firefox before version 58.0.1.	2019-04-26	not yet calculated	<a href="#">CVE-2018-5124</a> <a href="#">MISC</a>
mozilla -- firefox	Cross-origin images can be read in violation of the same-origin policy by exporting an image after using createImageBitmap to read the image and then rendering the resulting bitmap image within a canvas element. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9797</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A vulnerability exists during authorization prompting for FTP transaction where successive modal prompts are displayed and cannot be immediately dismissed. This allows for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9806</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If a Sandbox content process is compromised, it can initiate an FTP download which will then use a child process to render the downloaded data. The downloaded data can then be passed to the Chrome process with an arbitrary file length supplied by an attacker, bypassing sandbox protections and allow for a potential memory read of adjacent data from the privileged Chrome process, which may include sensitive data. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9802</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Cross-origin images can be read from a canvas element in violation of the same-origin policy using the transferFromImageBitmap method. *Note: This only affects Firefox 65. Previous versions are unaffected.*. This vulnerability affects Firefox < 65.0.1.	2019-04-26	not yet calculated	<a href="#">CVE-2018-18511</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	When arbitrary text is sent over an FTP connection and a page reload is initiated, it is possible to create a modal alert message with this text as the content. This could potentially be used for social engineering attacks. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9807</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If WebRTC permission is requested from documents with data: or blob: URLs, the permission notifications do not properly display the originating domain. The notification states "Unknown origin" as the requestee, leading to user confusion about which site is asking for this permission. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9808</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If the source for resources on a page is through an FTP connection, it is possible to trigger a series of modal alert messages for these resources through invalid credentials or locations. These messages cannot be immediately dismissed, allowing for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9809</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A crash can occur when processing a crafted S/MIME message or an XPI package containing a crafted signature. This can be used as a denial-of-service (DOS) attack because Thunderbird reopens the last seen message on restart, triggering the crash again. This vulnerability affects Thunderbird < 60.5.	2019-04-26	not yet calculated	<a href="#">CVE-2018-18513</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A flaw during verification of certain S/MIME signatures causes emails to be shown in Thunderbird as having a valid digital signature, even if the shown message contents aren't covered by the signature. The flaw allows an attacker to reuse a valid S/MIME signature to craft an email message with arbitrary content. This vulnerability affects Thunderbird < 60.5.1.	2019-04-26	not yet calculated	<a href="#">CVE-2018-18509</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	A vulnerability was discovered where specific command line arguments are not properly discarded during Firefox invocation as a shell handler for URLs. This could be used to retrieve and execute files whose location is supplied through these command line arguments if Firefox is configured as the default URI handler for a given URI scheme in third party applications and these applications insufficiently sanitize URL data. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9794</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9810</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	Incorrect handling of __proto__ mutations may lead to type confusion in IonMonkey JIT code and can be leveraged for arbitrary memory read and write. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9813</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	Firefox will accept any registered Program ID as an external protocol handler and offer to launch this local application when given a matching URL on Windows operating systems. This should only happen if the program has specifically registered itself as a "URL Handler" in the Windows registry. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9801</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. This vulnerability could allow an attacker to create an arbitrary value in compiled JavaScript, for which the range analysis will infer a fully controlled, incorrect range in circumstances where users have explicitly disabled Spectre mitigations. *Note: Spectre mitigations are currently enabled for all users by default settings.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9793</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript		not yet	<a href="#">CVE-2019-9792</a> <a href="#">MISC</a>

mozilla -- thunderbird_and_firefox_esr_and_firefox	to achieve memory corruption, which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	calculated	MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR). This allows for possible arbitrary reading and writing of objects during an exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9791 MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A vulnerability where type-confusion in the IonMonkey just-in-time (JIT) compiler could potentially be used by malicious JavaScript to trigger a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9795 MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A use-after-free vulnerability can occur when the SMIL animation controller incorrectly registers with the refresh driver twice when only a single registration is expected. When a registration is later freed with the removal of the animation controller element, the refresh driver incorrectly leaves a dangling pointer to the driver's observer array. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9796 MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant device with a build fingerprint of Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys, the ZTE ZMAX Pro with a build fingerprint of ZTE/P895T20/urd:6.0.1/MMB29M/20170418.114928:user/release-keys, and the T-Mobile Revvl Plus with a build fingerprint of Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys all contain a vulnerable, pre-installed Rich Communication Services (RCS) app. These devices contain an that app has a package name of com.suntek.mway.rcs.app.service (versionCode=1, versionName=RCS_sdk_M_native_20161008_01; versionCode=1, versionName=RCS_sdk_M_native_20170406_01) with a broadcast receiver app component named com.suntek.mway.rcs.app.test.TestReceiver and a refactored version of the app with a package name of com.rcs.gsma.na.sdk (versionCode=1, versionName=RCS_SDK_20170804_01) with a broadcast receiver app component named com.rcs.gsma.na.test.TestReceiver allow any app co-located on the device to programmatically send text messages where the number and body of the text message is controlled by the attacker due to an exported broadcast receiver app component. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. A separate vulnerability in the app allows a zero-permission app to programmatically delete text messages, so the sent text messages can be removed to not alert the user.	2019-04-25	not yet calculated	CVE-2018-14990 MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant device with a build fingerprint of Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys, the ZTE ZMAX Pro with a build fingerprint of ZTE/P895T20/urd:6.0.1/MMB29M/20170418.114928:user/release-keys, and the T-Mobile Revvl Plus with a build fingerprint of Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys all contain a vulnerable, pre-installed Rich Communication Services (RCS) app. These devices contain an that app has a package name of com.suntek.mway.rcs.app.service (versionCode=1, versionName=RCS_sdk_M_native_20161008_01; versionCode=1, versionName=RCS_sdk_M_native_20170406_01) with an exported content provider named com.suntek.mway.rcs.app.service.provider.message.MessageProvider and a refactored version of the app with a package name of com.rcs.gsma.na.sdk (versionCode=1, versionName=RCS_SDK_20170804_01) with a content provider named com.rcs.gsma.na.provider.message.MessageProvider allow any app co-located on the device to read, write, insert, and modify the user's text messages. This is enabled by an exported content provider app component that serves as a wrapper to the official content provider that contains the user's text messages. This app cannot be disabled by the user and the attack can be performed by a zero-permission app.	2019-04-25	not yet calculated	CVE-2018-14991 MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant (Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys) and the T-Mobile Revvl Plus (Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys) Android devices contain a pre-installed platform app with a package name of com.qualcomm.qti.telephony.extcarrierpack (versionCode=25, versionName=7.1.1) containing an exported broadcast receiver app component named com.qualcomm.qti.telephony.extcarrierpack.UiccReceiver that allows any app co-located on the device to programmatically perform a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	CVE-2018-15003 MISC MISC MISC
nopcommerce -- nopcommerce	Libraries/Nop.Services/Localization/LocalizationService.cs in nopCommerce through 4.10 allows XXE via the "Configurations -> Languages -> Edit Language -> Import Resources -> Upload XML file" screen.	2019-04-25	not yet calculated	CVE-2019-11519 MISC MISC
omniauth_ruby_gem -- omniauth_ruby_gem	The request phase of the OmniAuth Ruby gem is vulnerable to Cross-Site Request Forgery when used as part of the Ruby on Rails framework, allowing accounts to be connected without user intent, user interaction, or feedback to the user. This permits a secondary account to be able to sign into the web application as the primary account.	2019-04-26	not yet calculated	CVE-2015-9284 MISC MISC MLIST
openapi_tools -- openapi_generator	OpenAPI Tools OpenAPI Generator before 4.0.0-20190419.052012-560 uses http:// URLs in various build.gradle, build.gradle.mustache, and build.sbt files, which may have caused insecurely resolved dependencies.	2019-04-22	not yet calculated	CVE-2019-11405 MISC MISC MISC
oppo -- f5_android_device	The Oppo F5 Android device with a build fingerprint of OPPO/CPH1723/CPH1723:7.1.1/N6F26Q/1513597833:user/release-keys contains a pre-installed platform app with a package name of com.dropboxchmmod (versionCode=1, versionName=1.0) that contains an exported service named com.dropboxchmmod.DropboxChmmodService that allows any app co-located on the device to supply arbitrary commands to be executed as the system user. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. Executing commands as system user can allow a third-party app to video record the user's screen, factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), and obtains the user's text messages, and more. This vulnerability can also be used to secretly record audio of the user without their awareness on the Oppo F5 device. The pre-installed com.oppo.engineermode app (versionCode=25, versionName=V1.01) has an exported activity that can be started to initiate a recording and quickly dismissed. The activity can be started in a way that the user will not be able to see the app in the recent apps list. The resulting audio amr file can be copied from a location on internal storage using the arbitrary command execution as system user vulnerability. Executing commands as system user can allow a third-party app to factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), change the default Input Method Editor (IME) (e.g., keyboard) with one contained within the attacking app that contains keylogging functionality, obtain the user's text messages, and more.	2019-04-25	not yet calculated	CVE-2018-14996 MISC MISC MISC
oracle -- berkeley_db	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are Prior to 6.138, prior to 6.2.38 and prior to 18.1.32. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Data Store. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	not yet calculated	CVE-2019-2708 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-26	not yet calculated	CVE-2019-2725 MISC
phablet-team -- content_hub	Content Hub before version 0.04-15.04.20150331-0ubuntu1.0 DBUS API only requires a file path for a content item, it doesn't actually require the confined app have access to the file to create a transfer. This could allow a malicious application using the DBUS API to export	2019-04-22	not yet calculated	CVE-2015-1327 MISC

	file:///etc/passwd which would then send a copy of that file to another app.			
phablet-team -- ubuntu-download-manager	UDM provides support for running commands after a download is completed, this is currently made use of for click package installation. This functionality was not restricted to unconfined applications. Before UDM version 1.2+16.04.20160408-0ubuntu1 any confined application could make use of the UDM C++ API to run arbitrary commands in an unconfined environment as the phablet user.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1579</a> MISC
pivotal -- apps_manager_release	Pivotal Apps Manager Release, versions 665.0.x prior to 665.0.28, versions 666.0.x prior to 666.0.21, versions 667.0.x prior to 667.0.7, contain an invitation service that accepts HTTP. A remote unauthenticated user could listen to network traffic and gain access to the authorization credentials used to make the invitation requests.	2019-04-24	not yet calculated	<a href="#">CVE-2019-3793</a> CONFIRM
plum -- compass_android_device	The Plum Compass Android device with a build fingerprint of PLUM/c179_hwf_221/c179_hwf_221:6.0/MRA58K/W16.51.5-22:user/release-keys contains a pre-installed platform app with a package name of com.android.settings (versionCode=23, versionName=6.0-eng.root.20161223.224055) that contains an exported broadcast receiver app component which allows any app co-located on the device to programmatically perform a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14989</a> MISC MISC MISC
polycom -- vxv_products_using_ucs_software	VVX products using UCS software version 5.8.0 and earlier with Better Together over Ethernet Connector (BTtoE) application version 3.8.0 and earlier uses hard-coded credentials to establish a connection between the host application and device.	2019-04-23	not yet calculated	<a href="#">CVE-2019-10688</a> CONFIRM
printrion -- printrion	An XML external entity (XXE) vulnerability in PrinterOn version 4.1.4 and lower allows remote authenticated users to read arbitrary files or conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request.	2019-04-23	not yet calculated	<a href="#">CVE-2018-17169</a> MISC
projectsend -- projectsend	ProjectSend before r1070 writes user passwords to the server logs.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11492</a> CONFIRM
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4 and 8.3RX before 8.3R7.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2 and 5.4RX before 5.4R7.1, an unauthenticated, remote attacker can conduct a session hijacking attack.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11540</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.2RX before 8.2R12.1, users using SAML authentication with the Reuse Existing NC (Pulse) Session option may see authentication leaks.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11541</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, an authenticated attacker (via the admin web interface) can send a specially crafted message resulting in a stack buffer overflow.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11542</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, the admin web interface allows an authenticated attacker to inject and execute commands.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11539</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1, an NFS problem could allow an authenticated attacker to access the contents of arbitrary files on the affected device.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11538</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	XSS exists in the admin web console in Pulse Secure Pulse Connect Secure (PCS) 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, and 5.2RX before 5.2R12.1.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11543</a> BID CONFIRM MISC
python-dbusmock -- python-dbusmock	python-dbusmock before version 0.15.1 AddTemplate() D-Bus method call or DBusTestCase.spawn_server_template() method could be tricked into executing malicious code if an attacker supplies a .pyc file.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1326</a> MISC
robotronic -- runasspc	Robotronic RunAsSpc 3.7.0.0 protects stored credentials insufficiently, which allows locally authenticated attackers (under the same user context) to obtain cleartext credentials of the stored account.	2019-04-24	not yet calculated	<a href="#">CVE-2019-10239</a> MISC
rockwell_automation -- micrologix_and_compactlogix_controllers	In Rockwell Automation MicroLogix 1400 Controllers Series A, All Versions Series B, v15.002 and earlier, MicroLogix 1100 Controllers v14.00 and earlier, CompactLogix 5370 L1 controllers v30.014 and earlier, CompactLogix 5370 L2 controllers v30.014 and earlier, CompactLogix 5370 L3 controllers (includes CompactLogix GuardLogix controllers) v30.014 and earlier, an open redirect vulnerability could allow a remote unauthenticated attacker to input a malicious link to redirect users to a malicious site that could run or download arbitrary malware on the user's machine.	2019-04-25	not yet calculated	<a href="#">CVE-2019-10955</a> MISC BID
shenzhen_yunni_technology -- lnkp2p	An authentication flaw in Shenzhen Yunni Technology iLnkP2P allows remote attackers to actively intercept user-to-device traffic in cleartext, including video streams and device credentials.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11220</a> MISC
shenzhen_yunni_technology -- lnkp2p	The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11219</a> MISC
simplybook.me -- simplybook.me_enterprise	Incorrect Access Control in the Administrative Management Interface in SimplyBook.me Enterprise before 2019-04-23 allows Authenticated Low-Priv Users to Elevate Privileges to Full Admin Rights via a crafted HTTP PUT Request, as demonstrated by modified JSON data to a /v2/rest/ URL.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11489</a> MISC MISC
simplybook.me -- simplybook.me_enterprise	Incorrect Access Control in the Account Access / Password Reset Link in SimplyBook.me Enterprise before 2019-04-23 allows Unauthorized Attackers to READ/WRITE Customer or Administrator data via a persistent HTTP GET Request Hash Link Replay, as demonstrated by a login-link from the browser history.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11488</a> MISC MISC
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6995 has stored XSS. JavaScript code could be executed on the application by opening a malicious email or when viewing a malicious file attachment.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7211</a> MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 allows deserialization of untrusted data. An unauthenticated attacker could run commands on the server when port 17001 was remotely accessible. This port is not accessible remotely by default after applying the Build 6985 patch.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7214</a> MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 allows directory traversal. An authenticated user could delete arbitrary files or could create files in new folders in arbitrary locations on the mail server. This could lead to command execution on the server for instance by putting files inside the web directories.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7213</a> MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 has hardcoded secret keys. An unauthenticated attacker could access other users' emails and file attachments. It was also possible to interact with mailing lists.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7212</a> MISC CONFIRM
snapcore -- snapweb	The Snapweb interface before version 0.21.2 was exposing controls to install or remove snap packages without controlling the identity of the user, nor the origin of the connection. An attacker could have used the controls to remotely add a valid, but malicious, snap package, from the Store, potentially using system resources without permission from the legitimate administrator of the system.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1587</a> MISC
sonicwall -- global_management_system	A vulnerability in SonicWall Global Management System (GMS), allow a remote user to gain access to the appliance using existing SSH key. This vulnerability affects GMS versions 9.1, 9.0, 8.7, 8.6, 8.4, 8.3 and earlier.	2019-04-26	not yet calculated	<a href="#">CVE-2019-7476</a> CONFIRM
sony -- photo_sharing_plus_application	An incorrect access control exists in the Sony Photo Sharing Plus application in the firmware before PKG6.5629 version (for the X7500D TV and other applicable TVs). This vulnerability allows an attacker to read arbitrary files without authentication over HTTP when Photo Sharing Plus application is running. This may allow an attacker to browse a particular directory (e.g. images) inside the private network.	2019-04-19	not yet calculated	<a href="#">CVE-2019-10886</a> MISC FULL DISC BID BUGTRAO



				<a href="#">CONFIRM</a>
sony -- xperia_i1_android_device	The Sony Xperia L1 Android device with a build fingerprint of Sony/G3313/G3313:7.0/43.0.A.6.49/2867558199:user/release-keys contains the android framework (i.e., system_server) with a package name of android (versionCode=24, versionName=7.0) that has been modified by Sony or another entity in the supply chain. The system_server process in the core android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage. The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14983</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM) prior to and including 12.1 RU6 MP9 and prior to 14.2 RU1 may be susceptible to a DLL Preloading vulnerability, which is a type of issue that can occur when an application looks to call a DLL for execution and an attacker provides a malicious DLL to use instead.	2019-04-25	not yet calculated	<a href="#">CVE-2018-18367</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
symantec -- endpoint_protection_manager	SEP (Mac client) prior to and including 12.1 RU6 MP9 and prior to 14.2 RU1 may be susceptible to a CSV/DDE injection (also known as formula injection) vulnerability, which is a type of issue whereby an application or website allows untrusted input into CSV files.	2019-04-25	not yet calculated	<a href="#">CVE-2018-12244</a> <a href="#">MISC</a> <a href="#">BID</a>
symantec -- norton_security	Symantec Norton Security prior to 22.16.3, SEP (Windows client) prior to and including 12.1 RU6 MP9, and prior to 14.2 RU1, SEP SBE prior to Cloud Agent 3.00.31.2817, NIS-22.15.2.22, SEP-12.1.7484.7002 and SEP Cloud prior to 22.16.3 may be susceptible to a kernel memory disclosure, which is a type of issue where a specially crafted IRP request can cause the driver to return uninitialized memory.	2019-04-25	not yet calculated	<a href="#">CVE-2018-18366</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
symantec -- norton_security	Norton Security (Windows client) prior to 22.16.3 and SEP SBE (Windows client) prior to Cloud Agent 3.00.31.2817, NIS-22.15.2.22 & SEP-12.1.7484.7002, may be susceptible to a DLL Preloading vulnerability, which is a type of issue that can occur when an application looks to call a DLL for execution and an attacker provides a malicious DLL to use instead.	2019-04-25	not yet calculated	<a href="#">CVE-2018-18369</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
systemd -- systemd	It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3844</a> <a href="#">CONFIRM</a>
systemd -- systemd	It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3843</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a>
teamspeak_systems -- teamspeak_3_client	TeamSpeak 3 Client before 3.2.5 allows remote code execution in the Qt framework.	2019-04-19	not yet calculated	<a href="#">CVE-2019-11351</a> <a href="#">MISC</a> <a href="#">MISC</a>
tenda -- ac7_and_ac9_and_ac10_devices	An issue was discovered on Tenda AC7 devices with firmware through V15.03.06.44_CN(AC7), AC9 devices with firmware through V15.03.05.19(6318)_CN(AC9), and AC10 devices with firmware through V15.03.06.23_CN(AC10). A buffer overflow vulnerability exists in the router's web server (httpd). When processing the page parameters for a post request, the value is directly written with sprintf to a local variable placed on the stack, which overrides the return address of the function, causing a buffer overflow.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14557</a> <a href="#">MISC</a>
tenda -- ac7_and_ac9_and_ac10_devices	An issue was discovered on Tenda AC7 devices with firmware through V15.03.06.44_CN(AC7), AC9 devices with firmware through V15.03.05.19(6318)_CN(AC9), and AC10 devices with firmware through V15.03.06.23_CN(AC10). A buffer overflow vulnerability exists in the router's web server (httpd). When processing the list parameters for a post request, the value is directly written with sprintf to a local variable placed on the stack, which overrides the return address of the function, causing a buffer overflow.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14559</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrative server component of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains a vulnerability wherein a user without privileges to upload distributed application archives ("Upload DAA" permission) can theoretically upload arbitrary code, and in some circumstances then execute that code on ActiveMatrix Service Grid nodes. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric: versions up to and including 3.3.0, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8992</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The workspace client, openspace client, and app development client of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contain a vulnerability wherein a malicious URL could trick a user into visiting a website of the attacker's choice. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8995</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The workspace client of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contains vulnerabilities where an authenticated user can change settings that can theoretically adversely impact other users. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8994</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrative web server component of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains a vulnerability that could theoretically allow an unauthenticated user to download a file with credentials information. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric: versions up to and including 3.3.0, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8993</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrator web interface of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains multiple vulnerabilities that may allow for cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8991</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The workspace client, openspace client, app development client, and REST API of TIBCO			



tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contain cross site scripting (XSS) and cross-site request forgery vulnerabilities. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11203</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tildeslash -- m/monit	An issue was discovered in /admin/users/update in M/Monit before 3.7.3. It allows unprivileged users to escalate their privileges to an administrator by requesting a password change and specifying the admin parameter.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11393</a> <a href="#">MISC</a> <a href="#">MISC</a>
tildeslash -- monit	A buffer over-read in Util_urlDecode in util.c in Tildeslash Monit before 5.25.3 allows a remote authenticated attacker to retrieve the contents of adjacent memory via manipulation of GET or POST parameters. The attacker can also cause a denial of service (application outage).	2019-04-22	not yet calculated	<a href="#">CVE-2019-11455</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
tildeslash -- monit	Persistent cross-site scripting (XSS) in http/cervlet.c in Tildeslash Monit before 5.25.3 allows a remote unauthenticated attacker to introduce arbitrary JavaScript via manipulation of an unsanitized user field of the Authorization header for HTTP Basic Authentication, which is mishandled during an _viewlog operation.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11454</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
unity-scope-gdrive_logs -- unity-scope-gdrive_logs	All versions of unity-scope-gdrive logs search terms to syslog.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1343</a> <a href="#">MISC</a>
unity8-team -- unity8	Versions of Unity8 before 8.11+16.04.20160122-0ubuntu1 file plugins/Dash/CardCreator.js will execute any code found in place of a fallback image supplied by a scope.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1573</a> <a href="#">MISC</a>
unity8-team -- unity8	In all versions of Unity8 a running but not active application on a large-screen device could talk with Maliit and consume keyboard input.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1584</a> <a href="#">MISC</a>
vivo -- v7_android_device	The Vivo V7 Android device with a build fingerprint of vivo/1718/1718:7.1.2/N2G47H/compile11021857:user/release-keys contains a platform app with a package name of com.vivo.smartshot (versionCode=1, versionName=3.0.0). This app contains an exported service named com.vivo.smartshot.ui.service.ScreenRecordService that will record the screen for 60 minutes and write the mp4 file to a location of the user's choosing. Normally, a recording notification will be visible to the user, but we discovered an approach to make it mostly transparent to the user by quickly removing a notification and floating icon. The user can see a floating icon and notification appear and disappear quickly due to quickly stopping and restarting the service with different parameters that do not interfere with the ongoing screen recording. The screen recording lasts for 60 minutes and can be written directly to the attacking app's private directory.	2019-04-25	not yet calculated	<a href="#">CVE-2018-15000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
western_digital_technologies -- my_cloud_firmware_versions	Western Digital My Cloud, My Cloud Mirror Gen2, My Cloud EX2 Ultra, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100, My Cloud DL4100, My Cloud PR2100 and My Cloud PR4100 firmware before 2.31.174 is affected by an authentication bypass vulnerability. The login_mgr.cgi file checks credentials against /etc/shadow. However, the "nobody" account (which can be used to access the control panel API as a low-privilege logged-in user) has a default empty password, allowing an attacker to modify the My Cloud EX2 Ultra web page source code and obtain access to the My Cloud as a non-Admin My Cloud device user.	2019-04-24	not yet calculated	<a href="#">CVE-2019-9950</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
western_digital_technologies -- my_cloud_firmware_versions	Western Digital My Cloud, My Cloud Mirror Gen2, My Cloud EX2 Ultra, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100, My Cloud DL4100, My Cloud PR2100 and My Cloud PR4100 firmware before 2.31.174 is affected by an unauthenticated file upload vulnerability. The page web/query/uploader/uploadify.php can be accessed without any credentials, and allows uploading arbitrary files to any location on the attached storage.	2019-04-24	not yet calculated	<a href="#">CVE-2019-9951</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	Server Side Request Forgery (SSRF) exists in the Print My Blog plugin before 1.6.7 for WordPress via the site parameter.	2019-04-27	not yet calculated	<a href="#">CVE-2019-11565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WebDorado Contact Form Builder plugin before 1.0.69 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11557</a> <a href="#">MISC</a> <a href="#">MISC</a>
xiaomi -- mi_5s_devices	The gyroscope on Xiaomi Mi 5s devices allows attackers to cause a denial of service (resonance and false data) via a 20.4 kHz audio signal, aka a MEMS ultrasound attack.	2019-04-25	not yet calculated	<a href="#">CVE-2018-20823</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- adselfservice_plus	Zoho ManageEngine ADSelfService Plus before build 5708 has XSS via the mobile app API.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11511</a> <a href="#">MISC</a>
zotonic -- zotonic	Zotonic before version 0.47 has mod_admin XSS.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11504</a> <a href="#">MISC</a>
zyxel_communications -- multiple_devices	On Zyxel ATP200, ATP500, ATP800, USG20-VPN, USG20W-VPN, USG40, USG40W, USG60, USG60W, USG110, USG210, USG310, USG1100, USG1900, USG2200-VPN, ZyWALL 110, ZyWALL 310, ZyWALL 1100 devices, the security firewall login page is vulnerable to Reflected XSS via the unsanitized 'mp_idx' parameter.	2019-04-22	not yet calculated	<a href="#">CVE-2019-9955</a> <a href="#">MISC</a> <a href="#">FULL DISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](#). If you need help or have questions, please send an email to [info@us-cert.gov](#). Do not reply to this message since this email was sent from a non-facilitated on-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nrcis.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [Incgnis@sunrayva.ca.gov](#) using GovDelivery Communicate One Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) - 25 Murray Lane SW Bldg 10 - Washington, DC 20588 - (888) 282-0870



From: [US-CERT](#)  
To: [g.fate@cis.nyu.ac.ae](#)  
Subject: SB19-119: Vulnerability Summary for the Week of April 22, 2019  
Date: Monday, April 29, 2019 1:02:42 PM



National Cyber Awareness System:

## SB19-119 Vulnerability Summary for the Week of April 22, 2019

04/29/2019 09:00 AM EDT

Original release date: April 29, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology \(NIST\) National Vulnerability Database \(NVD\)](#) in the past week. The NVD is sponsored by the [Department of Homeland Security \(DHS\) National Cybersecurity and Communications Integration Center \(NCCIC\)](#) / [United States Computer Emergency Readiness Team \(US-CERT\)](#). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System \(CVSS\)](#) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database \(NVD\)](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
activision -- call_of_duty:advanced_warfare	SV_SteamAuthClient in various Activision Infinity Ward Call of Duty games before 2015-08-11 is missing a size check when reading authBlob data into a buffer, which allows one to execute code on the remote target machine when sending a steam authentication request. This affects Call of Duty: Modern Warfare 2, Call of Duty: Modern Warfare 3, Call of Duty: Ghosts, Call of Duty: Advanced Warfare, Call of Duty: Black Ops 1, and Call of Duty: Black Ops 2.	2019-04-19	7.5	<a href="#">CVE-2018-20817</a> MISC MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. The NumberToFixed() and numtostr implementations in jsnumber.c have a stack-based buffer overflow.	2019-04-22	7.5	<a href="#">CVE-2019-11411</a> MISC MISC MISC
atftp_project -- atftp	An issue was discovered in atftpd in atftp 0.7.1. A remote attacker may send a crafted packet triggering a stack-based buffer overflow due to an insecurely implemented strncpy call. The vulnerability is triggered by sending an error packet of 3 bytes or fewer. There are multiple instances of this vulnerable strncpy pattern within the code base, specifically within tftpd_file.c, tftp_file.c, tftpd_mfttp.c, and tftp_mfttp.c.	2019-04-20	7.5	<a href="#">CVE-2019-11365</a> MISC MISC
burrow-wheeler_aligner_project -- burrow-wheeler_aligner	BWA (aka Burrow-Wheeler Aligner) 0.7.17 r1198 has a Buffer Overflow via a long prefix that is mishandled in bns_fast2bntseq and bns_dump at bntseq.c.	2019-04-20	7.5	<a href="#">CVE-2019-11371</a> MISC
freeradius -- freeradius	FreeRADIUS before 3.0.19 does not prevent use of reflection for authentication spoofing, aka a "Dragonblood" issue, a similar issue to CVE-2019-9497.	2019-04-22	7.5	<a href="#">CVE-2019-11234</a> CONFIRM MISC MISC MISC UBUNTU MISC
freeradius -- freeradius	FreeRADIUS before 3.0.19 mishandles the "each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used" protection mechanism, aka a "Dragonblood" issue, a similar issue to CVE-2019-9498 and CVE-2019-9499.	2019-04-22	7.5	<a href="#">CVE-2019-11235</a> CONFIRM MISC MISC MISC UBUNTU MISC
google -- android	In floor0_inverse1 of floor0.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119120561.	2019-04-19	9.3	<a href="#">CVE-2019-2027</a> CONFIRM
google -- android	In numerous hand-crafted functions in libmpeg2, NEON registers are not preserved. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120644655.	2019-04-19	9.3	<a href="#">CVE-2019-2028</a> CONFIRM
google -- android	In removeInterfaceAddress of NetworkController.cpp, there is a possible use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-119496789.	2019-04-19	7.5	<a href="#">CVE-2019-2030</a> CONFIRM
ibm -- bladecenter_hs23_firmware	A potential vulnerability was found in an SMI handler in various BIOS versions of certain legacy IBM System x and IBM BladeCenter systems that could lead to denial of service.	2019-04-22	7.8	<a href="#">CVE-2019-6155</a> MISC
imagemagick -- imagemagick	The cineon parsing component in ImageMagick 7.0.8-26 Q16 allows attackers to cause a denial-of-service (uncontrolled resource consumption) by crafting a Cineon image with an incorrect claimed image size. This occurs because ReadCINImage in coders/cin.c lacks a check for insufficient image data in a file.	2019-04-23	7.1	<a href="#">CVE-2019-11470</a> MISC MISC
intelbras -- iwr_3000n_firmware	An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. A malformed login request allows remote attackers to cause a denial of service (reboot), as demonstrated by JSON misparsing of the {} string to v1/system/login.	2019-04-22	7.8	<a href="#">CVE-2019-11415</a> MISC
intelbras -- iwr_3000n_firmware	A CSRF issue was discovered on Intelbras IWR 3000N 1.5.0 devices, leading to complete control of the router, as demonstrated by v1/system/user.	2019-04-22	9.3	<a href="#">CVE-2019-11416</a> MISC
linux -- linux_kernel	cipso_v4_validate in include/net/cipso_ipv4.h in the Linux kernel before 3.11.7, when CONFIG_NETLABEL is disabled, allows attackers to cause a denial of service (infinite loop and crash), as demonstrated by icmpsic, a different vulnerability than CVE-2013-0310.	2019-04-22	7.1	<a href="#">CVE-2013-7470</a> MISC MISC MISC
mitel -- cmg_suite	SQL injection vulnerabilities in CMG Suite 8.4 SP2 and earlier, could allow an unauthenticated attacker to conduct an SQL injection attack due to insufficient input validation for the login interface. A successful exploit could allow an attacker to extract sensitive information from the database and execute arbitrary scripts.	2019-04-25	7.5	<a href="#">CVE-2018-18285</a> CONFIRM CONFIRM
mitel -- cmg_suite	SQL injection vulnerabilities in CMG Suite 8.4 SP2 and earlier, could allow an unauthenticated attacker to conduct an SQL injection attack due to insufficient input validation for the changepwd interface. A successful exploit could allow an attacker to extract sensitive information from the database and execute arbitrary scripts.	2019-04-25	7.5	<a href="#">CVE-2018-18286</a> CONFIRM CONFIRM
mozilla -- firefox	Mozilla developers and community members reported memory safety bugs present in Firefox 65, Firefox ESR 60.5, and Thunderbird 60.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code.	2019-04-26	7.5	<a href="#">CVE-2019-9788</a> MISC MISC MISC

	This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.			<a href="#">MISC</a>
mozilla -- firefox	Mozilla developers and community members reported memory safety bugs present in Firefox 65. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9789</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	7.5	<a href="#">CVE-2019-9790</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A use-after-free vulnerability can occur while playing a sound notification in Thunderbird. The memory storing the sound data is immediately freed, although the sound is still being played asynchronously, leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 60.5.	2019-04-26	7.5	<a href="#">CVE-2018-18512</a> <a href="#">MISC</a> <a href="#">MISC</a>
neatorobotics -- botvac_connected_firmware	A Buffer Overflow in Network:AuthenticationClient::VerifySignature in /bin/astro in Neato Botvac Connected 2.2.0 allows a remote attacker to execute arbitrary code with root privileges via a crafted POST request to a nucleo.neatocloud.com:4443/vendors/neato/robots/[robot_serial]/messages Neato cloud URL.	2019-04-25	10.0	<a href="#">CVE-2018-19442</a> <a href="#">MISC</a>
nice -- engage	In NICE Engage through 6.5, the default configuration binds an unauthenticated JMX/RMI interface to all network interfaces, without restricting registration of MBeans, which allows remote attackers to execute arbitrary code via the RMI protocol by using the JMX connector. The observed affected TCP port is 6338 but, based on the product's configuration, a different one could be vulnerable.	2019-04-23	7.5	<a href="#">CVE-2019-7727</a> <a href="#">FULLDISC</a> <a href="#">MISC</a> <a href="#">BUGTRAQ</a>
nmap -- npcap	An issue was discovered in Npcap 0.992. Sending a malformed .pcap file with the loopback adapter using either pcap_sendqueue_queue() or pcap_sendqueue_transmit() results in kernel pool corruption. This could lead to arbitrary code executing inside the Windows kernel and allow escalation of privileges.	2019-04-23	9.3	<a href="#">CVE-2019-11490</a> <a href="#">MISC</a>
openkm -- openkm	OpenKM 6.3.2 through 6.3.7 allows an attacker to upload a malicious JSP file into the /okm:root directories and move that file to the home directory of the site, via frontend/FileUpload and admin/repository_export.jsp. This is achieved by interfering with the Filesystem path control in the admin's Export field. As a result, attackers can gain remote code execution through the application server with root privileges.	2019-04-22	9.0	<a href="#">CVE-2019-11445</a> <a href="#">MISC</a> <a href="#">MISC</a>
openplcproject -- openplc_v2_firmware	A buffer overflow vulnerability was discovered in the OpenPLC controller, in the OpenPLC_v2 and OpenPLC_v3 versions. It occurs in the modbus.cpp mapUnusedIO() function, which can cause a runtime crash of the PLC or possibly have unspecified other impact.	2019-04-22	7.5	<a href="#">CVE-2018-20818</a> <a href="#">MISC</a>
oracle -- database_server	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having DBFS_ROLE privilege with network access via Oracle Net to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/H:I/H:A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2517</a> <a href="#">MISC</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	<a href="#">CVE-2019-2608</a> <a href="#">MISC</a>
oracle -- retail_convenience_store_back_office	Vulnerability in the Oracle Retail Convenience Store Back Office component of Oracle Retail Applications (subcomponent: Level 3 Maintenance Functions). The supported version that is affected is 3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Convenience Store Back Office. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Convenience Store Back Office accessible data as well as unauthorized read access to a subset of Oracle Retail Convenience Store Back Office accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Convenience Store Back Office. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	<a href="#">CVE-2019-2424</a> <a href="#">MISC</a>
oracle -- retail_point-of-service	Vulnerability in the Oracle Retail Point-of-Service component of Oracle Retail Applications (subcomponent: Infrastructure). Supported versions that are affected are 13.4, 14.0 and 14.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Point-of-Service. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Point-of-Service accessible data as well as unauthorized read access to a subset of Oracle Retail Point-of-Service accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Point-of-Service. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	7.5	<a href="#">CVE-2019-2558</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2645</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: EJB Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2646</a> <a href="#">MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	7.5	<a href="#">CVE-2019-2658</a> <a href="#">MISC</a>
pluck-cms -- pluck	data/inc/files.php in Pluck 4.7.8 allows remote attackers to execute arbitrary code by uploading a .htaccess file that specifies SetHandler x-httpd-php for a .txt file, because only certain PHP-related filename extensions are blocked.	2019-04-19	7.5	<a href="#">CVE-2019-11344</a> <a href="#">MISC</a>
rocboss -- rocboss	app/controllers/frontend/PostController.php in ROCBOS V2.2.1 has SQL injection via the Post:doReward score paramter, as demonstrated by the /do/reward/3 URI.	2019-04-20	7.5	<a href="#">CVE-2019-11362</a> <a href="#">MISC</a>
tabslab -- mailcarrier	A buffer overflow in MailCarrier 2.51 allows remote attackers to execute arbitrary code via a long string, as demonstrated by SMTP RCPT TO, POP3 USER, POP3 LIST, POP3 TOP, or POP3 RETR.	2019-04-22	7.5	<a href="#">CVE-2019-11395</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
trendnet -- tew-632brp_firmware	apply.cgi on the TRENDnet TEW-632BRP 1.010B32 router has a buffer overflow via long strings to the SOAPACTION:HNAP1 interface.	2019-04-22	7.5	<a href="#">CVE-2019-11418</a> <a href="#">MISC</a>
trendnet -- tv-ip110wn_firmware	system.cgi on TRENDnet TV-IP110WN cameras has a buffer overflow caused by an inadequate source-length check before a strcpy operation in the respondAsp function. Attackers can exploit the vulnerability by using the languse parameter with a long string. This affects 1.2.2 build 28, 64, 65, and 68.	2019-04-22	7.5	<a href="#">CVE-2019-11417</a> <a href="#">MISC</a>

whatsns -- whatsns	whatsns 4.0 allows index.php?question/ajaxadd.html title SQL injection.	2019-04-22	7.5	CVE-2019-11450 MISC
zohocorp -- manageengine_applications_manager	An issue was discovered in Zoho ManageEngine Applications Manager 11.0 through 14.0. An unauthenticated user can gain the authority of SYSTEM on the server due to a PopUp_SLA.jsp sid SQL injection vulnerability. For example, the attacker can subsequently write arbitrary text to a .vbs file.	2019-04-22	10.0	CVE-2019-11448 MISC EXPLOIT-DB CONFIRM
zohocorp -- manageengine_applications_manager	Zoho ManageEngine Applications Manager 12 through 14 allows FaultTemplateOptions.jsp resourceid SQL injection. Subsequently, an unauthenticated user can gain the authority of SYSTEM on the server by uploading a malicious file via the "Execute Program Action(s)" feature.	2019-04-23	10.0	CVE-2019-11469 MISC MISC MISC EXPLOIT-DB CONFIRM

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
74cms -- 74cms	74CMS v5.0.1 has a CSRF vulnerability to add a new admin user via the index.php?m=Admin&c=admin&a=add URL.	2019-04-20	6.8	CVE-2019-11374 MISC MISC EXPLOIT-DB
apache -- pony_mail	A vulnerability was discovered wherein a specially crafted URL could enable reflected XSS via JavaScript in the pony mail interface.	2019-04-22	4.3	CVE-2019-0218 MISC CONFIRM
apache -- zeppelin	Apache Zeppelin prior to 0.8.0 had a stored XSS issue via Note permissions. Issue reported by "Josna Joseph".	2019-04-23	4.3	CVE-2018-1328 MISC MISC MISC
aquaverde -- aquarius_cms	aquaverde Aquarius CMS through 4.3.5 allows Information Exposure through Log Files because of an error in the Log-File writer component.	2019-04-24	5.0	CVE-2019-9724 CONFIRM MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. jscompile.c can cause a denial of service (invalid stack-frame jump) because it lacks an ENDRY opcode call.	2019-04-22	5.0	CVE-2019-11412 MISC MISC MISC
artifex -- mujs	An issue was discovered in Artifex MuJS 1.0.5. It has unlimited recursion because the match function in regexp.c lacks a depth check.	2019-04-22	5.0	CVE-2019-11413 MISC MISC MISC
atftp_project -- atftp	An issue was discovered in atftpd in atftp 0.7.1. It does not lock the thread_list_mutex mutex before assigning the current thread data structure. As a result, the daemon is vulnerable to a denial of service attack due to a NULL pointer dereference. If thread_data is NULL when assigned to current, and modified by another thread before a certain tftp_list.c check, there is a crash when dereferencing current->next.	2019-04-20	4.3	CVE-2019-11366 MISC MISC
atutor -- atutor	An issue was discovered in ATutor through 2.2.4. It allows the user to run commands on the server with the teacher user privilege. The Upload Files section in the File Manager field contains an arbitrary file upload vulnerability via upload.php. The \$illegalExtensions value only lists lowercase (and thus .php is a bypass), and omits .shml and .phtml.	2019-04-22	6.5	CVE-2019-11446 MISC EXPLOIT-DB
audiocodes -- 405hd_firmware	Cross Site Scripting in different input fields (domain field and personal settings) in AudioCodes 405HD VoIP phone with firmware 2.2.12 allows an attacker (local or remote) to inject JavaScript into the web interface of the device by manipulating the phone book entries or manipulating the domain name sent to the device from the domain controller.	2019-04-25	4.3	CVE-2018-16220 MISC
block -- jit-wasm	EOS.IO jit-wasm 4.1 has a heap-based buffer overflow via a crafted wast file.	2019-04-24	6.8	CVE-2018-13443 MISC MISC MISC
brassica -- soy_cms	** DISPUTED ** SOY CMS v3.0.2 allows remote attackers to execute arbitrary PHP code via a <?php substring in the second text box. NOTE: the vendor indicates that there was an assumption that the content is "made editable on its own."	2019-04-20	6.5	CVE-2019-11376 MISC MISC
cloudbees -- jenkins_operations_center	CloudBees Jenkins Operations Center 2.150.2.3, when an expired trial license exists, allows Cleartext Password Storage and Retrieval via the proxy configuration page.	2019-04-19	5.0	CVE-2019-11350 MISC
cutephp -- cutenews	An issue was discovered in CutePHP CuteNews 2.1.2. An attacker can infiltrate the server through the avatar upload process in the profile area via the avatar_file field to index.php?mod=main&opt=personal. There is no effective control of \$imgsize in /core/modules/dashboard.php. The header content of a file can be changed and the control can be bypassed for code execution. (An attacker can use the GIF header for this.)	2019-04-22	6.5	CVE-2019-11447 MISC EXPLOIT-DB
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Heap-based overflow vulnerability, triggered when the user opens a malformed DIB format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9135 MISC
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Heap-based overflow vulnerability, triggered when the user opens a malformed JPEG2000 format file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9136 MISC
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed PhotoShop file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9138 MISC
datools -- daviewindy	Daviewindy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed PDF file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	6.8	CVE-2019-9139 MISC
dropbox -- lepton	read_ujpg in jpgcoder.cc in Dropbox Lepton 1.2.1 allows attackers to cause a denial-of-service (application runtime crash because of an integer overflow) via a crafted file.	2019-04-23	4.3	CVE-2018-20820 MISC MISC
drupal -- drupal	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.	2019-04-19	4.3	CVE-2019-11358 MISC MISC MISC MISC MISC MISC MISC

				MLIST BUGTRAQ MISC DEBIAN MISC
ea -- origin	The client in Electronic Arts (EA) Origin 10.5.36 on Windows allows template injection in the title parameter of the Origin2 URI handler. This can be used to escape the underlying AngularJS sandbox and achieve remote code execution via an origin2://game/launch URL for QtApplication QDesktopServices communication.	2019-04-19	6.8	CVE-2019-11354 MISC MISC MISC MISC MISC MISC MISC
eclipse -- jetty	In Eclipse Jetty version 9.2.26 and older, 9.3.25 and older, and 9.4.15 and older, the server is vulnerable to XSS conditions if a remote client USES a specially formatted URL against the DefaultServlet or ResourceHandler that is configured for showing a Listing of directory contents.	2019-04-22	4.3	CVE-2019-10241 CONFIRM
fortinet -- fortimanager	A cleartext transmission of sensitive information vulnerability in Fortinet FortiManager 5.2.0 through 5.2.7, 5.4.0 and 5.4.1 may allow an unauthenticated attacker in a man in the middle position to retrieve the admin password via intercepting REST API JSON responses.	2019-04-25	4.3	CVE-2018-1360 BID CONFIRM
gilacms -- gila_cms	Gila CMS 1.10.1 allows fm/save CSRF for executing arbitrary PHP code.	2019-04-22	6.8	CVE-2019-11456 MISC
gilacms -- gila_cms	core/classes/db_backup.php in Gila CMS 1.10.1 allows admin/db_backup?download= absolute path traversal to read arbitrary files.	2019-04-25	4.0	CVE-2019-11515 MISC
gitlab -- gitlab	GitLab CE & EE 11.2 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 have Persistent XSS.	2019-04-25	4.3	CVE-2018-18643 MISC MISC MISC
gitlab -- gitlab	GitLab Community and Enterprise Edition 8.9 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 has Incorrect Access Control.	2019-04-25	6.5	CVE-2018-19359 MISC MISC MISC
gnome -- evince	The tiff_document_render() and tiff_document_get_thumbnail() functions in the TIFF document backend in GNOME Evince through 3.32.0 did not handle errors from TIFFReadRGBAImageOriented(), leading to uninitialized memory use when processing certain TIFF image files.	2019-04-22	4.3	CVE-2019-11459 MISC
gnome -- gnome-desktop	An issue was discovered in GNOME gnome-desktop 3.26, 3.28, and 3.30 prior to 3.30.2.2, and 3.32 prior to 3.32.1.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCTST ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCTST ioctl on 64-bit systems, similar to CVE-2019-10063.	2019-04-22	6.8	CVE-2019-11460 MISC
google -- android	In updateAssistMenuItems of Editor.java, there is a possible escape from the Setup Wizard due to a missing permission check. This could lead to local escalation of privilege and FRP bypass with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android ID: A-120866126	2019-04-19	4.6	CVE-2019-2026 CONFIRM
google -- android	In btm_proc_smp_cbk of tm_ble.cc, there is a possible memory corruption due to a use after free. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120612744.	2019-04-19	6.8	CVE-2019-2029 CONFIRM
google -- android	In rw_t3t_act_handle_check_ndef_rsp of rw_t3t.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-120502559.	2019-04-19	4.6	CVE-2019-2031 CONFIRM
google -- android	In SetScanResponseData of ble_advertiser_hci_interface.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-121145627.	2019-04-19	4.6	CVE-2019-2032 CONFIRM
google -- android	In create_hdr of dnssd_clientstub.c, there is a possible use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-121327565.	2019-04-19	4.6	CVE-2019-2033 CONFIRM
google -- android	In rw_i93_sm_read_ndef of rw_i93.cc, there is a possible out-of-bounds write due to an integer overflow. This could lead to local escalation of privilege in the NFC process with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122035770.	2019-04-19	6.8	CVE-2019-2034 CONFIRM
google -- android	In rw_i93_sm_update_ndef of rw_i93.cc, there is a possible out-of-bound write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-122320256	2019-04-19	6.8	CVE-2019-2035 CONFIRM
google -- android	In I2cu_send_peer_config_rej of I2c_utils.cc, there is a possible out-of-bound read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-119870451.	2019-04-19	5.0	CVE-2019-2037 CONFIRM
google -- android	In rw_i93_process_sys_info of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121259048.	2019-04-19	4.3	CVE-2019-2038 CONFIRM
google -- android	In rw_i93_sm_detect_ndef of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-121260197.	2019-04-19	4.7	CVE-2019-2039 CONFIRM
google -- android	In rw_i93_process_ext_sys_info of rw_i93.cc, there is a possible out-of-bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-122316913.	2019-04-19	4.7	CVE-2019-2040 CONFIRM
google -- android	In the configuration of NFC modules on certain devices, there is a possible failure to distinguish individual devices due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-8.1 Android-9. Android ID: A-122034690.	2019-04-19	6.9	CVE-2019-2041 CONFIRM
google -- tensorflow	Google TensorFlow 1.6.x and earlier is affected by: Null Pointer Dereference. The type of exploitation is: context-dependent.	2019-04-23	4.3	CVE-2018-7576 CONFIRM
google -- tensorflow	Google TensorFlow 1.7 and below is affected by: Buffer Overflow. The impact is: execute arbitrary code (local).	2019-04-23	6.8	CVE-2018-8825 CONFIRM
google -- tensorflow	NULL pointer dereference in Google TensorFlow before 1.12.2 could cause a denial of service via an invalid GIF file.	2019-04-24	4.3	CVE-2019-9635 MISC
				CVE-2019-



gradle -- enterprise	In Gradle Enterprise before 2018.5.3, Build Cache Nodes did not store the credentials at rest in an encrypted format.	2019-04-22	5.0	11402 MISC
gradle -- enterprise	In Gradle Enterprise before 2018.5.2, Build Cache Nodes would reflect the configured password back when viewing the HTML page source of the settings page.	2019-04-22	5.0	11403 MISC
graphicsmagick -- graphicsmagick	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (out-of-bounds read and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.	2019-04-23	4.3	CVE-2019-11473 MISC MISC MISC BID
graphicsmagick -- graphicsmagick	coders/xwd.c in GraphicsMagick 1.3.31 allows attackers to cause a denial of service (floating-point exception and application crash) by crafting an XWD image file, a different vulnerability than CVE-2019-11008 and CVE-2019-11009.	2019-04-23	4.3	CVE-2019-11474 MISC MISC MISC BID
graphicsmagick -- graphicsmagick	In GraphicsMagick from version 1.3.8 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WritePDBImage of coders/pdb.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to MagickBitStreamMSBWrite in magick/bit_stream.c.	2019-04-24	6.8	CVE-2019-11505 MISC BID MISC
graphicsmagick -- graphicsmagick	In GraphicsMagick from version 1.3.30 to 1.4 snapshot-20190403 Q8, there is a heap-based buffer overflow in the function WriteMATLABImage of coders/mat.c, which allows an attacker to cause a denial of service or possibly have unspecified other impact via a crafted image file. This is related to ExportRedQuantumType in magick/export.c.	2019-04-24	6.8	CVE-2019-11506 MISC MISC
gstreamer_project -- gstreamer	GStreamer before 1.16.0 has a heap-based buffer overflow in the RTSP connection parser via a crafted response from a server, potentially allowing remote code execution.	2019-04-24	6.8	CVE-2019-9928 CONFIRM CONFIRM MLIST MLIST
i-librarian -- i-librarian	Cross-site scripting (XSS) vulnerability in display.php in I, Librarian 4.10 allows remote attackers to inject arbitrary web script or HTML via the project parameter.	2019-04-19	4.3	CVE-2019-11359 MISC
i-librarian -- i-librarian	I, Librarian 4.10 has XSS via the export.php export_files parameter.	2019-04-22	4.3	CVE-2019-11428 MISC
i-librarian -- i-librarian	I, Librarian 4.10 has XSS via the notes.php notes parameter.	2019-04-22	4.3	CVE-2019-11449 MISC
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0CD could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 157654.	2019-04-25	5.8	CVE-2019-4092 CONFIRM XF
ibm -- qradar_security_information_and_event_manager	IBM QRadar SIEM 7.3 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 147708.	2019-04-19	5.0	CVE-2018-1729 CONFIRM BID XF
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to view process definition of a business process without permission. IBM X-Force ID: 159231.	2019-04-25	4.0	CVE-2019-4222 XF CONFIRM
idreamsoft -- icms	An XSS issue was discovered in app/admincp/template/admincp.header.php in idreamsoft iCMS 7.0.14 via the admincp.php?app=config tab parameter.	2019-04-22	4.3	CVE-2019-11426 MISC
idreamsoft -- icms	An XSS issue was discovered in app/search/search.app.php in idreamsoft iCMS 7.0.14 via the public/api.php?app=search q parameter.	2019-04-22	4.3	CVE-2019-11427 MISC
imagemagick -- imagemagick	ReadXWDImage in coders/xwd.c in the XWD image parsing component of ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (divide-by-zero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first.	2019-04-23	4.3	CVE-2019-11472 MISC MISC
intelbras -- iwr_3000n_firmware	An issue was discovered on Intelbras IWR 3000N 1.5.0 devices. When the administrator password is changed from a certain client IP address, administrative authorization remains available to any client at that IP address, leading to complete control of the router.	2019-04-22	4.3	CVE-2019-11414 MISC
kubernetes -- kubernetes	In Kubernetes v1.12.0-v1.12.4 and v1.13.0, the rest AnonymousClientConfig() method returns a copy of the provided config, with credentials removed (bearer token, username/password, and client certificate/key data). In the affected versions, rest AnonymousClientConfig() did not effectively clear service account credentials loaded using rest.InClusterConfig()	2019-04-22	4.3	CVE-2019-11243 BID MISC
linux -- linux_kernel	The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions.	2019-04-23	6.9	CVE-2019-11486 MISC MISC MISC MISC
matrix -- sydent	util/emailutils.py in Matrix Sydent before 1.0.2 mishandles registration restrictions that are based on e-mail domain, if the allowed_local_3pids option is enabled. This occurs because of potentially unwanted behavior in Python, in which an email.utils.parseaddr call on user@bad.example.net@good.example.com returns the user@bad.example.net substring.	2019-04-19	4.3	CVE-2019-11340 MISC MISC MISC
mediaarea -- mediainfo	An out-of-bounds read in MediaInfoLib::File__Tags_Helper::Synched_Test in Tag/File__Tags.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash.	2019-04-20	4.3	CVE-2019-11372 MISC FEDORA MISC
mediaarea -- mediainfo	An out-of-bounds read in File__Analyze::Get_L8 in File__Analyze_Buffer.cpp in MediaInfoLib in MediaArea MediaInfo 18.12 leads to a crash.	2019-04-20	4.3	CVE-2019-11373 MISC FEDORA MISC
meisvod -- msvod	Msvod v10 has a CSRF vulnerability to change user information via the admin/member/edit.html URI.	2019-04-20	4.3	CVE-2019-11375 MISC MISC EXPLOIT-DB
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-942-APPLICATION-ATTACK-SQLi.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators.	2019-04-20	5.0	CVE-2019-11387 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-932-APPLICATION-ATTACK-RCE.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with nested repetition operators.	2019-04-20	5.0	CVE-2019-11388 MISC
	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0.			CVE-2019-

modsecurity -- owasp_modsecurity_core_rule_set	/rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with next# at the beginning and nested repetition operators.	2019-04-20	5.0	11389 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with set_error_handler# at the beginning and nested repetition operators.	2019-04-20	5.0	CVE-2019-11390 MISC
modsecurity -- owasp_modsecurity_core_rule_set	An issue was discovered in OWASP ModSecurity Core Rule Set (CRS) through 3.1.0. /rules/REQUEST-933-APPLICATION-ATTACK-PHP.conf allows remote attackers to cause a denial of service (ReDOS) by entering a specially crafted string with \$a# at the beginning and nested repetition operators.	2019-04-20	5.0	CVE-2019-11391 MISC
mozilla -- firefox	The about:crashcontent and about:crashparent pages can be triggered by web content. These pages are used to crash the loaded page or the browser for test purposes. This issue allows for a non-persistent denial of service (DOS) attack by a malicious site which links to these pages. This vulnerability affects Firefox < 64.	2019-04-26	4.3	CVE-2018-18510 MISC
openstack -- nova	Versions of nova before 2012.1 could expose hypervisor host files to a guest operating system when processing a maliciously constructed qcow filesystem.	2019-04-22	5.0	CVE-2011-3147 MISC
oracle -- advanced_outbound_telephony	Vulnerability in the Oracle Advanced Outbound Telephony component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Advanced Outbound Telephony. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Advanced Outbound Telephony, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Advanced Outbound Telephony accessible data as well as unauthorized update, insert or delete access to some of Oracle Advanced Outbound Telephony accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	5.8	CVE-2019-2663 MISC
oracle -- application_object_library	Vulnerability in the Oracle Application Object Library component of Oracle E-Business Suite (subcomponent: Diagnostics). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Object Library. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Application Object Library, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Object Library accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	4.3	CVE-2019-2621 MISC
oracle -- application_testing_suite	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). The supported version that is affected is 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	6.5	CVE-2019-2557 MISC
oracle -- applications_framework	Vulnerability in the Oracle Applications Framework component of Oracle E-Business Suite (subcomponent: Attachments / File Upload). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Framework. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Applications Framework, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Applications Framework accessible data as well as unauthorized update, insert or delete access to some of Oracle Applications Framework accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	5.8	CVE-2019-2682 MISC
oracle -- autovue_3d_professional_advanced	Vulnerability in the Oracle AutoVue 3D Professional Advanced component of Oracle Supply Chain Products Suite (subcomponent: Format Handling - 2D). Supported versions that are affected are 21.0.0 and 21.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle AutoVue 3D Professional Advanced. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle AutoVue 3D Professional Advanced accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A/N).	2019-04-23	5.0	CVE-2019-2575 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A/N).	2019-04-23	4.0	CVE-2019-2588 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A/N).	2019-04-23	5.8	CVE-2019-2595 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all BI Publisher (formerly XML Publisher) accessible data as well as unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/H/I/L/A/N).	2019-04-23	4.9	CVE-2019-2601 MISC
oracle -- business_intelligence_publisher	Vulnerability in the BI Publisher (formerly XML Publisher) component of Oracle Fusion Middleware (subcomponent: BI Publisher Security). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise BI Publisher (formerly XML Publisher). While the vulnerability is in BI Publisher (formerly XML Publisher), attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of BI Publisher (formerly XML Publisher) accessible data as well as unauthorized read access to a subset of BI Publisher (formerly XML Publisher) accessible data. CVSS 3.0 Base Score 7.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/H/I/L/A/N).	2019-04-23	6.4	CVE-2019-2616 MISC
oracle -- business_process_management_suite	Vulnerability in the Oracle Business Process Management Suite component of Oracle Fusion Middleware (subcomponent: BPM Foundation Services). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Process Management Suite. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Process Management Suite, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Business Process Management Suite accessible data as well as unauthorized update, insert or delete access to some of Oracle Business Process Management Suite accessible	2019-04-23	5.8	CVE-2019-2706 MISC BID

		data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).			
oracle -- commerce_merchandising	Vulnerability in the Oracle Commerce Merchandising component of Oracle Commerce (subcomponent: Asset Manager). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Merchandising. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Merchandising accessible data as well as unauthorized read access to a subset of Oracle Commerce Merchandising accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).	2019-04-23	6.4	<a href="#">CVE-2019-2712</a>	<a href="#">MISC</a>
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). The supported version that is affected is 11.2.0.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2659</a>	<a href="#">MISC</a>
oracle -- commerce_platform	Vulnerability in the Oracle Commerce Platform component of Oracle Commerce (subcomponent: Dynamo Application Framework). Supported versions that are affected are 11.2.0.3 and 11.3.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Commerce Platform. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data as well as unauthorized read access to a subset of Oracle Commerce Platform accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2712</a>	<a href="#">MISC</a>
oracle -- common_applications	Vulnerability in the Oracle Common Applications component of Oracle E-Business Suite (subcomponent: CRM User Management Framework). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Common Applications. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Common Applications, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Common Applications accessible data as well as unauthorized update, insert or delete access to some of Oracle Common Applications accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2665</a>	<a href="#">MISC</a>
oracle -- configurator	Vulnerability in the Oracle Configurator component of Oracle Supply Chain Products Suite (subcomponent: Active Model Generation). Supported versions that are affected are 12.1 and 12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Configurator. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Configurator accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2567</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2639</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	<a href="#">CVE-2019-2669</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2671</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2675</a>	<a href="#">MISC</a>
oracle -- crm_technical_foundation	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Preferences). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	<a href="#">CVE-2019-2676</a>	<a href="#">MISC</a>
oracle -- database	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:A/H).	2019-04-23	4.6	<a href="#">CVE-2019-2619</a>	<a href="#">MISC</a>
oracle -- database_server	Vulnerability in the Portable Clusterware component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Grid Infrastructure User privilege with logon to the infrastructure where Portable Clusterware executes to compromise Portable Clusterware. While the vulnerability is in Portable Clusterware, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Portable Clusterware. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:A/H).	2019-04-23	4.6	<a href="#">CVE-2019-2516</a>	<a href="#">MISC</a>

	(CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).			
oracle -- database_server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	<a href="#">CVE-2019-2518</a> MISC
oracle -- database_server	Vulnerability in the RDBMS DataPump component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Difficult to exploit vulnerability allows high privileged attacker having DBA role privilege with network access via Oracle Net to compromise RDBMS DataPump. Successful attacks of this vulnerability can result in takeover of RDBMS DataPump. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	<a href="#">CVE-2019-2571</a> MISC
oracle -- database_server	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2582</a> MISC
oracle -- e-business_suite	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2551</a> MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2600</a> MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2651</a> MISC
oracle -- email_center	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Email Center accessible data as well as unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2661</a> MISC
oracle -- general_ledger	Vulnerability in the Oracle General Ledger component of Oracle E-Business Suite (subcomponent: Consolidation Hierarchy Viewer). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle General Ledger. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle General Ledger accessible data as well as unauthorized access to critical data or complete access to all Oracle General Ledger accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-04-23	5.5	<a href="#">CVE-2019-2638</a> MISC
oracle -- health_sciences_data_management_workbench	Vulnerability in the Oracle Health Sciences Data Management Workbench component of Oracle Health Sciences Applications (subcomponent: User Interface). The supported version that is affected is 2.4.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Health Sciences Data Management Workbench. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Health Sciences Data Management Workbench accessible data as well as unauthorized read access to a subset of Oracle Health Sciences Data Management Workbench accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2019-04-23	5.5	<a href="#">CVE-2019-2629</a> MISC
oracle -- hospitality_cruise_dining_room_management	Vulnerability in the Oracle Hospitality Cruise Dining Room Management component of Oracle Hospitality Applications (subcomponent: Web Service). The supported version that is affected is 8.0.80. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Cruise Dining Room Management. While the vulnerability is in Oracle Hospitality Cruise Dining Room Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Cruise Dining Room Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Dining Room Management accessible data. CVSS 3.0 Base Score 9.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N).	2019-04-23	6.4	<a href="#">CVE-2019-2702</a> MISC
oracle -- interaction_center_intelligence	Vulnerability in the Oracle Interaction Center Intelligence component of Oracle E-Business Suite (subcomponent: Business Intelligence (OLTP)). Supported versions that are affected are 12.1.1, 12.1.2 and 12.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Interaction Center Intelligence. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Interaction Center Intelligence, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Interaction Center Intelligence accessible data as well as unauthorized update, insert or delete access to some of Oracle Interaction Center Intelligence accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2655</a> MISC
oracle -- istore	Vulnerability in the Oracle iStore component of Oracle E-Business Suite (subcomponent: Shopping Cart). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iStore. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iStore, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle iStore accessible data as well as unauthorized update, insert or delete access to some of Oracle iStore accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2652</a> MISC
oracle -- isupplier_portal	Vulnerability in the Oracle iSupplier Portal component of Oracle E-Business Suite (subcomponent: Attachments). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle iSupplier Portal. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle iSupplier Portal, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in	2019-04-23	5.8	<a href="#">CVE-2019-2683</a>



	unauthorized access to critical data or complete access to all Oracle iSupplier Portal accessible data as well as unauthorized update, insert or delete access to some of Oracle iSupplier Portal accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A:N).			MISC
oracle -- jd_edwards_enterpriseone_tools	Vulnerability in the JD Edwards EnterpriseOne Tools component of Oracle JD Edwards Products (subcomponent: Web Runtime). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise JD Edwards EnterpriseOne Tools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of JD Edwards EnterpriseOne Tools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	CVE-2019-2564 MISC
oracle -- jd_edwards_world_technical_foundation	Vulnerability in the JD Edwards World Technical Foundation component of Oracle JD Edwards Products (subcomponent: Service Enablement). Supported versions that are affected are A9.2, A9.3.1 and A9.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise JD Edwards World Technical Foundation. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all JD Edwards World Technical Foundation accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2019-2565 MISC
oracle -- jdk	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	5.0	CVE-2019-2602 MISC
oracle -- jdk	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H).	2019-04-23	4.3	CVE-2019-2684 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2697 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2698 MISC
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Windows DLL). The supported version that is affected is Java SE: 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. While the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	6.8	CVE-2019-2699 MISC CONFIRM
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge Management component of Oracle E-Business Suite (subcomponent: Setup, Admin). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Knowledge Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Knowledge Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H/I/L/A:N).	2019-04-23	5.8	CVE-2019-2660 MISC
oracle -- knowledge_management	Vulnerability in the Oracle Knowledge component of Oracle Siebel CRM (subcomponent: Web Applications (InfoCenter)). Supported versions that are affected are 8.5.1.0 - 8.5.1.7, 8.6.0 and 8.6.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Knowledge. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Knowledge, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Knowledge accessible data as well as unauthorized read access to a subset of Oracle Knowledge accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/L/I/L/A:N).	2019-04-23	5.8	CVE-2019-2719 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I/L/A:N).	2019-04-23	5.8	CVE-2019-2604 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I/L/A:N).	2019-04-23	5.8	CVE-2019-2664 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle	2019-04-23	4.3	CVE-2019-2670



	Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).			MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	CVE-2019-2673 MISC
oracle -- marketing	Vulnerability in the Oracle Marketing component of Oracle E-Business Suite (subcomponent: Marketing Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Marketing. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Marketing, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Marketing accessible data as well as unauthorized update, insert or delete access to some of Oracle Marketing accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	CVE-2019-2677 MISC
oracle -- micros_lucas	Vulnerability in the MICROS Lucas component of Oracle Retail Applications (subcomponent: Security). Supported versions that are affected are 2.9.5.6 and 2.9.5.7. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Lucas. Successful attacks of this vulnerability can result in takeover of MICROS Lucas. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	6.0	CVE-2018-3120 MISC
oracle -- micros_relate_customer_relationship_management_software	Vulnerability in the MICROS Relate CRM Software component of Oracle Retail Applications (subcomponent: Customer). The supported version that is affected is 11.4. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise MICROS Relate CRM Software. While the vulnerability is in MICROS Relate CRM Software, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MICROS Relate CRM Software accessible data as well as unauthorized access to critical data or complete access to all MICROS Relate CRM Software accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N).	2019-04-23	4.9	CVE-2018-3314 MISC
oracle -- micros_retail-j	Vulnerability in the MICROS Retail-J component of Oracle Retail Applications (subcomponent: Back Office). The supported version that is affected is 12.1.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise MICROS Retail-J. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MICROS Retail-J accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	CVE-2018-2880 MISC
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: libmysqld). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	4.3	CVE-2018-3123 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plugin). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2566 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2580 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2581 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2584 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2585 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2587 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2589 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2592 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2593 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2596 MISC CONFIRM
	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security:			

[illegible]

oracle -- mysql	Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	23	4.0	MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Roles). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2691 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2693 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2694 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.15 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-04-23	4.0	CVE-2019-2695 MISC CONFIRM
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I/L:A/N).	2019-04-23	5.8	CVE-2019-2603 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I/L:A/N).	2019-04-23	5.8	CVE-2019-2653 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle One-to-One Fulfillment accessible data as well as unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I/L:A/N).	2019-04-23	5.8	CVE-2019-2654 MISC
oracle -- one-to-one_fulfillment	Vulnerability in the Oracle One-to-One Fulfillment component of Oracle E-Business Suite (subcomponent: Print Server). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle One-to-One Fulfillment. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle One-to-One Fulfillment, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle One-to-One Fulfillment accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/N:I/L:A/N).	2019-04-23	4.3	CVE-2019-2674 MISC
oracle -- oracle_retail_customer_engagement	Vulnerability in the Oracle Retail Customer Engagement component of Oracle Retail Applications (subcomponent: Segment). Supported versions that are affected are 16.0 and 17.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Retail Customer Engagement. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Retail Customer Engagement accessible data as well as unauthorized read access to a subset of Oracle Retail Customer Engagement accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Customer Engagement. CVSS 3.0 Base Score 5.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L).	2019-04-23	6.0	CVE-2018-3312 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2609 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2610 MISC
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-04-23	6.4	CVE-2019-2611 MISC

	(CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)	2019-04-23	6.4	<a href="#">CVE-2019-2612 MISC</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L)	2019-04-23	6.4	<a href="#">CVE-2019-2613 MISC</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology as well as unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)	2019-04-23	6.4	<a href="#">CVE-2019-2705 MISC</a>
oracle -- peoplesoft_enterprise_elm_enterprise_learning_management	Vulnerability in the PeopleSoft Enterprise ELM component of Oracle PeopleSoft Products (subcomponent: Enterprise Learning Mgmt). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N)	2019-04-23	4.0	<a href="#">CVE-2019-2700 MISC</a>
oracle -- peoplesoft_enterprise_human_capital_management_candidate_gateway	Vulnerability in the PeopleSoft Enterprise HRMS component of Oracle PeopleSoft Products (subcomponent: Candidate Gateway). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HRMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HRMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise HRMS accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise HRMS accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2591 MISC</a>
oracle -- peoplesoft_enterprise_human_capital_management_talent_acquisition_manager	Vulnerability in the PeopleSoft Enterprise HCM Talent Acquisition Manager component of Oracle PeopleSoft Products (subcomponent: Job Opening). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Talent Acquisition Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise HCM Talent Acquisition Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data as well as unauthorized update, insert or delete access to some of PeopleSoft Enterprise HCM Talent Acquisition Manager accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2590 MISC</a>
oracle -- peoplesoft_enterprise_learning_management	Vulnerability in the PeopleSoft Enterprise ELM Enterprise Learning Management component of Oracle PeopleSoft Products (subcomponent: Application Search). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM Enterprise Learning Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise ELM Enterprise Learning Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2707 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Homepage & Navigation). Supported versions that are affected are 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N)	2019-04-23	4.3	<a href="#">CVE-2019-2573 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: RemoteCall). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)	2019-04-23	4.0	<a href="#">CVE-2019-2586 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PT PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.55, 8.56 and 8.57. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PT PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PT PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PT PeopleTools accessible data. CVSS 3.0 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N)	2019-04-23	4.9	<a href="#">CVE-2019-2594 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N)	2019-04-23	5.8	<a href="#">CVE-2019-2597 MISC</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: SQR). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. While the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise	2019-04-23	5.5	<a href="#">CVE-2019-2598 MISC</a>



	PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 8.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N).			
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Core Technology). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2637</a> MISC
oracle -- primavera_p6_enterprise_project_portfolio_management	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). The supported version that is affected is 18.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2701</a> MISC
oracle -- service_bus	Vulnerability in the Oracle Service Bus component of Oracle Fusion Middleware (subcomponent: Web Container). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Service Bus. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	5.0	<a href="#">CVE-2019-2576</a> MISC
oracle -- service_contracts	Vulnerability in the Oracle Service Contracts component of Oracle E-Business Suite (subcomponent: Renewals). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Service Contracts, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Service Contracts accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-04-23	4.3	<a href="#">CVE-2019-2622</a> MISC
oracle -- siebel_crm	Vulnerability in the Siebel Core - Server BizLogic Script component of Oracle Siebel CRM (subcomponent: Integration - Scripting). The supported version that is affected is 19.3. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Siebel Core - Server BizLogic Script. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Siebel Core - Server BizLogic Script accessible data as well as unauthorized read access to a subset of Siebel Core - Server BizLogic Script accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Siebel Core - Server BizLogic Script. CVSS 3.0 Base Score 4.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:L).	2019-04-23	6.5	<a href="#">CVE-2019-2570</a> MISC
oracle -- soa_suite	Vulnerability in the Oracle SOA Suite component of Oracle Fusion Middleware (subcomponent: Fabric Layer). The supported version that is affected is 11.1.1.9.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle SOA Suite. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle SOA Suite accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2572</a> MISC
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: IPS Package Manager). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Solaris accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2704</a> MISC
oracle -- territory_management	Vulnerability in the Oracle Territory Management component of Oracle E-Business Suite (subcomponent: Territory Administration). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Territory Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Territory Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Territory Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Territory Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2662</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2640</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2641</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2642</a> MISC
oracle -- trade_management	Vulnerability in the Oracle Trade Management component of Oracle E-Business Suite (subcomponent: User Interface). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Trade Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Trade Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Trade Management accessible data as well as unauthorized update, insert or delete access to some of Oracle Trade Management accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2643</a> MISC
	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: Security). Supported versions that are affected are 6.3.7, 6.4.2 and 6.4.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to			



oracle -- transportation_management	compromise Oracle Transportation Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Transportation Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Transportation Management accessible data as well as unauthorized read access to a subset of Oracle Transportation Management accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-04-23	5.8	<a href="#">CVE-2019-2709 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2656 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2657 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2680 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.4	<a href="#">CVE-2019-2690 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2696 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2703 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2721 MISC EXPLOIT: DB</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2722 MISC</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-04-23	4.6	<a href="#">CVE-2019-2723 MISC</a>
oracle -- webcenter_sites	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Sites. While the vulnerability is in Oracle WebCenter Sites, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 8.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2578 MISC</a>
oracle -- webcenter_sites	Vulnerability in the Oracle WebCenter Sites component of Oracle Fusion Middleware (subcomponent: Advanced UI). The supported version that is affected is 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebCenter Sites. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebCenter Sites accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2579 MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/N/I:L/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2568 MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	4.0	<a href="#">CVE-2019-2615 MISC</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS	2019-04-23	5.5	<a href="#">CVE-2019-2618 MISC</a>

	Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N).			
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2647</a> MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2648</a> MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2649</a> MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	2019-04-23	5.0	<a href="#">CVE-2019-2650</a> MISC
oracle -- work_in_process	Vulnerability in the Oracle Work in Process component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-04-23	5.5	<a href="#">CVE-2019-2633</a> MISC
osticket -- osticket	In osTicket before 1.12, XSS exists via /upload/file.php, /upload/scp/users.php?do=import-users, and /upload/scp/ajax.php/users/import if an agent manager user uploads a crafted .csv file to the User Importer, because file contents can appear in an error message. The XSS can lead to local file inclusion.	2019-04-25	4.3	<a href="#">CVE-2019-11537</a> MISC MISC MISC
projectsend -- projectsend	An issue was discovered in ProjectSend r1053. upload-process-form.php allows finished_files[]=./ directory traversal. It is possible for users to read arbitrary files and (potentially) access the supporting database, delete arbitrary files, access user passwords, or run arbitrary code.	2019-04-20	6.5	<a href="#">CVE-2019-11378</a> BID MISC
projectsend -- projectsend	Cross-site scripting (XSS) vulnerability in ProjectSend before r1070 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	4.3	<a href="#">CVE-2019-11533</a> BID CONFIRM
qemu -- qemu	hw/sparc64/sun4u.c in QEMU 3.1.50 is vulnerable to a NULL pointer dereference, which allows the attacker to cause a denial of service via a device driver.	2019-04-19	5.0	<a href="#">CVE-2019-5008</a> BID MISC MISC
redhat -- keycloak	Keycloak up to version 6.0.0 allows the end user token (access or id token JWT) to be used as the session cookie for browser sessions for OIDC. As a result an attacker with access to service provider backend could hijack user's browser session.	2019-04-24	5.5	<a href="#">CVE-2019-3868</a> BID CONFIRM
redhat -- virtualization	A memory leak in archive_read_format_zip_cleanup in archive_read_support_format_zip.c in libarchive 3.3.4-dev allows remote attackers to cause a denial of service via a crafted ZIP file because of a HAVE_LZMA_H typo. NOTE: this only affects users who downloaded the development code from GitHub. Users of the product's official releases are unaffected.	2019-04-22	4.3	<a href="#">CVE-2019-11463</a> MISC MISC
sass-lang -- libsass	The parsing component in LibSass through 3.5.5 allows attackers to cause a denial-of-service (uncontrolled recursion in Sass::Parser::parse_css_variable_value in parser.cpp).	2019-04-23	4.3	<a href="#">CVE-2018-20821</a> MISC
sass-lang -- libsass	LibSass 3.5.4 allows attackers to cause a denial-of-service (uncontrolled recursion in Sass::Complex_Selector::perform in ast.hpp and Sass::Inspect::operator in inspect.cpp).	2019-04-23	4.3	<a href="#">CVE-2018-20822</a> MISC
sem-cms -- semcms	An issue was discovered in SEMCMS 3.8. SEMCMS_Inquiry.php allows AID[] SQL Injection because the class.phpmailer.php inject_check_sql protection mechanism is incomplete.	2019-04-25	6.5	<a href="#">CVE-2019-11518</a> MISC
siteserver -- siteserver_cms	A issue was discovered in SiteServer CMS 6.9.0. It allows remote attackers to execute arbitrary code because an administrator can add the permitted file extension .aasp, which is converted to .asp because the "as" substring is deleted.	2019-04-22	6.5	<a href="#">CVE-2019-11401</a> MISC
struktur -- libheif	libheif 1.4.0 has a use-after-free in heif::HeifContext::Image::set_alpha_channel in heif_context.h because heif_context.cc mishandles references to non-existing alpha images.	2019-04-23	6.8	<a href="#">CVE-2019-11471</a> MISC MISC
veronalabs -- wp_statistics	The WP Statistics plugin through 12.6.2 for WordPress has XSS, allowing a remote attacker to inject arbitrary web script or HTML via the Referer header of a GET request.	2019-04-23	4.3	<a href="#">CVE-2019-10864</a> CONFIRM
verypdf -- verypdf	VeryPDF 4.1 has a Memory Overflow leading to Code Execution because pdfocx(CxImageTIF::operator in pdfocx.ocx (used by pdfeditor.exe and pdfcmd.exe) is mishandled.	2019-04-26	6.8	<a href="#">CVE-2019-11493</a> MISC
vestacp -- control_panel	Vesta Control Panel 0.9.8-23 allows XSS via a crafted URL.	2019-04-19	4.3	<a href="#">CVE-2019-9841</a> MISC CONFIRM CONFIRM
wavpack -- wavpack	WavpackSetConfiguration64 in pack_utils.c in libwavpack.a in WavPack through 5.1.0 has a "Conditional jump or move depends on uninitialised value" condition, which might allow attackers to cause a denial of service (application crash) via a DFF file that lacks valid sample-rate data.	2019-04-24	4.3	<a href="#">CVE-2019-11498</a> MISC MISC
wcms -- wcms	wcms/wex/finder/action.php in WCMS v0.3.2 has a Arbitrary File Upload Vulnerability via developer/finder because .php is a valid extension according to the fm_get_text_exts function.	2019-04-20	6.5	<a href="#">CVE-2019-11377</a> MISC MISC
whatsns -- whatsns	whatsns 4.0 allows index.php?inform/add.html qid SQL injection.	2019-04-22	6.5	<a href="#">CVE-2019-11451</a> MISC
whatsns -- whatsns	whatsns 4.0 allows index.php?admin_category/remove.html cid[] SQL injection.	2019-04-22	6.5	<a href="#">CVE-2019-11452</a> MISC
wifi_ftp_server_project -- wifi_ftp_server	An issue was discovered in the Medha WiFi FTP Server application 1.8.3 for Android. An attacker can read the username/password of a valid user via /data/data/com.medhaapps.wififtpserver/shared_prefs/com.medhaapps.wififtpserver_preferences.xml	2019-04-22	5.0	<a href="#">CVE-2019-11383</a> MISC
wordfence -- wordfence	The Wordfence plugin 7.2.3 for WordPress allows XSS via a unique attack vector.	2019-04-	4.3	<a href="#">CVE-2019-9669</a>

		25		MISC
zalora -- zalora	The Zalora application 6.15.1 for Android stores confidential information insecurely on the system (i.e. plain text), which allows a non-root user to find out the username/password of a valid user via /data/data/com.zalora.android/shared_prefs/login_data.xml.	2019-04-22	5.0	CVE-2019-11384 MISC
zohocorp -- servicedesk_plus	Zoho ManageEngine ServiceDesk 9.3 allows session hijacking and privilege escalation because an established guest session is automatically converted into an established administrator session when the guest user enters the administrator username, with an arbitrary incorrect password, in an mc/ login attempt within a different browser tab.	2019-04-24	6.5	CVE-2019-10008 EXPLOIT-DB CONFIRM

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
audiocodes -- 405hd_firmware	A missing password verification in the web interface in AudioCodes 405HD VoIP phone with firmware 2.2.12 allows an remote attacker (in the same network as the device) to change the admin password without authentication via a POST request.	2019-04-25	3.3	CVE-2018-16219 MISC
cmsmadesimple -- cms_made_simple	The File Manager in CMS Made Simple through 2.2.10 has Reflected XSS via the "New name" field in a Rename action.	2019-04-24	3.5	CVE-2019-11513 MISC
ibm -- content_navigator	IBM Content Navigator 2.0.3 and 3.0CD is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155999.	2019-04-25	3.5	CVE-2019-4033 XF CONFIRM
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 159464.	2019-04-25	3.5	CVE-2019-4238 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157107.	2019-04-25	3.5	CVE-2019-4073 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157108.	2019-04-25	3.5	CVE-2019-4074 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157109.	2019-04-25	3.5	CVE-2019-4075 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157110.	2019-04-25	3.5	CVE-2019-4076 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 157111.	2019-04-25	3.5	CVE-2019-4077 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 could allow an authenticated user to obtain sensitive document information under unusual circumstances. IBM X-Force ID: 158401.	2019-04-25	3.5	CVE-2019-4146 XF CONFIRM
ibm -- sterling_b2b_integrator	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 and 6.0.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 158414.	2019-04-25	3.5	CVE-2019-4148 XF CONFIRM
oracle -- business_intelligence	Vulnerability in the Oracle Business Intelligence Enterprise Edition component of Oracle Fusion Middleware (subcomponent: Web Catalog). Supported versions that are affected are 11.1.1.9.0, 12.2.1.3.0 and 12.2.1.4.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Business Intelligence Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/L/I:N/A/N).	2019-04-23	2.6	CVE-2019-2605 MISC
oracle -- data_integrator	Vulnerability in the Oracle Data Integrator component of Oracle Fusion Middleware (subcomponent: ODI Tools). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Data Integrator. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Data Integrator accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C/L/I:N/A/N).	2019-04-23	3.5	CVE-2019-2720 MISC
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2614 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2617 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2623 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2630 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with login to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	1.9	CVE-2019-2634 MISC CONFIRM
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Group Replication Plugin). Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via MySQL Protocol to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A/H).	2019-04-23	3.5	CVE-2019-2636 MISC CONFIRM
	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/J).			

oracle -- mysql_connector/j	Supported versions that are affected are 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with login to the infrastructure where MySQL Connectors executes to compromise MySQL Connectors. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).	2019-04-23	3.5	<a href="#">CVE-2019-2692</a> MISC
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: File Locking Services). The supported version that is affected is 11. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle Solaris executes to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Solaris. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	2.1	<a href="#">CVE-2019-2577</a> MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	2.1	<a href="#">CVE-2019-2574</a> MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-04-23	2.1	<a href="#">CVE-2019-2678</a> MISC
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are Prior to 5.2.28 and prior to 6.0.6. Easily exploitable vulnerability allows low privileged attacker with login to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:H).	2019-04-23	3.6	<a href="#">CVE-2019-2679</a> MISC
profiles_project -- profiles	XSS exists in the ProFiles 1.5 component for Joomla! via the name or path parameter when creating a new folder in the administrative panel.	2019-04-26	3.5	<a href="#">CVE-2018-18276</a> MISC
wolfcms -- wolfcms	WolfCMS 0.8.3.1 allows XSS via an SVG file to /?/admin/plugin/file_manager/browse/.	2019-04-25	3.5	<a href="#">CVE-2018-18823</a> MISC MISC MISC MISC
wolfcms -- wolfcms	WolfCMS v0.8.3.1 allows XSS via an SVG file to /?/admin/plugin/file_manager/browse/.	2019-04-25	3.5	<a href="#">CVE-2018-18824</a> MISC MISC MISC MISC

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aiikcms -- aiikcms	An issue was discovered in AiikCms v2.0. There is a File upload vulnerability, as demonstrated by an admin/page/system/nav.php request with PHP code in a .php file with the application/octet-stream content type.	2019-04-27	not yet calculated	<a href="#">CVE-2019-11568</a> MISC
aiikcms -- aiikcms	An issue was discovered in AiikCms v2.0. There is a SQL Injection vulnerability via \$_GET[del], as demonstrated by an admin/page/system/nav.php?del= URI.	2019-04-27	not yet calculated	<a href="#">CVE-2019-11567</a> MISC
apache -- pluto	The input fields of the Apache Pluto "Chat Room" demo portlet 3.0.0 and 3.0.1 are vulnerable to Cross-Site Scripting (XSS) attacks. Mitigation: * Uninstall the ChatRoomDemo war file - or - * migrate to version 3.1.0 of the chat-room-demo war file	2019-04-26	not yet calculated	<a href="#">CVE-2019-0186</a> MLIST MISC BID MLIST MISC EXPLOIT-DB MLIST
apache -- qpuid_proton	While investigating bug PROTON-2014, we discovered that under some circumstances Apache Qpid Proton versions 0.9 to 0.27.0 (C library and its language bindings) can connect to a peer anonymously using TLS "even when configured to verify the peer certificate" while used with OpenSSL versions before 1.1.0. This means that an undetected man in the middle attack could be constructed if an attacker can arrange to intercept TLS traffic.	2019-04-23	not yet calculated	<a href="#">CVE-2019-0223</a> MLIST BID REDHAT MISC MLIST MLIST MLIST MLIST
apache -- zeppelin	In Apache Zeppelin prior to 0.8.0 the cron scheduler was enabled by default and could allow users to run paragraphs as other users without authentication.	2019-04-23	not yet calculated	<a href="#">CVE-2018-1317</a> MLIST BID MLIST MISC
apache -- zeppelin	Apache Zeppelin prior to 0.7.3 was vulnerable to session fixation which allowed an attacker to hijack a valid user session. Issue was reported by "stone lone".	2019-04-23	not yet calculated	<a href="#">CVE-2017-12619</a> MLIST BID MLIST MISC
apparmor -- apparmor	In all versions of AppArmor mount rules are accidentally widened when compiled.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1585</a> MISC
aquaverde -- aquarius_cms	aquaverde Aquarius CMS through 4.3.5 writes POST and GET parameters (including passwords) to a log file because of incorrect if/else usage in the Log-File writer component.	2019-04-24	not yet calculated	<a href="#">CVE-2019-9734</a> MISC MISC
arrow-kt -- arrow	arrow-kt Arrow before 0.9.0 resolved Gradle build artifacts (for compiling and building the published JARs) over HTTP instead of HTTPS. Any of these dependent artifacts could have been maliciously compromised by an MITM attack.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11404</a> MISC MISC MISC MISC
asus -- zenfone_3_max_android_device	The ASUS ZenFone 3 Max Android device with a build fingerprint of asus/US_Phone/ASUS_X008_17.0/NRD90M/US_Phone-14.14.1711.92-20171208:user/release-keys contains the android framework (i.e., system_server) with a package name of android (versionCode=24, versionName=7.0) that has been modified by ASUS or another entity in the supply chain. The system_server process in the core android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage (i.e., sdcard). The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the	2019-04-25	not yet calculated	<a href="#">CVE-2018-14980</a> MISC MISC

	EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.			
asus -- zenfone_v_live_android_device	The ASUS Zenfone V Live Android device with a build fingerprint of asus/VZW_ASUS_A009/ASUS_A009:7.1.1/NMF26F/14.0610.1802.78-20180313:user/release-keys and the Asus ZenFone 3 Max Android device with a build fingerprint of asus/US_Phone/ASUS_X008_1:7.0/NRD90M/US_Phone-14.14.1711.92-20171208:user/release-keys both contain a pre-installed platform app with a package name of com.asus.splendidcommandagent (versionCode=1510200090, versionName=1.2.0.18_160928) that contains an exported service named com.asus.splendidcommandagent.SplendidCommandAgentService that allows any app co-located on the device to supply arbitrary commands to be executed as the system user. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. Executing commands as system user can allow a third-party app to video record the user's screen, factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), change the default Input Method Editor (IME) (e.g., keyboard) with one contained within the attacking app that contains keylogging functionality, obtain the user's text messages, and more.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14993</a> MISC MISC MISC
audiocodes -- audiocodes_405hd	A command injection (missing input validation, escaping) in the monitoring or memory status web interface in AudioCodes 405HD (firmware 2.2.12) VoIP phone allows an authenticated remote attacker in the same network as the device to trigger OS commands (like starting telnetd or opening a reverse shell) via a POST request to the web server. In combination with another attack (unauthenticated password change), the attacker can circumvent the authentication requirement.	2019-04-25	not yet calculated	<a href="#">CVE-2018-16216</a> MISC
c3p0 -- c3p0	c3p0 version < 0.9.5.4 may be exploited by a billion laughs attack when loading XML configuration due to missing protections against recursive entity expansion when loading configuration.	2019-04-22	not yet calculated	<a href="#">CVE-2019-5427</a> MISC
canonical -- appopt	Any Python module in sys.path can be imported if the command line of the process triggering the coredump is Python and the first argument is -m in Appopt before 2.19.2 function _python_module_path.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1341</a> MISC MISC
canonical -- oxide	A malicious webview could install long-lived unload handlers that re-use an incognito BrowserContext that is queued for destruction in versions of Oxide before 1.18.3.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1586</a> MISC
canonical -- snapd	A vulnerability in the seccomp filters of Canonical snapd before version 2.37.4 allows a strict mode snap to insert characters into a terminal on a 64-bit host. The seccomp rules were generated to match 64-bit ioctl(2) commands on a 64-bit platform; however, the Linux kernel only uses the lower 32 bits to determine which ioctl(2) commands to run. This issue affects: Canonical snapd versions prior to 2.37.4.	2019-04-23	not yet calculated	<a href="#">CVE-2019-7303</a> MISC MISC
canonical -- snapd	snap-confine as included in snapd before 2.39 did not guard against symlink races when performing the chdir() to the current working directory of the calling user, aka a "cwd restore permission bypass."	2019-04-24	not yet calculated	<a href="#">CVE-2019-11503</a> MLIST MISC MISC
canonical -- snapd	snap-confine in snapd before 2.38 incorrectly set the ownership of a snap application to the uid and gid of the first calling user. Consequently, that user had unintended access to a private /tmp directory.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11502</a> MLIST MISC MISC
canonical -- snapd	Canonical snapd before version 2.37.1 incorrectly performed socket owner validation, allowing an attacker to run arbitrary commands as root. This issue affects: Canonical snapd versions prior to 2.37.1.	2019-04-23	not yet calculated	<a href="#">CVE-2019-7304</a> MISC MISC MISC
canonical -- ubuntu_maas	A vulnerability in maasserver.api.get_file_by_name of Ubuntu MAAS allows unauthenticated network clients to download any file. This issue affects: Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2014-1426</a> MISC
canonical -- ubuntu_maas	A vulnerability in generate_filestorage_key of Ubuntu MAAS allows an attacker to brute-force filenames. This issue affects Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2014-1428</a> MISC
canonical -- ubuntu_maas	A vulnerability in the REST API of Ubuntu MAAS allows an attacker to cause a logged-in user to execute commands via cross-site scripting. This issue affects MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2014-1427</a> MISC
canonical -- ubuntu_maas	The SeaMicro provisioning of Ubuntu MAAS logs credentials, including username and password, for the management interface. This issue affects Ubuntu MAAS versions prior to 1.9.2.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1320</a> MISC
canonical -- ubuntu_selinux_initscript	The Ubuntu SELinux initscript before version 1.0:10 used touch to create a lockfile in a world-writable directory. If the OS kernel does not have symlink protections then an attacker can cause a zero byte file to be allocated on any writable filesystem.	2019-04-22	not yet calculated	<a href="#">CVE-2011-3151</a> MISC
cerner -- connectivity_engine_4_devices	An issue was discovered on Cerner Connectivity Engine (CCE) 4 devices. The hostname, timezone, and NTP server configurations on the CCE device are vulnerable to command injection by sending a crafted configuration file over the network.	2019-04-25	not yet calculated	<a href="#">CVE-2018-20053</a> MISC
cerner -- connectivity_engine_4_devices	An issue was discovered on Cerner Connectivity Engine (CCE) 4 devices. The user running the main CCE firmware has NOPASSWD sudo privileges to several utilities that could be used to escalate privileges to root. One example is the "sudo ln -s /tmp/script /etc/cron.hourly/script" command.	2019-04-25	not yet calculated	<a href="#">CVE-2018-20052</a> MISC
check_point -- zonealarm_and_endpoint_security_client_for_windows	A hard-link created from log file archive of Check Point ZoneAlarm up to 15.4.062 or Check Point Endpoint Security client for Windows before E80.96 to any file on the system will get its permission changed so that all users can access that linked file. Doing this on files with limited access gains the local attacker higher privileges to the file.	2019-04-22	not yet calculated	<a href="#">CVE-2019-8452</a> MISC
cloud_foundry -- bosh_backup_and_restore_cli	Cloud Foundry BOSH Backup and Restore CLI, all versions prior to 1.5.0, does not check the authenticity of backup scripts in BOSH. A remote authenticated malicious user can modify the metadata file of a Bosh Backup and Restore job to request extra backup files from different jobs upon restore. The exploited hooks in this metadata script were only maintained in the cfr-etc-d-release, so clusters deployed with the BBR job for etc-d in this release are vulnerable.	2019-04-24	not yet calculated	<a href="#">CVE-2019-3786</a> CONFIRM
cloud_foundry -- cf-deployment	Cloud Foundry cf-deployment, versions prior to 7.9.0, contain java components that are using an insecure protocol to fetch dependencies when building. A remote unauthenticated malicious attacker could hijack the DNS entry for the dependency, and inject malicious code into the component.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3801</a> CONFIRM
cloud_foundry -- routing_release	Cloud Foundry Routing Release, all versions prior to 0.188.0, contains a vulnerability that can hijack the traffic to route services hosted outside the platform. A user with space developer permissions can create a private domain that shadows the external domain of the route service, and map that route to an app. When the gorouter receives traffic destined for the external route service, this traffic will instead be directed to the internal app using the shadow route.	2019-04-24	not yet calculated	<a href="#">CVE-2019-3789</a> CONFIRM
cloud_foundry -- uaa_release	Cloud Foundry UAA Release, versions prior to 71.0, allows clients to be configured with an insecure redirect uri. Given a UAA client was configured with a wildcard in the redirect uri's subdomain, a remote malicious unauthenticated user can craft a phishing link to get a UAA access code from the victim.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3788</a> CONFIRM
contao -- contao	Contao 3.0.0 to 3.5.30 and 4.0.0 to 4.4.7 contains an SQL injection vulnerability in the back end as well as in the listing module.	2019-04-25	not yet calculated	<a href="#">CVE-2017-16558</a> CONFIRM CONFIRM
cribl -- cribl_ui	Cribl UI 1.5.0 allows remote attackers to run arbitrary commands via an unauthenticated web request.	2019-04-23	not yet calculated	<a href="#">CVE-2019-11076</a> CONFIRM MISC
daviewindy -- daviewindy	DaviewIndy 8.98.7 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed Image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution.	2019-04-25	not yet calculated	<a href="#">CVE-2019-9137</a> MISC
dell_emc -- idrac	Dell EMC iDRAC6 versions prior to 2.92, iDRAC7/iDRAC8 versions prior to 2.61.60.60, and iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22 and 3.23.23.23 contain a stack-based buffer overflow vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to crash the webserver or execute arbitrary code on the system with privileges of the webserver by sending specially crafted input data to the affected system.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3705</a> MISC
	Dell EMC iDRAC9 versions prior to 3.30.30.30 contain an authentication bypass vulnerability.		not yet	<a href="#">CVE-2019-3707</a>



dell_emc -- idrac9	A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted input data to the WS-MAN interface.	2019-04-26	calculated	<a href="#">MISC</a>
dell_emc -- idrac9	Dell EMC iDRAC9 versions prior to 3.24.24.24, 3.21.26.22, 3.22.22.22 and 3.21.25.22 contain an authentication bypass vulnerability. A remote attacker may potentially exploit this vulnerability to bypass authentication and gain access to the system by sending specially crafted data to the iDRAC web interface.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3706</a> <a href="#">MISC</a>
dell_emc -- open_manage_system_administrator	Dell EMC Open Manage System Administrator (OMSA) versions prior to 9.3.0 contain a Directory Traversal Vulnerability. A remote authenticated malicious user with admin privileges could potentially exploit this vulnerability to gain unauthorized access to the file system by exploiting insufficient sanitization of input parameters.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3720</a> <a href="#">MISC</a>
dell_emc -- open_manage_system_administrator	Dell EMC Open Manage System Administrator (OMSA) versions prior to 9.3.0 contain an Improper Range Header Processing Vulnerability. A remote unauthenticated attacker may send crafted requests with overlapping ranges to cause the application to compress each of the requested bytes, resulting in a crash due to excessive memory consumption and preventing users from accessing the system.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3721</a> <a href="#">MISC</a>
deltek -- vision	Deltek Vision 7.x before 7.6 permits the execution of any attacker supplied SQL statement through a custom RPC over HTTP protocol. The Vision system relies on the client binary to enforce security rules and integrity of SQL statements and other content being sent to the server. Client HTTP calls can be manipulated by one of several means to execute arbitrary SQL statements (similar to SQLi) or possibly have unspecified other impact via this custom protocol. To perform these attacks an authenticated session is first required. In some cases client calls are obfuscated by encryption, which can be bypassed due to hard-coded keys and an insecure key rotation protocol. Impacts may include remote code execution in some deployments; however, the vendor states that this cannot occur when the installation documentation is heeded.	2019-04-24	not yet calculated	<a href="#">CVE-2018-18251</a> <a href="#">CONFIRM</a>
dentsply_sirona -- sidexis	A default username and password in Dentsply Sirona Sidexis 4.2 and possibly others allows an attacker to gain administrative access to the application server.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11081</a> <a href="#">MISC</a>
dillon_kane_group -- tidal_workload_automation_agent	An issue was discovered in Dillon Kane Tidal Workload Automation Agent 3.2.0.5 (formerly known as Cisco Workload Automation or CWA). The Enterprise Scheduler for AIX allows local users to gain privileges via Command Injection in crafted Tidal Job Buffers (TJB) parameters. NOTE: this vulnerability exists because the CVE-2014-3272 solution did not address AIX operating systems.	2019-04-26	not yet calculated	<a href="#">CVE-2019-6689</a> <a href="#">MISC</a>
dovecot -- dovecot	The JSON encoder in Dovecot before 2.3.5.2 allows attackers to repeatedly crash the authentication service by attempting to authenticate with an invalid UTF-8 sequence as the username.	2019-04-24	not yet calculated	<a href="#">CVE-2019-10691</a> <a href="#">MUST</a> <a href="#">MUST</a>
dropbox -- lepton	io/ZlibCompression.cc in the decompression component in Dropbox Lepton 1.2.1 allows attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact by crafting a jpg image file. The root cause is a missing check of header payloads that may be (incorrectly) larger than the maximum file size.	2019-04-23	not yet calculated	<a href="#">CVE-2018-20819</a> <a href="#">MISC</a>
eclipse -- jetty	In Eclipse Jetty version 7.x, 8.x, 9.2.27 and older, 9.3.26 and older, and 9.4.16 and older, the server running on any OS and Jetty version combination will reveal the configured fully qualified directory base resource location on the output of the 404 error for not finding a Context that matches the requested path. The default server behavior on jetty-distribution and jetty-home will include at the end of the Handler tree a DefaultHandler, which is responsible for reporting this 404 error, it presents the various configured contexts as HTML for users to click through to. This produced HTML includes output that contains the configured fully qualified directory base resource location for each context.	2019-04-22	not yet calculated	<a href="#">CVE-2019-10247</a> <a href="#">CONFIRM</a>
eclipse -- jetty	In Eclipse Jetty version 9.2.27, 9.3.26, and 9.4.16, the server running on Windows is vulnerable to exposure of the fully qualified Base Resource directory name on Windows to a remote client when it is configured for showing a Listing of directory contents. This information reveal is restricted to only the content in the configured base resource directories.	2019-04-22	not yet calculated	<a href="#">CVE-2019-10246</a> <a href="#">CONFIRM</a>
eclipse -- openj9	In Eclipse OpenJ9 prior to the 0.14.0 release, the Java bytecode verifier incorrectly allows a method to execute past the end of bytecode array causing crashes. Eclipse OpenJ9 v0.14.0 correctly detects this case and rejects the attempted class load.	2019-04-19	not yet calculated	<a href="#">CVE-2019-10245</a> <a href="#">CONFIRM</a>
eclipse -- vorto	Eclipse Vorto versions prior to 0.11 resolved Maven build artifacts for the Xtext project over HTTP instead of HTTPS. Any of these dependent artifacts could have been maliciously compromised by a MITM attack. Hence produced build artifacts of Vorto might be infected.	2019-04-22	not yet calculated	<a href="#">CVE-2019-10248</a> <a href="#">CONFIRM</a>
ekiga -- ekiga	Ekiga versions before 3.3.0 attempted to load a module from /tmp/ekiga_test.so.	2019-04-22	not yet calculated	<a href="#">CVE-2011-1830</a> <a href="#">MISC</a>
envoy_proxy -- envoy	When parsing HTTP/1.x header values, Envoy 1.9.0 and before does not reject embedded zero characters (NUL, ASCII 0x0). This allows remote attackers crafting header values containing embedded NUL characters to potentially bypass header matching rules, gaining access to unauthorized resources.	2019-04-25	not yet calculated	<a href="#">CVE-2019-9900</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
envoy_proxy -- envoy	Envoy 1.9.0 and before does not normalize HTTP URL paths. A remote attacker may craft a relative path, e.g., something/.admin, to bypass access control, e.g., a block on /admin. A backend server could then interpret the non-normalized path and provide an attacker access beyond the scope provided for by the access control policy.	2019-04-25	not yet calculated	<a href="#">CVE-2019-9901</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
essential_products -- phone_android_device	The Essential Phone Android device with a build fingerprint of essential/mata/mata;8.1.0/OPM1.180104.166/297:user/release-keys contains a pre-installed platform app with a package name of com.ts.android.hiddenmenu (versionName=1.0, platformBuildVersionName=8.1.0) that contains an exported activity app component named com.ts.android.hiddenmenu.rtn.RTNResetActivity that allows any app co-located on the device to programmatically initiate a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14994</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
flarum -- flarum	User/Command/ConfirmEmailHandler.php in Flarum before 0.1.0-beta.8 mishandles invalidation of user email tokens.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11514</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitea -- gitea	Gitea before 1.8.0 allows 1FA for user accounts that have completed 2FA enrollment. If a user's credentials are known, then an attacker could send them to the API without requiring the 2FA one-time password.	2019-04-27	not yet calculated	<a href="#">CVE-2019-11576</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- nautilus	An issue was discovered in GNOME Nautilus 3.30 prior to 3.30.6 and 3.32 prior to 3.32.1. A compromised thumbnailer may escape the bubblewrap sandbox used to confine thumbnailers by using the TIOCSTI ioctl to push characters into the input buffer of the thumbnailer's controlling terminal, allowing an attacker to escape the sandbox if the thumbnailer has a controlling terminal. This is due to improper filtering of the TIOCSTI ioctl on 64-bit systems, similar to CVE-2019-10063.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11461</a> <a href="#">MISC</a>
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/faqmasterformupdate.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	<a href="#">CVE-2018-15581</a> <a href="#">CONFIRM</a>
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/boardgroup_form_update.php and adm/boardgroup_list_update.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	<a href="#">CVE-2018-15584</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/sms_admin/num_book_write.php and adm/sms_admin/num_book_update.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	<a href="#">CVE-2018-15582</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
gnuboard5 -- gnuboard5	Cross-Site Scripting (XSS) vulnerability in adm/contentformupdate.php in gnuboard5 before 5.3.1.6 allows remote attackers to inject arbitrary web script or HTML.	2019-04-26	not yet calculated	<a href="#">CVE-2018-15580</a> <a href="#">CONFIRM</a>
google -- tensorflow	Invalid memory access and/or a heap buffer overflow in the TensorFlow XLA compiler in Google TensorFlow before 1.7.1 could cause a crash or read from other parts of process memory via a crafted configuration file.	2019-04-24	not yet calculated	<a href="#">CVE-2018-10055</a> <a href="#">CONFIRM</a>
google -- tensorflow	Google TensorFlow 1.7.x and earlier is affected by a Buffer Overflow vulnerability. The type of exploitation is context-dependent.	2019-04-24	not yet calculated	<a href="#">CVE-2018-7575</a> <a href="#">CONFIRM</a>
google -- tensorflow	Memcpy parameter overlap in Google Snappy library 1.1.4, as used in Google TensorFlow before 1.7.1, could result in a crash or read from other parts of process memory.	2019-04-24	not yet calculated	<a href="#">CVE-2018-7577</a> <a href="#">CONFIRM</a>

google -- tensorflow	Google TensorFlow 1.6.x and earlier is affected by a Null Pointer Dereference vulnerability. The type of exploitation is: context-dependent.	2019-04-24	not yet calculated	<a href="#">CVE-2018-7574</a> CONFIRM
heketi -- heketi	It was found that default configuration of Heketi does not require any authentication potentially exposing the management interface to misuse. This issue only affects heketi as shipped with OpenShift Container Platform 3.11.	2019-04-22	not yet calculated	<a href="#">CVE-2019-3899</a> CONFIRM
hisilicon -- hi3510_firmware	Incorrect access control in the RTSP stream and web portal on all IP cameras based on Hisilicon Hi3510 firmware (until Webware version V1.0.1) allows attackers to view an RTSP stream by connecting to the stream with hidden credentials (guest or user) that are neither displayed nor configurable in the camera's CamHi or keye mobile management application. This affects certain devices labeled as Hi3510, Hi3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Uniotek, ESCAM, etc.	2019-04-23	not yet calculated	<a href="#">CVE-2019-10711</a> MISC
hisilicon -- hi3510_firmware	Insecure permissions in the Web management portal on all IP cameras based on Hisilicon Hi3510 firmware allow authenticated attackers to receive a network's cleartext WiFi credentials via a specific HTTP request. This affects certain devices labeled as Hi3510, Hi3518, LOOSAFE, LEVCOECAM, Sywstoda, BESDER, WUSONGLUSAN, GADINAN, Uniotek, ESCAM, etc.	2019-04-23	not yet calculated	<a href="#">CVE-2019-10710</a> MISC
hostapd_and_wpa_supplicant -- hostapd_and_wpa_supplicant	The EAP-pwd implementation in hostapd (EAP server) before 2.8 and wpa_supplicant (EAP peer) before 2.8 does not validate fragmentation reassembly state properly for a case where an unexpected fragment could be received. This could result in process termination due to a NULL pointer dereference (denial of service). This affects eap_server/eap_server_pwd.c and eap_peer/eap_pwd.c.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11555</a> MLIST MISC MISC MISC
hr-technologies -- easytorecruit	In EasyToRecruit (EZR) before 2.11, the upload feature and the Candidate Profile Management feature are prone to Cross Site Scripting (XSS) injection in multiple locations.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11032</a> MISC MISC
ibm -- mq	IBM MQ 8.0.0.0 through 8.0.0.10, 9.0.0.0 through 9.0.0.5, and 9.1.0.0 through 9.1.1 is vulnerable to a denial of service attack within the TLS key renegotiation function. IBM X-Force ID: 156564.	2019-04-19	not yet calculated	<a href="#">CVE-2019-4055</a> BID XF CONFIRM
ibm -- sterling_b2b_integrator_standard_edition	IBM Sterling B2B Integrator Standard Edition 5.2.0.1, 5.2.6.3, 6, 6.0.0.0, and 6.0.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 147294.	2019-04-25	not yet calculated	<a href="#">CVE-2018-1720</a> XF CONFIRM
imperva -- securesphere	A command injection vulnerability in PWS in Imperva SecureSphere 13.0.0.10 and 13.1.0.10 Gateway allows an attacker with authenticated access to execute arbitrary OS commands on a vulnerable installation.	2019-04-25	not yet calculated	<a href="#">CVE-2018-16660</a> MISC MISC
jakub_chodounskey -- bonobo_git_server	Improper handling of extra parameters in the AccountController (User Profile edit) in Jakub Chodounskey Bonobo Git Server before 6.5.0 allows authenticated users to gain application administrator privileges via additional form parameter submissions.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11218</a> CONFIRM MISC
jakub_chodounskey -- bonobo_git_server	The GitController in Jakub Chodounskey Bonobo Git Server before 6.5.0 allows execution of arbitrary commands in the context of the web server via a crafted http request.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11217</a> CONFIRM MISC
juju_core -- joyent_provider	Juju Core's Joyent provider before version 1.25.5 uploads the user's private ssh key.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1316</a> MISC
kubernetes -- kubernetes	In Kubernetes v1.8.x-v1.14.x, schema info is cached by kubectrl in the location specified by --cache-dir (defaulting to \$HOME/.kube/http-cache), written with world-writable permissions (rw-rw-rw-). If --cache-dir is specified and pointed at a different location accessible to other users/groups, the written files may be modified by other users/groups and disrupt the kubectrl invocation.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11244</a> BID MISC
leagoo -- p1_android_device	The Leagoo P1 Android device with a build fingerprint of sp7731c_1h10_32v4_bird:6.0/MRA58K/android.20170629.214736:user/release-keys contains the android framework (i.e., system_server) with a package name of android that has been modified by Leagoo or another entity in the supply chain. The system_server process in the core Android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage. The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14997</a> MISC MISC MISC
leagoo -- p1_android_device	The Leagoo P1 device with a build fingerprint of sp7731c_1h10_32v4_bird:6.0/MRA58K/android.20170629.214736:user/release-keys contains a pre-installed platform app with a package name of com.wtk.factory (versionCode=1, versionName=1.0) that contains an exported broadcast receiver named com.wtk.factory.MMTestReceiver allows any app co-located on the device to programmatically initiate a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14999</a> MISC MISC MISC
lenovo -- system_x	In various firmware versions of Lenovo System x, the integrated management module II (IMM2)'s first failure data capture (FFDC) includes the web server's private key in the generated log file for support.	2019-04-22	not yet calculated	<a href="#">CVE-2019-6157</a> MISC
librenms -- librenms	LibreNMS 1.46 allows remote attackers to execute arbitrary OS commands by using the \$_POST[community] parameter to html/pages/addhost.inc.php during creation of a new device, and then making a /ajax_output.php?id=capture&format=text&type=snmpwalk&hostname=localhost request that triggers html/includes/output/capture.inc.php command mishandling.	2019-04-24	not yet calculated	<a href="#">CVE-2018-20434</a> MISC MISC MISC
libseccomp-golang -- libseccomp-golang	libseccomp-golang 0.9.0 and earlier incorrectly generates BPFs that OR multiple arguments rather than ANDING them. A process running under a restrictive seccomp filter that specified multiple syscall arguments could bypass intended access restrictions by specifying a single matching argument.	2019-04-24	not yet calculated	<a href="#">CVE-2017-18367</a> MLIST MISC MISC
liferay -- portal_community_edition	An issue was discovered in Liferay Portal CE 7.1.2 GA3. An attacker can use Liferay's Groovy script console to execute OS commands. Commands can be executed via a [command].execute() call, as demonstrated by "def cmd =" in the ServerAdminPortlet_script value to group/control_panel/manage. Valid credentials for an application administrator user account are required.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11444</a> MISC MISC
linux -- linux_kernel	The Linux kernel before 5.1-rc5 allows page-> refcount reference count overflow, with resultant use-after-free issues, if about 140 GiB of RAM exists. This is related to fs/fuse/dev.c, fs/pipe.c, fs/splice.c, include/linux/mm.h, include/linux/pipe_fs_i.h, kernel/trace/trace.c, mm/gup.c, and mm/hugetlb.c. It can occur with FUSE requests.	2019-04-23	not yet calculated	<a href="#">CVE-2019-11487</a> BID MISC MISC MISC MISC MISC MISC MISC MISC MISC MISC
linux -- linux_kernel	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.	2019-04-25	not yet calculated	<a href="#">CVE-2019-3900</a> BID CONFIRM CONFIRM
	A flaw was found in the Linux kernel's vfoo interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfoo driver, such as vfoo-pci, and the		not yet	<a href="#">CVE-2019-3882</a>

linux -- linux_kernel	local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.	2019-04-24	calculated	<a href="#">CONFIRM</a>
linux -- linux_kernel	A race condition in perf_event_open() allows local attackers to leak sensitive data from setuid programs. As no relevant locks (in particular the cred_guard_mutex) are held during the ptrace_may_access() call, it is possible for the specified target task to perform an execve() syscall with setuid execution before perf_event_alloc() actually attaches to it, allowing an attacker to bypass the ptrace_may_access() check and the perf_event_exit_task(current) call that is performed in install_exec_creds() during privileged execve() calls. This issue affects kernel versions before 4.8.	2019-04-22	not yet calculated	<a href="#">CVE-2019-3901</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
lxd -- lxd	LXD before version 0.19-0ubuntu5 doUidshiftIntoContainer() has an unsafe Chmod() call that races against the stat in the Filepath.Walk() function. A symbolic link created in that window could cause any file on the system to have any mode of the attacker's choice.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1340</a> <a href="#">MISC</a>
mercurial -- mercurial	A flaw was found in Mercurial before 4.9. It was possible to use symlinks and subrepositories to defeat Mercurial's path-checking logic and write files outside a repository.	2019-04-22	not yet calculated	<a href="#">CVE-2019-3902</a> <a href="#">CONFIRM</a> <a href="#">LIST</a> <a href="#">MISC</a>
mount.ecryptfs_private -- mount.ecryptfs_private	When mount.ecryptfs_private before version 87-0ubuntu1.2 calls setreuid() it doesn't also set the effective group id. So when it creates the new version, mtab.tmp, it's created with the group id of the user running mount.ecryptfs_private.	2019-04-22	not yet calculated	<a href="#">CVE-2011-3145</a> <a href="#">MISC</a>
mozilla -- firefox	On Android systems, Firefox can load a library from APITRACE_LIB, which is writable by all users and applications. This could allow malicious third party applications to execute a man-in-the-middle attack if a malicious code was written to that location and loaded. *Note: This issue only affects Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9798</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A latent vulnerability exists in the Prio library where data may be read from uninitialized memory for some functions, leading to potential memory corruption. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9805</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	In Firefox Developer Tools it is possible that pasting the result of the 'Copy as cURL' command into a command shell on macOS will cause the execution of unintended additional bash script commands if the URL was maliciously crafted. This is the result of an issue with the native version of Bash on macOS. *Note: This issue only affects macOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9804</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Insufficient bounds checking of data during inter-process communication might allow a compromised content process to be able to read memory from the parent process under certain conditions. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9799</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	The Upgrade-Insecure-Requests (UIR) specification states that if UIR is enabled through Content Security Policy (CSP), navigation to a same-origin URL must be upgraded to HTTPS. Firefox will incorrectly navigate to an HTTP URL rather than perform the security upgrade requested by the CSP in some circumstances, allowing for potential man-in-the-middle attacks on the linked resources. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9803</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A service worker can send the activate event on itself periodically which allows it to run perpetually, allowing it to monitor activity by users. Affects all versions prior to Firefox 60.	2019-04-26	not yet calculated	<a href="#">CVE-2018-5179</a> <a href="#">MISC</a>
mozilla -- firefox	Unsanitized output in the browser UI leaves HTML tags in place and can result in arbitrary code execution in Firefox before version 58.0.1.	2019-04-26	not yet calculated	<a href="#">CVE-2018-5124</a> <a href="#">MISC</a>
mozilla -- firefox	Cross-origin images can be read in violation of the same-origin policy by exporting an image after using createImageBitmap to read the image and then rendering the resulting bitmap image within a canvas element. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9797</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	A vulnerability exists during authorization prompting for FTP transaction where successive modal prompts are displayed and cannot be immediately dismissed. This allows for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9806</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If a Sandbox content process is compromised, it can initiate an FTP download which will then use a child process to render the downloaded data. The downloaded data can then be passed to the Chrome process with an arbitrary file length supplied by an attacker, bypassing sandbox protections and allow for a potential memory read of adjacent data from the privileged Chrome process, which may include sensitive data. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9802</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	Cross-origin images can be read from a canvas element in violation of the same-origin policy using the transferFromImageBitmap method. *Note: This only affects Firefox 65. Previous versions are unaffected.*. This vulnerability affects Firefox < 65.0.1.	2019-04-26	not yet calculated	<a href="#">CVE-2018-18511</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	When arbitrary text is sent over an FTP connection and a page reload is initiated, it is possible to create a modal alert message with this text as the content. This could potentially be used for social engineering attacks. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9807</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If WebRTC permission is requested from documents with data: or blob: URLs, the permission notifications do not properly display the originating domain. The notification states "Unknown origin" as the requestee, leading to user confusion about which site is asking for this permission. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9808</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- firefox	If the source for resources on a page is through an FTP connection, it is possible to trigger a series of modal alert messages for these resources through invalid credentials or locations. These messages cannot be immediately dismissed, allowing for a denial of service (DOS) attack. This vulnerability affects Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9809</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A crash can occur when processing a crafted S/MIME message or an XPI package containing a crafted signature. This can be used as a denial-of-service (DOS) attack because Thunderbird reopens the last seen message on restart, triggering the crash again. This vulnerability affects Thunderbird < 60.5.	2019-04-26	not yet calculated	<a href="#">CVE-2018-18513</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird	A flaw during verification of certain S/MIME signatures causes emails to be shown in Thunderbird as having a valid digital signature, even if the shown message contents aren't covered by the signature. The flaw allows an attacker to reuse a valid S/MIME signature to craft an email message with arbitrary content. This vulnerability affects Thunderbird < 60.5.1.	2019-04-26	not yet calculated	<a href="#">CVE-2018-18509</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	A vulnerability was discovered where specific command line arguments are not properly discarded during Firefox invocation as a shell handler for URLs. This could be used to retrieve and execute files whose location is supplied through these command line arguments if Firefox is configured as the default URI handler for a given URI scheme in third party applications and these applications insufficiently sanitize URL data. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9794</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9810</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	Incorrect handling of __proto__ mutations may lead to type confusion in IonMonkey JIT code and can be leveraged for arbitrary memory read and write. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9813</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	Firefox will accept any registered Program ID as an external protocol handler and offer to launch this local application when given a matching URL on Windows operating systems. This should only happen if the program has specifically registered itself as a "URL Handler" in the Windows registry. *Note: This issue only affects Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9801</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mozilla -- thunderbird_and_firefox_esr_and_firefox	A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. This vulnerability could allow an attacker to create an arbitrary value in compiled JavaScript, for which the range analysis will infer a fully controlled, incorrect range in circumstances where users have explicitly disabled Spectre mitigations. *Note: Spectre mitigations are currently enabled for all users by default settings.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	<a href="#">CVE-2019-9793</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript		not yet	<a href="#">CVE-2019-9792</a> <a href="#">MISC</a>

mozilla -- thunderbird_and_firefox_esr_and_firefox	to achieve memory corruption, which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	calculated	MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR). This allows for possible arbitrary reading and writing of objects during an exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9791 MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A vulnerability where type-confusion in the IonMonkey just-in-time (JIT) compiler could potentially be used by malicious JavaScript to trigger a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9795 MISC MISC MISC
mozilla -- thunderbird_and_firefox_esr_and_firefox	A use-after-free vulnerability can occur when the SMIL animation controller incorrectly registers with the refresh driver twice when only a single registration is expected. When a registration is later freed with the removal of the animation controller element, the refresh driver incorrectly leaves a dangling pointer to the driver's observer array. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.	2019-04-26	not yet calculated	CVE-2019-9796 MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant device with a build fingerprint of Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys, the ZTE ZMAX Pro with a build fingerprint of ZTE/P895T20/urd:6.0.1/MMB29M/20170418.114928:user/release-keys, and the T-Mobile Revvl Plus with a build fingerprint of Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys all contain a vulnerable, pre-installed Rich Communication Services (RCS) app. These devices contain an that app has a package name of com.suntek.mway.rcs.app.service (versionCode=1, versionName=RCS_sdk_M_native_20161008_01; versionCode=1, versionName=RCS_sdk_M_native_20170406_01) with a broadcast receiver app component named com.suntek.mway.rcs.app.test.TestReceiver and a refactored version of the app with a package name of com.rcs.gsma.na.sdk (versionCode=1, versionName=RCS_SDK_20170804_01) with a broadcast receiver app component named com.rcs.gsma.na.test.TestReceiver allow any app co-located on the device to programmatically send text messages where the number and body of the text message is controlled by the attacker due to an exported broadcast receiver app component. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. A separate vulnerability in the app allows a zero-permission app to programmatically delete text messages, so the sent text messages can be removed to not alert the user.	2019-04-25	not yet calculated	CVE-2018-14990 MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant device with a build fingerprint of Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys, the ZTE ZMAX Pro with a build fingerprint of ZTE/P895T20/urd:6.0.1/MMB29M/20170418.114928:user/release-keys, and the T-Mobile Revvl Plus with a build fingerprint of Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys all contain a vulnerable, pre-installed Rich Communication Services (RCS) app. These devices contain an that app has a package name of com.suntek.mway.rcs.app.service (versionCode=1, versionName=RCS_sdk_M_native_20161008_01; versionCode=1, versionName=RCS_sdk_M_native_20170406_01) with an exported content provider named com.suntek.mway.rcs.app.service.provider.message.MessageProvider and a refactored version of the app with a package name of com.rcs.gsma.na.sdk (versionCode=1, versionName=RCS_SDK_20170804_01) with a content provider named com.rcs.gsma.na.provider.message.MessageProvider allow any app co-located on the device to read, write, insert, and modify the user's text messages. This is enabled by an exported content provider app component that serves as a wrapper to the official content provider that contains the user's text messages. This app cannot be disabled by the user and the attack can be performed by a zero-permission app.	2019-04-25	not yet calculated	CVE-2018-14991 MISC MISC MISC
multiple_vendors -- multiple_products	The Coolpad Defiant (Coolpad/cp3632a/cp3632a:7.1.1/NMF26F/099480857:user/release-keys) and the T-Mobile Revvl Plus (Coolpad/alchemy/alchemy:7.1.1/143.14.171129.3701A-TMO/buildf_nj_02-206:user/release-keys) Android devices contain a pre-installed platform app with a package name of com.qualcomm.qti.telephony.extcarrierpack (versionCode=25, versionName=7.1.1) containing an exported broadcast receiver app component named com.qualcomm.qti.telephony.extcarrierpack.UiccReceiver that allows any app co-located on the device to programmatically perform a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	CVE-2018-15003 MISC MISC MISC
nopcommerce -- nopcommerce	Libraries/Nop.Services/Localization/LocalizationService.cs in nopCommerce through 4.10 allows XXE via the "Configurations -> Languages -> Edit Language -> Import Resources -> Upload XML file" screen.	2019-04-25	not yet calculated	CVE-2019-11519 MISC MISC
omniauth_ruby_gem -- omniauth_ruby_gem	The request phase of the OmniAuth Ruby gem is vulnerable to Cross-Site Request Forgery when used as part of the Ruby on Rails framework, allowing accounts to be connected without user intent, user interaction, or feedback to the user. This permits a secondary account to be able to sign into the web application as the primary account.	2019-04-26	not yet calculated	CVE-2015-9284 MISC MISC MLIST
openapi_tools -- openapi_generator	OpenAPI Tools OpenAPI Generator before 4.0.0-20190419.052012-560 uses http:// URLs in various build.gradle, build.gradle.mustache, and build.sbt files, which may have caused insecurely resolved dependencies.	2019-04-22	not yet calculated	CVE-2019-11405 MISC MISC MISC
oppo -- f5_android_device	The Oppo F5 Android device with a build fingerprint of OPPO/CPH1723/CPH1723:7.1.1/N6F26Q/1513597833:user/release-keys contains a pre-installed platform app with a package name of com.dropboxchmmod (versionCode=1, versionName=1.0) that contains an exported service named com.dropboxchmmod.DropboxChmmodService that allows any app co-located on the device to supply arbitrary commands to be executed as the system user. This app cannot be disabled by the user and the attack can be performed by a zero-permission app. Executing commands as system user can allow a third-party app to video record the user's screen, factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), and obtains the user's text messages, and more. This vulnerability can also be used to secretly record audio of the user without their awareness on the Oppo F5 device. The pre-installed com.oppo.engineermode app (versionCode=25, versionName=V1.01) has an exported activity that can be started to initiate a recording and quickly dismissed. The activity can be started in a way that the user will not be able to see the app in the recent apps list. The resulting audio amr file can be copied from a location on internal storage using the arbitrary command execution as system user vulnerability. Executing commands as system user can allow a third-party app to factory reset the device, obtain the user's notifications, read the logcat logs, inject events in the Graphical User Interface (GUI), change the default Input Method Editor (IME) (e.g., keyboard) with one contained within the attacking app that contains keylogging functionality, obtain the user's text messages, and more.	2019-04-25	not yet calculated	CVE-2018-14996 MISC MISC MISC
oracle -- berkeley_db	Vulnerability in the Data Store component of Oracle Berkeley DB. Supported versions that are affected are Prior to 6.138, prior to 6.2.38 and prior to 18.1.32. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Data Store executes to compromise Data Store. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Data Store. CVSS 3.0 Base Score 3.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).	2019-04-23	not yet calculated	CVE-2019-2708 MISC
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2019-04-26	not yet calculated	CVE-2019-2725 MISC
phablet-team -- content_hub	Content Hub before version 0.04-15.04.20150331-Oubuntu1.0 DBUS API only requires a file path for a content item, it doesn't actually require the confined app have access to the file to create a transfer. This could allow a malicious application using the DBUS API to export	2019-04-22	not yet calculated	CVE-2015-1327 MISC



	file:///etc/passwd which would then send a copy of that file to another app.			
phablet-team -- ubuntu-download-manager	UDM provides support for running commands after a download is completed, this is currently made use of for click package installation. This functionality was not restricted to unconfined applications. Before UDM version 1.2+16.04.20160408-0ubuntu1 any confined application could make use of the UDM C++ API to run arbitrary commands in an unconfined environment as the phablet user.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1579</a> MISC
pivotal -- apps_manager_release	Pivotal Apps Manager Release, versions 665.0.x prior to 665.0.28, versions 666.0.x prior to 666.0.21, versions 667.0.x prior to 667.0.7, contain an invitation service that accepts HTTP. A remote unauthenticated user could listen to network traffic and gain access to the authorization credentials used to make the invitation requests.	2019-04-24	not yet calculated	<a href="#">CVE-2019-3793</a> CONFIRM
plum -- compass_android_device	The Plum Compass Android device with a build fingerprint of PLUM/c179_hwf_221/c179_hwf_221:6.0/MRA58K/W16.51.5-22:user/release-keys contains a pre-installed platform app with a package name of com.android.settings (versionCode=23, versionName=6.0-eng.root.20161223.224055) that contains an exported broadcast receiver app component which allows any app co-located on the device to programmatically perform a factory reset. In addition, the app initiating the factory reset does not require any permissions. A factory reset will remove all user data and apps from the device. This will result in the loss of any data that have not been backed up or synced externally. The capability to perform a factory reset is not directly available to third-party apps (those that the user installs themselves with the exception of enabled Mobile Device Management (MDM) apps), although this capability can be obtained by leveraging an unprotected app component of a pre-installed platform app.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14989</a> MISC MISC MISC
polycom -- vxv_products_using_ucs_software	VVX products using UCS software version 5.8.0 and earlier with Better Together over Ethernet Connector (BTtoE) application version 3.8.0 and earlier uses hard-coded credentials to establish a connection between the host application and device.	2019-04-23	not yet calculated	<a href="#">CVE-2019-10688</a> CONFIRM
printeron -- printeron	An XML external entity (XXE) vulnerability in PrinterOn version 4.1.4 and lower allows remote authenticated users to read arbitrary files or conduct server-side request forgery (SSRF) attacks via a crafted DTD in an XML request.	2019-04-23	not yet calculated	<a href="#">CVE-2018-17169</a> MISC
projectsend -- projectsend	ProjectSend before r1070 writes user passwords to the server logs.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11492</a> CONFIRM
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4 and 8.3RX before 8.3R7.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2 and 5.4RX before 5.4R7.1, an unauthenticated, remote attacker can conduct a session hijacking attack.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11540</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.2RX before 8.2R12.1, users using SAML authentication with the Reuse Existing NC (Pulse) Session option may see authentication leaks.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11541</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, an authenticated attacker (via the admin web interface) can send a specially crafted message resulting in a stack buffer overflow.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11542</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure version 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, 5.3RX before 5.3R12.1, 5.2RX before 5.2R12.1, and 5.1RX before 5.1R15.1, the admin web interface allows an authenticated attacker to inject and execute commands.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11539</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	In Pulse Secure Pulse Connect Secure version 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, 8.2RX before 8.2R12.1, and 8.1RX before 8.1R15.1, an NFS problem could allow an authenticated attacker to access the contents of arbitrary files on the affected device.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11538</a> BID CONFIRM MISC
pulse_secure -- pulse_connect_secure	XSS exists in the admin web console in Pulse Secure Pulse Connect Secure (PCS) 9.0RX before 9.0R3.4, 8.3RX before 8.3R7.1, and 8.1RX before 8.1R15.1 and Pulse Policy Secure 9.0RX before 9.0R3.2, 5.4RX before 5.4R7.1, and 5.2RX before 5.2R12.1.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11543</a> BID CONFIRM MISC
python-dbusmock -- python-dbusmock	python-dbusmock before version 0.15.1 AddTemplate() D-Bus method call or DBusTestCase.spawn_server_template() method could be tricked into executing malicious code if an attacker supplies a .pyc file.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1326</a> MISC
robotronic -- runasspc	Robotronic RunAsSpc 3.7.0.0 protects stored credentials insufficiently, which allows locally authenticated attackers (under the same user context) to obtain cleartext credentials of the stored account.	2019-04-24	not yet calculated	<a href="#">CVE-2019-10239</a> MISC
rockwell_automation -- micrologix_and_compactlogix_controllers	In Rockwell Automation MicroLogix 1400 Controllers Series A, All Versions Series B, v15.002 and earlier, MicroLogix 1100 Controllers v14.00 and earlier, CompactLogix 5370 L1 controllers v30.014 and earlier, CompactLogix 5370 L2 controllers v30.014 and earlier, CompactLogix 5370 L3 controllers (includes CompactLogix GuardLogix controllers) v30.014 and earlier, an open redirect vulnerability could allow a remote unauthenticated attacker to input a malicious link to redirect users to a malicious site that could run or download arbitrary malware on the user's machine.	2019-04-25	not yet calculated	<a href="#">CVE-2019-10955</a> MISC BID
shenzhen_yunni_technology -- lnkp2p	An authentication flaw in Shenzhen Yunni Technology iLnkP2P allows remote attackers to actively intercept user-to-device traffic in cleartext, including video streams and device credentials.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11220</a> MISC
shenzhen_yunni_technology -- lnkp2p	The algorithm used to generate device IDs (UIDs) for devices that utilize Shenzhen Yunni Technology iLnkP2P suffers from a predictability flaw that allows remote attackers to establish direct connections to arbitrary devices.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11219</a> MISC
simplybook.me -- simplybook.me_enterprise	Incorrect Access Control in the Administrative Management Interface in SimplyBook.me Enterprise before 2019-04-23 allows Authenticated Low-Priv Users to Elevate Privileges to Full Admin Rights via a crafted HTTP PUT Request, as demonstrated by modified JSON data to a /v2/rest/ URL.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11489</a> MISC MISC
simplybook.me -- simplybook.me_enterprise	Incorrect Access Control in the Account Access / Password Reset Link in SimplyBook.me Enterprise before 2019-04-23 allows Unauthorized Attackers to READ/WRITE Customer or Administrator data via a persistent HTTP GET Request Hash Link Replay, as demonstrated by a login-link from the browser history.	2019-04-25	not yet calculated	<a href="#">CVE-2019-11488</a> MISC MISC
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6995 has stored XSS. JavaScript code could be executed on the application by opening a malicious email or when viewing a malicious file attachment.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7211</a> MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 allows deserialization of untrusted data. An unauthenticated attacker could run commands on the server when port 17001 was remotely accessible. This port is not accessible remotely by default after applying the Build 6985 patch.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7214</a> MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 allows directory traversal. An authenticated user could delete arbitrary files or could create files in new folders in arbitrary locations on the mail server. This could lead to command execution on the server for instance by putting files inside the web directories.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7213</a> MISC CONFIRM
smartertools -- smartermail	SmarterTools SmarterMail 16.x before build 6985 has hardcoded secret keys. An unauthenticated attacker could access other users' emails and file attachments. It was also possible to interact with mailing lists.	2019-04-24	not yet calculated	<a href="#">CVE-2019-7212</a> MISC CONFIRM
snapcore -- snapweb	The Snapweb interface before version 0.21.2 was exposing controls to install or remove snap packages without controlling the identity of the user, nor the origin of the connection. An attacker could have used the controls to remotely add a valid, but malicious, snap package, from the Store, potentially using system resources without permission from the legitimate administrator of the system.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1587</a> MISC
sonicwall -- global_management_system	A vulnerability in SonicWall Global Management System (GMS), allow a remote user to gain access to the appliance using existing SSH key. This vulnerability affects GMS versions 9.1, 9.0, 8.7, 8.6, 8.4, 8.3 and earlier.	2019-04-26	not yet calculated	<a href="#">CVE-2019-7476</a> CONFIRM
sony -- photo_sharing_plus_application	An incorrect access control exists in the Sony Photo Sharing Plus application in the firmware before PKG6.5629 version (for the X7500D TV and other applicable TVs). This vulnerability allows an attacker to read arbitrary files without authentication over HTTP when Photo Sharing Plus application is running. This may allow an attacker to browse a particular directory (e.g. images) inside the private network.	2019-04-19	not yet calculated	<a href="#">CVE-2019-10886</a> MISC FULL DISC BID BUGTRAO



				<a href="#">CONFIRM</a>
sony -- xperia_l1_android_device	The Sony Xperia L1 Android device with a build fingerprint of Sony/G3313/G3313:7.0/43.0.A.6.49/2867558199:user/release-keys contains the android framework (i.e., system_server) with a package name of android (versionCode=24, versionName=7.0) that has been modified by Sony or another entity in the supply chain. The system_server process in the core android package has an exported broadcast receiver that allows any app co-located on the device to programmatically initiate the taking of a screenshot and have the resulting screenshot be written to external storage. The taking of a screenshot is not transparent to the user; the device has a screen animation as the screenshot is taken and there is a notification indicating that a screenshot occurred. If the attacking app also requests the EXPAND_STATUS_BAR permission, it can wake the device up using certain techniques and expand the status bar to take a screenshot of the user's notifications even if the device has an active screen lock. The notifications may contain sensitive data such as text messages used in two-factor authentication. The system_server process that provides this capability cannot be disabled, as it is part of the Android framework. The notification can be removed by a local Denial of Service (DoS) attack to reboot the device.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14983</a> <a href="#">MISC</a> <a href="#">MISC</a>
symantec -- endpoint_protection_manager	Symantec Endpoint Protection Manager (SEPM) prior to and including 12.1 RU6 MP9 and prior to 14.2 RU1 may be susceptible to a DLL Preloading vulnerability, which is a type of issue that can occur when an application looks to call a DLL for execution and an attacker provides a malicious DLL to use instead.	2019-04-25	not yet calculated	<a href="#">CVE-2018-18367</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
symantec -- endpoint_protection_manager	SEP (Mac client) prior to and including 12.1 RU6 MP9 and prior to 14.2 RU1 may be susceptible to a CSV/DDE injection (also known as formula injection) vulnerability, which is a type of issue whereby an application or website allows untrusted input into CSV files.	2019-04-25	not yet calculated	<a href="#">CVE-2018-12244</a> <a href="#">MISC</a> <a href="#">BID</a>
symantec -- norton_security	Symantec Norton Security prior to 22.16.3, SEP (Windows client) prior to and including 12.1 RU6 MP9, and prior to 14.2 RU1, SEP SBE prior to Cloud Agent 3.00.31.2817, NIS-22.15.2.22, SEP-12.1.7484.7002 and SEP Cloud prior to 22.16.3 may be susceptible to a kernel memory disclosure, which is a type of issue where a specially crafted IRP request can cause the driver to return uninitialized memory.	2019-04-25	not yet calculated	<a href="#">CVE-2018-18366</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
symantec -- norton_security	Norton Security (Windows client) prior to 22.16.3 and SEP SBE (Windows client) prior to Cloud Agent 3.00.31.2817, NIS-22.15.2.22 & SEP-12.1.7484.7002, may be susceptible to a DLL Preloading vulnerability, which is a type of issue that can occur when an application looks to call a DLL for execution and an attacker provides a malicious DLL to use instead.	2019-04-25	not yet calculated	<a href="#">CVE-2018-18369</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
systemd -- systemd	It was discovered that a systemd service that uses DynamicUser property can get new privileges through the execution of SUID binaries, which would allow to create binaries owned by the service transient group with the setgid bit set. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the GID will be recycled.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3844</a> <a href="#">CONFIRM</a>
systemd -- systemd	It was discovered that a systemd service that uses DynamicUser property can create a SUID/SGID binary that would be allowed to run as the transient service UID/GID even after the service is terminated. A local attacker may use this flaw to access resources that will be owned by a potentially different service in the future, when the UID/GID will be recycled.	2019-04-26	not yet calculated	<a href="#">CVE-2019-3843</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a>
teamspeak_systems -- teamspeak_3_client	TeamSpeak 3 Client before 3.2.5 allows remote code execution in the Qt framework.	2019-04-19	not yet calculated	<a href="#">CVE-2019-11351</a> <a href="#">MISC</a> <a href="#">MISC</a>
tenda -- ac7_and_ac9_and_ac10_devices	An issue was discovered on Tenda AC7 devices with firmware through V15.03.06.44_CN(AC7), AC9 devices with firmware through V15.03.05.19(6318)_CN(AC9), and AC10 devices with firmware through V15.03.06.23_CN(AC10). A buffer overflow vulnerability exists in the router's web server (httpd). When processing the page parameters for a post request, the value is directly written with sprintf to a local variable placed on the stack, which overrides the return address of the function, causing a buffer overflow.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14557</a> <a href="#">MISC</a>
tenda -- ac7_and_ac9_and_ac10_devices	An issue was discovered on Tenda AC7 devices with firmware through V15.03.06.44_CN(AC7), AC9 devices with firmware through V15.03.05.19(6318)_CN(AC9), and AC10 devices with firmware through V15.03.06.23_CN(AC10). A buffer overflow vulnerability exists in the router's web server (httpd). When processing the list parameters for a post request, the value is directly written with sprintf to a local variable placed on the stack, which overrides the return address of the function, causing a buffer overflow.	2019-04-25	not yet calculated	<a href="#">CVE-2018-14559</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrative server component of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains a vulnerability wherein a user without privileges to upload distributed application archives ("Upload DAA" permission) can theoretically upload arbitrary code, and in some circumstances then execute that code on ActiveMatrix Service Grid nodes. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric: versions up to and including 3.3.0, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8992</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The workspace client, openspace client, and app development client of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contain a vulnerability wherein a malicious URL could trick a user into visiting a website of the attacker's choice. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8995</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The workspace client of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contains vulnerabilities where an authenticated user can change settings that can theoretically adversely impact other users. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8994</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrative web server component of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains a vulnerability that could theoretically allow an unauthenticated user to download a file with credentials information. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO ActiveMatrix Service Grid Distribution for TIBCO Silver Fabric: versions up to and including 3.3.0, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8993</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	The administrator web interface of TIBCO Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, TIBCO ActiveMatrix Policy Director, TIBCO ActiveMatrix Service Bus, TIBCO ActiveMatrix Service Grid, TIBCO Silver Fabric Enabler for ActiveMatrix BPM, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid contains multiple vulnerabilities that may allow for cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, TIBCO ActiveMatrix Policy Director: versions up to and including 1.1.0, TIBCO ActiveMatrix Service Bus: versions up to and including 3.3.0, TIBCO ActiveMatrix Service Grid: versions up to and including 3.3.1, TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1, and TIBCO Silver Fabric Enabler for ActiveMatrix Service Grid: versions up to and including 1.3.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-8991</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
	The workspace client, openspace client, app development client, and REST API of TIBCO			

tibco_software -- activematrix_bpm_and_silver_fabric_enabler_for_activematrix_bpm	Software Inc.'s TIBCO ActiveMatrix BPM, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM contain cross site scripting (XSS) and cross-site request forgery vulnerabilities. Affected releases are TIBCO Software Inc.'s TIBCO ActiveMatrix BPM: versions up to and including 4.2.0, TIBCO ActiveMatrix BPM Distribution for TIBCO Silver Fabric: versions up to and including 4.2.0, and TIBCO Silver Fabric Enabler for ActiveMatrix BPM: versions up to and including 1.4.1.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11203</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
tildeslash -- m/monit	An issue was discovered in /admin/users/update in M/Monit before 3.7.3. It allows unprivileged users to escalate their privileges to an administrator by requesting a password change and specifying the admin parameter.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11393</a> <a href="#">MISC</a> <a href="#">MISC</a>
tildeslash -- monit	A buffer over-read in Util_urlDecode in util.c in Tildeslash Monit before 5.25.3 allows a remote authenticated attacker to retrieve the contents of adjacent memory via manipulation of GET or POST parameters. The attacker can also cause a denial of service (application outage).	2019-04-22	not yet calculated	<a href="#">CVE-2019-11455</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
tildeslash -- monit	Persistent cross-site scripting (XSS) in http/cervlet.c in Tildeslash Monit before 5.25.3 allows a remote unauthenticated attacker to introduce arbitrary JavaScript via manipulation of an unsanitized user field of the Authorization header for HTTP Basic Authentication, which is mishandled during an _viewlog operation.	2019-04-22	not yet calculated	<a href="#">CVE-2019-11454</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MLIST</a>
unity-scope-gdrive_logs -- unity-scope-gdrive_logs	All versions of unity-scope-gdrive logs search terms to syslog.	2019-04-22	not yet calculated	<a href="#">CVE-2015-1343</a> <a href="#">MISC</a>
unity8-team -- unity8	Versions of Unity8 before 8.11+16.04.20160122-0ubuntu1 file plugins/Dash/CardCreator.js will execute any code found in place of a fallback image supplied by a scope.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1573</a> <a href="#">MISC</a>
unity8-team -- unity8	In all versions of Unity8 a running but not active application on a large-screen device could talk with Maliit and consume keyboard input.	2019-04-22	not yet calculated	<a href="#">CVE-2016-1584</a> <a href="#">MISC</a>
vivo -- v7_android_device	The Vivo V7 Android device with a build fingerprint of vivo/1718/1718:7.1.2/N2G47H/compile11021857:user/release-keys contains a platform app with a package name of com.vivo.smartshot (versionCode=1, versionName=3.0.0). This app contains an exported service named com.vivo.smartshot.ui.service.ScreenRecordService that will record the screen for 60 minutes and write the mp4 file to a location of the user's choosing. Normally, a recording notification will be visible to the user, but we discovered an approach to make it mostly transparent to the user by quickly removing a notification and floating icon. The user can see a floating icon and notification appear and disappear quickly due to quickly stopping and restarting the service with different parameters that do not interfere with the ongoing screen recording. The screen recording lasts for 60 minutes and can be written directly to the attacking app's private directory.	2019-04-25	not yet calculated	<a href="#">CVE-2018-15000</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
western_digital_technologies -- my_cloud_firmware_versions	Western Digital My Cloud, My Cloud Mirror Gen2, My Cloud EX2 Ultra, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100, My Cloud DL4100, My Cloud PR2100 and My Cloud PR4100 firmware before 2.31.174 is affected by an authentication bypass vulnerability. The login_mgr.cgi file checks credentials against /etc/shadow. However, the "nobody" account (which can be used to access the control panel API as a low-privilege logged-in user) has a default empty password, allowing an attacker to modify the My Cloud EX2 Ultra web page source code and obtain access to the My Cloud as a non-Admin My Cloud device user.	2019-04-24	not yet calculated	<a href="#">CVE-2019-9950</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
western_digital_technologies -- my_cloud_firmware_versions	Western Digital My Cloud, My Cloud Mirror Gen2, My Cloud EX2 Ultra, My Cloud EX2100, My Cloud EX4100, My Cloud DL2100, My Cloud DL4100, My Cloud PR2100 and My Cloud PR4100 firmware before 2.31.174 is affected by an unauthenticated file upload vulnerability. The page web/query/uploader/uploadify.php can be accessed without any credentials, and allows uploading arbitrary files to any location on the attached storage.	2019-04-24	not yet calculated	<a href="#">CVE-2019-9951</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	Server Side Request Forgery (SSRF) exists in the Print My Blog plugin before 1.6.7 for WordPress via the site parameter.	2019-04-27	not yet calculated	<a href="#">CVE-2019-11565</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WebDorado Contact Form Builder plugin before 1.0.69 for WordPress allows CSRF via the wp-admin/admin-ajax.php action parameter, with resultant local file inclusion via directory traversal, because there can be a discrepancy between the \$_POST['action'] value and the \$_GET['action'] value, and the latter is unsanitized.	2019-04-26	not yet calculated	<a href="#">CVE-2019-11557</a> <a href="#">MISC</a> <a href="#">MISC</a>
xiaomi -- mi_5s_devices	The gyroscope on Xiaomi Mi 5s devices allows attackers to cause a denial of service (resonance and false data) via a 20.4 kHz audio signal, aka a MEMS ultrasound attack.	2019-04-25	not yet calculated	<a href="#">CVE-2018-20823</a> <a href="#">MISC</a> <a href="#">MISC</a>
zoho_manageengine -- adselfservice_plus	Zoho ManageEngine ADSelfService Plus before build 5708 has XSS via the mobile app API.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11511</a> <a href="#">MISC</a>
zotonic -- zotonic	Zotonic before version 0.47 has mod_admin XSS.	2019-04-24	not yet calculated	<a href="#">CVE-2019-11504</a> <a href="#">MISC</a>
zyxel_communications -- multiple_devices	On Zyxel ATP200, ATP500, ATP800, USG20-VPN, USG20W-VPN, USG40, USG40W, USG60, USG60W, USG110, USG210, USG310, USG1100, USG1900, USG2200-VPN, ZyWALL 110, ZyWALL 310, ZyWALL 1100 devices, the security firewall login page is vulnerable to Reflected XSS via the unsanitized 'mp_idx' parameter.	2019-04-22	not yet calculated	<a href="#">CVE-2019-9955</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a non-official on-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nrcis.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [wguitarle@cl.sunnyvale.ca.us](mailto:wguitarle@cl.sunnyvale.ca.us) using GovDelivery Community Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 25 Murray Lane SW Bldg 10 · Washington, DC 20598 · (888) 282-0870



**From:** [Association of Deputy District Attorneys](#)  
**To:** [ggiquiere@ci.sunnyvale.ca.us](mailto:ggiquiere@ci.sunnyvale.ca.us)  
**Subject:** Monday Morning Memo for April 15, 2019  
**Date:** Monday, April 15, 2019 5:02:35 AM

---

Having trouble viewing this email? [Click here](#)



## Courts & Rulings

### **Work product privilege yields to right to unbiased jury**

A criminal defendant's constitutional right to an unbiased jury trumps the prosecution's work product privilege, the Fourth District Court of

Appeal held yesterday, denying a writ petition by the San Diego Office of District Attorney contesting an order to turn over to a convicted murderer's habeas counsel the prosecution's jury selection notes.

[Metropolitan News-Enterprise](#)

### **Supreme Court won't review case of man convicted in brutal 1993 rape-murder**

The California Supreme Court refused Wednesday to review the case of a man convicted of the November 1993 rape-murder of a woman whose nude and battered body was discovered near the Harbor 110 Freeway in an unincorporated area near Torrance. Christopher Goree - who was 17 at the time of Dr. Josephine Tan's killing - was convicted in April 2011 of first-degree murder.

[City News Service](#)

### **30-year-plus incarceration for robbery was cruel, unusual**

The First District Court of Appeal held Friday that a man who pled guilty in 1988 to kidnapping for robbery and was sentenced to an indeterminate term of life with the possibility of parole should have been paroled sooner than he was and is entitled to habeas corpus relief. Post-release relief comes in the case of William Palmer who, after 10 parole suitability hearings over a 19-year period, had been found unfit for release, but was recently freed following an eleventh hearing.

[Metropolitan News-Enterprise](#)

### **As more people go without a lawyer, courts offer self-help services. Advice from the judge? No way**

The divorced couple appearing before Judge Helen E. Zukin was fighting over visitation. The man said he had kicked his heroin addiction and wanted to spend time with his children, whom he hadn't seen in three years. His ex was against it, saying she did not trust that he was clean, and that he had let his children down before. Neither party had an attorney, and it showed.

[Los Angeles Times](#)

### **Judge erred in ordering litigants to supply hair follicle evidence**

The First District Court of Appeal has declared that nothing has changed since 2005 when the Fourth District held that there's no legal authority for a court to order parties to a custody dispute to submit to hair follicle drug testing. Testing of hair follicles can reveal drug use during the preceding 90 days while conventional urine tests can only reflect such use in the past three days.

[Metropolitan News-Enterprise](#)

### **Judge declines to cancel Los Angeles gun permits**

A judge in Los Angeles has declined a request from LAPD Chief Michel Moore to cancel a decades-old agreement that granted concealed weapons permits to a handful of citizens. The decision means those citizens will continue to be issued permits to carry guns, at least

temporarily. The judge's ruling has not been finalized, but the city and the plaintiffs' attorneys confirmed the decision.

[NBC4](#)

### **Draft opinion cautions against use of CMS for judges' investigations**

The California Supreme Court Committee on Judicial Ethics Committee yesterday said it is seeking public input on its tentative formal opinion which declares that a judge should generally avoid searching the court case management system for information about a party or an attorney or facts relating to a case before the judicial officer.

[Metropolitan News-Enterprise](#)

### **Judge stays his own order to allow high-capacity gun magazines**

California residents who have acquired high-capacity gun magazines in the week since a federal judge found the state's voter-approved ban on the firearms unconstitutional will be allowed to keep their weapons, but will not be able to import more into the state starting Friday at 5 p.m., a federal judge ruled Thursday in staying his order.

[Courthouse News Service](#)

### **Noncustodial parent reasonably ordered to prove decreasing use of marijuana**

The Court of Appeal on Friday upheld an order that a noncustodial father submit to six drug tests to establish a decreasing dependency on marijuana. The admitted use by the father of marijuana to treat his headaches and relieve stress was not a basis for the order by Los Angeles Superior Court Judge Pete Navarro awarding custody of A.K. to the mother.

[Metropolitan News-Enterprise](#)

### **San Francisco can reject 5G equipment it views as too ugly**

San Francisco can reject 5G wireless equipment that it views as detracting from the city's beauty, a setback for wireless carriers which may now have to remap new networks or disguise antennas as palm fronds or building cornices. California's highest court disagreed Thursday with T-Mobile US Inc and other companies which argued San Francisco overreached in asserting its authority to regulate wireless telephone equipment on aesthetic grounds.

[The Star](#)

### **No reversal based on judge's misstatement of law**

A judge's statement reflecting an erroneous view of the applicable legal standard does not necessitate reversal where the order is supportable under the correct standard, the Court of Appeal for this district held yesterday in an opinion affirming the issuance of a civil harassment restraining order. Presiding Justice Arthur Gilbert of Div. Six wrote the opinion, which was not certified for publication.

[Metropolitan News-Enterprise](#)



### **Circuit holds no reasonable expectation of privacy in rental car for unauthorized and unlicensed driver**

In *United States v. Lyle*, 15-058-cr (April 1, 2019) (Raggi, Chin, Lohier), the Second Circuit, following a remand from the United States Supreme Court, once again held that the search of a rental car that James Lyle was driving (1) without a valid driver's license, (2) without the permission of the rental car company, but (3) with the permission of the authorized driver, was lawful.

[JD Supra](#)

### **Search of youth's electronic devices properly ordered**

The Court of Appeal for this district, in a 2-1 opinion, yesterday validated a condition of probation that a youthful offender, who got into a fist fight on the schoolyard and directed a racial epithet at a teacher who attempted to intercede, be subject to a search of his electronic devices.

[Metropolitan News-Enterprise](#)

### **High-salaried lawyers should pay more in dues than others: Lawmaker**

A key state lawmaker says his colleagues should use their authority over the annual bar dues bill to "restructure" the fee schedule so high-salaried attorneys pay more than their lower-earning counterparts in the profession. Assemblyman Mark Stone, D-Scotts Valley, told members of the Judiciary Committee, which he chairs, that bar leaders' pending request to the Legislature for a \$100 annual fee hike - plus \$330 in one-time assessments in 2020 - is "our opportunity to take some of the regressive nature of that fee structure out."

[Law.com](#)

### **Court won't extend deadline for inmate to file appeal**

A California appellate court ruled that principles of equity can allow more time for an inmate to appeal the denial of his request to belatedly file a personal injury action, but the circumstances did not warrant an extension. Case: *De Leon v. Flores*, No. F077038, 04/04/2019, unpublished. Facts: Rene De Leon was an inmate of the California Department of Corrections and Rehabilitation.

[Work Comp Central](#)

### **Retired judges grumble at assignment program reforms, as audit raises questions**

California's assigned judges program, a constitutionally provided system that uses retired jurists to cover judicial absences, is under mounting scrutiny amid allegations of cost overruns, questionable practices and new rules that some judges say amount to age discrimination.

[The Recorder](#)

### **No additional fees to lawyers who garnered \$10 million in 2016**

The Ninth U.S. Circuit Court of Appeals yesterday upheld the denial of supplemental attorney fees in a case in which the City of Los Angeles agreed in 2016 to pay \$1.4 billion over a 30 year period to render its sidewalks fully accessible to persons with mobility disabilities.

[Metropolitan News-Enterprise](#)

## **Prosecutions/Prosecutors**

### **Man faces murder charges in crash that killed CHP veteran**

A man faces murder charges after he hit a California Highway Patrol officer on Interstate 15 in Lake Elsinore this weekend, the agency announced Sunday. Sgt. Steve Licon, 53, died at the Inland Valley Medical Center following the 4:30 p.m. crash on the southbound side of I-15 just north of Nichols Road, CHP spokesman Ramon Duran said.

[KTLA](#)

### **Lawyers for Newport doctor accused of sexual assaults seek communications related to ex-DA's claim of 'a thousand' potential victims**

Lawyers for a Newport Beach doctor and his girlfriend who are accused of numerous cases of sexual assault appeared in a Newport Beach courtroom Friday to try to obtain verbal and written communications within the Orange County district attorney's office that could form the basis for an argument that the prosecution's actions deprived their clients of the opportunity for a fair trial by misrepresenting them to the media.

[Los Angeles Times](#)

### **Owners of crime-ridden Valley motel may be forced to live in it**

The managers of a troublesome San Fernando Valley motel may soon get a taste of their own medicine. The Los Angeles City Attorney's Office wants to force three managers at the Studio 6 motel on Sherman Way to live in the motel until it tackles its alleged problems with drugs, prostitution and gang activity.

[North Hollywood-Toluca Lake](#)

### **L.A. man faces charges after crashing into police cars, vehicle with baby on board during chase: DA**

A Los Angeles man was charged Monday with felony counts of assaulting a police officer and other charges after allegedly crashing into multiple vehicles during a pursuit last week, including one carrying a baby, prosecutors said. Pharuehat Wilaisophakun, 27, led officers on a chase April 4 after an officer witnessed him get into a crash in a 2018 Prius and he refused to stop in Hollywood, according to the Los Angeles County District Attorney's Office.

[KTLA](#)

### **Social justice prosecutors**

For years, many have bemoaned the slide of America's higher education

system down the slippery slope of moral relativism and the embracing of virtually all facets of progressive dogma while rejecting most elements of conservatism. The mere invitation of a conservative commentator to speak on college campuses is now reason enough for rioting and mass student protests.

[American Thinker](#)

### **OCDA speaks for victims, families at victims' rights march**

Family members of murder victims rallied at the Victims' Rights March in Orange County, to stand shoulder to shoulder in a show of solidarity after California's governor has declared an end to the death penalty during his term of office. This year, in advance of the accused Golden State Killer Joseph DeAngelo's pretrial hearing, Orange County District Attorney Todd Spitzer made his stance clear.

[Laguna Niguel-Dana Point](#)

### **Deputy D.A. becomes latest to challenge Jackie Lacey**

A Los Angeles County deputy district attorney announced plans Wednesday to challenge Jackie Lacey in the 2020 election, making him the second insurgent candidate promising to bring a more progressive bent to the county's top law enforcement post. Joseph Iniguez, a 33-year-old prosecutor currently trying cases in the Alhambra courthouse, said that although he respects Lacey, he believes she has prevented the district attorney's office from leading the country in the kinds of criminal justice reforms that have sprouted under other progressive prosecutors in Philadelphia and San Francisco.

[Los Angeles Times](#)

### **"Golden State Killer" case death penalty decision renews debate in California**

California prosecutors announced Wednesday they will seek the death penalty if they convict the man suspected of being the notorious "Golden State Killer," renewing debate over Gov. Gavin Newsom's moratorium on executing any of the 737 inmates on the nation's largest death row. Newsom's reprieve lasts only so long as he is governor, and it does not prevent prosecutors from seeking the death penalty nor judges and juries from imposing death sentences.

[CBS/AP](#)

### **California prosecutors accuse Avenatti of bilking clients, including a paraplegic man**

A federal grand jury in California on Thursday indicted Michael Avenatti on 36 counts of fraud, perjury and other financial crimes, the latest barrage of charges against the attorney who rocketed into the national spotlight while representing adult film actress Stormy Daniels in her case against President Donald Trump.

[Politico](#)

---

### **A new method of DNA testing could solve more shootings**

Police found 19 spent shell casings scattered in the San Diego street where Gregory Benton was murdered on April 12, 2014. Benton and his cousin had gone to buy cigarettes, a witness later said. As they returned to a family party, two men pulled up in a car behind them. They got out, and at least one of them opened fire.

[PoliceOne](#)

### **LAPD Chief hails new County Office of Violence Prevention**

Los Angeles County's recently established Office of Violence Prevention drew praise today from Los Angeles Police Department Chief Michel Moore. "I'm encouraged for the first time that the County of Los Angeles is establishing a means to identify resources that exist, gaps that need to be filled and coordinate the delivery of all those services to a county of more than 10 million people," Moore said at a news conference at the Martin Luther King Jr. Center for Public Health in the unincorporated Willowbrook area.

[City News Service](#)

### **Q & A with Public Safety Chief**

Recently, there have been a string of thefts on campus of students' personal items. This week, Isabella Murillo, news editor, sat down with Danny Martinez, chief of Department of Public Safety (DPS) to discuss this. What is the department doing about the increase in thefts of student property on campus? DPS thoroughly investigates every theft brought to our attention.

[Los Angeles Loyolan](#)

### **Citizen App texts you in real time if a crime or fire is happening nearby**

Chances are you've seen a helicopter circling above your neighborhood, an accident or road shut down due to police activity. Now, thanks to a new app called Citizen, you can finally understand exactly what's going on. The company behind the app is doing something really interesting: they're going around to major cities and installing antennas to allow them to listen to police and fire scanners.

[KTLA](#)

### **Secret Service under fire after agent testifies agency inserted malicious thumb drive into computer**

The Secret Service is under fire after one of its members testified a fellow agent inserted a malicious thumb drive, found in the possession of a Chinese woman arrested at President Trump's Mar-a-Lago club last month, into an agency computer - that then began installing unwanted files.

[Fox News](#)

### **LAPD officer Ken Lew on starting organization that helps families**

## **in need**

After patrolling the streets of Los Angeles for more than two decades, Officer Ken Lew saw a lot of families and crime victims in need. In 2014 he decided to start a nonprofit organization to help out those families. Badge of Heart has provided food, clothing, housing assistance and baby essentials to families.

[KTLA](#)

## **Policy & Legal Issues**

### **LAPD to scrap some crime data programs after criticism**

Los Angeles Police Chief Michel Moore plans to scrap a controversial program that uses data to identify individuals who are most likely to commit violent crimes, bowing to criticism included in an audit and by privacy groups. In a five-page memo sent Friday to the Police Commission, the civilian panel that oversees the LAPD, Moore detailed a host of changes in response to a 52-page audit by Inspector General Mark Smith.

[Los Angeles Times](#)

### **L.A. Times and other news outlets sue for 911 call records from Borderline shooting**

The Los Angeles Times, the Associated Press and the publisher of the Ventura County Star sued Ventura County on Friday, seeking the release of 911 call records from the Borderline shooting that left 12 people dead. The lawsuit alleges that the county has violated the state's Public Records Act by denying requests for 911 calls, dispatch calls and body and dash camera audio or video.

[Los Angeles Times](#)

### **Santa Rosa declines to release police misconduct records despite new court ruling**

Santa Rosa officials say they will continue to withhold records detailing past misconduct by city police officers, contending a decision by the state Supreme Court on a pending case was needed to clarify the extent to which such law enforcement personnel records can be made public.

[The Press Democrat](#)

### **LAPD chief talks pursuit policies after string of Southern California chases**

Following a string of dangerous chases in Los Angeles County, L.A. Police Department Chief Michel Moore talked to Eyewitness News on Friday about law enforcement's policies and decision-making during pursuits. A crash into an innocent motorist would end a chase in Pasadena. The 63-year-old woman inside the vehicle is now out of the hospital. It was just one of four chases that happened just on Thursday.

[ABC7](#)

### **A rapid deployment team for victims**



When the special agent leading the FBI's response to a church shooting in Sutherland Springs, Texas, arrived on the scene in 2017 to join local police in assessing the crisis - in which a gunman killed 26 people before being shot dead - he made quick determinations about which FBI assets to deploy. Special agent bomb technicians and evidence response teams from the FBI's San Antonio Field Office were already on scene supporting the Texas Rangers, the state law enforcement agency leading the investigation.

[FBI](#)

### **Police Use-Of-Force bill moves forward in California legislature despite concerns from some lawmakers**

Lawmakers needed an entire chamber, a balcony, and a long hallway on Tuesday morning to hold all the people who wanted to speak about when law-enforcement officers should be allowed to use deadly force. Several family members of shooting victims waited in line during the three-hour hearing to speak in front of lawmakers: "Yeah, my name is Stevante Clark, of the Stephon Clark family ..."

[Capital Public Radio](#)

### **What should replace cash bail?**

Last August, California's former governor, Jerry Brown, signed Senate Bill No. 10, better known as the California Money Bail Reform Act. The legislation made the Golden State the first in the nation to end cash bail, or the practice of detaining defendants until their trials unless they are able to pay a bond ensuring their return. After signing the bill into law, the then-governor stated, "Today, California reforms its bail system so that rich and poor alike are treated fairly."

[Pacific Standard](#)

### **City Council members frustrated no pot shop landlords facing civil penalties**

Several members of the Los Angeles City Council expressed frustration Wednesday that the City Attorney's Office is not pursuing civil penalties against landlords whose properties are the site of illegal pot shops. The comments came before the council approved a set of actions aimed at cracking down on illegal shops, including the formation of a working group comprised of the Los Angeles Police Department, the Los Angeles Fire Department and other city departments to manage and direct enforcement efforts.

[NBC4](#)

## **Crime**

### **Police reports list shootings at Nipsey Hussle vigil**

Los Angeles Police Department crime reports say two women were the victims of shootings at a vigil for Nipsey Hussle that happened at the same shopping center where the rapper was murdered a day earlier. The police data characterized the April 1 shootings as, "assault with a

deadly weapon, aggravated assault," and listed the weapon used as an, "unknown firearm."

[NBC4](#)

### **Encino home of Los Angeles Rams coach Sean McVay reportedly burglarized**

An Encino home of Los Angeles Rams coach Sean McVay was reportedly burglarized Thursday night. Los Angeles police only confirmed officers responded to a burglary on the 16900 block of Encino Hills Drive around 9 p.m. and a report was taken. Surveillance video posted to Ring's Neighbors app shows two masked people exiting the home, one carrying a bag.

[ABC7](#)

### **Four shot, one killed during Nipsey Hussle's funeral procession**

Nipsey Hussle's funeral procession was interrupted by a "senseless" act of violence when gunfire erupted as fans celebrated the late rapper's life. According to the Los Angeles Police Department, a drive-by shooting took place along Nipsey's 25.5-mile long funeral procession route on Thursday (April 11). LAPD Chief Michael Moore revealed that victims are three black males and one black female, "ages 30-50 years old. Tragically one is deceased," he wrote on Twitter.

[KC 101](#)

## **Prop 47 & 57**

### **Santa Clara County may revise sanctuary policy in light of homicide**

A recent homicide in San Jose that was allegedly committed by an illegal immigrant has sparked debate over the sanctuary policy of Santa Clara County. Carlos Arevalo Carranza is accused of stabbing Bambi Larson to death in her home on Feb. 28 in the Thousand Oaks neighborhood of South San Jose. Police say Arevalo Carranza was caught on a surveillance camera walking down a street around 4:30 a.m.

[The Epoch Times](#)

### **Funds from ballot initiative help newly released prisoners find a home in Los Angeles**

As Latanja Madison's release date from prison inched closer, she felt more terrified than elated. During a decade behind bars at the California Institution for Women in Corona, the 55-year-old Madison underwent multiple orthopedic surgeries and now uses a walker. Her immediate family members passed away during her incarceration, creating grave doubts she would have a support system.

[Witness LA](#)

### **Hearing set for Madera County killer hoping Prop 57 will set her free**

Once a teenager found guilty of orchestrating the murder of a girl she

viewed as a romantic rival, a Madera County woman is fighting to get out of prison under the new rules of Prop 57. Eleven years ago, Brittany Navarra arranged the murder of Krista Rae Pike. Four years ago, a judge sentenced her to life in prison without parole. When a jury found Brittany Navarra guilty of murder, a dark cloud finally broke for her victim's family.

[ABC30 Fresno](#)

### **Gleason makes KRV pit stop**

Kern County First District Supervisor Mick Gleason met with the Kern Valley Exchange Club last Thursday, April 4, to update residents on issues facing the county. At the top of the list were homelessness and code compliance, two ongoing issues that valley residents have been working hard to address. Gleason said that while the county was not funded specifically to address homelessness and has no "homeless department," it had become more involved with the Kern County Homeless Collaborative, a group of organizations dedicated to providing resources to the homeless.

[Kern Valley Sun](#)

## **Los Angeles County Sheriff**

### **Sheriff's move to old digs raises eyebrows**

Los Angeles County Sheriff Alex Villanueva says his eighth-floor executive office complex at the Hall of Justice in downtown has proved to be inconvenient, so he's relocating to a second office in Monterey Park. Villanueva says he plans to keep the Hall of Justice office open but will do his job from the old Sheriff's headquarters building on Ramona Boulevard just south of the 10 Freeway.

[NBC4](#)

### **Sheriff Villanueva's reinstatement of deputies at odds with reforms, federal monitor says**

For several years, Los Angeles County's vast jail system has been under careful monitoring by a team of court-appointed watchdogs who've helped implement policies to curb excessive force and retaliation against inmates. But the lead monitor, Richard Drooyan, is now saying he's concerned that years of progress could be undermined by recent decisions by Sheriff Alex Villanueva, whose department operates the jail system.

[Los Angeles Times](#)

### **LA County Supervisors want to see if sheriff's 'truth panel' is legal**

The L.A. County Board of Supervisors Tuesday asked the county's lawyer to determine whether Sheriff Alex Villanueva's proposed Truth and Reconciliation Panel is legal. Villanueva wants to use the panel to review the cases of upwards of 400 deputies who he says may have been wrongly fired by his predecessor.

## Los Angeles County

### **Lawsuits cost taxpayers more than \$1 billion over past decade. Will that go up under new sheriff?**

During the past decade, Los Angeles County's taxpayers have doled out more than \$1 billion for other people's mistakes. Fire engines crash. Public Works and Animal Control workers collide with other drivers as they move from site to site. Department of Children and Family Services employees make errors and sheriff's deputies shoot and kill unarmed people. People are convicted of crimes they did not commit.

[KCET](#)

### **LA business groups gear up for an opposition campaign against LAUSD parcel tax on June 4th ballot**

Members of the Los Angeles Unified School District school board cheerily wore yellow Measure EE lapel pins at their meeting Tuesday and encouraged attendees to vote in favor of a parcel tax ballot initiative that would generate millions in local revenue to help ease the district's financial woes, if passed on June 4 in a special election.

[Los Angeles Daily News](#)

### **L.A. County Jail begins a mental health renovation**

California is often imagined within the American tapestry as the fulfillment of our notions of the American Dream, a land of opportunity where all are welcome and progress reaches everyone. "Now more than ever, America needs California," Governor Gavin Newsom said in his inaugural address in January.

[America/The Jesuit Review](#)

### **Long Beach will host California Democratic convention - and presidential hopefuls?**

Long Beach will play host to the California Democratic Party convention this November, almost certainly attracting candidates campaigning for the state's presidential primary that will take place a little more than 100 days later, the city said Tuesday. Although the party hadn't announced it yet, Long Beach Mayor Robert Garcia tweeted excitedly about the agreement on Tuesday.

[Los Angeles Daily News](#)

## Convictions/Sentences/Parole

### **Former LAPD officer pleads guilty to charges involving 13-year-old girl**

A former Los Angeles police officer pleaded guilty Friday to sex-related charges involving a friend's 13-year-old daughter at her home in Torrance. Kenneth Collard, 52, is facing five years in state prison in connection with his guilty plea to two counts of lewd act upon a child,

according to the Los Angeles County District Attorney's Office. He is set to be sentenced April 19 in a Torrance courtroom.

[City News Service](#)

### **Teen convicted of killing dad at Scripps Ranch condo sent to juvenile prison**

A teenage boy who shot his father five times in the master bedroom of the family's Scripps Ranch condominium last year, then fired another shot through the door of another bedroom, where his mother and half-brother had barricaded themselves, will be remanded to a juvenile detention facility for as much as nine years, a judge ruled Friday.

[City News Service](#)

### **Convictions of two men upheld for killings of pregnant woman**

A state appellate court panel Thursday upheld the convictions of two men for the contract killings of a pregnant woman and her unborn son outside her Hawthorne apartment in 2001. The three-justice panel from California's 2nd District Court of Appeal rejected the defense's contention that there were errors in the Los Angeles Superior Court trial of Derek Paul Smyer and Skyler Moore.

[City News Service](#)

### **Former Glendale police officer sentenced for helping Mexican mafia**

A former Los Angeles-area police officer who helped the Mexican Mafia and Armenian organized crime has been sentenced to federal prison, authorities said. John Balian received a 21-month-sentence on Friday. He pleaded guilty earlier this year to bribery, obstruction of justice and lying.

[AP](#)

### **Man sentenced to 26 years to life for killing reality star with hammer, burying body in backyard**

Jackie Jerome Rogers, 36, has been sentenced to 26 years to life in state prison for the brutal Dec. 2016 murder of a nurse and former reality star. According to prosecutors, Rogers used a hammer to strike 36-year-old Lisa Marie Naegle, a former star of the show Bridalplasty, eight times. The two, who had been involved in an affair, were sitting in his car at the time of the attack.

[People](#)

### **Man convicted of 2017 Chinatown double-murder**

In January 2017, a man burst into a Chinatown social club, interrupting a game of mahjong, demanding money and wielding a six-inch buck style knife, which he used to stab and kill two of the club members, according to testimony during the suspect's trial. It took police a day to find the man who was hiding in Rosemead after fleeing the clubhouse, leaving behind a trail of blood.

[San Gabriel Valley Tribune](#)



## Consumer News

### **Amazon, eBay, and Alibaba sell tons of counterfeits. Trump wants them to stop.**

You can buy a fake version of just about anything. From counterfeit olive oil and wine to fake Yeezy sneakers and Kylie beauty products, virtually whatever knockoff you could want is available, thanks to the giant \$1.2 trillion global counterfeit industry. This shadowy industry used to thrive mainly in alleyways in certain cities, but these days, many counterfeits hide in plain sight on the internet.

[Vox](#)

## California/National

### **Who monitors sheriffs? Proposed law would place that power firmly with counties**

Across California and other states, elected leaders and law enforcement are mired in debates about the authority of counties to monitor elected sheriffs. Some sheriffs argue that they are accountable only to the ballot box, and say acquiescence to any oversight by a local government is largely voluntary and limited.

[Los Angeles Times](#)

### **Hackers attacked California DMV voter registration system marred by bugs, glitches**

California has launched few government projects with higher stakes than its ambitious 2018 program for registering millions of new voters at the Department of Motor Vehicles, an effort with the potential to shape elections for years to come. Yet six days before the scheduled launch of the DMV's new "motor voter" system last April, state computer security officials noticed something ominous: The department's computer network was trying to connect to internet servers in Croatia.

[Los Angeles Times](#)

### **Bill targets ag theft, proposes directing fines to rural crimes enforcement**

A bill pending in the state Legislature would divert fines from the theft of tractors and other agricultural equipment to fund law enforcement activities in Kern and other rural areas where such crimes have long been a problem for farmers. Senate Bill 224, introduced this year by state Sen. Shannon Grove, R-Bakersfield, would create a new classification for grand theft of agricultural equipment.

[Bakersfield.com](#)

### **Rhetoric vs. reality: Kamala Harris' progressive platform undercut by prosecutor past**

Kamala Harris began her 2020 presidential campaign with a sweeping anti-Trump speech on Jan. 27 that took pains to mollify progressive

critics arguing that, when Harris was a prosecutor and California's attorney general, she shunned some of the same proposals she now claims are critical to stem racial injustice in the court system.

[Fox News](#)

### **Sacramento wants to tax soda, tires, guns, water, pain pills, lawyers, car batteries...**

To plagiarize T.S. Eliot, April is the cruelest month. But not for the reasons the poet wrote. Rather, for all the taxes. And there are bills in the Legislature to make taxes sting even worse. By April 10, Californians must pay their local property taxes. Five days later is the deadline for filing state and federal income tax returns.

[Los Angeles Times](#)

### **Does legalizing marijuana help or harm Americans? Weighing the statistical evidence**

The legalization of marijuana has been a topic of contention and confusion for both sides of the debate. The federal government still deems it illegal. But marijuana has been legalized for recreational use in 10 states and the District of Columbia, and a further 21 broadly legalize medical marijuana. Researchers like myself finally have some data to assess claims made on both sides.

[The Conversation](#)

### **California's emergency alert system has been a disaster. A statewide fix is planned**

In Mendocino County, emergency staffers waited for a supervisor to show up before they warned residents of a growing fire siege in 2017. In Santa Barbara County, officials hesitated to issue blanket evacuation orders before mudslides ripped through Montecito in 2018 because they worried they might trigger a panic.

[Los Angeles Times](#)

### **California statewide marijuana delivery survives assembly bill vote, but cities' lawsuit still a threat**

At a packed hearing Tuesday, a California legislative committee killed a measure aimed at overturning a controversial policy that allows licensed cannabis companies to deliver product anywhere in the state. The upshot is that the status quo will continue for marijuana delivery operators - at least for the foreseeable future - and that they'll be able to continue expanding their footprint all over the Golden State.

[Marijuana Business Daily](#)

## **Guns**

### **What to know about the Supreme Court's first gun case in 9 years**

The Supreme Court in its next term is expected to hear a challenge to New York City's ban on transporting a licensed handgun to a home or

shooting range outside the city. It's the first gun case the court will consider in nearly a decade. The regulation, which doesn't exist in any other American city, applies to holders of a "premises permit," one of two handgun permits residents can obtain, which allows them to keep guns in their homes and transport them, locked and unloaded, to one of the city's seven shooting ranges.

[The Trace](#)

## Corrections

### **California prison inmate Joseph Saucedo's death being investigated as homicide**

Authorities say the death of a 60-year-old inmate at a central California prison is being investigated as a homicide. The state Department of Corrections and Rehabilitation says guards found Joseph Saucedo unresponsive Friday on the floor of his cell at Pleasant Valley State Prison. He was pronounced dead a short time later.

[AP](#)

### **Maggots, mice fall into California prison dining hall**

Maggots and mice have fallen onto inmates' dining tables at a California state prison where holes in the roof also allow rain and bird droppings to seep through and streak the walls, according to an inmate lawsuit that charges the state isn't moving fast enough to repair deteriorating prisons.

[AP](#)

## Homeless

### **LA will spend \$30M this year on homeless sweeps. Do they even work?**

The email goes out every weekday from the Mayor's Unified Homeless Response Center to a long list of recipients in L.A.: Details of all planned cleanup operations. On any given day, plans can call for operations at up to 40 homeless encampment locations in the city, an analysis of six months of daily emails by KPCC/LAist found.

[LAist](#)

### **A shelter in all 15 of LA's council districts? Maybe not**

Roughly one year after Los Angeles Mayor Eric Garcetti announced plans for an emergency shelter program to address the city's homeless crisis, representatives from two council districts haven't yet proposed a single site where a shelter could be built. Both districts - six and 12 - are in the San Fernando Valley, where the number of homeless residents rose last year, in spite of a slight countywide drop in homelessness.

[Curbed Los Angeles](#)

### **Whittier will temporarily remove homeless from Parnell Park**

Whittier will employ a number of strategies to address its homeless

population - which has drawn the ire of many residents in the past month - including temporarily removing them from Parnell Park on Thursday, the city's top boss told council members this week. City Manager Jeff Collier's comments were later posted on the city website. [Whittier Daily News](#)

## Pensions

### **Will CalPERS board shake-up continue this year?**

A former CalPERS board member, J.J. Jelincic, plans to run against the new CalPERS board president, Henry Jones, as he seeks a fourth 4-year term on the board of the nation's largest pension system. Jelincic hopes to become the third challenger in as many years to unseat a CalPERS board member. He would join the two previous upset winners he supported, Margaret Brown and Jason Perez, as outsiders endorsed by retiree groups.

[Calpensions](#)

### **CalPERS investment committee rejects tobacco reinvestment again**

The investment committee of the California Public Employees' Retirement System (CalPERS) has rejected a proposal for the largest US retirement plan to consider reinvesting in tobacco stocks. The plan was floated by CalPERS investment committee member Jason Perez, a police sergeant in Corona, California. Perez joined the CalPERS board in January after defeating board president Priya Mathur.

[Chief Investment Officer](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ ggiguere@ci.sunnyvale.ca.us](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [Association of Deputy District Attorneys](#)  
**To:** [fgurina@sunnyvale.ca.gov](mailto:fgurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for April 15, 2019  
**Date:** Monday, April 15, 2019 5:02:24 AM

---

Having trouble viewing this email? [Click here](#)



## Courts & Rulings

### **Work product privilege yields to right to unbiased jury**

A criminal defendant's constitutional right to an unbiased jury trumps the prosecution's work product privilege, the Fourth District Court of



Appeal held yesterday, denying a writ petition by the San Diego Office of District Attorney contesting an order to turn over to a convicted murderer's habeas counsel the prosecution's jury selection notes.

[Metropolitan News-Enterprise](#)

### **Supreme Court won't review case of man convicted in brutal 1993 rape-murder**

The California Supreme Court refused Wednesday to review the case of a man convicted of the November 1993 rape-murder of a woman whose nude and battered body was discovered near the Harbor 110 Freeway in an unincorporated area near Torrance. Christopher Goree - who was 17 at the time of Dr. Josephine Tan's killing - was convicted in April 2011 of first-degree murder.

[City News Service](#)

### **30-year-plus incarceration for robbery was cruel, unusual**

The First District Court of Appeal held Friday that a man who pled guilty in 1988 to kidnapping for robbery and was sentenced to an indeterminate term of life with the possibility of parole should have been paroled sooner than he was and is entitled to habeas corpus relief. Post-release relief comes in the case of William Palmer who, after 10 parole suitability hearings over a 19-year period, had been found unfit for release, but was recently freed following an eleventh hearing.

[Metropolitan News-Enterprise](#)

### **As more people go without a lawyer, courts offer self-help services. Advice from the judge? No way**

The divorced couple appearing before Judge Helen E. Zukin was fighting over visitation. The man said he had kicked his heroin addiction and wanted to spend time with his children, whom he hadn't seen in three years. His ex was against it, saying she did not trust that he was clean, and that he had let his children down before. Neither party had an attorney, and it showed.

[Los Angeles Times](#)

### **Judge erred in ordering litigants to supply hair follicle evidence**

The First District Court of Appeal has declared that nothing has changed since 2005 when the Fourth District held that there's no legal authority for a court to order parties to a custody dispute to submit to hair follicle drug testing. Testing of hair follicles can reveal drug use during the preceding 90 days while conventional urine tests can only reflect such use in the past three days.

[Metropolitan News-Enterprise](#)

### **Judge declines to cancel Los Angeles gun permits**

A judge in Los Angeles has declined a request from LAPD Chief Michel Moore to cancel a decades-old agreement that granted concealed weapons permits to a handful of citizens. The decision means those citizens will continue to be issued permits to carry guns, at least

temporarily. The judge's ruling has not been finalized, but the city and the plaintiffs' attorneys confirmed the decision.

[NBC4](#)

### **Draft opinion cautions against use of CMS for judges' investigations**

The California Supreme Court Committee on Judicial Ethics Committee yesterday said it is seeking public input on its tentative formal opinion which declares that a judge should generally avoid searching the court case management system for information about a party or an attorney or facts relating to a case before the judicial officer.

[Metropolitan News-Enterprise](#)

### **Judge stays his own order to allow high-capacity gun magazines**

California residents who have acquired high-capacity gun magazines in the week since a federal judge found the state's voter-approved ban on the firearms unconstitutional will be allowed to keep their weapons, but will not be able to import more into the state starting Friday at 5 p.m., a federal judge ruled Thursday in staying his order.

[Courthouse News Service](#)

### **Noncustodial parent reasonably ordered to prove decreasing use of marijuana**

The Court of Appeal on Friday upheld an order that a noncustodial father submit to six drug tests to establish a decreasing dependency on marijuana. The admitted use by the father of marijuana to treat his headaches and relieve stress was not a basis for the order by Los Angeles Superior Court Judge Pete Navarro awarding custody of A.K. to the mother.

[Metropolitan News-Enterprise](#)

### **San Francisco can reject 5G equipment it views as too ugly**

San Francisco can reject 5G wireless equipment that it views as detracting from the city's beauty, a setback for wireless carriers which may now have to remap new networks or disguise antennas as palm fronds or building cornices. California's highest court disagreed Thursday with T-Mobile US Inc and other companies which argued San Francisco overreached in asserting its authority to regulate wireless telephone equipment on aesthetic grounds.

[The Star](#)

### **No reversal based on judge's misstatement of law**

A judge's statement reflecting an erroneous view of the applicable legal standard does not necessitate reversal where the order is supportable under the correct standard, the Court of Appeal for this district held yesterday in an opinion affirming the issuance of a civil harassment restraining order. Presiding Justice Arthur Gilbert of Div. Six wrote the opinion, which was not certified for publication.

[Metropolitan News-Enterprise](#)

### **Circuit holds no reasonable expectation of privacy in rental car for unauthorized and unlicensed driver**

In *United States v. Lyle*, 15-058-cr (April 1, 2019) (Raggi, Chin, Lohier), the Second Circuit, following a remand from the United States Supreme Court, once again held that the search of a rental car that James Lyle was driving (1) without a valid driver's license, (2) without the permission of the rental car company, but (3) with the permission of the authorized driver, was lawful.

[JD Supra](#)

### **Search of youth's electronic devices properly ordered**

The Court of Appeal for this district, in a 2-1 opinion, yesterday validated a condition of probation that a youthful offender, who got into a fist fight on the schoolyard and directed a racial epithet at a teacher who attempted to intercede, be subject to a search of his electronic devices.

[Metropolitan News-Enterprise](#)

### **High-salaried lawyers should pay more in dues than others: Lawmaker**

A key state lawmaker says his colleagues should use their authority over the annual bar dues bill to "restructure" the fee schedule so high-salaried attorneys pay more than their lower-earning counterparts in the profession. Assemblyman Mark Stone, D-Scotts Valley, told members of the Judiciary Committee, which he chairs, that bar leaders' pending request to the Legislature for a \$100 annual fee hike - plus \$330 in one-time assessments in 2020 - is "our opportunity to take some of the regressive nature of that fee structure out."

[Law.com](#)

### **Court won't extend deadline for inmate to file appeal**

A California appellate court ruled that principles of equity can allow more time for an inmate to appeal the denial of his request to belatedly file a personal injury action, but the circumstances did not warrant an extension. Case: *De Leon v. Flores*, No. F077038, 04/04/2019, unpublished. Facts: Rene De Leon was an inmate of the California Department of Corrections and Rehabilitation.

[Work Comp Central](#)

### **Retired judges grumble at assignment program reforms, as audit raises questions**

California's assigned judges program, a constitutionally provided system that uses retired jurists to cover judicial absences, is under mounting scrutiny amid allegations of cost overruns, questionable practices and new rules that some judges say amount to age discrimination.

[The Recorder](#)

### **No additional fees to lawyers who garnered \$10 million in 2016**

The Ninth U.S. Circuit Court of Appeals yesterday upheld the denial of supplemental attorney fees in a case in which the City of Los Angeles agreed in 2016 to pay \$1.4 billion over a 30 year period to render its sidewalks fully accessible to persons with mobility disabilities.

[Metropolitan News-Enterprise](#)

## **Prosecutions/Prosecutors**

### **Man faces murder charges in crash that killed CHP veteran**

A man faces murder charges after he hit a California Highway Patrol officer on Interstate 15 in Lake Elsinore this weekend, the agency announced Sunday. Sgt. Steve Licon, 53, died at the Inland Valley Medical Center following the 4:30 p.m. crash on the southbound side of I-15 just north of Nichols Road, CHP spokesman Ramon Duran said.

[KTLA](#)

### **Lawyers for Newport doctor accused of sexual assaults seek communications related to ex-DA's claim of 'a thousand' potential victims**

Lawyers for a Newport Beach doctor and his girlfriend who are accused of numerous cases of sexual assault appeared in a Newport Beach courtroom Friday to try to obtain verbal and written communications within the Orange County district attorney's office that could form the basis for an argument that the prosecution's actions deprived their clients of the opportunity for a fair trial by misrepresenting them to the media.

[Los Angeles Times](#)

### **Owners of crime-ridden Valley motel may be forced to live in it**

The managers of a troublesome San Fernando Valley motel may soon get a taste of their own medicine. The Los Angeles City Attorney's Office wants to force three managers at the Studio 6 motel on Sherman Way to live in the motel until it tackles its alleged problems with drugs, prostitution and gang activity.

[North Hollywood-Toluca Lake](#)

### **L.A. man faces charges after crashing into police cars, vehicle with baby on board during chase: DA**

A Los Angeles man was charged Monday with felony counts of assaulting a police officer and other charges after allegedly crashing into multiple vehicles during a pursuit last week, including one carrying a baby, prosecutors said. Pharuehat Wilaisophakun, 27, led officers on a chase April 4 after an officer witnessed him get into a crash in a 2018 Prius and he refused to stop in Hollywood, according to the Los Angeles County District Attorney's Office.

[KTLA](#)

### **Social justice prosecutors**

For years, many have bemoaned the slide of America's higher education

system down the slippery slope of moral relativism and the embracing of virtually all facets of progressive dogma while rejecting most elements of conservatism. The mere invitation of a conservative commentator to speak on college campuses is now reason enough for rioting and mass student protests.

[American Thinker](#)

### **OCDA speaks for victims, families at victims' rights march**

Family members of murder victims rallied at the Victims' Rights March in Orange County, to stand shoulder to shoulder in a show of solidarity after California's governor has declared an end to the death penalty during his term of office. This year, in advance of the accused Golden State Killer Joseph DeAngelo's pretrial hearing, Orange County District Attorney Todd Spitzer made his stance clear.

[Laguna Niguel-Dana Point](#)

### **Deputy D.A. becomes latest to challenge Jackie Lacey**

A Los Angeles County deputy district attorney announced plans Wednesday to challenge Jackie Lacey in the 2020 election, making him the second insurgent candidate promising to bring a more progressive bent to the county's top law enforcement post. Joseph Iniguez, a 33-year-old prosecutor currently trying cases in the Alhambra courthouse, said that although he respects Lacey, he believes she has prevented the district attorney's office from leading the country in the kinds of criminal justice reforms that have sprouted under other progressive prosecutors in Philadelphia and San Francisco.

[Los Angeles Times](#)

### **"Golden State Killer" case death penalty decision renews debate in California**

California prosecutors announced Wednesday they will seek the death penalty if they convict the man suspected of being the notorious "Golden State Killer," renewing debate over Gov. Gavin Newsom's moratorium on executing any of the 737 inmates on the nation's largest death row. Newsom's reprieve lasts only so long as he is governor, and it does not prevent prosecutors from seeking the death penalty nor judges and juries from imposing death sentences.

[CBS/AP](#)

### **California prosecutors accuse Avenatti of bilking clients, including a paraplegic man**

A federal grand jury in California on Thursday indicted Michael Avenatti on 36 counts of fraud, perjury and other financial crimes, the latest barrage of charges against the attorney who rocketed into the national spotlight while representing adult film actress Stormy Daniels in her case against President Donald Trump.

[Politico](#)



---

### **A new method of DNA testing could solve more shootings**

Police found 19 spent shell casings scattered in the San Diego street where Gregory Benton was murdered on April 12, 2014. Benton and his cousin had gone to buy cigarettes, a witness later said. As they returned to a family party, two men pulled up in a car behind them. They got out, and at least one of them opened fire.

[PoliceOne](#)

### **LAPD Chief hails new County Office of Violence Prevention**

Los Angeles County's recently established Office of Violence Prevention drew praise today from Los Angeles Police Department Chief Michel Moore. "I'm encouraged for the first time that the County of Los Angeles is establishing a means to identify resources that exist, gaps that need to be filled and coordinate the delivery of all those services to a county of more than 10 million people," Moore said at a news conference at the Martin Luther King Jr. Center for Public Health in the unincorporated Willowbrook area.

[City News Service](#)

### **Q & A with Public Safety Chief**

Recently, there have been a string of thefts on campus of students' personal items. This week, Isabella Murillo, news editor, sat down with Danny Martinez, chief of Department of Public Safety (DPS) to discuss this. What is the department doing about the increase in thefts of student property on campus? DPS thoroughly investigates every theft brought to our attention.

[Los Angeles Loyolan](#)

### **Citizen App texts you in real time if a crime or fire is happening nearby**

Chances are you've seen a helicopter circling above your neighborhood, an accident or road shut down due to police activity. Now, thanks to a new app called Citizen, you can finally understand exactly what's going on. The company behind the app is doing something really interesting: they're going around to major cities and installing antennas to allow them to listen to police and fire scanners.

[KTLA](#)

### **Secret Service under fire after agent testifies agency inserted malicious thumb drive into computer**

The Secret Service is under fire after one of its members testified a fellow agent inserted a malicious thumb drive, found in the possession of a Chinese woman arrested at President Trump's Mar-a-Lago club last month, into an agency computer - that then began installing unwanted files.

[Fox News](#)

### **LAPD officer Ken Lew on starting organization that helps families**

## **in need**

After patrolling the streets of Los Angeles for more than two decades, Officer Ken Lew saw a lot of families and crime victims in need. In 2014 he decided to start a nonprofit organization to help out those families. Badge of Heart has provided food, clothing, housing assistance and baby essentials to families.

[KTLA](#)

## **Policy & Legal Issues**

### **LAPD to scrap some crime data programs after criticism**

Los Angeles Police Chief Michel Moore plans to scrap a controversial program that uses data to identify individuals who are most likely to commit violent crimes, bowing to criticism included in an audit and by privacy groups. In a five-page memo sent Friday to the Police Commission, the civilian panel that oversees the LAPD, Moore detailed a host of changes in response to a 52-page audit by Inspector General Mark Smith.

[Los Angeles Times](#)

### **L.A. Times and other news outlets sue for 911 call records from Borderline shooting**

The Los Angeles Times, the Associated Press and the publisher of the Ventura County Star sued Ventura County on Friday, seeking the release of 911 call records from the Borderline shooting that left 12 people dead. The lawsuit alleges that the county has violated the state's Public Records Act by denying requests for 911 calls, dispatch calls and body and dash camera audio or video.

[Los Angeles Times](#)

### **Santa Rosa declines to release police misconduct records despite new court ruling**

Santa Rosa officials say they will continue to withhold records detailing past misconduct by city police officers, contending a decision by the state Supreme Court on a pending case was needed to clarify the extent to which such law enforcement personnel records can be made public.

[The Press Democrat](#)

### **LAPD chief talks pursuit policies after string of Southern California chases**

Following a string of dangerous chases in Los Angeles County, L.A. Police Department Chief Michel Moore talked to Eyewitness News on Friday about law enforcement's policies and decision-making during pursuits. A crash into an innocent motorist would end a chase in Pasadena. The 63-year-old woman inside the vehicle is now out of the hospital. It was just one of four chases that happened just on Thursday.

[ABC7](#)

### **A rapid deployment team for victims**

When the special agent leading the FBI's response to a church shooting in Sutherland Springs, Texas, arrived on the scene in 2017 to join local police in assessing the crisis - in which a gunman killed 26 people before being shot dead - he made quick determinations about which FBI assets to deploy. Special agent bomb technicians and evidence response teams from the FBI's San Antonio Field Office were already on scene supporting the Texas Rangers, the state law enforcement agency leading the investigation.

[FBI](#)

### **Police Use-Of-Force bill moves forward in California legislature despite concerns from some lawmakers**

Lawmakers needed an entire chamber, a balcony, and a long hallway on Tuesday morning to hold all the people who wanted to speak about when law-enforcement officers should be allowed to use deadly force. Several family members of shooting victims waited in line during the three-hour hearing to speak in front of lawmakers: "Yeah, my name is Stevante Clark, of the Stephon Clark family ..."

[Capital Public Radio](#)

### **What should replace cash bail?**

Last August, California's former governor, Jerry Brown, signed Senate Bill No. 10, better known as the California Money Bail Reform Act. The legislation made the Golden State the first in the nation to end cash bail, or the practice of detaining defendants until their trials unless they are able to pay a bond ensuring their return. After signing the bill into law, the then-governor stated, "Today, California reforms its bail system so that rich and poor alike are treated fairly."

[Pacific Standard](#)

### **City Council members frustrated no pot shop landlords facing civil penalties**

Several members of the Los Angeles City Council expressed frustration Wednesday that the City Attorney's Office is not pursuing civil penalties against landlords whose properties are the site of illegal pot shops. The comments came before the council approved a set of actions aimed at cracking down on illegal shops, including the formation of a working group comprised of the Los Angeles Police Department, the Los Angeles Fire Department and other city departments to manage and direct enforcement efforts.

[NBC4](#)

## **Crime**

### **Police reports list shootings at Nipsey Hussle vigil**

Los Angeles Police Department crime reports say two women were the victims of shootings at a vigil for Nipsey Hussle that happened at the same shopping center where the rapper was murdered a day earlier. The police data characterized the April 1 shootings as, "assault with a

deadly weapon, aggravated assault," and listed the weapon used as an, "unknown firearm."

[NBC4](#)

### **Encino home of Los Angeles Rams coach Sean McVay reportedly burglarized**

An Encino home of Los Angeles Rams coach Sean McVay was reportedly burglarized Thursday night. Los Angeles police only confirmed officers responded to a burglary on the 16900 block of Encino Hills Drive around 9 p.m. and a report was taken. Surveillance video posted to Ring's Neighbors app shows two masked people exiting the home, one carrying a bag.

[ABC7](#)

### **Four shot, one killed during Nipsey Hussle's funeral procession**

Nipsey Hussle's funeral procession was interrupted by a "senseless" act of violence when gunfire erupted as fans celebrated the late rapper's life. According to the Los Angeles Police Department, a drive-by shooting took place along Nipsey's 25.5-mile long funeral procession route on Thursday (April 11). LAPD Chief Michael Moore revealed that victims are three black males and one black female, "ages 30-50 years old. Tragically one is deceased," he wrote on Twitter.

[KC 101](#)

## **Prop 47 & 57**

### **Santa Clara County may revise sanctuary policy in light of homicide**

A recent homicide in San Jose that was allegedly committed by an illegal immigrant has sparked debate over the sanctuary policy of Santa Clara County. Carlos Arevalo Carranza is accused of stabbing Bambi Larson to death in her home on Feb. 28 in the Thousand Oaks neighborhood of South San Jose. Police say Arevalo Carranza was caught on a surveillance camera walking down a street around 4:30 a.m.

[The Epoch Times](#)

### **Funds from ballot initiative help newly released prisoners find a home in Los Angeles**

As Latanja Madison's release date from prison inched closer, she felt more terrified than elated. During a decade behind bars at the California Institution for Women in Corona, the 55-year-old Madison underwent multiple orthopedic surgeries and now uses a walker. Her immediate family members passed away during her incarceration, creating grave doubts she would have a support system.

[Witness LA](#)

### **Hearing set for Madera County killer hoping Prop 57 will set her free**

Once a teenager found guilty of orchestrating the murder of a girl she

viewed as a romantic rival, a Madera County woman is fighting to get out of prison under the new rules of Prop 57. Eleven years ago, Brittany Navarra arranged the murder of Krista Rae Pike. Four years ago, a judge sentenced her to life in prison without parole. When a jury found Brittany Navarra guilty of murder, a dark cloud finally broke for her victim's family.

[ABC30 Fresno](#)

### **Gleason makes KRV pit stop**

Kern County First District Supervisor Mick Gleason met with the Kern Valley Exchange Club last Thursday, April 4, to update residents on issues facing the county. At the top of the list were homelessness and code compliance, two ongoing issues that valley residents have been working hard to address. Gleason said that while the county was not funded specifically to address homelessness and has no "homeless department," it had become more involved with the Kern County Homeless Collaborative, a group of organizations dedicated to providing resources to the homeless.

[Kern Valley Sun](#)

## **Los Angeles County Sheriff**

### **Sheriff's move to old digs raises eyebrows**

Los Angeles County Sheriff Alex Villanueva says his eighth-floor executive office complex at the Hall of Justice in downtown has proved to be inconvenient, so he's relocating to a second office in Monterey Park. Villanueva says he plans to keep the Hall of Justice office open but will do his job from the old Sheriff's headquarters building on Ramona Boulevard just south of the 10 Freeway.

[NBC4](#)

### **Sheriff Villanueva's reinstatement of deputies at odds with reforms, federal monitor says**

For several years, Los Angeles County's vast jail system has been under careful monitoring by a team of court-appointed watchdogs who've helped implement policies to curb excessive force and retaliation against inmates. But the lead monitor, Richard Drooyan, is now saying he's concerned that years of progress could be undermined by recent decisions by Sheriff Alex Villanueva, whose department operates the jail system.

[Los Angeles Times](#)

### **LA County Supervisors want to see if sheriff's 'truth panel' is legal**

The L.A. County Board of Supervisors Tuesday asked the county's lawyer to determine whether Sheriff Alex Villanueva's proposed Truth and Reconciliation Panel is legal. Villanueva wants to use the panel to review the cases of upwards of 400 deputies who he says may have been wrongly fired by his predecessor.



## Los Angeles County

### **Lawsuits cost taxpayers more than \$1 billion over past decade. Will that go up under new sheriff?**

During the past decade, Los Angeles County's taxpayers have doled out more than \$1 billion for other people's mistakes. Fire engines crash. Public Works and Animal Control workers collide with other drivers as they move from site to site. Department of Children and Family Services employees make errors and sheriff's deputies shoot and kill unarmed people. People are convicted of crimes they did not commit.

[KCET](#)

### **LA business groups gear up for an opposition campaign against LAUSD parcel tax on June 4th ballot**

Members of the Los Angeles Unified School District school board cheerily wore yellow Measure EE lapel pins at their meeting Tuesday and encouraged attendees to vote in favor of a parcel tax ballot initiative that would generate millions in local revenue to help ease the district's financial woes, if passed on June 4 in a special election.

[Los Angeles Daily News](#)

### **L.A. County Jail begins a mental health renovation**

California is often imagined within the American tapestry as the fulfillment of our notions of the American Dream, a land of opportunity where all are welcome and progress reaches everyone. "Now more than ever, America needs California," Governor Gavin Newsom said in his inaugural address in January.

[America/The Jesuit Review](#)

### **Long Beach will host California Democratic convention - and presidential hopefuls?**

Long Beach will play host to the California Democratic Party convention this November, almost certainly attracting candidates campaigning for the state's presidential primary that will take place a little more than 100 days later, the city said Tuesday. Although the party hadn't announced it yet, Long Beach Mayor Robert Garcia tweeted excitedly about the agreement on Tuesday.

[Los Angeles Daily News](#)

## Convictions/Sentences/Parole

### **Former LAPD officer pleads guilty to charges involving 13-year-old girl**

A former Los Angeles police officer pleaded guilty Friday to sex-related charges involving a friend's 13-year-old daughter at her home in Torrance. Kenneth Collard, 52, is facing five years in state prison in connection with his guilty plea to two counts of lewd act upon a child,

according to the Los Angeles County District Attorney's Office. He is set to be sentenced April 19 in a Torrance courtroom.

[City News Service](#)

### **Teen convicted of killing dad at Scripps Ranch condo sent to juvenile prison**

A teenage boy who shot his father five times in the master bedroom of the family's Scripps Ranch condominium last year, then fired another shot through the door of another bedroom, where his mother and half-brother had barricaded themselves, will be remanded to a juvenile detention facility for as much as nine years, a judge ruled Friday.

[City News Service](#)

### **Convictions of two men upheld for killings of pregnant woman**

A state appellate court panel Thursday upheld the convictions of two men for the contract killings of a pregnant woman and her unborn son outside her Hawthorne apartment in 2001. The three-justice panel from California's 2nd District Court of Appeal rejected the defense's contention that there were errors in the Los Angeles Superior Court trial of Derek Paul Smyer and Skyler Moore.

[City News Service](#)

### **Former Glendale police officer sentenced for helping Mexican mafia**

A former Los Angeles-area police officer who helped the Mexican Mafia and Armenian organized crime has been sentenced to federal prison, authorities said. John Balian received a 21-month-sentence on Friday. He pleaded guilty earlier this year to bribery, obstruction of justice and lying.

[AP](#)

### **Man sentenced to 26 years to life for killing reality star with hammer, burying body in backyard**

Jackie Jerome Rogers, 36, has been sentenced to 26 years to life in state prison for the brutal Dec. 2016 murder of a nurse and former reality star. According to prosecutors, Rogers used a hammer to strike 36-year-old Lisa Marie Naegle, a former star of the show Bridalplasty, eight times. The two, who had been involved in an affair, were sitting in his car at the time of the attack.

[People](#)

### **Man convicted of 2017 Chinatown double-murder**

In January 2017, a man burst into a Chinatown social club, interrupting a game of mahjong, demanding money and wielding a six-inch buck style knife, which he used to stab and kill two of the club members, according to testimony during the suspect's trial. It took police a day to find the man who was hiding in Rosemead after fleeing the clubhouse, leaving behind a trail of blood.

[San Gabriel Valley Tribune](#)

## Consumer News

### **Amazon, eBay, and Alibaba sell tons of counterfeits. Trump wants them to stop.**

You can buy a fake version of just about anything. From counterfeit olive oil and wine to fake Yeezy sneakers and Kylie beauty products, virtually whatever knockoff you could want is available, thanks to the giant \$1.2 trillion global counterfeit industry. This shadowy industry used to thrive mainly in alleyways in certain cities, but these days, many counterfeits hide in plain sight on the internet.

[Vox](#)

## California/National

### **Who monitors sheriffs? Proposed law would place that power firmly with counties**

Across California and other states, elected leaders and law enforcement are mired in debates about the authority of counties to monitor elected sheriffs. Some sheriffs argue that they are accountable only to the ballot box, and say acquiescence to any oversight by a local government is largely voluntary and limited.

[Los Angeles Times](#)

### **Hackers attacked California DMV voter registration system marred by bugs, glitches**

California has launched few government projects with higher stakes than its ambitious 2018 program for registering millions of new voters at the Department of Motor Vehicles, an effort with the potential to shape elections for years to come. Yet six days before the scheduled launch of the DMV's new "motor voter" system last April, state computer security officials noticed something ominous: The department's computer network was trying to connect to internet servers in Croatia.

[Los Angeles Times](#)

### **Bill targets ag theft, proposes directing fines to rural crimes enforcement**

A bill pending in the state Legislature would divert fines from the theft of tractors and other agricultural equipment to fund law enforcement activities in Kern and other rural areas where such crimes have long been a problem for farmers. Senate Bill 224, introduced this year by state Sen. Shannon Grove, R-Bakersfield, would create a new classification for grand theft of agricultural equipment.

[Bakersfield.com](#)

### **Rhetoric vs. reality: Kamala Harris' progressive platform undercut by prosecutor past**

Kamala Harris began her 2020 presidential campaign with a sweeping anti-Trump speech on Jan. 27 that took pains to mollify progressive

critics arguing that, when Harris was a prosecutor and California's attorney general, she shunned some of the same proposals she now claims are critical to stem racial injustice in the court system.

[Fox News](#)

### **Sacramento wants to tax soda, tires, guns, water, pain pills, lawyers, car batteries...**

To plagiarize T.S. Eliot, April is the cruelest month. But not for the reasons the poet wrote. Rather, for all the taxes. And there are bills in the Legislature to make taxes sting even worse. By April 10, Californians must pay their local property taxes. Five days later is the deadline for filing state and federal income tax returns.

[Los Angeles Times](#)

### **Does legalizing marijuana help or harm Americans? Weighing the statistical evidence**

The legalization of marijuana has been a topic of contention and confusion for both sides of the debate. The federal government still deems it illegal. But marijuana has been legalized for recreational use in 10 states and the District of Columbia, and a further 21 broadly legalize medical marijuana. Researchers like myself finally have some data to assess claims made on both sides.

[The Conversation](#)

### **California's emergency alert system has been a disaster. A statewide fix is planned**

In Mendocino County, emergency staffers waited for a supervisor to show up before they warned residents of a growing fire siege in 2017. In Santa Barbara County, officials hesitated to issue blanket evacuation orders before mudslides ripped through Montecito in 2018 because they worried they might trigger a panic.

[Los Angeles Times](#)

### **California statewide marijuana delivery survives assembly bill vote, but cities' lawsuit still a threat**

At a packed hearing Tuesday, a California legislative committee killed a measure aimed at overturning a controversial policy that allows licensed cannabis companies to deliver product anywhere in the state. The upshot is that the status quo will continue for marijuana delivery operators - at least for the foreseeable future - and that they'll be able to continue expanding their footprint all over the Golden State.

[Marijuana Business Daily](#)

## **Guns**

### **What to know about the Supreme Court's first gun case in 9 years**

The Supreme Court in its next term is expected to hear a challenge to New York City's ban on transporting a licensed handgun to a home or

shooting range outside the city. It's the first gun case the court will consider in nearly a decade. The regulation, which doesn't exist in any other American city, applies to holders of a "premises permit," one of two handgun permits residents can obtain, which allows them to keep guns in their homes and transport them, locked and unloaded, to one of the city's seven shooting ranges.

[The Trace](#)

## Corrections

### **California prison inmate Joseph Saucedo's death being investigated as homicide**

Authorities say the death of a 60-year-old inmate at a central California prison is being investigated as a homicide. The state Department of Corrections and Rehabilitation says guards found Joseph Saucedo unresponsive Friday on the floor of his cell at Pleasant Valley State Prison. He was pronounced dead a short time later.

[AP](#)

### **Maggots, mice fall into California prison dining hall**

Maggots and mice have fallen onto inmates' dining tables at a California state prison where holes in the roof also allow rain and bird droppings to seep through and streak the walls, according to an inmate lawsuit that charges the state isn't moving fast enough to repair deteriorating prisons.

[AP](#)

## Homeless

### **LA will spend \$30M this year on homeless sweeps. Do they even work?**

The email goes out every weekday from the Mayor's Unified Homeless Response Center to a long list of recipients in L.A.: Details of all planned cleanup operations. On any given day, plans can call for operations at up to 40 homeless encampment locations in the city, an analysis of six months of daily emails by KPCC/LAist found.

[LAist](#)

### **A shelter in all 15 of LA's council districts? Maybe not**

Roughly one year after Los Angeles Mayor Eric Garcetti announced plans for an emergency shelter program to address the city's homeless crisis, representatives from two council districts haven't yet proposed a single site where a shelter could be built. Both districts - six and 12 - are in the San Fernando Valley, where the number of homeless residents rose last year, in spite of a slight countywide drop in homelessness.

[Curbed Los Angeles](#)

### **Whittier will temporarily remove homeless from Parnell Park**

Whittier will employ a number of strategies to address its homeless



population - which has drawn the ire of many residents in the past month - including temporarily removing them from Parnell Park on Thursday, the city's top boss told council members this week. City Manager Jeff Collier's comments were later posted on the city website. [Whittier Daily News](#)

## Pensions

### **Will CalPERS board shake-up continue this year?**

A former CalPERS board member, J.J. Jelincic, plans to run against the new CalPERS board president, Henry Jones, as he seeks a fourth 4-year term on the board of the nation's largest pension system. Jelincic hopes to become the third challenger in as many years to unseat a CalPERS board member. He would join the two previous upset winners he supported, Margaret Brown and Jason Perez, as outsiders endorsed by retiree groups.

[Calpensions](#)

### **CalPERS investment committee rejects tobacco reinvestment again**

The investment committee of the California Public Employees' Retirement System (CalPERS) has rejected a proposal for the largest US retirement plan to consider reinvesting in tobacco stocks. The plan was floated by CalPERS investment committee member Jason Perez, a police sergeant in Corona, California. Perez joined the CalPERS board in January after defeating board president Priya Mathur.

[Chief Investment Officer](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™](#) [fgrgurina@sunnyvale.ca.gov](mailto:fgrgurina@sunnyvale.ca.gov)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [Association of Deputy District Attorneys](#)  
**To:** [ggiguire@ci.sunnyvale.ca.us](mailto:ggiguire@ci.sunnyvale.ca.us)  
**Subject:** Monday Morning Memo for April 8, 2019  
**Date:** Monday, April 08, 2019 5:04:02 AM

---

Having trouble viewing this email? [Click here](#)



## Courts & Rulings

### **Verdict affirmed in favor of city in action alleging false arrest of videographer**

A freelance videographer who was taken into custody after he continued

to walk toward City Hall as persons encamped on the grounds as part of Occupy Los Angeles were being dispersed, and became combative with police, yesterday lost his bid for reversal of a judgment in favor of the City of Los Angeles and several of its officers in his action for false arrest and a civil rights violation.

[Metropolitan News-Enterprise](#)

### **Man asked incriminating questions by police was not under detention**

A pedestrian who changed direction when he spotted a patrol car, stuck something in his pocket, and darted onto the driveway of an apartment complex, was not "detained" when officers questioned him as to what he had in his pocket and he admitted possessing a "meth pipe," the Court of Appeal for this district has held, affirming the denial of his suppression motion.

[Metropolitan News-Enterprise](#)

### **Ninth Circuit upholds 27-year sentence for Russian hacker**

A Ninth Circuit panel upheld the 27-year prison sentence of a Russian computer hacker who was extradited to the United States while on vacation with his family in the Maldives to face charges he stole credit card numbers and millions of dollars. Roman Seleznev claimed the U.S. government kidnapped him when he was finally arrested several years after some of his most lucrative heists.

[Courthouse News Service](#)

### **C.A. orders publication of portion of opinion lifting prior restraint**

The Court of Appeal for this district has decided to publish that portion of its Feb. 26 opinion in which it holds that a domestic violence restraining order against a Los Angeles attorney is an unconstitutional prior restraint in the extent that it forbids him from posting "anything" on Facebook about the case in which he is being sued for divorce.

[Metropolitan News-Enterprise](#)

### **Lawyer fingerprinting in this state turns up over 2,200 convictions unknown to bar**

A California court rule requiring lawyers to be fingerprinted has turned up more than 6,000 criminal history reports, including more than 2,200 convictions previously unknown to the state bar. The 2,200 unknown convictions include 20 unreported felonies, Above the Law reports. The number of convictions likely will increase as more lawyers get fingerprinted ahead of an April 30 deadline.

[ABA Journal](#)

### **Judge Anderson barred from third sentencing of defendant**

The Ninth U.S. Circuit Court of Appeals yesterday, for a second time, remanded a case for resentencing, declaring that the matter must be heard by a judge of the District Court for the Central District of California other than Percy Anderson who, the three-judge panel said,

failed to adhere to the appeals court's 2016 opinion in the case.

[Metropolitan News-Enterprise](#)

### **Justices rule against Missouri inmate with rare health issue**

Missouri can execute an inmate who argued his rare medical condition will result in severe pain if he is put to death by lethal injection, the Supreme Court ruled Monday. The justices split along ideological lines in ruling 5-4 against inmate Russell Bucklew, who is on death row for a 1996 murder. The court's five conservative justices rejected Bucklew's argument that subjecting him to lethal injection would violate the Constitution's ban on cruel and unusual punishment.

[Kansas City Star](#)

### **Judge dismisses suit based on San Bernardino terrorist attack**

A federal judge in Santa Ana Monday dismissed a lawsuit filed by relatives of three of the victims killed in the 2015 terrorist attack in San Bernardino, saying the tort claim of negligence is outweighed by the government's sovereign immunity. Relatives of shooting victims Nicholas Thalasinis, Sierra Clayborn and Tin Nguyen accused the government of negligence for failing to investigate Syed Rizwan Farook and Tashfeen Malik, the husband-and-wife jihadis who killed 14 people and wounded two dozen others during a Christmas party at the Inland Regional Center on Dec. 2, 2015.

[My News LA](#)

### **Prop. 63: Federal judge declares California's ban on high-capacity gun magazines unconstitutional**

A federal judge on Friday declared unconstitutional a key provision of California's Proposition 63 that banned possession of high-capacity gun magazines often used in mass shootings, ensuring that the voter-approved prohibition will remain tied up in court for some time to come. San Diego-based U.S. District Judge Roger Benitez wrote in his 86-page decision, upholding a lawsuit against the proposed ban of magazines holding more than 10 rounds, that such a statute "hits at the center of the Second Amendment and its burden is severe."

[San Francisco Chronicle](#)

### **Public has access to pre-2019 police personnel files**

Amendments to a statute which increases public access to personnel files of peace officers may permissibly be applied to records that were in existence prior to the Jan. 1 effective date of the legislation, the First District Court of Appeal has held. Div. Four's decision comes in a "By the Court" order denying petitions for writs of supersedeas filed by the Walnut Creek Police Officers' Association and others in five consolidated matters.

[Metropolitan News-Enterprise](#)

### **The far-reach of the 9th Circuit's decision to stand firm on landmark homeless case**

If you're a homeless person with nowhere to go but a city sidewalk, park or other public space, can authorities force you off the street? This week, federal judges again said: "No." That answer - the same given by three judges on the 9th Circuit Court of Appeals back in September - came after yet another review of a case that's been making its way through the courts for a decade.

[LAist](#)

### **Challenge to barring of 2018 ballot designation is moot**

The Fourth District Court of Appeal has dismissed as moot a challenge by an unsuccessful candidate in 2018 for the post of district attorney of Orange County to the denial of her use of the ballot designation, "Civil Rights Attorney." Div. Three on Friday, in an unpublished opinion by Justice Raymond J. Ikola, spurned erstwhile candidate Lenore L. Albert's appeal of orders by Orange Superior Court Judge Craig L. Griffin, finding no justification for addressing the merits notwithstanding mootness.

[Metropolitan News-Enterprise](#)

### **Jury says Pomona police officer did not obstruct justice, mistrial declared on charges of lying to FBI**

A federal jury Wednesday found the Pomona police officer who investigated the violent arrest of a teenage boy at the Los Angeles County Fair in 2015 not guilty of deterring the boy and his mother from coming forward during the investigation - but jurors did not reach unanimous verdicts on two charges of lying to the FBI.

[San Gabriel Valley Tribune](#)

## **Prosecutions/Prosecutors**

### **L.A., San Joaquin County prosecutors to clear thousands of pot convictions**

Los Angeles and San Joaquin county prosecutors announced a plan Monday to automatically clear more than 50,000 marijuana-related convictions eligible for reconsideration in light of the state's legalization of pot under Proposition 64. District attorneys from both counties said they will partner with nonprofit Code for America, which has developed a computerized system known as Clear My Record that quickly identify cannabis convictions eligible to be cleared.

[My News LA](#)

### **Orange County DA charges 4 women in connection with multistate prostitution ring**

Authorities say they have charged four women with running a prostitution network in California, Nevada and Utah that netted tens of thousands of dollars a month. Orange County District Attorney Todd Spitzer said Wednesday the women had a website that appeared to be a legitimate service but was not. The four are charged with pimping and pandering and the two alleged ringleaders are also charged with conspiracy.



[KTLA](#)

### **Man ordered to stand trial for alleged hate crime attack near synagogue**

A Seattle resident who allegedly tried to run over two men last November near a synagogue in a Jewish neighborhood in the Wilshire area while yelling anti-Semitic remarks was ordered Wednesday to stand trial. Los Angeles Superior Court Judge Deborah S. Brazil found sufficient evidence to require Mohamed Abdi Mohamed, 33, to stand trial on two counts each of attempted murder and assault with a deadly weapon - a vehicle - along with a hate crime allegation.

[City News Service](#)

### **Deputy pleads guilty to leaving gun in 8-year-old son's backpack, sentenced to community service**

A Los Angeles County sheriff's deputy who left a gun in his 8-year-old son's backpack a year ago pleaded guilty Wednesday to an infraction and was immediately sentenced to 80 hours of community service. Manuel Murillo, 37, was off-duty when he put the loaded service weapon in his son's backpack last April 11 by mistake, then dropped off the child with a caretaker, according to his attorney, Michael D. Schwartz.

[City News Service](#)

### **District Attorney's Office to honor, empower victims at 2019 Victims' Rights March and Rally**

The Orange County District Attorney's Office invites members of the community to the Victims' Rights March on April 8, 2019. The event, held as part of National Crime Victims' Rights Week, is an opportunity to honor victims and listen to survivors tell their stories of how they are moving forward and reshaping their lives - and how they continue to fight for victims' rights. This year's theme is "Victims Fighting for Justice."

[Orange County Breeze](#)

### **The bizarre story of the L.A. dad who exposed the college admissions scandal**

Morrie Tobin was in Boston to cut the deal of his life. It was early April last year. A few weeks before, federal agents had descended on the multimillion-dollar home Tobin shares with his wife and some of their six children in Hancock Park, a moneyed Los Angeles enclave. Warrant in hand, the agents searched the French chateau-style mansion for financial records and other evidence to nail Tobin, the suspected ringleader of a stock scam that defrauded investors of millions of dollars.

[Los Angeles Times](#)

## **Criminal Justice/Public Safety**

**Why police academies are letting recruits down (and how to fix it)**

Today's entry-level police officer must be better prepared emotionally, physically and technically to meet the herculean challenges of modern-day law enforcement and the often-unrealistic performance expectations we demand from officers. While these challenges and demands are drastically different from previous decades, training delivery methods in academies have remained relatively stagnant.

[PoliceOne](#)

### **Tesla vandal arrested after footage of incident was captured on Sentry Mode**

Tesla's new Sentry Mode is quickly proving useful as a woman who vandalized a Tesla vehicle was arrested after the footage of the incident was captured through Sentry Mode and reported to the police by the owner. Over the last year, we reported an uptick in break-ins involving Tesla vehicles. The automaker reacted by releasing its own dashcam feature using the Autopilot cameras around its vehicles.

[Electrek](#)

### **OC sheriff releases statistics on ICE detainees**

Orange County sheriff's officials Wednesday released department statistics showing that in 2018, the first year of the so-called Sanctuary State law, the agency handed off 717 of the county jail's inmates to federal immigration authorities. The law prevents the sheriff's department from turning over inmates to ICE within the jail, but deputies have gotten around that by posting the release date of inmates on the jail website, which gives the federal agency a chance to track when an ICE detainee is going to be released and pick them up as they walk out of jail.

[City News Service](#)

## **Policy & Legal Issues**

### **Why California's proposed law on deadly police force isn't as tough as it seems**

In the aftermath of several controversial police shootings in California, activists and victims' families have hoped their anguish would lead to action. They have protested, pleaded and lobbied for a law that would clear long-standing hurdles to criminal prosecution in some cases. But the focus of their hopes - a bill facing its first public hearing next week - may come up short.

[Los Angeles Times](#)

### **The troubling limits of the 'great crime decline'**

New York University sociologist Patrick Sharkey opened his revelatory 2018 book *Uneasy Peace: The Great Crime Decline, the Renewal of City Life, and the Next War on Violence* by calling the dramatic fall in violence in American cities since the early 1990s a "fundamental change in the nature of U.S. urban life," one that "no one predicted and that many people still do not believe."

[Citylab](#)

### **Legalized marijuana linked to a sharp rise in car crashes**

There has been an increase by up to 6 percent in the number of highway crashes in four of the states where the recreational use of marijuana has been legalized, according to a pair of new studies. The new reports do not prove there's a direct risk caused by the use of marijuana among motorists, but they raise caution flags, especially since there is no easy way to test drivers to be sure if they are, in fact, under the influence of THC, the active ingredient in marijuana, said David Harkey, president of the Insurance Institute for Highway Safety's Highway Loss Data Institute.

[NBC News](#)

### **After recreational weed has been legal for a year, cops are still figuring out DUIs**

A year after recreational marijuana became legal, cops and prosecutors are still dealing with the question: what is considered "legally impaired" when it comes to pot? Point .08 is the limit for drunken driving but testing for marijuana and other drugs that could impair a driver is not as clear cut. Specially trained drug recognition, or DRE officers like Brian Duncan look for clues and things that affect the body differently than alcohol.

[NBC4 Los Angeles](#)

### **Sacramento's 'community of victims' fight law shortening sentences for young killers**

They are a community now, sharing a bond known only by those whose lives have been ravaged by violent crime. Nicole Clavo lost a young son, killed by a gunshot three years ago as he sat at a north Sacramento intersection in a car full of his high school football teammates. The alleged gunman was 15. Victoria Hurd's mother and her mother's husband were attacked as they slept in 2013, murdered, then mutilated in the bedroom of their Davis condominium.

[Sacramento Bee](#)

### **The criminal justice system's algorithms need transparency**

The use of risk assessment algorithms in our nation's criminal justice system is expanding. The notion of this sounds innocent enough and maybe even pretty cool - a technologically advanced method solving the inequality in how people are handled after an arrest. Thanks to continuing advancements, building these models is now easier than ever before.

[Law360](#)

### **U.S. Supreme Court affirms constitutionality of bail, but CA still in legal bail limbo**

For four years activist Plaintiffs lawyers have been suing smaller cities arguing that the existing bail system is unconstitutional because it

violates the principle of equal protection under the law. In San Francisco, such a lawsuit claims, "Wealthy arrestees purchase their freedom by paying an arbitrary amount set by the bail schedule. Poor arrestees must languish behind bars until the resolution of their case, simply because they cannot afford to pay a pre-determined sum of money."

[California Globe](#)

### **Date rape isn't a violent crime in California. Seriously**

Under current California law, more than 20 clearly violent crimes aren't classified as violent, including rape of an unconscious person, trafficking a child for prostitution, assault with a deadly weapon and domestic violence. You can pimp a child for sex, beat a spouse or rape a young woman who passes out at a frat party, and it's not considered a violent offense under state law, and that's offensive.

[CALmatters](#)

### **LA's black market pot shops could disappear from Weedmaps if legal sellers get their way**

More than a year after recreational marijuana sales became legal in California, cannabis businesses that are following state rules are struggling to compete with a black market that's still thriving. Now, legal shop owners are backing a new state assembly bill that would stop websites from hosting ads for unlicensed weed businesses.

[LAist](#)

## **Death Penalty**

### **Assemblyman Lackey proposes bill to protect victims over death row killers**

Assemblyman Tom Lackey (R-Palmdale) is livid that Gov. Gavin Newsom prioritized death row killers in his recent reprieve on the 737 killers on death row, over the actual victims and families of victims. "The people on death row are not the victims," Lackey said in an interview. "They are not who the state should be working to protect. They have abused, they have raped, they have kidnapped, they have tortured, and some of them have even murdered their own children."

[California Globe](#)

### **For Gavin Newsom, and most Democrats, rule of law is an adjustable state of mind**

A few months ago, Gavin Newsom, during his campaign for governor of California, declared that the death penalty was the law of the land. He said he would respect the clearly expressed will of California voters and would not obstruct the enforcement of the death penalty. Now, though, the election is over, Newsom is the governor of our most populous state and he reserves the right to have a change of heart.

[Olean Times Herald](#)

## **Deputy District Attorneys release the 'Death Penalty Exhausted Appeals'**

The Association of Deputy District Attorneys just released their first set of blogs focusing on California's murderers on death row. Recently, Gov. Gavin Newsom signed an order to reprieve all 737 prisoners on death row. His plan is to suspend all executions as long as he is governor... ADDA's main goal is to make sure that doesn't happen. Michele Hanisee is the President of the Association of Los Angeles Deputy District Attorneys, and represents nearly 1,000 Deputy District Attorneys who work for the County of Los Angeles.

[KFI AM 640](#)

## **Could Gov. Gavin Newsom's death penalty moratorium mean life for state GOP in 2020?**

California Republicans hope voters will dish out some punishment to Democrats next year, following Gov. Gavin Newsom's reprieve for the state's death-row inmates. Leaders of the state GOP believe the public is solidly in favor of the death penalty and that their party can win back some power by turning Newsom's death penalty moratorium into an election-year attack on vulnerable Democratic incumbents.

[Riverside Press-Enterprise](#)

## **Californians voted twice in 2016 in favor of the death penalty. That matters more than poll results**

To the editor: A Public Policy Institute of California poll finds that people would rather have life without parole than the death penalty imposed as the punishment for first-degree murder. The "polls" also predicted that Hillary Clinton would be president - how did that work out? Here's an idea: Let's actually put the question to the voters.

[Letters/Los Angeles Times](#)

## **Crime**

### **Suspect in Nipsey Hussle murder being held on \$7 million bail**

The man arrested as a suspect in the slaying of rapper Nipsey Hussle is in custody Wednesday in lieu of \$7 million bail amid reports that he has a violent criminal history. Eric Holder, 29, was arrested around 1 p.m. Tuesday in the 9000 block of Artesia Boulevard in Bellflower by Los Angeles County sheriff's deputies after a witness called authorities to report seeing a person believed to be Holder.

[My News LA](#)

### **Bus driver who crashed into parked cars arrested on suspicion of DUI**

An on-duty Long Beach bus driver was arrested on suspicion of driving under the influence of alcohol when he hit several parked cars with a city bus early Monday morning, police said. Long Beach police officers responded to a call of a traffic collision around midnight near the intersection of Pacific Avenue and Anaheim Street, authorities said.



[Los Angeles Times](#)

### **17-year-old facing possible murder charges in fatal crash in Woodland Hills**

A 17-year-old boy was arrested and may face murder charges following a crash that left one person dead and several people injured on Friday night in Woodland Hills, according to the Los Angeles Police Department. The boy, who has not been identified, is suspected of driving a 2019 Mercedes-Benz recklessly for several blocks before running a red light and crashing into a Toyota Tacoma at the intersection of Winnetka Ave. and Ventura Blvd., police say.

[NBC4](#)

### **After Rafael Reyna viciously attacked in Dodger Stadium parking lot, fans call for better security**

Police are still looking for a man who attacked 45-year-old Rafael Reyna in the Dodger Stadium parking lot, leaving him on life support with a fractured skull. The suspect reportedly confronted Reyna as he walked to his car after Friday night's extra innings game against the Arizona Diamondbacks. Reyna was on the phone with his wife, Christel, when the attack happened.

[CBS LA](#)

### **91-year-old Tarzana woman riding again after community replaces stolen tricycle**

A 91-year-old Tarzana woman refuses to let a thief slow her down, and now she's thanking the people who replaced her stolen tricycle. Someone stole Louise Bianco's tricycle after she rode it to a fitness class at Pierce College. This wasn't just any scooter, it helped her get around. Louise had ridden 25,000 miles on it! "I do it for exercise, and I do it because it's beautiful," Bianco said.

[ABC7](#)

### **California man on parole for child sex crimes accused of sexually assaulting girl on playground**

A registered sex offender has been arrested after being accused of sexually assaulting a female student at an elementary school playground in Torrance, police announced Monday. The girl told one of her parents she had been sexually assaulted on the playground of Lincoln Elementary School last Thursday morning, according to a Torrance Police Department news release.

[KPLR](#)

### **Police use bolt cutters to reach trapped Hollywood burglar**

Police had to use bolt cutters to reach a burglary suspect who got stuck while trying to escape officers in a Hollywood shopping center early Tuesday morning. According to Los Angeles police, at around 1 a.m., officers responded to a burglary call at a shopping center in the 900 block of Western Avenue, near Santa Monica Boulevard, to find the

suspect on the roof of a business.

[CBS LA](#)

## **Los Angeles County Sheriff**

### **L.A. County Sheriff Alex Villanueva reinstates four more fired deputies**

Los Angeles County Sheriff Alex Villanueva has reinstated at least six deputies who were previously discharged, according to county documents obtained by The Times. Villanueva has previously defended his department's decisions to rehire two deputies fired for misconduct - one accused of assaulting and harassing a woman and lying about it, the other for using unreasonable force during an arrest. But The Times found four additional rehires, a revelation that is likely to stoke more scrutiny from county supervisors and department watchdogs who have called on the sheriff to stop the practice.

[Los Angeles Times](#)

### **Deputy fired for using unreasonable force during arrest has been reinstated**

A Los Angeles County sheriff's deputy who was fired in 2018 for using unreasonable force while arresting a man in Lancaster in 2016 has been reinstated, it was reported Wednesday. This is the second deputy who was fired prior to Sheriff Alex Villanueva's election to return to duty since the new sheriff took office. Michael Courtial was fired last June but has since been reinstated and assigned to the sheriff's Palmdale station, the Los Angeles Times reported.

[City News Service](#)

### **Police interview of Deputy Caren Mandoyan's ex-girlfriend**

Accusations of domestic violence upended the career of Los Angeles County Sheriff's Department Deputy Caren Carl Mandoyan and put newly elected Sheriff Alex Villanueva on a collision course with the L.A. County Board of Supervisors. Mandoyan's ex-girlfriend, a fellow deputy, filed a temporary restraining order against him in 2015, dissolved it two weeks later, resigned from the department in 2017 and now declines to comment on the matter.

[ABC7](#)

### **L.A. County Sheriff's Deputy whose rehiring sparked controversy speaks about domestic abuse claims that got him fired**

Though a Los Angeles County appeals board upheld then-Sheriff Jim McDonnell's decision to fire Deputy Caren Carl Mandoyan in 2016 after he was accused of stalking and domestic abuse, according to the Los Angeles Times, Mandoyan spoke out Friday against the claims as his rehiring last December by newly instated Sheriff Alex Villanueva is putting renewed focus on the case - including new allegations that Mandoyan belongs to a violent clique within the department known as the Reapers.

[KTLA](#)

### **De-coding the case files of rehired LA Sheriff's Deputy Carl Mandoyan: Part 1 - Command & control**

The past two weeks have been active ones in the unendingly controversial case of Los Angeles County Sheriff's Deputy Caren Carl Mandoyan, the deputy fired by the LASD in 2016 under former Sheriff Jim McDonnell, who was rehired early this year by Sheriff Alex Villanueva. Much of the controversy has pertained to the fact that Mandoyan was fired for alleged domestic abuse, along with reported stalking and bullying behavior against his ex-girlfriend, who was also a deputy at the time.

[Witness LA](#)

## **Los Angeles County**

### **LA approves permanent street memorial signs at sites of deadly bicycle crashes around city**

Fatal bicycle crashes on L.A. streets have long been marked by so-called 'ghost bikes', bicycles painted white in memory of a lost life, flanked by flowers and other tokens to form ad-hoc public memorials. They serve as a haunting reminder of the vulnerability of cyclists on city streets, but tend to disappear in time.

[Los Angeles Daily News](#)

### **L.A. County crews who allegedly used Darknet to traffic narcotics face federal criminal conspiracy charges**

Members of two alleged Los Angeles County crime rings have been charged in separate federal criminal cases alleging they conspired to use the Darknet to illicitly and secretly sell methamphetamine and other illegal narcotics nationwide, including one shipment of heroin in a stuffed animal that led to the fatal overdose of a customer in Tennessee.

[FBI](#)

### **With business groups allied against it, L.A. parcel tax faces big hurdle**

Three Los Angeles area business associations have signed the official ballot argument opposing L.A. Unified's sizable 12-year parcel tax on the June 4 ballot - compounding the district's challenge of getting a two-thirds majority required to pass it. The opponents include the influential Los Angeles Area Chamber of Commerce. Parcel tax backers had hoped that business community leaders would take no position, if they couldn't support a parcel tax.

[EdSource](#)

### **LA's City Council District 12 seat is up for grabs. Here are the 15 people vying to fill it**

When Mitch Englander resigned his L.A. City Council seat last October, District 12 - which includes Chatsworth, North Hills, Northridge, Granada

Hills, Porter Ranch, Reseda, Sherwood Forest and West Hills - was left with temporary representation (Greig Smith, his former chief of staff, stepped into the role). Englander was the lone Republican on the 15-member council.

[LAist](#)

### **Los Angeles County Supervisor Janice Hahn will seek re-election in 2020**

Hews Media Group-Los Cerritos Community News has exclusively learned that Los Angeles County 4th District and Chair of the Board of Supervisors Janice Hahn will seek reelection in 2020. Hahn told HMG-LCCN publisher Brian Hews during a wide ranging interview this morning. "This is much more fulfilling than my Congressional position. Washington was, and still is, in gridlock. I can get things done here and I've accomplished a lot, but I want to accomplish much more."

[Hews Media Group](#)

## **Convictions/Sentences/Parole**

### **Assault with a deadly weapon inmate walks away from conservation camp in Antelope Valley**

An inmate in custody for assault with a deadly weapon walked away from a conservation camp in the Antelope Valley early Tuesday. Jon Nicholas, 37, was at Fenner Canyon Conservation Camp in Valyermo, but at 4:20 a.m., staff discovered that he was missing. Officers immediately began searching the camp, but he was not found.

[KTLA](#)

### **Man sentenced to 40 years for molesting relative under 8 years old for years**

A 58-year-old man who repeatedly sexually assaulted a young relative in Temecula was sentenced Wednesday to 40 years to life in state prison. Jose Benito Fabian was convicted in December of four counts of lewd acts on a child under 10 years old. Riverside County Superior Court Judge John Molloy imposed the sentence required by law for the offenses.

[NBC4](#)

## **Consumer News**

### **Walmart misled customers with oversized containers, California prosecutors say. Now it'll pay**

Walmart misled customers by packaging some of its health and beauty products in oversized containers, prosecutors say, and now the company will pay \$495,000 in costs and penalties. The Fresno County District Attorney's Office announced in a news release Wednesday that its office, along with five other California district attorney's offices, reached a settlement with Walmart Inc. in a civil enforcement action.

[Fresno Bee](#)

### **Amazon corporate counsel says counterfeits will remain**

When you make a claim, you better make sure it's true and that you're actually doing what you claim you're doing. When you get caught in a lie or exaggeration, your credibility is destroyed. That's happened to Amazon, who is facing an avalanche of counterfeit and fraudulent product sales, scams, and fake reviews, along with allegations of data leaks and employee bribes.

[The Counterfeit Report](#)

### **Trump puts Amazon, Alibaba on notice for sale of counterfeit goods**

President Donald Trump put Amazon, eBay and Alibaba and other online marketplaces on notice Wednesday, signing a memorandum that aims to curb the sale of counterfeit items online. "This is a shot across the bow to those companies. If you don't clean it up, then the government will," Trump trade advisor Peter Navarro told reporters.

[CNBC](#)

### **Facebook to finally explain the decisions of its news feed algorithm**

Facebook will finally begin telling its users why posts appear in their news feeds as it seeks to assuage public concerns about the spread of fake news and its influence over billions of people's reading habits. The social network will today introduce a button on each post revealing why users are seeing it, including factors such as whether they have interacted often with the person who made the post or whether it is popular with other users.

[The Telegraph](#)

## **California/National**

### **Funds from ballot initiative help newly released prisoners find a home in Los Angeles**

As Latanja Madison's release date from prison inched closer, she felt more terrified than elated. During a decade behind bars at the California Institution for Women in Corona, the 55-year-old Madison underwent multiple orthopedic surgeries and now uses a walker. Her immediate family members passed away during her incarceration, creating grave doubts she would have a support system.

[Witness LA](#)

### **Walters: California Gov. Newsom gets surprising grade just 90 days in**

Gavin Newsom coasted into the governorship last year, defeating his Republican rival by more than a 3-2 margin. It seems a little odd, therefore, that three months into his governorship, he enjoys only tepid popular support. A new poll by the Public Policy Institute of California found that just 45 percent of all adults, and the same percentage of



likely voters, approve of Newsom's governorship so far.

[Mercury News](#)

### **State warns NASA it must uphold agreement to clean up its part of Santa Susana field lab**

For the second time in two months, the California Department of Toxic Substances Control has warned another federal agency to stick to a 2010 agreement to fully clean up its portion of the contaminated Santa Susana Field Laboratory outside Simi Valley. In late January, the state agency, which is overseeing the long-planned, much-delayed cleanup, put the U.S. Department of Energy on notice not to waver from the legally binding agreement.

[Ventura County Star](#)

### **Saudis hacked Jeff Bezos' phone and leaked racy texts, investigator claims**

Saudi Arabia nationals hacked the phone of Amazon CEO Jeff Bezos and were the source of private information that was published by The National Enquirer, according to longtime security consultant Gavin de Becker, who works for Bezos. In an op-ed in The Daily Beast, de Becker said that he and other security experts probed how anyone could access Bezos' private phone messages to his girlfriend, Lauren Sanchez, after some of them were published on The National Enquirer and became the subject of an extortion plot.

[Fox News](#)

### **Chinese woman carrying malware allegedly got into Mar-a-Lago**

A woman carrying two Chinese passports and a device containing computer malware lied to Secret Service agents and briefly gained admission to President Donald Trump's Mar-a-Lago club over the weekend during his Florida visit, federal prosecutors allege in court documents. Yujing Zhang, 32, approached a Secret Service agent at a checkpoint outside the Palm Beach club early Saturday afternoon and said she was a member who wanted to use the pool, court documents said. She showed the passports as identification.

[AP](#)

### **California's Attorney General says immigration should be decriminalized**

Unauthorized immigration should be decriminalized, California Attorney General Xavier Becerra (D) said in an interview with HuffPost on Friday, becoming one of the few prominent Democrats to challenge a key aspect of the Trump administration's crackdown. "They are not criminals," Becerra said of migrants who cross without authorization.

[HuffPost](#)

## **Guns**

### **LAPD asks to cancel citizens' concealed weapons permits**

The Los Angeles Police Department has moved to cancel most of the few remaining concealed weapons permits in civilian hands, according to new filings in a decades-old legal case. Chief Michel Moore said in a sworn declaration he did not believe a group of people who obtained so-called CCWs as the result of a 1994 lawsuit were still entitled to the permits, because it was unlikely the individuals still faced extraordinary physical danger to their lives.

[NBC4](#)

### **NRA and CRPA oppose California's request to immediately halt "large-capacity" magazine ruling**

On Tuesday, April 2, NRA and CRPA filed an opposition to California's request seeking an immediate stay of enforcement of Friday's decision in the case of *Duncan v. Becerra*, which found California's restrictions against so-called "large-capacity" magazines unconstitutional and unenforceable.

[NRA-ILA](#)

## **Public Records**

### **Release of Santa Maria police officer misconduct records on hold, pending open court cases**

Citing nearly a dozen open legal challenges statewide to a new police transparency law, the city of Santa Maria won't release records detailing investigations into confirmed instances of police misconduct that occurred prior to Jan. 1 until the lawsuits are resolved. The city response follows a public records request by the Santa Maria Times in January seeking records covered by SB 1421, a landmark state law passed by the California legislature last year that aims to bring more transparency to internal investigations of police misconduct.

[Santa Maria Times](#)

### **California AG slammed on police transparency record**

Press and free speech advocates blasted California Attorney General Xavier Becerra on Monday over his approach to government transparency and law enforcement accountability. "I think the Attorney General's office has behaved disturbingly and inappropriately," said David Snyder, the director of the First Amendment Coalition, a California-based nonprofit dedicated to government transparency and press freedom.

[Courthouse News Service](#)

### **Court upholds broad release of police misconduct records in California**

A new law granting public access to police misconduct records and investigations of officers' use of force applies to all records that existed when the law took effect this year no matter when they were created, a state appeals court has ruled in a decision with immediate statewide impact. Police unions in numerous localities, including Contra Costa

County and five of its cities in the current case, sued to block release of records created before 2019.

[San Francisco Chronicle](#)

### **Prodded by court ruling, Sonoma County Sheriff relents and agrees to release police records**

The Sonoma County Sheriff's Office said Wednesday that within a week it will begin releasing police records it had previously withheld, following an appeals court decision last week on the issue and a legal threat to the county Tuesday. California news organizations, including The Press Democrat, had requested the records under a new state law known as Senate Bill 1421.

[The Press Democrat](#)

## **Corrections**

### **State prison officials reviewing request to allow imprisoned father to see Oakland son in hospital**

State prison officials are considering a request to allow the imprisoned father of an Oakland boy on life support to visit his son as he clings to life in the hospital, authorities said Monday. Four-year-old Navaun Jackson shot himself in the head last week and has been in critical condition at UCSF Benioff Children's Hospital in Oakland, his family said. Family members pleaded with Gov. Gavin Newsom over the weekend to allow the boy's father, Nathan Jackson, to visit his son in the hospital.

[San Francisco Chronicle](#)

## **Homeless**

### **Legislation would allow West L.A. Armory to operate as shelter year round**

Federal legislation introduced Monday would allow the West Los Angeles National Guard Armory to operate year-round as a homeless shelter instead of only during the winter months. The bill is sponsored by Sens. Dianne Feinstein and Kamala Harris, D-Calif., and Rep. Ted Lieu, D-Torrance. In a letter to the Senate and House Armed Services Committees, they requested that the legislation be included in the next National Defense Authorization Act.

[My News LA](#)

### **Despite Measure H, cities and agencies struggle to get money for homeless services; LA County to investigate**

Los Angeles County cities and homeless services providers could soon more easily access Measure H funding. The Los Angeles County Board of Supervisors approved a motion by supervisors Kathryn Barger and Hilda Solis Tuesday directing staff to report back in 45 days with recommendations to streamline the process through which the Los Angeles Homeless Services Authority grants Measure H dollars to cities and service providers.

[San Gabriel Valley Tribune](#)

### **Citing 'frustration' on homeless crisis, San Fernando, San Gabriel Valley county leaders call for more collaboration with cities**

The Los Angeles County Board of Supervisors voted Tuesday to find ways to work more collaboratively with dozens of cities to solve the problem of homelessness. Supervisor Kathryn Barger recommended streamlining processes to grant Measure H dollars to local cities and homelessness agencies.

[City News Service](#)

## **Pensions**

### **Cities struggle to cut retirement health care costs**

The cost of providing health care for retired state and local government employees, a benefit rarely found in the private sector, was mostly ignored until around 2007, when a government accounting board said the debt should be calculated. So little attention was paid to the growing retiree health care debt that it's still called "Other Post Employment Benefits" in government reports, a catchall phrase for benefits beyond pensions that could include life, disability, and long-term care insurance if offered.

[Calpensions](#)

### **California beats back challenge of CalSavers retirement plan**

California's state-sponsored retirement plan for private workers cleared a major hurdle Friday, with a federal judge tossing a lawsuit brought by an influential anti-tax group that hoped to kill the program before its July launch date. Lawmakers passed the retirement plan, now called CalSavers, in 2016 with the goal of extending benefits to an estimated 7.5 million workers that aren't offered pensions or 401(k) plans by their employers.

[Courthouse News Service](#)

### **Marin Voice: Public pension debate is about values and priorities**

The ongoing discussion of public employee pensions is currently focused on litigation before our state's Supreme Court. It may come as a surprise, but I agree with Jody Morales (Marin Voice, March 8) that most observers expected the court's recent decision in the Cal Fire case on air time to be a narrow one. We at Marin Association of Public Employees (MAPE) did.

[Marin Independent Journal](#)

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ ggiguire@ci.sunnyvale.ca.us](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](#)



**From:** [Association of Deputy District Attorneys](#)  
**To:** [fggurina@sunnyvale.ca.gov](mailto:fggurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for April 8, 2019  
**Date:** Monday, April 08, 2019 5:04:00 AM

---

Having trouble viewing this email? [Click here](#)



## Courts & Rulings

### **Verdict affirmed in favor of city in action alleging false arrest of videographer**

A freelance videographer who was taken into custody after he continued

to walk toward City Hall as persons encamped on the grounds as part of Occupy Los Angeles were being dispersed, and became combative with police, yesterday lost his bid for reversal of a judgment in favor of the City of Los Angeles and several of its officers in his action for false arrest and a civil rights violation.

[Metropolitan News-Enterprise](#)

### **Man asked incriminating questions by police was not under detention**

A pedestrian who changed direction when he spotted a patrol car, stuck something in his pocket, and darted onto the driveway of an apartment complex, was not "detained" when officers questioned him as to what he had in his pocket and he admitted possessing a "meth pipe," the Court of Appeal for this district has held, affirming the denial of his suppression motion.

[Metropolitan News-Enterprise](#)

### **Ninth Circuit upholds 27-year sentence for Russian hacker**

A Ninth Circuit panel upheld the 27-year prison sentence of a Russian computer hacker who was extradited to the United States while on vacation with his family in the Maldives to face charges he stole credit card numbers and millions of dollars. Roman Seleznev claimed the U.S. government kidnapped him when he was finally arrested several years after some of his most lucrative heists.

[Courthouse News Service](#)

### **C.A. orders publication of portion of opinion lifting prior restraint**

The Court of Appeal for this district has decided to publish that portion of its Feb. 26 opinion in which it holds that a domestic violence restraining order against a Los Angeles attorney is an unconstitutional prior restraint in the extent that it forbids him from posting "anything" on Facebook about the case in which he is being sued for divorce.

[Metropolitan News-Enterprise](#)

### **Lawyer fingerprinting in this state turns up over 2,200 convictions unknown to bar**

A California court rule requiring lawyers to be fingerprinted has turned up more than 6,000 criminal history reports, including more than 2,200 convictions previously unknown to the state bar. The 2,200 unknown convictions include 20 unreported felonies, Above the Law reports. The number of convictions likely will increase as more lawyers get fingerprinted ahead of an April 30 deadline.

[ABA Journal](#)

### **Judge Anderson barred from third sentencing of defendant**

The Ninth U.S. Circuit Court of Appeals yesterday, for a second time, remanded a case for resentencing, declaring that the matter must be heard by a judge of the District Court for the Central District of California other than Percy Anderson who, the three-judge panel said,

failed to adhere to the appeals court's 2016 opinion in the case.

[Metropolitan News-Enterprise](#)

### **Justices rule against Missouri inmate with rare health issue**

Missouri can execute an inmate who argued his rare medical condition will result in severe pain if he is put to death by lethal injection, the Supreme Court ruled Monday. The justices split along ideological lines in ruling 5-4 against inmate Russell Bucklew, who is on death row for a 1996 murder. The court's five conservative justices rejected Bucklew's argument that subjecting him to lethal injection would violate the Constitution's ban on cruel and unusual punishment.

[Kansas City Star](#)

### **Judge dismisses suit based on San Bernardino terrorist attack**

A federal judge in Santa Ana Monday dismissed a lawsuit filed by relatives of three of the victims killed in the 2015 terrorist attack in San Bernardino, saying the tort claim of negligence is outweighed by the government's sovereign immunity. Relatives of shooting victims Nicholas Thalasinis, Sierra Clayborn and Tin Nguyen accused the government of negligence for failing to investigate Syed Rizwan Farook and Tashfeen Malik, the husband-and-wife jihadis who killed 14 people and wounded two dozen others during a Christmas party at the Inland Regional Center on Dec. 2, 2015.

[My News LA](#)

### **Prop. 63: Federal judge declares California's ban on high-capacity gun magazines unconstitutional**

A federal judge on Friday declared unconstitutional a key provision of California's Proposition 63 that banned possession of high-capacity gun magazines often used in mass shootings, ensuring that the voter-approved prohibition will remain tied up in court for some time to come. San Diego-based U.S. District Judge Roger Benitez wrote in his 86-page decision, upholding a lawsuit against the proposed ban of magazines holding more than 10 rounds, that such a statute "hits at the center of the Second Amendment and its burden is severe."

[San Francisco Chronicle](#)

### **Public has access to pre-2019 police personnel files**

Amendments to a statute which increases public access to personnel files of peace officers may permissibly be applied to records that were in existence prior to the Jan. 1 effective date of the legislation, the First District Court of Appeal has held. Div. Four's decision comes in a "By the Court" order denying petitions for writs of supersedeas filed by the Walnut Creek Police Officers' Association and others in five consolidated matters.

[Metropolitan News-Enterprise](#)

### **The far-reach of the 9th Circuit's decision to stand firm on landmark homeless case**

If you're a homeless person with nowhere to go but a city sidewalk, park or other public space, can authorities force you off the street? This week, federal judges again said: "No." That answer - the same given by three judges on the 9th Circuit Court of Appeals back in September - came after yet another review of a case that's been making its way through the courts for a decade.

[LAist](#)

### **Challenge to barring of 2018 ballot designation is moot**

The Fourth District Court of Appeal has dismissed as moot a challenge by an unsuccessful candidate in 2018 for the post of district attorney of Orange County to the denial of her use of the ballot designation, "Civil Rights Attorney." Div. Three on Friday, in an unpublished opinion by Justice Raymond J. Ikola, spurned erstwhile candidate Lenore L. Albert's appeal of orders by Orange Superior Court Judge Craig L. Griffin, finding no justification for addressing the merits notwithstanding mootness.

[Metropolitan News-Enterprise](#)

### **Jury says Pomona police officer did not obstruct justice, mistrial declared on charges of lying to FBI**

A federal jury Wednesday found the Pomona police officer who investigated the violent arrest of a teenage boy at the Los Angeles County Fair in 2015 not guilty of deterring the boy and his mother from coming forward during the investigation - but jurors did not reach unanimous verdicts on two charges of lying to the FBI.

[San Gabriel Valley Tribune](#)

## **Prosecutions/Prosecutors**

### **L.A., San Joaquin County prosecutors to clear thousands of pot convictions**

Los Angeles and San Joaquin county prosecutors announced a plan Monday to automatically clear more than 50,000 marijuana-related convictions eligible for reconsideration in light of the state's legalization of pot under Proposition 64. District attorneys from both counties said they will partner with nonprofit Code for America, which has developed a computerized system known as Clear My Record that quickly identify cannabis convictions eligible to be cleared.

[My News LA](#)

### **Orange County DA charges 4 women in connection with multistate prostitution ring**

Authorities say they have charged four women with running a prostitution network in California, Nevada and Utah that netted tens of thousands of dollars a month. Orange County District Attorney Todd Spitzer said Wednesday the women had a website that appeared to be a legitimate service but was not. The four are charged with pimping and pandering and the two alleged ringleaders are also charged with conspiracy.

[KTLA](#)

### **Man ordered to stand trial for alleged hate crime attack near synagogue**

A Seattle resident who allegedly tried to run over two men last November near a synagogue in a Jewish neighborhood in the Wilshire area while yelling anti-Semitic remarks was ordered Wednesday to stand trial. Los Angeles Superior Court Judge Deborah S. Brazil found sufficient evidence to require Mohamed Abdi Mohamed, 33, to stand trial on two counts each of attempted murder and assault with a deadly weapon - a vehicle - along with a hate crime allegation.

[City News Service](#)

### **Deputy pleads guilty to leaving gun in 8-year-old son's backpack, sentenced to community service**

A Los Angeles County sheriff's deputy who left a gun in his 8-year-old son's backpack a year ago pleaded guilty Wednesday to an infraction and was immediately sentenced to 80 hours of community service. Manuel Murillo, 37, was off-duty when he put the loaded service weapon in his son's backpack last April 11 by mistake, then dropped off the child with a caretaker, according to his attorney, Michael D. Schwartz.

[City News Service](#)

### **District Attorney's Office to honor, empower victims at 2019 Victims' Rights March and Rally**

The Orange County District Attorney's Office invites members of the community to the Victims' Rights March on April 8, 2019. The event, held as part of National Crime Victims' Rights Week, is an opportunity to honor victims and listen to survivors tell their stories of how they are moving forward and reshaping their lives - and how they continue to fight for victims' rights. This year's theme is "Victims Fighting for Justice."

[Orange County Breeze](#)

### **The bizarre story of the L.A. dad who exposed the college admissions scandal**

Morrie Tobin was in Boston to cut the deal of his life. It was early April last year. A few weeks before, federal agents had descended on the multimillion-dollar home Tobin shares with his wife and some of their six children in Hancock Park, a moneyed Los Angeles enclave. Warrant in hand, the agents searched the French chateau-style mansion for financial records and other evidence to nail Tobin, the suspected ringleader of a stock scam that defrauded investors of millions of dollars.

[Los Angeles Times](#)

## **Criminal Justice/Public Safety**

### **Why police academies are letting recruits down (and how to fix it)**



Today's entry-level police officer must be better prepared emotionally, physically and technically to meet the herculean challenges of modern-day law enforcement and the often-unrealistic performance expectations we demand from officers. While these challenges and demands are drastically different from previous decades, training delivery methods in academies have remained relatively stagnant.

[PoliceOne](#)

### **Tesla vandal arrested after footage of incident was captured on Sentry Mode**

Tesla's new Sentry Mode is quickly proving useful as a woman who vandalized a Tesla vehicle was arrested after the footage of the incident was captured through Sentry Mode and reported to the police by the owner. Over the last year, we reported an uptick in break-ins involving Tesla vehicles. The automaker reacted by releasing its own dashcam feature using the Autopilot cameras around its vehicles.

[Electrek](#)

### **OC sheriff releases statistics on ICE detainees**

Orange County sheriff's officials Wednesday released department statistics showing that in 2018, the first year of the so-called Sanctuary State law, the agency handed off 717 of the county jail's inmates to federal immigration authorities. The law prevents the sheriff's department from turning over inmates to ICE within the jail, but deputies have gotten around that by posting the release date of inmates on the jail website, which gives the federal agency a chance to track when an ICE detainee is going to be released and pick them up as they walk out of jail.

[City News Service](#)

## **Policy & Legal Issues**

### **Why California's proposed law on deadly police force isn't as tough as it seems**

In the aftermath of several controversial police shootings in California, activists and victims' families have hoped their anguish would lead to action. They have protested, pleaded and lobbied for a law that would clear long-standing hurdles to criminal prosecution in some cases. But the focus of their hopes - a bill facing its first public hearing next week - may come up short.

[Los Angeles Times](#)

### **The troubling limits of the 'great crime decline'**

New York University sociologist Patrick Sharkey opened his revelatory 2018 book *Uneasy Peace: The Great Crime Decline, the Renewal of City Life, and the Next War on Violence* by calling the dramatic fall in violence in American cities since the early 1990s a "fundamental change in the nature of U.S. urban life," one that "no one predicted and that many people still do not believe."

[Citylab](#)

### **Legalized marijuana linked to a sharp rise in car crashes**

There has been an increase by up to 6 percent in the number of highway crashes in four of the states where the recreational use of marijuana has been legalized, according to a pair of new studies. The new reports do not prove there's a direct risk caused by the use of marijuana among motorists, but they raise caution flags, especially since there is no easy way to test drivers to be sure if they are, in fact, under the influence of THC, the active ingredient in marijuana, said David Harkey, president of the Insurance Institute for Highway Safety's Highway Loss Data Institute.

[NBC News](#)

### **After recreational weed has been legal for a year, cops are still figuring out DUIs**

A year after recreational marijuana became legal, cops and prosecutors are still dealing with the question: what is considered "legally impaired" when it comes to pot? Point .08 is the limit for drunken driving but testing for marijuana and other drugs that could impair a driver is not as clear cut. Specially trained drug recognition, or DRE officers like Brian Duncan look for clues and things that affect the body differently than alcohol.

[NBC4 Los Angeles](#)

### **Sacramento's 'community of victims' fight law shortening sentences for young killers**

They are a community now, sharing a bond known only by those whose lives have been ravaged by violent crime. Nicole Clavo lost a young son, killed by a gunshot three years ago as he sat at a north Sacramento intersection in a car full of his high school football teammates. The alleged gunman was 15. Victoria Hurd's mother and her mother's husband were attacked as they slept in 2013, murdered, then mutilated in the bedroom of their Davis condominium.

[Sacramento Bee](#)

### **The criminal justice system's algorithms need transparency**

The use of risk assessment algorithms in our nation's criminal justice system is expanding. The notion of this sounds innocent enough and maybe even pretty cool - a technologically advanced method solving the inequality in how people are handled after an arrest. Thanks to continuing advancements, building these models is now easier than ever before.

[Law360](#)

### **U.S. Supreme Court affirms constitutionality of bail, but CA still in legal bail limbo**

For four years activist Plaintiffs lawyers have been suing smaller cities arguing that the existing bail system is unconstitutional because it

violates the principle of equal protection under the law. In San Francisco, such a lawsuit claims, "Wealthy arrestees purchase their freedom by paying an arbitrary amount set by the bail schedule. Poor arrestees must languish behind bars until the resolution of their case, simply because they cannot afford to pay a pre-determined sum of money."

[California Globe](#)

### **Date rape isn't a violent crime in California. Seriously**

Under current California law, more than 20 clearly violent crimes aren't classified as violent, including rape of an unconscious person, trafficking a child for prostitution, assault with a deadly weapon and domestic violence. You can pimp a child for sex, beat a spouse or rape a young woman who passes out at a frat party, and it's not considered a violent offense under state law, and that's offensive.

[CALmatters](#)

### **LA's black market pot shops could disappear from Weedmaps if legal sellers get their way**

More than a year after recreational marijuana sales became legal in California, cannabis businesses that are following state rules are struggling to compete with a black market that's still thriving. Now, legal shop owners are backing a new state assembly bill that would stop websites from hosting ads for unlicensed weed businesses.

[LAist](#)

## **Death Penalty**

### **Assemblyman Lackey proposes bill to protect victims over death row killers**

Assemblyman Tom Lackey (R-Palmdale) is livid that Gov. Gavin Newsom prioritized death row killers in his recent reprieve on the 737 killers on death row, over the actual victims and families of victims. "The people on death row are not the victims," Lackey said in an interview. "They are not who the state should be working to protect. They have abused, they have raped, they have kidnapped, they have tortured, and some of them have even murdered their own children."

[California Globe](#)

### **For Gavin Newsom, and most Democrats, rule of law is an adjustable state of mind**

A few months ago, Gavin Newsom, during his campaign for governor of California, declared that the death penalty was the law of the land. He said he would respect the clearly expressed will of California voters and would not obstruct the enforcement of the death penalty. Now, though, the election is over, Newsom is the governor of our most populous state and he reserves the right to have a change of heart.

[Olean Times Herald](#)

## **Deputy District Attorneys release the 'Death Penalty Exhausted Appeals'**

The Association of Deputy District Attorneys just released their first set of blogs focusing on California's murderers on death row. Recently, Gov. Gavin Newsom signed a order to reprieve all 737 prisoners on death row. His plan is to suspend all executions as long as he is governor... ADDA's main goal is to make sure that doesn't happen. Michele Hanisee is the President of the Association of Los Angeles Deputy District Attorneys, and represents nearly 1,000 Deputy District Attorneys who work for the County of Los Angeles.

[KFI AM 640](#)

## **Could Gov. Gavin Newsom's death penalty moratorium mean life for state GOP in 2020?**

California Republicans hope voters will dish out some punishment to Democrats next year, following Gov. Gavin Newsom's reprieve for the state's death-row inmates. Leaders of the state GOP believe the public is solidly in favor of the death penalty and that their party can win back some power by turning Newsom's death penalty moratorium into an election-year attack on vulnerable Democratic incumbents.

[Riverside Press-Enterprise](#)

## **Californians voted twice in 2016 in favor of the death penalty. That matters more than poll results**

To the editor: A Public Policy Institute of California poll finds that people would rather have life without parole than the death penalty imposed as the punishment for first-degree murder. The "polls" also predicted that Hilary Clinton would be president - how did that work out? Here's an idea: Let's actually put the question to the voters.

[Letters/Los Angeles Times](#)

## **Crime**

### **Suspect in Nipsey Hussle murder being held on \$7 million bail**

The man arrested as a suspect in the slaying of rapper Nipsey Hussle is in custody Wednesday in lieu of \$7 million bail amid reports that he has a violent criminal history. Eric Holder, 29, was arrested around 1 p.m. Tuesday in the 9000 block of Artesia Boulevard in Bellflower by Los Angeles County sheriff's deputies after a witness called authorities to report seeing a person believed to be Holder.

[My News LA](#)

### **Bus driver who crashed into parked cars arrested on suspicion of DUI**

An on-duty Long Beach bus driver was arrested on suspicion of driving under the influence of alcohol when he hit several parked cars with a city bus early Monday morning, police said. Long Beach police officers responded to a call of a traffic collision around midnight near the intersection of Pacific Avenue and Anaheim Street, authorities said.

[Los Angeles Times](#)

### **17-year-old facing possible murder charges in fatal crash in Woodland Hills**

A 17-year-old boy was arrested and may face murder charges following a crash that left one person dead and several people injured on Friday night in Woodland Hills, according to the Los Angeles Police Department. The boy, who has not been identified, is suspected of driving a 2019 Mercedes-Benz recklessly for several blocks before running a red light and crashing into a Toyota Tacoma at the intersection of Winnetka Ave. and Ventura Blvd., police say.

[NBC4](#)

### **After Rafael Reyna viciously attacked in Dodger Stadium parking lot, fans call for better security**

Police are still looking for a man who attacked 45-year-old Rafael Reyna in the Dodger Stadium parking lot, leaving him on life support with a fractured skull. The suspect reportedly confronted Reyna as he walked to his car after Friday night's extra innings game against the Arizona Diamondbacks. Reyna was on the phone with his wife, Christel, when the attack happened.

[CBS LA](#)

### **91-year-old Tarzana woman riding again after community replaces stolen tricycle**

A 91-year-old Tarzana woman refuses to let a thief slow her down, and now she's thanking the people who replaced her stolen tricycle. Someone stole Louise Bianco's tricycle after she rode it to a fitness class at Pierce College. This wasn't just any scooter, it helped her get around. Louise had ridden 25,000 miles on it! "I do it for exercise, and I do it because it's beautiful," Bianco said.

[ABC7](#)

### **California man on parole for child sex crimes accused of sexually assaulting girl on playground**

A registered sex offender has been arrested after being accused of sexually assaulting a female student at an elementary school playground in Torrance, police announced Monday. The girl told one of her parents she had been sexually assaulted on the playground of Lincoln Elementary School last Thursday morning, according to a Torrance Police Department news release.

[KPLR](#)

### **Police use bolt cutters to reach trapped Hollywood burglar**

Police had to use bolt cutters to reach a burglary suspect who got stuck while trying to escape officers in a Hollywood shopping center early Tuesday morning. According to Los Angeles police, at around 1 a.m., officers responded to a burglary call at a shopping center in the 900 block of Western Avenue, near Santa Monica Boulevard, to find the



suspect on the roof of a business.

[CBS LA](#)

## **Los Angeles County Sheriff**

### **L.A. County Sheriff Alex Villanueva reinstates four more fired deputies**

Los Angeles County Sheriff Alex Villanueva has reinstated at least six deputies who were previously discharged, according to county documents obtained by The Times. Villanueva has previously defended his department's decisions to rehire two deputies fired for misconduct - one accused of assaulting and harassing a woman and lying about it, the other for using unreasonable force during an arrest. But The Times found four additional rehires, a revelation that is likely to stoke more scrutiny from county supervisors and department watchdogs who have called on the sheriff to stop the practice.

[Los Angeles Times](#)

### **Deputy fired for using unreasonable force during arrest has been reinstated**

A Los Angeles County sheriff's deputy who was fired in 2018 for using unreasonable force while arresting a man in Lancaster in 2016 has been reinstated, it was reported Wednesday. This is the second deputy who was fired prior to Sheriff Alex Villanueva's election to return to duty since the new sheriff took office. Michael Courtial was fired last June but has since been reinstated and assigned to the sheriff's Palmdale station, the Los Angeles Times reported.

[City News Service](#)

### **Police interview of Deputy Caren Mandoyan's ex-girlfriend**

Accusations of domestic violence upended the career of Los Angeles County Sheriff's Department Deputy Caren Carl Mandoyan and put newly elected Sheriff Alex Villanueva on a collision course with the L.A. County Board of Supervisors. Mandoyan's ex-girlfriend, a fellow deputy, filed a temporary restraining order against him in 2015, dissolved it two weeks later, resigned from the department in 2017 and now declines to comment on the matter.

[ABC7](#)

### **L.A. County Sheriff's Deputy whose rehiring sparked controversy speaks about domestic abuse claims that got him fired**

Though a Los Angeles County appeals board upheld then-Sheriff Jim McDonnell's decision to fire Deputy Caren Carl Mandoyan in 2016 after he was accused of stalking and domestic abuse, according to the Los Angeles Times, Mandoyan spoke out Friday against the claims as his rehiring last December by newly instated Sheriff Alex Villanueva is putting renewed focus on the case - including new allegations that Mandoyan belongs to a violent clique within the department known as the Reapers.

[KTLA](#)

### **De-coding the case files of rehired LA Sheriff's Deputy Carl Mandoyan: Part 1 - Command & control**

The past two weeks have been active ones in the unendingly controversial case of Los Angeles County Sheriff's Deputy Caren Carl Mandoyan, the deputy fired by the LASD in 2016 under former Sheriff Jim McDonnell, who was rehired early this year by Sheriff Alex Villanueva. Much of the controversy has pertained to the fact that Mandoyan was fired for alleged domestic abuse, along with reported stalking and bullying behavior against his ex-girlfriend, who was also a deputy at the time.

[Witness LA](#)

## **Los Angeles County**

### **LA approves permanent street memorial signs at sites of deadly bicycle crashes around city**

Fatal bicycle crashes on L.A. streets have long been marked by so-called 'ghost bikes', bicycles painted white in memory of a lost life, flanked by flowers and other tokens to form ad-hoc public memorials. They serve as a haunting reminder of the vulnerability of cyclists on city streets, but tend to disappear in time.

[Los Angeles Daily News](#)

### **L.A. County crews who allegedly used Darknet to traffic narcotics face federal criminal conspiracy charges**

Members of two alleged Los Angeles County crime rings have been charged in separate federal criminal cases alleging they conspired to use the Darknet to illicitly and secretly sell methamphetamine and other illegal narcotics nationwide, including one shipment of heroin in a stuffed animal that led to the fatal overdose of a customer in Tennessee.

[FBI](#)

### **With business groups allied against it, L.A. parcel tax faces big hurdle**

Three Los Angeles area business associations have signed the official ballot argument opposing L.A. Unified's sizable 12-year parcel tax on the June 4 ballot - compounding the district's challenge of getting a two-thirds majority required to pass it. The opponents include the influential Los Angeles Area Chamber of Commerce. Parcel tax backers had hoped that business community leaders would take no position, if they couldn't support a parcel tax.

[EdSource](#)

### **LA's City Council District 12 seat is up for grabs. Here are the 15 people vying to fill it**

When Mitch Englander resigned his L.A. City Council seat last October, District 12 - which includes Chatsworth, North Hills, Northridge, Granada

Hills, Porter Ranch, Reseda, Sherwood Forest and West Hills - was left with temporary representation (Greig Smith, his former chief of staff, stepped into the role). Englander was the lone Republican on the 15-member council.

[LAist](#)

### **Los Angeles County Supervisor Janice Hahn will seek re-election in 2020**

Hews Media Group-Los Cerritos Community News has exclusively learned that Los Angeles County 4th District and Chair of the Board of Supervisors Janice Hahn will seek reelection in 2020. Hahn told HMG-LCCN publisher Brian Hews during a wide ranging interview this morning. "This is much more fulfilling than my Congressional position. Washington was, and still is, in gridlock. I can get things done here and I've accomplished a lot, but I want to accomplish much more."

[Hews Media Group](#)

## **Convictions/Sentences/Parole**

### **Assault with a deadly weapon inmate walks away from conservation camp in Antelope Valley**

An inmate in custody for assault with a deadly weapon walked away from a conservation camp in the Antelope Valley early Tuesday. Jon Nicholas, 37, was at Fenner Canyon Conservation Camp in Valyermo, but at 4:20 a.m., staff discovered that he was missing. Officers immediately began searching the camp, but he was not found.

[KTLA](#)

### **Man sentenced to 40 years for molesting relative under 8 years old for years**

A 58-year-old man who repeatedly sexually assaulted a young relative in Temecula was sentenced Wednesday to 40 years to life in state prison. Jose Benito Fabian was convicted in December of four counts of lewd acts on a child under 10 years old. Riverside County Superior Court Judge John Molloy imposed the sentence required by law for the offenses.

[NBC4](#)

## **Consumer News**

### **Walmart misled customers with oversized containers, California prosecutors say. Now it'll pay**

Walmart misled customers by packaging some of its health and beauty products in oversized containers, prosecutors say, and now the company will pay \$495,000 in costs and penalties. The Fresno County District Attorney's Office announced in a news release Wednesday that its office, along with five other California district attorney's offices, reached a settlement with Walmart Inc. in a civil enforcement action.

[Fresno Bee](#)

### **Amazon corporate counsel says counterfeits will remain**

When you make a claim, you better make sure it's true and that you're actually doing what you claim you're doing. When you get caught in a lie or exaggeration, your credibility is destroyed. That's happened to Amazon, who is facing an avalanche of counterfeit and fraudulent product sales, scams, and fake reviews, along with allegations of data leaks and employee bribes.

[The Counterfeit Report](#)

### **Trump puts Amazon, Alibaba on notice for sale of counterfeit goods**

President Donald Trump put Amazon, eBay and Alibaba and other online marketplaces on notice Wednesday, signing a memorandum that aims to curb the sale of counterfeit items online. "This is a shot across the bow to those companies. If you don't clean it up, then the government will," Trump trade advisor Peter Navarro told reporters.

[CNBC](#)

### **Facebook to finally explain the decisions of its news feed algorithm**

Facebook will finally begin telling its users why posts appear in their news feeds as it seeks to assuage public concerns about the spread of fake news and its influence over billions of people's reading habits. The social network will today introduce a button on each post revealing why users are seeing it, including factors such as whether they have interacted often with the person who made the post or whether it is popular with other users.

[The Telegraph](#)

## **California/National**

### **Funds from ballot initiative help newly released prisoners find a home in Los Angeles**

As Latanja Madison's release date from prison inched closer, she felt more terrified than elated. During a decade behind bars at the California Institution for Women in Corona, the 55-year-old Madison underwent multiple orthopedic surgeries and now uses a walker. Her immediate family members passed away during her incarceration, creating grave doubts she would have a support system.

[Witness LA](#)

### **Walters: California Gov. Newsom gets surprising grade just 90 days in**

Gavin Newsom coasted into the governorship last year, defeating his Republican rival by more than a 3-2 margin. It seems a little odd, therefore, that three months into his governorship, he enjoys only tepid popular support. A new poll by the Public Policy Institute of California found that just 45 percent of all adults, and the same percentage of

likely voters, approve of Newsom's governorship so far.

[Mercury News](#)

### **State warns NASA it must uphold agreement to clean up its part of Santa Susana field lab**

For the second time in two months, the California Department of Toxic Substances Control has warned another federal agency to stick to a 2010 agreement to fully clean up its portion of the contaminated Santa Susana Field Laboratory outside Simi Valley. In late January, the state agency, which is overseeing the long-planned, much-delayed cleanup, put the U.S. Department of Energy on notice not to waver from the legally binding agreement.

[Ventura County Star](#)

### **Saudis hacked Jeff Bezos' phone and leaked racy texts, investigator claims**

Saudi Arabia nationals hacked the phone of Amazon CEO Jeff Bezos and were the source of private information that was published by The National Enquirer, according to longtime security consultant Gavin de Becker, who works for Bezos. In an op-ed in The Daily Beast, de Becker said that he and other security experts probed how anyone could access Bezos' private phone messages to his girlfriend, Lauren Sanchez, after some of them were published on The National Enquirer and became the subject of an extortion plot.

[Fox News](#)

### **Chinese woman carrying malware allegedly got into Mar-a-Lago**

A woman carrying two Chinese passports and a device containing computer malware lied to Secret Service agents and briefly gained admission to President Donald Trump's Mar-a-Lago club over the weekend during his Florida visit, federal prosecutors allege in court documents. Yujing Zhang, 32, approached a Secret Service agent at a checkpoint outside the Palm Beach club early Saturday afternoon and said she was a member who wanted to use the pool, court documents said. She showed the passports as identification.

[AP](#)

### **California's Attorney General says immigration should be decriminalized**

Unauthorized immigration should be decriminalized, California Attorney General Xavier Becerra (D) said in an interview with HuffPost on Friday, becoming one of the few prominent Democrats to challenge a key aspect of the Trump administration's crackdown. "They are not criminals," Becerra said of migrants who cross without authorization.

[HuffPost](#)

## **Guns**

### **LAPD asks to cancel citizens' concealed weapons permits**



The Los Angeles Police Department has moved to cancel most of the few remaining concealed weapons permits in civilian hands, according to new filings in a decades-old legal case. Chief Michel Moore said in a sworn declaration he did not believe a group of people who obtained so-called CCWs as the result of a 1994 lawsuit were still entitled to the permits, because it was unlikely the individuals still faced extraordinary physical danger to their lives.

[NBC4](#)

### **NRA and CRPA oppose California's request to immediately halt "large-capacity" magazine ruling**

On Tuesday, April 2, NRA and CRPA filed an opposition to California's request seeking an immediate stay of enforcement of Friday's decision in the case of *Duncan v. Becerra*, which found California's restrictions against so-called "large-capacity" magazines unconstitutional and unenforceable.

[NRA-ILA](#)

## **Public Records**

### **Release of Santa Maria police officer misconduct records on hold, pending open court cases**

Citing nearly a dozen open legal challenges statewide to a new police transparency law, the city of Santa Maria won't release records detailing investigations into confirmed instances of police misconduct that occurred prior to Jan. 1 until the lawsuits are resolved. The city response follows a public records request by the Santa Maria Times in January seeking records covered by SB 1421, a landmark state law passed by the California legislature last year that aims to bring more transparency to internal investigations of police misconduct.

[Santa Maria Times](#)

### **California AG slammed on police transparency record**

Press and free speech advocates blasted California Attorney General Xavier Becerra on Monday over his approach to government transparency and law enforcement accountability. "I think the Attorney General's office has behaved disturbingly and inappropriately," said David Snyder, the director of the First Amendment Coalition, a California-based nonprofit dedicated to government transparency and press freedom.

[Courthouse News Service](#)

### **Court upholds broad release of police misconduct records in California**

A new law granting public access to police misconduct records and investigations of officers' use of force applies to all records that existed when the law took effect this year no matter when they were created, a state appeals court has ruled in a decision with immediate statewide impact. Police unions in numerous localities, including Contra Costa

County and five of its cities in the current case, sued to block release of records created before 2019.

[San Francisco Chronicle](#)

### **Prodded by court ruling, Sonoma County Sheriff relents and agrees to release police records**

The Sonoma County Sheriff's Office said Wednesday that within a week it will begin releasing police records it had previously withheld, following an appeals court decision last week on the issue and a legal threat to the county Tuesday. California news organizations, including The Press Democrat, had requested the records under a new state law known as Senate Bill 1421.

[The Press Democrat](#)

## **Corrections**

### **State prison officials reviewing request to allow imprisoned father to see Oakland son in hospital**

State prison officials are considering a request to allow the imprisoned father of an Oakland boy on life support to visit his son as he clings to life in the hospital, authorities said Monday. Four-year-old Navaun Jackson shot himself in the head last week and has been in critical condition at UCSF Benioff Children's Hospital in Oakland, his family said. Family members pleaded with Gov. Gavin Newsom over the weekend to allow the boy's father, Nathan Jackson, to visit his son in the hospital.

[San Francisco Chronicle](#)

## **Homeless**

### **Legislation would allow West L.A. Armory to operate as shelter year round**

Federal legislation introduced Monday would allow the West Los Angeles National Guard Armory to operate year-round as a homeless shelter instead of only during the winter months. The bill is sponsored by Sens. Dianne Feinstein and Kamala Harris, D-Calif., and Rep. Ted Lieu, D-Torrance. In a letter to the Senate and House Armed Services Committees, they requested that the legislation be included in the next National Defense Authorization Act.

[My News LA](#)

### **Despite Measure H, cities and agencies struggle to get money for homeless services; LA County to investigate**

Los Angeles County cities and homeless services providers could soon more easily access Measure H funding. The Los Angeles County Board of Supervisors approved a motion by supervisors Kathryn Barger and Hilda Solis Tuesday directing staff to report back in 45 days with recommendations to streamline the process through which the Los Angeles Homeless Services Authority grants Measure H dollars to cities and service providers.

[San Gabriel Valley Tribune](#)

### **Citing 'frustration' on homeless crisis, San Fernando, San Gabriel Valley county leaders call for more collaboration with cities**

The Los Angeles County Board of Supervisors voted Tuesday to find ways to work more collaboratively with dozens of cities to solve the problem of homelessness. Supervisor Kathryn Barger recommended streamlining processes to grant Measure H dollars to local cities and homelessness agencies.

[City News Service](#)

## **Pensions**

### **Cities struggle to cut retirement health care costs**

The cost of providing health care for retired state and local government employees, a benefit rarely found in the private sector, was mostly ignored until around 2007, when a government accounting board said the debt should be calculated. So little attention was paid to the growing retiree health care debt that it's still called "Other Post Employment Benefits" in government reports, a catchall phrase for benefits beyond pensions that could include life, disability, and long-term care insurance if offered.

[Calpensions](#)

### **California beats back challenge of CalSavers retirement plan**

California's state-sponsored retirement plan for private workers cleared a major hurdle Friday, with a federal judge tossing a lawsuit brought by an influential anti-tax group that hoped to kill the program before its July launch date. Lawmakers passed the retirement plan, now called CalSavers, in 2016 with the goal of extending benefits to an estimated 7.5 million workers that aren't offered pensions or 401(k) plans by their employers.

[Courthouse News Service](#)

### **Marin Voice: Public pension debate is about values and priorities**

The ongoing discussion of public employee pensions is currently focused on litigation before our state's Supreme Court. It may come as a surprise, but I agree with Jody Morales (Marin Voice, March 8) that most observers expected the court's recent decision in the Cal Fire case on air time to be a narrow one. We at Marin Association of Public Employees (MAPE) did.

[Marin Independent Journal](#)

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](#)

From: [Security Management Weekly](#)  
To: [Ruben Cortez](#)  
Subject: Security Management Weekly - April 5, 2019  
Date: Friday, April 05, 2019 11:55:39 AM



Banner



Advertising/Sponsorship Opportunities | Professional Edition

## Lead Story

### Guard Force Trends Multipliers and the Market

Security Management Magazine April 2019 Issue

Security guard forces, and the methods used to manage them, have seen transformational change in recent decades. Twenty years ago, the tools of the trade were a notepad and a pen, and the required technical skills peaked with the ability to use a handheld two-way radio. Guard force security was not viewed in a professional manner; guard jobs were often considered "no specific skills needed" entry level positions. Recruiters frequently told applicants, "If you can stay awake, you can do this job." ([More](#))

## Top Security News

### Malware Arrest Exposes Security Gaps at Trump's Mar-a-Lago Club

From "Malware Arrest Exposes Security Gaps at Trump's Mar-a-Lago Club" *New York Times* (04/04/19) Kanno-Youngs, Zolan; Rogers, Katie; Stevenson, Alexandra

The security breach on Saturday at Mar-a-Lago, President Trump's Florida resort, highlights the extent to which the estate falls short of the tight security protocols at the actual White House, exposing tensions between Secret Service agents and the resort's staff members, who vet guest lists and allow people onto the sprawling grounds. Secret Service agents must rely on club receptionists and other employees to crosscheck visitors, former officials say, and communication breakdowns allow for security breaches. Yujing Zhang, 32, was arrested at Mar-a-Lago with four cellphones, a hard drive, a laptop, and a malware-infected thumb drive. She said she was there to attend a "United Nations Friendship Event" that had never been scheduled. Her arrest revealed gaps in Trump's security as well as the challenge of protecting a president who spends less time at the remote, fortified Camp David and more time at his busy resort with sometimes hundreds of guests. Advertisements for the resort promise the prospect of mingling with the president and his associates at banquets, fundraisers, and other events. Federal officials say they are still investigating Zhang and what kind of malware was on her thumb drive. It is not yet clear if she has links to Chinese intelligence.

Share | [Web Link](#)

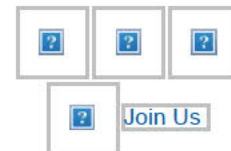


### Tailgate Detection

This unique optical security device from **Designed Security, Inc. (DSI)**, using proprietary sensing technology to detect direction and tailgating, is suited for areas requiring tighter security. Compatible with all card reader technologies and access control systems, the

April 5, 2019

## Follow Us



## Calendar of Events

### UPCOMING EVENTS

- [12th Annual CSO Summit \(5-7 May\)](#)  
Washington D.C.
- [Global Security Exchange \(8-12 September\)](#)  
McCormick Place, Chicago
- [ASIS Latin American 2019 \(15-16 October\)](#) Mexico City, Mexico
- [ASIS Middle East 2019 \(4-6 November\)](#) Manama, Bahrain

### UPCOMING WEBINARS

- [Building a Business Case \(9 April\)](#)
- [High Rise Security A to Z: Security Practices in a High-Rise Environment \(24 April\)](#)
- [How to Conduct a CPTED Site Assessment in 2019 and Beyond \(15 May\)](#)

[Global Events](#)  
[More Classroom Programs](#)  
[More Webinars](#)



Entry Sentry helps to ensure that only one individual enters through a secured doorway for each valid authorization. Its subtle design does not distract from interior aesthetics and mounts easily on standard door frames and hallway walls. Entry Sentry consist of two self-contained, narrow door/wall mounted units providing both local and remote alarm indications.

#### ASIS News

---

##### **Former White House Chief of Staff and Secretary of Homeland Security, General John Kelly, to be GSX Keynote Presenter**

Join us at **Global Security Exchange (GSX)**, 8-12 September 2019, and enjoy a truly engaging experience, that includes hearing unique and high-level insights from one of America's most respected generals.

General Kelly's keynote presentation will start Military and Law Enforcement Appreciation Day off at 8:30 am. GSX will honor all military, law enforcement, and first responders with a full complimentary day of education sessions and access to our exhibit hall—an interactive learning lab full of immersive experiences and cutting-edge technology. [Learn more and register today.](#)

Share    | [Web Link](#)



#### Top Security News

---

##### **Facebook Removes Exposed User Records Stored on Amazon's Servers**

From "Facebook Removes Exposed User Records Stored on Amazon's Servers"  
*Reuters (04/03/19)*

Facebook recently said that it removed public databases containing its user data on Amazon.com Inc's cloud servers after cybersecurity firm UpGuard discovered millions of exposed records. In a blog post, UpGuard's Cyber Risk team announced that Mexico City-based news website Cultura Colectiva had used Amazon servers to openly store 540 million records on Facebook users, including identification numbers, comments, reactions, and account names. Another database, from an app called At the Pool, listed names, passwords and email addresses of 22,000 people, UpGuard said. Cultura Colectiva said that all of its Facebook records came from user interactions with its three pages on Facebook and is the same information publicly accessible to anyone browsing those pages.

Share    | [Web Link](#) - May Require Paid Subscription



##### **Tailgate Detection Where You Need It**

Detex puts dependable in restricted secure areas - at gym and dorm entrances, offices, and any other area where unauthorized entry must be controlled, and authorized entry must be easy, quick and reliable. You may also need to protect departments within your facility. The Restricted Access System is easy to retrofit, compatible with most access control technologies, and can be customized for your needs.

##### **Countries Want to Ban 'Weaponized' Social Media. What Would That Look Like?**

From "Countries Want to Ban 'Weaponized' Social Media. What Would That Look Like?"

*New York Times (04/01/19) Cave, Damien*

Politicians in Australia and New Zealand are discussing proposals such as treating Facebook, YouTube, and Twitter like traditional publishers, expected to vet every post, comment, and image before they reach the public, as well as potentially jailing technology executives for failing to censor hate and violence. Both nations are moving to address popular outrage over the massacre this month of 50 people at two mosques in Christchurch, New Zealand. The gunman, believed to be an Australian white nationalist, distributed a manifesto online before streaming part of the mass shootings on Facebook. If the two countries move ahead, it could be a watershed moment for the era of global social media. No established democracies have ever come as close to applying such sweeping restrictions on online communication, and the demand for change has both harnessed and amplified rising global frustration with the technology industry. "Big social media companies have a responsibility to take every possible action to ensure their technology products are not exploited by murderous terrorists," Scott Morrison, Australia's prime minister, said Saturday. "It should not just be a matter of just doing the right thing. It should be the law." Prime Minister Jacinda Ardern of New Zealand argues that there must be a middle ground, and that some kind of international consensus is needed to keep the platforms from limiting public protection only to certain countries. "Ultimately, we can all promote good rules locally, but these platforms are global," she said.

Share    | [Web Link](#)



### **There Are Probably Cameras on Your Flight, but Relax, They're Not On (Yet)**

From "There Are Probably Cameras on Your Flight, but Relax, They're Not On (Yet)"

*New York Times (04/02/19) Negroni, Christine*

Sens. Jeff Merkley (D-Ore.) and John Kennedy (R-La.) have asked eight U.S.-based airlines to respond in the next few weeks to reports of secret cameras hidden on flights, including whether the airlines have used them "to monitor passengers" and whether passengers have been "informed of this practice." Of the carriers that received the letter, at least three do not have any kind of embedded seat back screen. In addition, the American carriers that do have cameras built into the backs of the seats have not made them operational, according to the Airline Passenger Experience Association, an airline trade group. The high-definition cameras and the microphones that go with them are part of a new generation of systems offered by Panasonic and Thales, two of the biggest airline entertainment system manufacturers. Panasonic chief technology officer David Bartlett says the devices allow passengers to have the same kind of interactive technology on board the plane that they do on the ground. Bartlett cited several potential uses for the cameras, including seat-to-seat or seat-to-ground video chats; motion activated control of movies, games and other options displayed on the screen; and smart lighting that dims when the camera detects that the passenger is sleeping. Airlines could also create digitally branded frames so passengers could take selfies and share them on social media. However, the two senators, in a statement, said that "The notion that in-flight cameras may monitor passengers while they sleep, eat or have private conversations is troubling."

Share    | [Web Link](#) - May Require Paid Subscription



### **Find the balance between threat detection and positive visitor experience**

Visitors to your venue are looking for a hassle-free, safe and welcoming experience. But if your security process is too time-consuming and invasive, they'll turn away. Which is why finding a



balance between effective screening and a positive customer experience should be a key consideration in your security plan. Learn more on the limitations of traditional screening technology and the new approach for protecting soft targets. [Get the eBook.](#)

### **Boeing Software Engaged Repeatedly Before Crash**

From "Boeing Software Engaged Repeatedly Before Crash"

*Reuters (04/03/19) Hephher, Tim; Johnson, Eric. M.*

Boeing anti-stall software on a doomed Ethiopian Airlines jet re-engaged as many as four times after the crew initially turned it off due to suspect data from an airflow sensor, according to two people familiar with the matter. It was not immediately clear whether the crew had chosen to re-deploy the system, which pushes the nose of the Boeing 737 MAX downwards, but one person said investigators were studying the possibility that the software had kicked in again without human intervention. Boeing's anti-stall software known as MCAS is at the center of investigations into both the Ethiopian Airlines crash last month and a Lion Air accident in Indonesia in October. The investigation has now turned toward how MCAS was initially disabled by pilots following an emergency checklist procedure, but then appeared to start working again before the jet plunged to the ground, the people said. A directive issued after the Indonesian crash instructed pilots to use cut-out switches to disengage the system in the event of problems and leave it switched off. Doing so does not shut down the MCAS system completely but severs an electrical link between the software and aircraft systems, a person familiar with the technology said. Investigators are studying whether there are any conditions under which MCAS could re-activate itself automatically, without the pilots reversing the cut-out maneuver.

Share    | [Web Link](#)



### **FTC Has Received 26,000 Complaints About Facebook Privacy Violations Since 2012**

From "FTC Has Received 26,000 Complaints About Facebook Privacy Violations Since 2012"

*The Hill (04/04/19) Birnbaum, Emily*

The FTC has received 26,000 complaints about potential Facebook privacy violations over the past eight years, according to records made public by the Electronic Privacy Information Center. The agency, which oversees data privacy issues, received 8,391 consumer complaints about Facebook last year, compared with 138 that it received in 2012. This week, the FTC told Congress that it only has 40 full-time employees dedicated to overseeing internet privacy and data security, which Reps. Frank Pallone Jr. (D-N.J.) and Jan Schakowsky (D-Ill.) said is "shocking" for a country of 320 million people.

Share    | [Web Link](#)

### **Elite U.S. School MIT Cuts Ties With Chinese Tech Firms Huawei, ZTE**

From "Elite U.S. School MIT Cuts Ties With Chinese Tech Firms Huawei, ZTE"

*Reuters (04/04/19)*

The Massachusetts Institute of Technology has severed ties with Huawei Technologies and ZTE Corp., the latest top educational institution to refuse telecom equipment made by Huawei and other Chinese companies to avoid losing federal funding. U.S. authorities are investigating the Chinese firms for alleged sanctions violations. "MIT is not accepting new engagements or renewing existing ones with Huawei and ZTE or their respective subsidiaries due to federal investigations regarding violations of sanction restrictions," Maria Zuber, its vice president for research, said in a letter on its website. Collaborations with China, Russia, and Saudi Arabia would face additional administrative review procedures, Zuber added. "The institute will revisit

collaborations with these entities as circumstances dictate," she said. "We're disappointed by MIT's decision, but we understand the pressure they're under at the moment," Huawei said on Thursday. The company denies the allegations of the U.S. government. "We trust the U.S. judicial system will ultimately reach the right conclusion," Huawei said. Chinese telecoms equipment makers have also been facing mounting scrutiny, led by the United States, amid worries Beijing could use their equipment for spying. The companies, however, have said the concerns are unfounded.

Share    | [Web Link](#)

### **Since Super Bowl Ended, Minneapolis Police Have Been Prepping to Host the Final Four**

From "Since Super Bowl Ended, Minneapolis Police Have Been Prepping to Host the Final Four"

*Twin Cities Pioneer Press (04/01/19) Gottfried, Mara H.*

This weekend, thousands of people will visit the Twin Cities in Minnesota for the NCAA Final Four, and a team of law enforcement leaders will aim to ensure safety for everyone during one of the U.S.'s biggest annual events. The police will be using lessons learned and equipment obtained from when the Twin Cities hosted the Super Bowl in 2018. Officers from dozens of departments helped with the Super Bowl detail, which at times had a military atmosphere and proceeded without any major incidents. One of the lessons police learned from the 2018 Super Bowl was the importance of the high-tech Multi-Agency Command Center, where decision makers from various departments can view what is happening on the streets in real time from the city's public safety cameras, see the locations of officers on a large 3D map, and coordinate with each other face to face. In order to keep the expected 94,000 visitors safe, law enforcement from 23 local agencies have partnered with the Minneapolis police to provide officers during the events. In February, the FBI put local departments through a tabletop exercise, in which they practices their responses to various situations, ranging from worst-case disasters to a foodborne illness outbreak.

Share    | [Web Link](#)

### **White House Whistle-Blower Tells Congress of Irregularities in Security Clearances**

From "White House Whistle-Blower Tells Congress of Irregularities in Security Clearances"

*New York Times (04/02/19) Fandos, Nicholas; Haberman, Maggie*

A White House whistleblower told lawmakers that 25 denials for security clearances have been overturned during the Trump administration, calling Congress her "last hope" for addressing what she considers improper conduct that has left the nation's secrets exposed. Tricia Newbold, a longtime White House security adviser, told the House Oversight and Reform Committee that she and her colleagues issued "dozens" of denials for security clearance applications that were later approved despite their concerns about blackmail, foreign influence, or other red flags, according to panel documents released Monday. Newbold, an 18-year veteran of the security clearance process who has served under both Republican and Democratic presidents, said she warned her superiors that clearances "were not always adjudicated in the best interest of national security" — and that she faced retaliation for doing so. Newbold told the committee's staff members that she and other career officials had denied the 25 applications for a variety of reasons, including "foreign influence, conflicts of interest, concerning personal conduct, financial problems, drug use and criminal conduct." The denials by the career employees were overturned, she said, by officials with more seniority who, by her account, did not follow the normal procedures meant to mitigate security risks and generally adhered to by other administrations. Newbold's statements are likely to increase pressure on the White House to address lingering questions about its general practices around keeping the nation's secrets and several high-profile cases.

Share    | [Web Link](#)



### **Chinese Companies Have Leaked Hundreds of Millions of Resumes**

From "Chinese Companies Have Leaked Hundreds of Millions of Resumes"

*ZDNet (04/04/19) Cimpanu, Catalin*

In the first three months of 2019, Chinese companies leaked 590 million resumes. Most of the resume leaks have occurred because of poorly secured MongoDB databases and Elasticsearch servers that have been left exposed online without a password, or have ended up online following unexpected firewall errors. Sanyam Jain, a security researcher and a member of the GDI Foundation, discovered and reported seven such cases in the past month alone. His discoveries include an Elasticsearch server containing resumes for 33 million Chinese users that he found on March 10.

Share    | [Web Link](#)

### **Remote Work Brings Benefits — But Also Greater Security Risks, Survey Says**

From "Remote Work Brings Benefits — But Also Greater Security Risks, Survey Says"

*CIO Dive (04/01/19) Bolden-Barrett, Valerie*

According to a recent OpenVPN survey, 92 percent of IT professionals recognize the benefits of remote work, but most said the perk comes with security risks. The survey found 73 percent of VP and C-suite IT leaders think remote workers present a greater risk than onsite employees. Although nearly all survey respondents have a policy in place, OpenVPN said restrictions should apply, such as making VPNs and password managers mandatory and prohibiting remote workers from using their personal devices for work to protect employers' proprietary information. HR and IT professionals must work together to create cybersecurity policies, design employee training programs, and communicate their rationale for both to workers. OpenVPN recommended that employers lower their security risk by regularly revisiting their policies for continuous improvement and allowing IT to take the lead role in developing a security policy.

Share    | [Web Link](#)

### **Israelis Prepare for Elections as Experts Cite Cyber Threats**

From "Israelis Prepare for Elections as Experts Cite Cyber Threats"

*Associated Press (04/04/19) Debre, Isabel*

Experts say Israel is vulnerable to foreign hacks and cyber campaigns as it prepares to hold a national election next week. Although Prime Minister Benjamin Netanyahu says there is "no country better prepared" to combat election interference, experts say Israel's laws are outdated and that Netanyahu's government hasn't made cyber threats a priority. Campaigning had just started to ramp up in January when the director of the Shin Bet, Israel's internal security agency, said that a world power had tried to disrupt the April 9 vote. Boaz Dolev, the CEO of cybersecurity firm ClearSky, said Iranian operatives have honed their phone-hacking skills over the past five years and targeted nearly all of Israel's senior army officials. Meanwhile, Karine Nahon, president of the Israel Internet Association, says the main danger comes from Israeli politicians and their supporters spreading disinformation on social media. She said there is little legislation to prevent such activities as laws on political propaganda were written before the digital age and are poorly enforced. Election systems in Israel are not formally designated as "critical infrastructure," a move that would expand the mandate of security agencies to protect them. The Shin Bet and the Cyber Directorate, the main bodies tasked with overseeing election security, pointed out that Israel still uses paper ballots, enhancing security on election day. However, the vote count is digitized, which means that "in the last and most critical stage of the voting process, our database is vulnerable," said Lotem Finkelstein, head of the threat intelligence team at Check Point, a cybersecurity firm.

Share    | [Web Link](#)

### **Facebook CEO Zuckerberg Calls for More Outside Regulation**



From "Facebook CEO Zuckerberg Calls for More Outside Regulation"  
*Associated Press (03/30/19)*

Facebook CEO Mark Zuckerberg is calling for more outside regulation in several areas, including harmful content, election integrity, privacy and data portability. In an opinion piece published over the weekend in the Washington Post, Zuckerberg wrote that governments and regulators instead of private companies like Facebook should be more active in policing the World Wide Web. He added that privacy rules, such as the General Data Protection Regulation, should be adopted elsewhere around the world. Zuckerberg's editorial comes days after the social networking giant was criticized after a shooting rampage in New Zealand that killed 50 people was broadcast live on the site.

Share    | [Web Link](#)

#### **Tech Groups Push Back on Social Media Law in Australia**

From "Tech Groups Push Back on Social Media Law in Australia"  
*Financial Times (04/03/19) Smyth, Jamie*

Australia's new draft law imposes criminal penalties for social media companies that permit the sharing of abhorrent material on their platforms, and possible jail sentences for executives. Technology groups, including Google, Facebook, and Twitter, have warned that the proposed law risks damaging U.S.-Australia security cooperation. The law includes provisions that U.S. companies fear could require them to share content data with Australian police, in contravention of U.S. law. The U.S. tech groups also said the bill would encourage proactive surveillance by internet companies of internet users.

Share    | [Web Link](#) - May Require Paid Subscription

#### **N.S.A. Contractor Arrested in Biggest Breach of U.S. Secrets Pleads Guilty**

From "N.S.A. Contractor Arrested in Biggest Breach of U.S. Secrets Pleads Guilty"  
*New York Times (03/28/19) Shane, Scott*

Harold T. Martin III, a former National Security Agency (NSA) contractor pleaded guilty on Thursday to taking classified documents home in a deal likely to put him in prison for nine years. Martin, who worked in the NSA's Tailored Access Operations hacking unit, admitted his guilt in what may be the biggest breach of classified information in history. FBI agents raided his Baltimore-area home in 2016 and found stacks of documents and electronic storage devices hidden in his car, his home, and a garden shed. However, investigators never found proof that Martin had shared the stolen secrets with anyone else, though there is evidence he may have considered doing so. Investigators found that for 20 years, Martin had been carrying classified material out of the NSA and other security agencies where he had worked. The FBI focused on Martin after receiving a tip from two Kaspersky Lab employees, who had gotten cryptic messages from Martin—calling himself "HAL999999999"—via Twitter that seemed to be offering secrets. The FBI quickly linked the HAL999999999 Twitter account to Martin, which led them to his home where they found a total of 50 terabytes of government data, much of which was classified at a high level.

Share    | [Web Link](#) - May Require Paid Subscription

News summaries © copyright 2019 [SmithBucklin](#)



#### **ASIS INTERNATIONAL**

If you have questions, please contact Member Services at [asis@asisonline.org](mailto:asis@asisonline.org) or +1.703.519.6200, or via 1625 Prince Street, Alexandria, VA 22314 USA.

[Log in to manage your privacy settings.](#) | [Unsubscribe SM Weekly](#)

ASIS International values the privacy and integrity of our members, partners, attendees, exhibitors, and sponsors, and we do not sell your contact information, nor do we provide it to third-party vendors for distribution. [View privacy policy.](#)

**From:** [CLA Public Section](#)  
**To:** [Melissa Tronquet](#)  
**Subject:** CLA Public Law Section Newsstand - Powered by Lexology  
**Date:** Friday, April 05, 2019 3:06:24 AM

To ensure delivery to your mailbox please add domain @lexology.com to your safe senders list [View in Browser](#)

Lexology



[My Account](#) | [About](#) | [Search Archive \(835,300 articles\)](#)



[North America](#) | [Global](#)

**USA**

[North America](#)

[Employee Benefits & Pensions](#)



**NJ Employers and Out-of-State Employers with NJ Residents Prepare: State Updates Website on Employer Reporting for New Jersey Health Insurance Mandate** [New Jersey](#)

**Epstein Becker Green**

As employers are wrapping up their reporting under the Affordable Care Act ("ACA") for the 2018 tax year (filings of Forms 1094-B/C and 1095-C/B with...

**A One-Time Offer from the IRS for 403(b) Plans Nears its Expiration Date**

**Boutwell Fay LLP**

Albert Einstein theorized that because time is relative, a space traveler who leaves earth and travels near the speed of light will return to earth...

**[Podcast]: Suspension of Benefits Issues** [Audio](#)

**Proskauer Rose LLP**

In this Episode of the Proskauer Benefits Brief, partner Paul Hamburger, and associate Katrina McCann discuss some of the interesting and unique...

**Don't Be Fooled! Compensation Definitions Are Tricky!**

**Holland & Hart LLP**

Contributions to your 401(k) plan are calculated as a percentage of an employee's compensation. Seems simple, right? Not so fast. The definition of...

## **IRS No Longer Forbids Pension Plans From Offering Lump Sum Payouts To Retirees Currently Receiving Payments**

**Jackson Lewis PC**

Over the past several years, sponsors of defined benefit pension plans have examined and implemented ways to reduce their pension liabilities. This...

---

## **SDNY Hands Self-Insured Health Plans a Total Win**

**Kilpatrick Townsend & Stockton LLP**

In what can only be described as a complete and total win for self-insured health plan sponsors, the Southern District of New York recently upheld a...

---

## **PBGC Proposes Simplified Methods for Withdrawal Liability Calculations**

**Proskauer Rose LLP**

On February 6, 2019, the Pension Benefit Guaranty Corporation ("PBGC") issued a proposed rule that impacts how multiemployer pension plans in...

---

## **DOL's Proposed Change in OT Rules? Retirement Plans Affected**

**FisherBroyles LLP**

Last month, the U.S. Department of Labor announced a proposed rule that will likely mean that more American employees will be eligible for overtime...

---

## **March 28, 2019 Group Health Plan Section 111 Reporting is Back**

**Kilpatrick Townsend & Stockton LLP**

Self-insured plan sponsors thought they had seen the last of Group Health Plan Section 111 Reporting in 2009, but like a character in a movie ..... it's...

---

## **Tenth Circuit Upholds Great-West Stable Value Win in ERISA Case**

**Holland & Knight LLP**

The U.S. Court of Appeals for the Tenth Circuit affirms a District Court's holding that Great-West Life & Annuity Insurance Co. was not a...

---

## **Retirement Plan Guidance and Compliance Trends in 2019**

**Akerman LLP**

2019 will be a busy compliance year for companies' human resource and finance leaders and other tasked with overseeing employer-sponsored qualified...

---

## **Some Retirement Plan Advisors Need ERISA/Tax Finetuning**

**FisherBroyles LLP**

Of all the retirement plan events held annually and across the nation, I favor and respect the NAPA 401(k) Summit(the National Association of...

---

## **SEC Scrutinizes Sale of Mortgage Interests Among Affiliated Funds**

**Ropes & Gray LLP**

The sale of mortgage assets between investment vehicles managed by the same adviser has come under scrutiny by the Securities and Exchange Commission...

---

**The emerging patchwork of fiduciary investment advice regulation - Putting the**



pieces together

### **Eversheds Sutherland (US) LLP**

By all accounts, 2019 will see the advancement of a number of fiduciary and best interest investment advice regulations at both the federal and state...

---

### **Court Unravels New Association Health Plan Rules**

#### **Crowell & Moring LLP**

It's been just over a year since the new Association Health Plan (AHP) rules were released to the thrill and equal dismay of many. At least...

---

### **Federal Budget 2019: Key Tax Measures**

#### **Piper Alderman**

The 2019-20 Federal Budget delivers a budget surplus together with a raft of tax concessions aimed mostly at low to middle income earners. The tax...

---

## **Employment & Labor**



### **Sponsored business immigration in the USA**

#### **BAL**

A structured guide to employer-sponsored immigration in the USA

---

### **Employee termination law in Utah**

Utah

#### **Holland & Hart LLP**

A structured guide to employee termination law in Utah...

---

### **Employment & Labor in Nevada**

Nevada

#### **Holland & Hart LLP**

A structured guide to employment & labor law in Nevada...

---

### **Managing the employment relationship in Vermont**

Vermont

#### **Downs Rachlin Martin PLLC**

A structured guide to country specific laws, misclassification and contracts in Vermont

---

### **Employment & Labor in Arizona**

Arizona

#### **Ogletree Deakins**

A structured guide to employment and labor law in Arizona

---

### **Rethinking Pay Equity: Being Transparent — Should Employers Publish Information About Pay?**

#### **Jackson Lewis PC**

This is the final article in our four-part series titled "Rethinking Pay Equity," designed to provide practical guidance to help employers understand...

---

### **Two Whistleblowers Net US \$50 Million in SEC Awards for Top-Notch Information**

#### **Katten Muchin Rosenman LLP**

The Securities and Exchange Commission awarded US \$50 million in total to two



separate whistleblowers with one receiving US \$37 million, the third...

---

### **Customs and Border Protection Proposes to Require a Social Compliance Program as Part of Its CTPAT Cargo Security Program**

**Arent Fox LLP**

As part of its response to the changes regarding forced labor enforcement brought about by the Trade Facilitation and Trade Enforcement Act of 2015...

---

### **Dear Littler: Can Employees be Exempt from Income Tax?**

**Littler Mendelson PC**

My company recently hired a new employee who is giving our human resources department some pushback on submitting his W-4. The HR manager says the...

---

### **New Mexico Increases Minimum Wage and Creates Uncertainty in Tip Pooling**

[New Mexico](#)

**Littler Mendelson PC**

On April 1, 2019, New Mexico Governor Lujan Grisham (D) signed Senate Bill (SB) 437, which amends the New Mexico Minimum Wage Act (MWA) by increasing...

---

### **D.C. Circuit Strikes Down Key Parts of DOL's Association Health Plan Rule**

**Ogletree Deakins**

On March 28, 2019, the U.S. District Court for the District of Columbia struck down key parts of the U.S. Department of Labor's (DOL) final rule...

---

### **New York City Issues Final Guidance on Sexual Harassment Training Requirements**

[New York](#)

**Proskauer Rose LLP**

As we previously reported, New York City has enacted the Stop Sexual Harassment in NYC Act, which is a package of bills aimed at addressing and...

---

### **Breaking: Second Jury Finds That Glyphosate Causes Non-Hodgkin's Lymphoma**

**Goldberg Segalla LLP**

Approximately seven months after a California state jury found that DeWayne Johnson's workplace exposure to glyphosate-containing Roundup and Ranger...

---

### **Seyfarth Shaw Policy Matters Newsletter - March 28, 2019**

**Seyfarth Shaw LLP**

Paycheck Fairness Act Passes House. As predicted in last week's newsletter, the Paycheck Fairness Act (H.R. 7) passed the House on Wednesday. The...

---

### **Reed Smith drives progress with #SeeHer featuring Marsha Houston**

**Reed Smith LLP**

"A woman could be in business, they could be an engineer, they could be a lawyer, they could be a doctor." In the most recent edition of our video...

---

## **Severance Agreements for Executives at Tax-Exempt Organizations: Beware Unintended Consequences of Excise Taxes, Early Inclusion, and Intermediate Sanctions**

### **Jackson Lewis PC**

When it's time for tax-exempt organizations such as colleges/universities, museums, and hospital systems to part ways with their senior executives...

---

## **2018 in review - ERISA enforcement**

### **Eversheds Sutherland (US) LLP**

The US Department of Labor (DOL) recently published its Fiscal Year 2018 "Fact Sheet" documenting the criminal and civil enforcement activities of...

---

## **The BakerHostetler Quarterly New York Employment Law Newsletter - Spring 2019**

### **Baker & Hostetler LLP**

On March 4, 2019, Judge Tanya S. Chutkan of the U.S. District Court for the District of Columbia vacated an Aug. 29, 2017, decision by the Office of...

---

## **Maryland General Assembly Approves Minimum Wage Increase**

Maryland

### **Goldberg Segalla LLP**

The minimum wage in Maryland is increasing from \$10.10 to \$15 per hour. The Maryland General Assembly approved legislation for the raise. Under the...

---

## **The Department of Labor Proposes New Rule Regarding the Regular Rate of Pay**

### **Vandeventer Black LLP**

The U.S. Department of Labor (DOL) will publish a proposed rule on March 29, 2019, to amend the Fair Labor Standards Act (FLSA) regulations regarding...

---

## **New Illinois #MeToo Legislation Targets Sexual Harassment in the Workplace**

Illinois

### **Barnes & Thornburg LLP**

As the #MeToo movement continues to sweep across the country, Illinois lawmakers are considering two proposed laws aimed at curbing sexual harassment...

---

## **Predictive Scheduling is Becoming the New Normal for Hospitality and Retail Industry**

### **Epstein Becker Green**

Our colleagues Jeff Landes, Jeff Ruzal, and Adriana Kosovych are featured on Employment Law This Week - Predictive Scheduling Laws, the New Normal? -...

---

## **Assembly Bill Codifying Dynamex Moves Forward, with Notable Exemptions**

California

### **Jackson Lewis PC**

On March 26, 2019, proposed Assembly Bill 5, which would codify the California Supreme Court's controversial Dynamex decision, was amended to exempt...

---



**Employment Law This Week®: NJ Limits NDAs, DOL's Proposed Overtime Rule, Pay Data Collection, Sexual Harassment Training** [Video](#)

**Epstein Becker Green**

The month of March brought important regulatory changes for employers on the federal and state levels, including some long-anticipated rules and some...

---

**No-Poach Clauses in Franchise Agreements: Four More Franchisors Agree to Drop Them and the DOJ Weighs In on Class Actions Alleging Antitrust Violations**

**Epstein Becker Green**

On March 12, 2019, Dunkin' Donuts, Arby's, Five Guys Burgers and Fries, and Little Caesars agreed to stop including "no-poach" clauses in their...

---

**Botched Drug Test Opens Door to SC Worker's Suit Against Testing Company**

[South Carolina](#)

**Fox Rothschild LLP**

A drug testing company may be liable for negligence if a worker is damaged in employment as a result of a botched test, the South Carolina Supreme...

---

**eLABORate: No More Super Sizing: DOL Scales Back on Franchiser Joint Employer Liability**

**Phelps Dunbar LLP**

The Department of Labor (DOL) proposed new legislation on April 1, 2019, which will likely narrow the instances in which certain businesses will be...

---

**Resolutions for 2019? Here are a Few Small, Measurable Goals for New York Employers**

**Perlman & Perlman LLP**

The New Year typically invites personal reflection on what we've accomplished last year and what we resolve to improve in the coming year. But...

---

**More NLRB Advice Memos - Cooperation in Investigations, Workplace Policies, and Facebook Posts**

**Shawe Rosenthal LLP**

The National Labor Relations Board's Office of the General Counsel (OGC) continues to issue Advice Memoranda, as it has regularly done for the past...

---

**Littler Lightbulb: Highlighting Five Trends in Hospitality**

**Littler Mendelson PC**

As part of our practice, we like to keep an eye on significant legislative, regulatory, and judicial developments affecting our clients in the...

---

**Medical Marijuana Users May Not Be Discriminated Against In New Jersey** [New](#)

[Jersey](#)

**Jackson Lewis PC**

A New Jersey appellate court has held that a disabled employee may sue his former employer under the New Jersey Law Against Discrimination ("NJLAD")...

---

## **Colorado Equal Pay for Equal Work Act**

Colorado

Audio

### **Brownstein Hyatt Farber Schreck LLP**

Employment Shareholder Lisa Hogan discusses Colorado Senate Bill 85, the Equal Pay For Equal Work Act, with proponent Charlotte Sweeney. Lisa and...

---

## **Happy Friday, Michiganders!**

Michigan

### **Constangy Brooks Smith & Prophete LLP**

Paid leave law and wage laws should take effect today. I've written about the Michigan Paid Medical Leave Act here and here. There was a question...

---

## **Summary judgment by Railroad Defendant Denied; Attorney's Fees Also Denied Based on Reasonable Grounds to Deny Discovery Admissions**

### **Goldberg Segalla LLP**

The plaintiff filed suit against the Budd Company (Budd) alleging her decedent passed from mesothelioma for which the Defendant was liable...

---

## **Reed Smith drives progress with #SeeHerTM featuring John Lukanski**

### **Reed Smith LLP**

In the most recent edition of our video series celebrating our membership in #SeeHer, John Lukanski explains the hardships his mother went through as...

---

## **DOL Issues Opinion Letters on Designating FMLA Leave, as well as Volunteer Activities and State Law Exemptions Under the FLSA**

### **Shawe Rosenthal LLP**

The Department of Labor (DOL) has released three new opinion letters one on the Family and Medical Leave Act and two on the Fair Labor Standards Act...

---

## **Women's History Month FOCUS: Women as breadwinners**

### **Constangy Brooks Smith & Prophete LLP**

We recognize the immeasurable value of women leaders supporting other women in the workplace through example, mentorship, education and empathy. We...

---

## **No good deed goes unpunished: Public and other for-profit employers may be subject to new section 4960 21% excise tax originally aimed at non-profits**

### **Winston & Strawn LLP**

Now that Notice 2019-09 has been out for several months, the Notice's very serious implications are becoming clearer for taxable entities, in...

---

## **Several Claims in Consolidated Action Dismissed Based Upon Statute of Limitations**

### **Goldberg Segalla LLP**

Following W.R. Grace's filing for bankruptcy in April 2001, a series of cases were filed against Maryland Casualty, which was the company's primary...

---

## **Maryland Joins Growing List of States Increasing Statewide Minimum Wage to \$15 Per Hour**

Maryland

### **Littler Mendelson PC**



On March 28, 2019, Maryland lawmakers passed an increase in the state minimum wage to \$15 per hour starting January 1, 2025. Governor Larry Hogan had...

---

## **Minnesota Legislative Update, Part II: Bills to Watch** Minnesota

### **Ogletree Deakins**

In part one of this series, we reported on several legislative developments in Minnesota that could impact employers. Now the Minnesota Legislature...

---

## **Cell Phone Distractions in the Workplace**

### **Vinson & Elkins LLP**

We've all seen the driver behind the wheel talking on his cell phone and weaving across lanes, making turns without signals, and all sorts of other...

---

## **Seventh Circuit Upholds Wisconsin Ordinance Prohibiting Inflatable "Scabby the Rat"** Wisconsin

### **Otten Johnson Robinson Neff + Ragonetti PC**

The rats and cats are back. We first reported on this case in 2016, after the Seventh Circuit determined that it might be moot. As it turns out, the...

---

## **No Fooling: DOL Announces Joint-Employer Proposal**

### **Ogletree Deakins**

On April 1, 2019, the Department of Labor (DOL) announced that it will publish a notice of proposed rulemaking (NPRM) to amend its existing...

---

## **Age Discrimination Claims Limited for Job Applicants**

### **Akerman LLP**

A second federal appellate circuit has ruled that the Age Discrimination in Employment Act (the ADEA) does not apply to job applicants' claims that a...

---

## **Pre-Employment Tests: Best Practices to Minimize Risks** Audio

### **Ogletree Deakins**

While pre-employment tests can be a useful tool in the hiring process, such tests are susceptible to legal challenges and employers should exercise...

---

## **March 2019: The Top 14 Labor And Employment Law Stories**

### **Fisher Phillips**

It's hard to keep up with all the recent changes to labor and employment law. While the law always seems to evolve at a rapid pace, there have been...

---

## **Labor law for non-union employers - Part 3**

### **Constangy Brooks Smith & Prophete LLP**

In the third and final installment of our three-part introduction to labor law, Host Leigh Tyson and her guest, Jonathan Martin, talk about the...

---

## **N.Y. Court of Appeals Delivers Wage and Hour Victory to Home Care Industry Employers** New York



### **Proskauer Rose LLP**

On March 26, 2019, New York's highest court delivered a victory for employers in the home care industry, clarifying that employers need only...

---

### **New York City Anti-Sexual Harassment Training Law Takes Effect on April 1, 2019** New York

#### **Hunton Andrews Kurth LLP**

Today, New York City's anti-sexual harassment training law goes into effect. Under the new law, private employers must provide annual "interactive"...

---

### **Can an Airport Skycap's Complaint About the Poor Tipping Habits of French Soccer Players Really Become a Federal Case?** New York

#### **Cozen O'Connor**

One of the least appreciated federal workplace laws is Section 7 of the National Labor Relations Act, the 1935 law which gives most private sector...

---

### **Newly Proposed Legislation To Restrict Biometric Privacy Class Actions In Illinois** Illinois

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: Although the Illinois Supreme Court's recent decision in *Rosenbach v. Six Flags* may have upped the ante for employers facing...

---

### **EEO-1 Pay Data Reporting Update**

#### **Jackson Lewis PC**

In a brief filed April 3, 2019, the government informed the court that EEOC could complete collection of the required EEO-1 Component 2 pay data by...

---

### **Department of Labor Proposes Update to FLSA Regulations Governing the Regular Rate of Pay**

#### **Paul Hastings LLP**

On March 29, 2019, the Department of Labor ("DOL") issued a proposal to modernize the Fair Labor Standards Act ("FLSA") regulations governing the...

---

### **New California Law Mandates Female Representation on Boards of Directors by December 2019** California

#### **Ogletree Deakins**

On September 30, 2018, Governor Jerry Brown of California signed Senate Bill (SB) 826, a pioneering law mandating each publicly-held company...

---

### **March 31 is International Transgender Day of Visibility**

#### **Jackson Lewis PC**

Gender identity, transgender status, gender non-conformance, and workplace gender transitions are timely topics, both societally and within...

---

### **Reed Smith drives progress with #SeeHerTM featuring Jeni Taylor**

#### **Reed Smith LLP**

"They're trying to fit themselves into some sort of shape, some sort of box, which isn't real." In the most recent edition of our video series...

---

## **Round Two of the Department of Labor's Revised Overtime Threshold Requirements**

### **Weil Gotshal & Manges LLP**

On March 7, 2019, the U.S. Department of Labor (DOL) released its long-awaited proposed rule to amend the overtime exemption regulations under the Fair...

---

## **Department of Labor Issues Replacement Rule for FLSA Overtime Exemptions**

New York

### **Phillips Lytle LLP**

Department of Labor Issues Replacement Rule for FLSA Overtime Exemptions  
The United States Department of Labor (DOL) recently issued proposed new...

---

## **WPI Wage Watch: Minimum Wage, Tip, and Overtime Developments (March Edition)**

### **Littler Mendelson PC**

It was a busy third month of 2019, so we will march right into discussing developments concerning the minimum wage, tips, and overtime. A Busy Month...

---

## **USDOL's Proposal Reaffirming That There Is Nothing "Regular" About The Regular Rate**

### **Fisher Phillips**

The USDOL has continued to plow through its regulator agenda. Today it released its proposed guidance regarding the "regular rate" for purposes of...

---

## **4 Steps Employers Must Take to Ensure FCRA Compliance**

### **Cozen O'Connor**

What are the four primary steps that employers must take in the Fair Credit Reporting Act (FCRA) process for onboarding an applicant? Bethany...

---

## **DOL Issues Third Proposed Rule in Two Weeks, This Time on Joint Employment**

### **Littler Mendelson PC**

On April 1, 2019, the U.S. Department of Labor released a Notice of Proposed Rulemaking (NPRM) on joint employment under the Fair Labor Standards...

---

## **Washington Healthcare Update- Apr 1, 2019**

District of Columbia

### **McGuireWoods Consulting LLC**

House Committee on Energy and Commerce: "Priced Out of a Lifesaving Drug: The Human Impact of Rising Insulin Costs" The Subcommittee on Oversight and...

---

## **Employers Should Look for Litigation Threats That Cross the Line Highlighted by Michael Avenatti's Indictment**

### **Kelley Drye & Warren LLP**



The fact-pattern is familiar to employers who have been on the receiving end of attorney litigation threats. A Plaintiff's lawyer calls, or writes a...

---

### **Appellate Court Confirms that Steering Contracts to a Third Party Can Violate the Hobbs Act**

#### **Vinson & Elkins LLP**

The First Circuit Court of Appeals recently ruled that steering contracts to a third party may violate the federal prohibition against extortion —...

---

### **Debunking SPD Myths, Part 2: Think That Emailing Your SPD to Employees is Always Enough? Think Again**

#### **Dickinson Wright**

Most employers are familiar with the requirement to prepare and distribute a summary plan description ("SPD"). Many employers, however, assume that...

---

### **Caution: Precertification Communications with Absent Class Members**

Pennsylvania

#### **Baker & Hostetler LLP**

Are absent members of an uncertified class or Fair Labor Standards Act (FLSA) collective action "parties" and thus "represented" by plaintiff's...

---

### **New York Court of Appeals Upholds Thirteen Hour Rule for Home Health Aide Pay**

New York

#### **Robinson & Cole LLP**

On March 26, 2019, the New York Court of Appeals upheld the State Department of Labor's (the "DOL") so-called "13-hour rule" governing payment of...

---

### **Wage Statement Litigation Continues To Clog California Courts**

California

#### **Fisher Phillips**

Most employers do not spend much time reviewing pay statements—often a single piece of paper provided to employees each pay period containing the...

---

### **Updated Massachusetts Paid Family and Leave Act Regulations Offer Additional Guidance as July 1 Effective Date Draws Near**

Massachusetts

#### **Littler Mendelson PC**

On March 29, 2019, the Massachusetts Executive Office of Labor and Workforce Development (EOLWD) released an updated version of the proposed...

---

### **Former Employee Accused of Spilling Secret Beer Recipe in Furtherance of Class Action Cannot Strike Claims Under Anti-SLAPP Statute**

#### **Seyfarth Shaw LLP**

Last week, the Ninth Circuit finally ruled that a former Anheuser-Busch employee cannot avoid claims filed by the brewer alleging misappropriation of...

---

### **Home Health Care Agencies Benefit From NY Wage Ruling**

New York

#### **Fox Rothschild LLP**

Employers of in-home health care aides in New York are allowed to compensate

employees for only 13 hours of work in a 24-hour shift, given that aides...

---

### **The DOL Is On Fire - Proposed Joint Employer Rule Issued**

**Shawe Rosenthal LLP**

An active and activist Department of Labor has issued its third proposed rule in less than a month - this one on joint employer status under the Fair...

---

### **Department of Labor Proposes Updates and Clarifications to the Definition of "Regular Rate"**

**Leech Tishman Fuscaldo & Lampl LLC**

On March 28, 2019, the Department of Labor (DOL) released its newest proposed changes to the Fair Labor Standards Act (FLSA). These proposed updates...

---

### **DOL Proposes Revisions to Calculation of Regular Rate of Pay**

**Shawe Rosenthal LLP**

The Fair Labor Standards Act requires employers to pay overtime to non-exempt employees for all hours worked over 40 in a workweek, calculated at one...

---

### **Section 481 Film Regulations 2019**

**Philip Lee**

In December 2018 the Finance Act, 2018 (the "Act") was enacted. Section 26 of the Act extended the tax credit available to film and television...

---

### **NYC Employers, Get Out Your Handbooks: Reproductive Health Choices Are A New Protected Category**

New York

**Patterson Belknap Webb & Tyler LLP**

Earlier this year, the New York City Council passed an amendment to the New York City Human Rights Law, adding "sexual and reproductive health...

---

### **Suffering Fools and Foolish Employment Stories Gladly**

New Jersey

New York

**Littler Mendelson PC**

"What kind of fool are we?"<sup>1</sup> Musing over Cole Porter's immortal lyrics in today's workplace may surely spur contact from a plaintiffs' lawyer...

---

### **Did New Jersey Just Try to Ban Employment Arbitration Agreements?**

New Jersey

**Sheppard Mullin Richter & Hampton LLP**

On March 18, 2018, the New Jersey Law Against Discrimination (NJLAD) was amended to prohibit prospective waivers of substantive and procedural rights...

---

### **Proposed USDOL Interpretations: The Regular Rate Is Anything But "Regular"**

**Fisher Phillips**

The USDOL has proposed to update its guidance (for the most part not regulations) regarding the "regular rate" for purposes of calculating FLSA...

---

### **House of Representatives Passes Paycheck Fairness Act, But its Future is Uncertain**

**Littler Mendelson PC**



On March 27, 2019, the U.S. House of Representatives passed H.R. 7, the Paycheck Fairness Act. The bill would amend the Equal Pay Act of 1963 (EPA)...

---

**NY Court of Appeals Decision Saves Live-In Home Care** New York

**Riker Danzig Scherer Hyland & Perretti LLP**

On March 26, 2019, the NY Court of Appeals issued a stunning ruling, affirming that “live-in” aides can be paid for 13 hours of work as opposed to 24...

---

**Strict Requirements for Background Checks: Federal and State Mandated Disclosures Must Stand Alone in Separate Documents** California

**Hopkins & Carley**

California employers who use background checks in making personnel decisions about employees and job applicants must comply with a variety of strict...

---

**[Podcast]: The NYCCHR Issues New Enforcement Guidance on Appearance & Grooming Policies** New York Audio

**Proskauer Rose LLP**

In this Episode of The Proskauer Brief, partner Harris Mufson and associate Arielle Kobetz discuss the New York City Commission on Human Rights...

---

**Cincinnati, Ohio Passes Ban on Salary History Inquiries** Ohio

**Proskauer Rose LLP**

Cincinnati, Ohio recently became the latest jurisdiction to pass a law that prohibits employers from asking job applicants for their salary history...

---

**The Department of Labor’s “End Run” Around the Affordable Care Act Ends in Defeat**

**Winston & Strawn LLP**

In June of last year, at the Trump administration’s direction, the Department of Labor (Department) issued final regulations (Final Rule) which...

---

**EEOC and Industry Leaders Convene to Focus on Harassment Prevention**

**Hunton Andrews Kurth LLP**

In the wake of the #MeToo movement, the EEOC reconvened its task force on sexual harassment in June 2018. Most recently, in a continued effort to...

---

**Employee May Bring Hostile Work Environment Claim Under the ADA**

**Shawe Rosenthal LLP**

The U.S. Court of Appeals for the Second Circuit joined several other federal Circuits in finding that hostile work environment claims are cognizable...

---

**EEO-1 Reporting Requirements Become More Onerous . . . Maybe.**

**Kelley Drye & Warren LLP**

The Equal Opportunity Employment Commission (“EEOC”) has always required employers with 50 or more employees to submit annual reports, known as...

---

**D.C. District Court Vacates Core Elements of New Association Health Plan**



## Regulations District of Columbia

### **Littler Mendelson PC**

A federal court struck down key portions of the new association health plan (AHP) regulations last week, just days before the fledgling rules for...

---

## Injured Employee Triggers Additional Insured Coverage New York

### **Goldberg Segalla LLP**

While awaiting the Appellate Division's decision in M & M Realty of New York LLC v. Burlington Ins. Co., No. 153949/16, 2019 WL 1028971 (1st Dept. Mar...

---

## DOL Confirms ERISA Preemption of State Laws Affecting Automatic Enrollment Features in ERISA Plans

### **King & Spalding LLP**

The U.S. Department of Labor (the "DOL") issued an Information Letter on December 8, 2018 (the "Letter") confirming that state laws requiring written...

---

## DOL Releases a Proposed Rule to Clarify the Types of Compensation that Employers Must Include in the Overtime Calculation

### **Littler Mendelson PC**

On March 28, 2019, the U.S. Department of Labor (DOL) released a proposed rule to amend the regulations at 29 CFR Part 778 to clarify and update the...

---

## [Podcast]: Attorney-Client Privilege in the Employee Benefit Plan Context Audio

### **Proskauer Rose LLP**

In this episode of the Proskauer Benefits Brief, Paul Hamburger, co-chair of Proskauer's Employee Benefits & Executive Compensation Group, and...

---

## Labor Unions, Advocacy Groups, and Academics Ask Federal Trade Commission to Issue Rules Banning Non-Competes

### **Seyfarth Shaw LLP**

Academics and advocacy groups—including nonprofit organizations and several major labor unions—have filed a petition with the Federal Trade...

---

## California Legislators Take Another Stab At Preventing Employment Arbitration Agreements California

### **Hunton Andrews Kurth LLP**

California has long been considered one of the most - if not the most - protective states of employee rights. This continues to ring true, as the...

---

## Court Ruling Revives Pay Data EEO-1 Reporting Requirements District of Columbia

### **Akerman LLP**

Employers may need to begin collecting pay and hours data to report on EEO-1 forms, now that a federal district judge revived the controversial...

---

## Massachusetts Department of Family and Medical Leave Publishes Draft Paid Family Leave Regulations Massachusetts

### **Jackson Lewis PC**

The Massachusetts Department of Family and Medical Leave has published updated draft regulations implementing the Massachusetts Paid Family and...

---

### **NLRB Responds to Congressional Inquiry Regarding Proposed Joint-Employer Rule**

#### **Epstein Becker Green**

Since 2015, employers have faced continued uncertainty regarding which standard the National Labor Relations Board (“NLRB” or the “Board”) will apply...

---

### **New Jersey Bans Non-Disclosure Provisions for Claims of Discrimination, Retaliation & Harassment**

[New Jersey](#)

#### **Hogan Lovells**

Recent #MeToo-inspired media attention to workplace sexual harassment claims has caused a number of states to pass employee-friendly legislation...

---

### **DOL proposes to “update and clarify” its interpretation of joint employer status under FLSA**

#### **Constangy Brooks Smith & Prophete LLP**

On April 1, the U.S. Department of Labor issued proposed regulations to clarify its interpretation of joint employer status under the Fair Labor...

---

### **NYC Sues Over Floating Billboards**

#### **Frankfurt Kurnit Klein & Selz PC**

New York City recently sued Ballyhoo Media for displaying “Times Square-style billboards” on a barge that travels along the Manhattan and Brooklyn...

---

### **Did Mr. Stinky Create a Hostile Work Environment?**

#### **FisherBroyles LLP**

It ostensibly involves bullying, which, as we know, is not actionable in virtually every jurisdiction in the US unless it consists of acts of...

---

### **1st Cir. Rejects Challenges to Arbitration of Putative Class Action**

#### **Maurice Wutscher LLP**

The U.S. Court of Appeals for the First Circuit recently affirmed dismissal of a putative class action lawsuit that challenged the company’s...

---

### **For Employers, Sitting on the Throne Can Be Harder than Winning It**

#### **Ford & Harrison LLP**

April is a big month for Game of Thrones (GoT) fans: GoT’s eighth and final season is set to premiere on April 14...

---

### **EEO-1 Reporting Requirements Become More Onerous . . . Maybe.**

[District of](#)

[Columbia](#)

#### **Kelley Drye & Warren LLP**

The Equal Opportunity Employment Commission (“EEOC”) has always required employers with 50 or more employees to submit annual reports, known as...



---

**Fifth Circuit Affirms Preemption of Claims Under Longshore and Harbor Workers' Compensation Act - U.S. Court of Appeals for the Fifth Circuit, March 18, 2019**

**Goldberg Segalla LLP**

In a per curiam opinion, the U.S. Court of Appeals for the Fifth Circuit addressed the appeal of pro se appellant, Johnny Kirkland. He alleged...

---

**Modern Slavery and Transparency Legislation in the U.S. - States May Follow Suit** California

**K&L Gates**

In January 2012, California's Transparency in Supply Chains Act of 2010 took effect, and many non-California businesses simply shrugged. The...

---

**New DOL Opinion Letter Clarifies that Employers May Not Delay FMLA Leave Designations**

**Winston & Strawn LLP**

A recently issued Opinion Letter from the Department of Labor (DOL), Letter FMLA2019-1-A, provides that an employer may not delay designating paid...

---

**NLRB's General Counsel Issues Memos on Union Obligations**

**Shawe Rosenthal LLP**

The General Counsel (GC) of the National Labor Relations Board, Peter Robb, issued two General Counsel memos this month dealing primarily with...

---

**Fighting An Age Old Problem in the UK - Acas Issues Guidance Concerning Discrimination Against Elderly Employees**

**Littler Mendelson PC**

In the United Kingdom, the Advisory, Conciliation and Arbitration Service (ACAS) serves as an independent body providing "free and impartial..."

---

**New Jersey expands employee family and safe leave benefits** New Jersey

**Pepper Hamilton LLP**

On February 19, 2019, New Jersey Governor Phil Murphy signed legislation that amends and expands some of the State's leave laws, including the Family...

---

**New association health plan rules vacated, but old rules still valid**

**Greensfelder, Hemker & Gale, P.C.**

The battle over health benefits rages on. In the latest salvo, a group of states scored a major court victory against the Trump administration's new...

---

**Damned if You Do - Damned if You Don't - How Much Can I say?**

**Fisher Phillips**

How often have you wished that you could candidly respond to reference requests or to attacks on your organization or questions about a catastrophe ...

---

**The latest: DOJ distinguishes 'no-poach' agreements**

### **McDermott Will & Emery**

The Department of Justice filed a Statement of Interest in three related cases in the Eastern District of Washington yesterday dealing with alleged...

---

### **Maryland Raises Minimum Wage** [Maryland](#)

#### **Ford & Harrison LLP**

Maryland joined the parade of states raising the minimum wage to the magic number of \$15 per hour when the state legislature voted to override the...

---

### **Password Fatigue**

#### **Robinson & Cole LLP**

Everyone hates passwords. They are difficult to remember, and human nature is to re-use them across platforms, which is well-known to be a no-no...

---

### **What's in a Name? Stamping Out Bias in Employment Screening Processes**

[Audio](#)

#### **Littler Mendelson PC**

Implicit bias in the workplace can start as early as the application process. A key study conducted by National Bureau of Economic Research found...

---

### **U.S. Department of Labor Publishes Notice to Update "Regular Rate" Regulations**

#### **Cozen O'Connor**

Breaking its 50-year silence on the matter, on March 28 the U.S. Department of Labor Announced its intention to update the federal regulations...

---

### **New Jersey Becomes First State to Require Employers to Offer Pre-Tax Transportation Fringe Benefits**

#### **Epstein Becker Green**

On March 1, 2019, when Governor Phil Murphy signed into law Senate Bill No. 1567, "An Act concerning pre-tax transportation fringe benefits" ("NJ...

---

### **The NYC Commission on Human Rights' Online Anti-Sexual Harassment Training Video Is Now Available** [New York](#)

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: The Stop Sexual Harassment in NYC Act requires employers with 15 or more employees to conduct annual, interactive anti-sexual...

---

### **Public Sector Workers' Compensation** [Audio](#)

#### **Goldberg Segalla LLP**

Greg Horner, of Goldberg Segalla's Workers' Compensation Practice Group, joins the podcast to talk about the nuanced handling of workers' compensation...

---

### **DOT-Regulated Truck Driver's Claims Dismissed Because He Could Not Prove "Shy Bladder" Condition**

#### **Jackson Lewis PC**

An employer lawfully terminated a commercial motor vehicle driver after the driver



was unable to provide a sufficient amount of urine during a random...

---

### **Maine Lawmakers Celebrate 'Equal Pay Day' by Passing Pay History Ban**

**Jackson Lewis PC**

On April 2, Equal Pay Day, Maine's House and Senate passed a bill prohibiting employers from asking about a potential worker's wage history before...

---

### **The Consequences of Elections: Are Texas Courts Becoming More Employee Friendly?**

[Texas](#)

**Vinson & Elkins LLP**

Texas is still a long way from becoming California when it comes to employment law, and no one expects the Republican dominated Texas Legislature to...

---

### **Is the Construction Industry Building-up to a Pay Increase?**

**William Fry**

Construction workers' unions in Ireland recently lodged a claim with the Labour Court seeking, amongst other things, a 12% pay increase for...

---

### **2018 Year-End Cross-Border Government Investigations and Regulatory Enforcement Review**

**Baker & Hostetler LLP**

In the second year of the Trump administration, U.S. white collar law enforcement priorities became clearer, particularly with regard to...

---

### **Freefall: UAW Membership Declines Nearly 10 Percent**

**Barnes & Thornburg LLP**

The United Autoworkers Union (UAW) saw its membership ranks decrease drastically last year by nearly 10 percent according to a new report from the...

---

### **Eleventh Circuit Opinion Clarifies Definition of 'Similarly Situated' Comparators**

**Ogletree Deakins**

On March 21, 2019, finding in favor of an employer seeking summary judgment, the U.S. Court of Appeals for the Eleventh Circuit, in *Lewis v. City of...*

---

### **DOL Issues Long-Awaited Proposed Guidance on Application of "Regular Rate" of Pay**

**Holland & Knight LLP**

The U.S. Department of Labor has proposed a rule updating the calculation of a nonexempt employee's regular rate of pay for overtime pay...

---

### **Department of Labor Announces Proposed Joint Employer Rule**

**Dinsmore & Shohl LLP**

On April 1, 2019, the Department of Labor announced it will publish a notice of proposed rulemaking to amend its existing regulations, currently...

---

### **Equal Pay Day 2019: Introducing Seyfarth's Developments in Pay Equity Litigation Report and the 3rd Annual 50-State Pay Equity Desktop Reference**



### **Seyfarth Shaw LLP**

Synopsis: Seyfarth's Pay Equity Group is pleased to release two reference guides: the 2019 Developments in Pay Equity Litigation Report and the 3rd...

---

### **Voluntary Internal Safety Audits: "Do's" and "Don'ts"**

#### **Goldberg Segalla LLP**

There is no disputing that taking a proactive approach to safety and ensuring compliance within your company is not only prudent - but critical - for...

---

### **Cincinnati City Council Passes Ordinance Prohibiting Salary History Inquiries**

#### **Ogletree Deakins**

In a thinly veiled attempt to steal the spotlight from Cleveland, the new destination city for the National Football League, on March 13, 2019, the...

---

### **New Jersey Appellate Division Holds That Employer May Have To Provide Accommodation To Licensed Medical Marijuana User**

#### **Montgomery McCracken Walker & Rhoads LLP**

On March 27, 2019, the New Jersey Appellate Division decided that the New Jersey Law Against Discrimination's (NJLAD's) protection of employees' use...

---

### **Possession Of A Medical Marijuana Card Alone Does Not Prove Marijuana Use, Appeals Court Holds**

#### **Jackson Lewis PC**

The Ninth Circuit Court of Appeals refused to dismiss a medical marijuana-using applicant's disability discrimination claim because he did not state...

---

### **Restrictive Covenants in the Second Circuit**

#### **Crowell & Moring LLP**

Unlike in the Ninth Circuit, in states comprising the Second Circuit, common law generally governs the use of restrictive covenants. Still, many of...

---

### **City of Baldwin Park Hit with \$7 Million Sex Discrimination Verdict**

#### **Proskauer Rose LLP**

Just another day in paradise in Los Angeles... Unless you happen to be an employer. Continuing the recent spate of multi-million dollar verdicts, an LA...

---

### **Web Exclusive: If I Could Turn Back Time: Can You Find a Way To Correct Erroneous Accident Or Injury Reports To Avoid An OSHA Inspection?**

#### **Fisher Phillips**

An accident happens at your workplace, leading to an employee injury. During the hectic response, incorrect information funnels its way up to the...

---

### **"Foreign and Chinese Beauties and Hunks" - OK For Job Ads?**

#### **FisherBroyles LLP**

Both countries prohibit job discrimination based on gender and age, but not, as we shall see, based on looks or beauty per se. So, is a job ad for...

---

## **Massachusetts Releases Updated Proposed Paid Family And Medical Leave Regulations—What You Need To Know**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: On Friday evening, the Massachusetts Department of Paid Family and Medical Leave (DFML) published its revised version of the...

---

## **Utah Hopes That Third Time's a Charm for Non-Compete Statute**

**Epstein Becker Green**

The State of Utah on March 22, 2019 returned to the topic of non-competes for the third time in three years. It had passed that statute in 2016 (as...

---

## **Commission Guides Employers In How To Avoid Multi-Employer Worksite And "Controlling Employer" Liability**

**Seyfarth Shaw LLP**

Seyfarth Synopsis: Since it codified the Multi-Employer Worksite Doctrine twenty years ago, OSHA has routinely cited multiple employers at the same...

---

## **Federal Court Dismisses Independent Contractor Misclassification Suit in Favor of Arbitration**

**Holland & Knight LLP**

In a prior article following the U.S. Supreme Court's decision in *New Prime Inc. v. Oliveira*, we noted that there is likely to be future litigation...

---

## **Wisconsin Supreme Court Holds Carrying "Necessary and Indispensable" Tools in a Company Van Does Not Make a Commute Compensable**

[Wisconsin](#)

**Ogletree Deakins**

Last year, a Wisconsin court of appeals held that it was unsettled under Wisconsin law whether employers may be required to pay employees for time...

---

## **The Battle For A National Paid Leave Law Is On**

**Troutman Sanders LLP**

For the first time in many years, there seems to be momentum in Washington D.C. for the adoption of a national paid sick leave policy. Currently, nine...

---

## **Department of Labor Proposes Update To Rules Governing Calculation Of Overtime Pay (US)**

**Squire Patton Boggs**

On March 28, 2019, the United States Department of Labor ("DOL") issued a Notice of Proposed Rulemaking announcing proposed updates to the rules that...

---

## **USMCA Unlocked: Working Under the New NAFTA**

**Step toe & Johnson LLP**

USMCA Unlocked: Working Under the New NAFTA Ambassador Susan Esserman, Arun Venkataraman, Luke Tillman, and Lauren Shapiro Introduction The Trump...

---

## **Illinois Passes Bill Lifting 25 Year Statute of Repose for Occupational Disease**



## **Lawsuits** [Illinois](#)

### **Goldberg Segalla LLP**

Senate Bill 1596 passed in the House on Thursday, March 14, and is expected to be signed by Governor J.B. Pritzker in short order...

---

### **Issue 119: Court Vacates New Rules on Association Health Plans**

#### **Seyfarth Shaw LLP**

This is the one hundred and nineteenth issue in our series of alerts for employers on selected topics on Health Care Reform. (Click here to access...

---

### **Paid Family and Medical Leave Coming to Massachusetts**

#### **Raymond Law Group LLC**

In June 2018, Massachusetts took the step of passing legislation aimed at providing paid family and Medical Leave for employees. Becoming effective...

---

### **Employment Law Focus: Sexual harassment at work** [Audio](#)

#### **TLT LLP**

The Me Too campaign has led to an increase in awareness of sexual harassment. In this first Episode of our new podcast we find out how this is...

---

### **California Committee Includes Ultrafine Titanium Dioxide on Its Draft Priority 1 List for PEL Review**

#### **Bergeson & Campbell PC**

The California Division of Occupational Safety and Health's (Cal/OSHA) Health Effects Advisory Committee (HEAC) for the Development of Permissible...

---

### **ERISA Newsletter**

#### **Proskauer Rose LLP**

We often talk about the importance of evaluating whether there are any procedural obstacles to plaintiffs pursuing their ERISA...

---

### **Out Like a Lion: March Brings New Obligations to Employers Doing Business in New Jersey**

#### **Crowell & Moring LLP**

Employers that do business in the State of New Jersey, and particularly those who hold services contracts with the State of New Jersey, are finding...

---

### **Hey 2019, How Is Corporate America Doing With LGBT Policies?**

#### **FisherBroyles LLP**

Last week, the HRC released its 2019 Corporate Equality Index report—a national benchmarking tool on corporate policies and practices related to...

---

### **Eleventh Circuit Clarifies Standard for Identifying Comparators in Title VII and ADA Discrimination Cases**

#### **Ford & Harrison LLP**

On March 21, 2019, in *Lewis v. Union City*, No. 15-11362, the U.S. Court of Appeals for the Eleventh Circuit (1) clarified the...

---

## **Employer Which Helps People With Disabilities Get Jobs Fires Employee With a Disability: And Other Sad Tales from The Workplace**

### **FisherBroyles LLP**

That is, the EEOC's seemingly insatiable targeting of health care providers for alleged violations of the Americans With Disabilities Act ("ADA").

---

## **Kentucky Rejoins the Majority - New Law Permits Mandatory Arbitration Agreements**

[Kentucky](#)

### **Baker & Hostetler LLP**

A Sept. 27, 2018, Kentucky Supreme Court ruling found that mandatory arbitration agreements conditioned on employment were not enforceable. See...

---

## **Termination agreements: Employees have no right of withdrawal**

### **DLA Piper**

On February 7, 2019 the Federal Labour Court (docket number 6 AZR 75/18) ruled that employees cannot withdraw a termination agreement even if it was...

---

## **Department of Labor Proposes Amended Regulations Concerning FLSA's 'Regular Rate'**

### **Jackson Lewis PC**

The Department of Labor (DOL) has issued a Notice of Proposed Rulemaking (NPRM) to revise the regulations governing the calculation of the regular...

---

## **Federal Funding Opportunity for Transit Buses Provides Reminder to Keep Labor Concerns in Mind**

### **Fisher Phillips**

The U.S. Department of Transportation's Federal Transit Administration (FTA) recently announced an opportunity to apply for up to \$85 million in...

---

## **Labor Department's Proposed Four-Factor Rule Would Limit Joint Employment**

### **Fisher Phillips**

The U.S. Department of Labor just became the latest federal agency to propose a rule to limit the scope of joint employment liability, this time for...

---

## **Eleventh Circuit Clarifies Its 'Similarly Situated' Standard for Workplace Discrimination Claims**

### **Jackson Lewis PC**

The proper standard for comparator evidence in cases alleging intentional discrimination is "similarly situated in all material aspects," the U.S...

---

## **Germany: Premium for overtime for part-time employees - less is more?**

### **Kliemt Arbeitsrecht**

The German Federal Labour Court has clarified how premiums for overtime for part-time workers should be calculated to avoid discrimination...

---

## **DOL Publishes Proposals Interpreting "Regular Rate of Pay" in Overtime**



## **Regulations**

### **Spencer Fane LLP**

Under the Fair Labor Standards Act (FLSA), employers must generally pay non-exempt employees overtime at a rate of one and one half times the...

---

### **“Very Short” and Incredibly Loud: New EU Copyright Directive a Shot in the FANGs**

#### **Womble Bond Dickinson (US) LLP**

Opening another front in the data wars, the Members of the European Parliament, on March 26, 2019, adopted the text of a new Copyright Directive...

---

### **SEC Awards \$50 Million to Two Whistleblowers**

#### **Proskauer Rose LLP**

On March 26, 2019, the SEC’s Office of the Whistleblower announced two multi-million dollar awards to whistleblowers who provided the SEC with...

---

### **Regulatory Developments: Final SNURs Will Break New Ground under Amended TSCA**

#### **Bergeson & Campbell PC**

On March 27, 2019, the U.S. Environmental Protection Agency (EPA) posted a signed final rule that will establish final significant new use rules...

---

### **Employers Beware: Judge Greenlights Employee’s Privacy Lawsuit Over Dropbox Access**

#### **Mintz**

Many employers maintain policies limiting their employees’ expectation of privacy in the workplace, including policies that eliminate any expectation...

---

### **U.S. Supreme Court Hears Oral Argument on Agency-Deference Doctrine**

#### **Jackson Lewis PC**

Should courts defer to agency interpretations of their own regulations so long as the interpretations are reasonable, even if a court believes...

---

### **Maryland Approves Minimum Wage Increase to \$15 an Hour**

#### **Jackson Lewis PC**

Maryland has become the sixth state in the nation to adopt a minimum wage of \$15.00 per hour. The state's Democratic-controlled legislature overrode...

---

### **Department of Labor Proposes Update to FLSA Regular Rate Requirements**

#### **Frost Brown Todd LLC**

The Department of Labor (“DOL”) recently announced a proposed rule to amend and clarify the regulations governing regular rate requirements under the...

---

### **Employers Take Note: A Third California Court Invalidates Employee Non-Solicitation Agreement**

California

#### **Paul Hastings LLP**

On April 1, 2019, the United States District Court for the Northern District of



California decided the latest case in a recent trend of California...

---

### **When Union Contracts And Overtime Law Conflict: Court Provides Balance For Employers**

California

#### **Fisher Phillips**

The federal appeals court that oversees cases arising from California recently handed down an opinion that helps provide guidance to those employers...

---

### **DOL Proposes Updates to Regulations Regarding Calculating Regular Rate**

#### **Michael Best & Friedrich LLP**

On March 29, 2019, the Department of Labor (DOL) published proposed updates to regulations regarding what employers may exclude from employees'...

---

### **Process Safety Management and Small Businesses**

#### **Goldberg Segalla LLP**

OSHA has issued a Process Safety Management standard pertaining to Highly Hazardous Chemicals (HHCs), which is contained in 29 CFR 1910.119. The...

---

### **Illinois Court Dismantles Equal Pay Act Collective Action Of Group Of Female Doctors**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On March 29, 2019, in *Ahad v. Board of Trustees of Southern Illinois University, et al.*, Case No. 15-CV-3308 (C.D. Ill. Mar. 29...

---

### **Germany - Premium for overtime for part-time employees: less is more?**

#### **Ius Laboris**

The German Federal Labour Court has clarified how premiums for overtime for part-time workers should be calculated to avoid discrimination...

---

### **SEC Announces First Whistleblower Awards of 2019**

#### **Drinker Biddle & Reath LLP**

The SEC announced yesterday that it has awarded more than \$50 million to two whistleblowers—specifically, more than \$37 million to one whistleblower...

---

### **U.S. Department of Labor Issues New FMLA Guidance**

#### **Drinker Biddle & Reath LLP**

On March 14, 2019, the U.S. Department of Labor (DOL) issued an opinion letter concerning the Family Medical Leave Act (FMLA). The FMLA provides...

---

### **Cintas Becomes First Employer to Reach 100 Certified OSHA VPP-Star Worksites**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: Cintas Corporation has recently become the first company to reach 100 sites with OSHA's Voluntary Protection Program (VPP)...

---

### **Avoiding Women Is No #MeToo Answer—Good Training, Messaging Is**

#### **Duane Morris LLP**

Men cannot engage in discriminatory avoidance as a strategy to avoid sexual

harassment claims. How do we mitigate this very real risk...

---

### **Do arbitration agreements have to comply with the OWBPA?**

#### **Constangy Brooks Smith & Prophete LLP**

I can't imagine why they would. In 2014, I blogged that IBM Corporation had made a conscious decision in its separation agreements to quit including...

---

### **Employment Practices and Future Technologies - Taking the Human out of Human Resources**

#### **Morrison & Foerster LLP**

The machines are taking over. Not always apparent, but Artificial Intelligence (AI) and machine learning (ML) are finding footholds in numerous...

---

### **Department of Labor Proposes New Rule on Joint Employment Status**

#### **Vandeventer Black LLP**

On April 1, 2019, the Department of Labor (DOL) announced a proposed rule revising the standard for joint employer status under the Fair Labor...

---

### **California Supreme Court Holds Employees Cannot Sue Their Employers' Payroll Companies for Wage Claims**

California

#### **Ogletree Deakins**

On February 7, 2019, the Supreme Court of California issued its decision in *Goonewardene v. ADP, LLC*, holding that employees may not sue their...

---

### **The Big Uneasy (Part 3): When is a Release not a Release?**

#### **Vinson & Elkins LLP**

Much to the surprise of many business managers, a terminated employee who has been paid a severance may still sue for age discrimination after...

---

### **Reminder To ALL New York Employers - Training To Prevent Sexual Harassment Is Mandatory - Now!**

#### **FisherBroyles LLP**

The EEOC just sued a Chili's restaurant in Colorado alleging that "the restaurant's managing partner and assistant manager subjected female servers...

---

### **April Rules: DOL Continues Rulemaking Sprint With New Proposed Joint Employment Standard**

#### **Seyfarth Shaw LLP**

Seyfarth Synopsis: On April 1, 2019, the U.S. DOL announced a proposed rule to clarify joint employment under the FLSA. The rule would establish a...

---

### **FAQs About the DOL's Proposed Regular Rate Requirements**

#### **Ogletree Deakins**

On March 28, 2019, the U.S. Department of Labor (DOL) announced a proposed rule that would update and clarify regular rate requirements. Specifically...

---

### **Equal Pay Act Amendment Passes House of Representatives**



### **Sheppard Mullin Richter & Hampton LLP**

On March 27, 2019, the U.S. House of Representatives voted to pass the Paycheck Fairness Act, an act designed to amend and strengthen the existing...

---

### **NYC Rolls Out Comprehensive Anti-Sexual Harassment Training** New York

#### **Hogan Lovells**

As of April 1, 2019, sexual harassment prevention training has become fully ingrained in both New York State and City law. As noted in past posts...

---

### **Tipoff: New Washington State Guidance on Tips, Gratuities and Service Charges**

#### **Lane Powell PC**

Tips, gratuities and service charges increasingly have become the subject of employment disputes and the focus of government enforcement, litigation...

---

### **Not so fast ... New York City Council proposes ban on no-cause firings**

#### **Reed Smith LLP**

A New York City Council member recently proposed an amendment to the New York City Human Rights Law (NYCHRL) that would restrict fast food...

---

### **OSHA Eliminates Electronic Submission Requirement for Certain Workplace Injuries and Illness Forms, Citing Concerns for Employee Privacy**

#### **Hunton Andrews Kurth LLP**

Last August, we reported on OSHA's proposed rulemaking regarding electronic submissions of workplace injuries and illnesses in our blog entitled...

---

### **NASA Incident Reminds Employers about Proper Fit for PPE**

#### **Fisher Phillips**

As you may have seen in the news, an anticipated first all-female astronaut spacewalk had to be cancelled because the International Space Station did...

---

### **Workers' Compensation Exclusivity Provision Leads to Dismissal of Construction Worker's Complaint**

#### **Goldberg Segalla LLP**

Plaintiff Johnson Carter filed suit against Henry Carlson's Construction Company (HCCC) alleging he suffered "a variety of severe medical...

---

### **Paid Medical Leave Act, Minimum Wage Increase Take Effect** Michigan

#### **Miller Canfield PLC**

On March 29, 2019, the Improved Workforce Opportunity Wage Act (IWOWA) and the Paid Medical Leave Act (PMLA) take effect. These laws are the result...

---

### **The New "Gold Standard" - A Primer On ISO 45001**

#### **Fisher Phillips**

There's a new tool that can give businesses around the world an edge over their competition. In many cases, this advantage could be the difference...

---

### **Gonna Have To Face It We're Addicted to...Everything?! Digital Addictions In**

## **The Workplace**

### **Fisher Phillips**

Cell phones. Video games. YouTube. TV. iPads. Kindles. Online Gaming. Netflix. Hulu. Amazon Prime. Stream, click, stream, repeat...

---

## **Queensland Government Bulletin**

Queensland

### **Holding Redlich**

Channel Seven breaches children's privacy Channel Seven Melbourne Pty Ltd breached the Commercial Television Code of Practice in Seven...

---

## **DOL Proposes Another Major FLSA Rule Change: This Time on Calculating the "Regular Rate of Pay" for Overtime**

### **Dykema Gossett PLLC**

Earlier this month, the DOL published a Notice of Proposed Rulemaking ("NPRM") to increase the minimum salary level most exempt employees must be...

---

## **More DOL Letters Needed For Clarity On Enforcement Strategy (US)**

### **Squire Patton Boggs**

The U.S. Department of Labor recently issued a trio of opinion letters offering employers guidance in implementing the Family and Medical Leave Act...

---

## **Fourth Circuit Reaffirms That Regular, Reliable Attendance Is Essential Function Of Most Jobs**

### **Jackson Lewis PC**

The Fourth Circuit has reaffirmed its position that regular and reliable attendance is an essential function of most jobs. The Court held that an...

---

## **NLRB GC Clarifies Duty of Fair Representation Standards**

### **Arent Fox LLP**

In two recent memoranda, NLRB General Counsel Peter Robb has clarified the standards to be used by the Board's Regions in evaluating cases alleging...

---

## **DOL's Proposed Overtime Rule to Increase Minimum Salary for Store Managers to Remain Exempt**

### **Crowell & Moring LLP**

The U.S. Department of Labor recently issued a proposed final rule that would increase the minimum salary required for most 'white collar' employees...

---

## **USDOL Proposes Significant Changes To Joint Employment Analysis**

### **Fisher Phillips**

The US Department of Labor (USDOL) today released its much anticipated and significant Notice of Proposed Rulemaking (NPRM) intended to update and...

---

## **US - New Jersey's response to #MeToo: new law makes non-disclosure agreements for employee harassment and discrimination claims invalid**

### **Ius Laboris**



A legislative amendment implemented in New Jersey means that any agreement in which employees agree to keep details of harassment and discrimination...

---

### **U.S. Court Holds No Foreign Law Exception to the ADEA and Title VII in GM Bias Case**

#### **Proskauer Rose LLP**

On January 30, 2018, Shawn Wang ("Plaintiff"), filed suit against GM (China) Investment Co., Ltd. ("GMCIC") and General Motors (collectively...

---

### **DOL Calling! 5 Tips for Navigating a FMLA Audit**

#### **Bradley Arant Boult Cummings LLP**

Have you ever been audited by the Department of Labor? Most employers know that the DOL can perform a Fair Labor Standards Act audit to determine...

---

### **Beltway Buzz, March 29, 2019**

#### **Ogletree Deakins**

On March 29, 2019, the U.S. Department of Labor's (DOL) Wage and Hour Division (WHD) published a notice of proposed...

---

### **Eleventh Circuit holds that comparators in discrimination cases must be "similarly situated in all material respects"**

#### **Reed Smith LLP**

On March 21, 2019, the full en banc U.S. Court of Appeals for the Eleventh Circuit clarified that in order to establish a prima facie case of...

---

### **Department of Labor Proposes Updated Interpretation of Joint Employer Standard Under the FLSA**

#### **Jackson Lewis PC**

Since 1939, regulations interpreting the Fair Labor Standards Act (FLSA) have recognized that two or more "employers" can be jointly and severally...

---

## **Environment & Climate Change**



---

### **Electricity Regulation in the USA**

#### **White & Case LLP**

A structured guide to complex commercial litigation in the USA

---

### **New Mexico Joins the PFAS Fight with Major Enforcement Action**

New Mexico

#### **Goldberg Segalla LLP**

We recently reported that the lately-inaugurated governor of New Mexico, Michelle Lujan Grisham, has taken a strong stance on environmental issues...

---

### **EPA Announces New Owner Audit Program Agreement for Oil & Natural Gas Exploration and Production Facilities**

#### **Greenberg Traurig LLP**

On March 29, 2019, the Environmental Protection Agency issued its final Oil & Natural Gas Exploration and Production Facilities New Owner Audit...



---

**New Jersey Takes Aim at PFAS and Chemical Manufacturers** New Jersey**Riker Danzig Scherer Hyland & Perretti LLP**

In a move that has assuredly grabbed the attention of the regulated community, the New Jersey Department of Environmental Protection ("NJDEP")...

---

**Plant Biostimulants and Plant Regulators: EPA Publishes Draft Guidance on the Applicability of FIFRA****Bryan Cave Leighton Paisner LLP**

The past decade has seen explosive growth in the market for plant biostimulant products, with estimates of a global market approaching \$20 billion by...

---

**WildEarth Guardians v. Zinke - How Should GHG Emissions be Estimated?****Goldberg Segalla LLP**

On March 19, 2019, the United States District Court for the District of Columbia issued a ruling blocking, at least temporarily, approved oil and gas...

---

**Regulatory Update: EPA and New York Actions on PFOA and PFOS****Phillips Lytle LLP**

There has been a growing focus on per- and polyfluoroalkyl substances (PFAS) recently. This focus will pose new challenges for the regulated...

---

**New EPA Composite Wood Product Labeling Requirements Are In Effect**California**Leech Tishman Fuscaldo & Lampl LLC**

Manufacturers and other employers, including construction contractors, are obligated to advise consumers and employees of risks related to exposure...

---

**NWF Publishes Report Linking The RFS Biofuel Mandate To Environmental Harm****Bergeson & Campbell PC**

In March 2019, the National Wildlife Federation (NWF), a conservation organization working across the U.S., published a report called New Research...

---

**Las modificaciones sustanciales tras la información pública de un PGOU se consideran de interés casacional objetivo** Texas**Terraqui**

El Plan General de Ordenación Urbana de Laredo (de ahora en adelante, el PGOU de Laredo) se aprobó definitivamente mediante Acuerdo de la Comisión...

---

**Judge Orders Government to Account for Climate Change Impacts before Leasing Federal Lands to Energy Developers****White & Case LLP**

The US District Court for the District of Columbia has blocked the US Bureau of Land Management (BLM) from issuing new oil and gas drilling permits...

---

**SCOTUS declines to review Sixth Circuit decision affirming class "issue" certification** Ohio

### **Kilpatrick Townsend & Stockton LLP**

Federal Rule 23(c)(4) allows class certification of "particular issues." The question of "issue" certification has divided the Courts of Appeals...

---

### **FTC Warning Letters to Jewelry Marketers Highlight Concerns About Environmental Marketing and the Use of Hashtags . . . as well as Diamonds** **Frankfurt Kurnit Klein & Selz PC**

The Federal Trade Commission announced today that it sent letters to eight jewelry marketers, warning them that some of their online diamond...

---

### **California's Green Chemistry Program Accelerates With Several Chemicals And Products Facing Regulation** California

#### **Buchalter**

What chemical law is flying under the radar but has the potential to drastically change a variety of products and entire industries, and potentially...

---

### **New Jersey's New PFOA/PFOS Environmental Guidance Raises Authority Questions** New Jersey

#### **Duane Morris LLP**

Has NJDEP gone beyond its statutory authority in&hellip; requiring that all "persons responsible for conducting the remediation" at "all site...

---

### **EPA Releases Draft Guidance for Pesticide Registrants on Plant Regulator Label Claims, Including Plant Biostimulants**

#### **Bergeson & Campbell PC**

On March 25, 2019, the U.S. Environmental Protection Agency (EPA) posted Draft Guidance for Plant Regulator Label Claim, Including Plant...

---

### **Partially Stripped**

#### **Goldberg Segalla LLP**

On March 15, 2019, the EPA proposed as a Final Rule a scaled down version of the total ban on the use of methyl chloride in paint stripper. The EPA...

---

### **First Circuit Finds FERC Certificate Preempts Application of Local Ordinance to Deny Gas Pipeline Project Permit**

#### **Troutman Sanders LLP**

On March 19, 2019, the U.S. Court of Appeals for the First Circuit ("First Circuit") found that FERC's issuance of a certificate of public convenience...

---

### **Court Ruling a Win for Outdoor/Adventure Businesses** British Columbia

#### **MLT Aikins LLP**

There are two essential ingredients to enjoying the great outdoors. First, you need a place that has something to special to offer—let's say a lake...

---

### **Energy & Sustainability Washington Updates - April 2019**

#### **Mintz**

Since our last Washington update, Senators Grassley (R-IA) and Wyden (D-OR),



the Chairman and Ranking Member of the Senate Finance...

---

### **Oregon Air Toxic Sources Need to Focus on Their Priority and Plan** Oregon

#### **Davis Wright Tremaine LLP**

Oregon moved to regulate air toxics with SB 1541, which became effective April 10, 2018. Regulations implementing the air toxics requirements were...

---

### **Cannabis Growers and Investors: Be Sure of Your Water Rights** California

#### **Davis Wright Tremaine LLP**

In western states that have legalized cannabis over the last few years, water agencies have seen a sharp increase of permit applications to secure...

---

### **As Mobile Source Enforcement Revs Up, Does UPHE v. Diesel Power Gear Presage a Wave of Citizen Suits?**

#### **Beveridge & Diamond PC**

U.S. EPA Clean Air Act mobile source enforcement is on the upswing. Following a recent settlement with an aftermarket automotive parts manufacturer...

---

### **Trends in Climate Change Litigation: Part 1**

#### **Jenner & Block LLP**

The term “climate change litigation” has become a shorthand for a wide range of different legal proceedings associated with addressing the...

---

### **AI and Text-Based Analytics in Complex Environmental Litigation - What Environmental Practitioners Need to Know**

#### **Marten Law LLP**

The phrase “artificial intelligence” or “AI” is often used to describe several computational advances in use across many industries, including...

---

### **Breaking Bad Habitats?**

#### **Davis Wright Tremaine LLP**

As reported in this space, in November 2018, the U.S. Supreme Court remanded to the Court of Appeals for the Fifth Circuit a determination by the U.S...

---

### **Pennsylvania Lawmakers Push Nuclear Power Bailout, Further Define Alternative Energy Initiative** Pennsylvania

#### **Goldberg Segalla LLP**

Pennsylvania legislators have proposed a new law that would preserve the existence of nuclear power by funding operations via large-scale government...

---

### **Fatmucket Mussels and the March of Environmental Science**

#### **Hunton Andrews Kurth LLP**

Everyone can agree that environmental assessments should be based on the best science. The “best” science, however, is an ever-advancing standard...

---

### **FERC to Address Pipeline Overbuilding and Excessive Returns**

#### **Davis Wright Tremaine LLP**

Although primarily focused on the electric transmission industry, a recent Federal Energy Regulatory Commission (FERC) Notice of Inquiry (NOI)...

---

**Religious Organizations Legal Updates: Riparian rights: use and enjoyment of water adjacent to owned property**

**GrayRobinson PA**

Many religious organizations own land adjacent to bodies of water. Ownership of the land is established by the title to the land. But what about the...

---

**U.S. EPA Finalizes New Owner Clean Air Act Audit Program for Oil and Natural Gas Sector**

**Vorys Sater Seymour and Pease LLP**

On March 29, 2019, U.S. EPA finalized a New Owner Clean Air Act (CAA) Audit Program for new owners of upstream oil and natural gas exploration and...

---

**Plant Biostimulants and Plant Regulators: EPA Publishes Draft Guidance on the Applicability of FIFRA**

**Bryan Cave Leighton Paisner LLP**

The past decade has seen explosive growth in the market for plant biostimulant products, with estimates of a global market approaching \$20 billion by...

---

**Regulatory Developments: EPA Releases Draft Guidance for Pesticide Registrants on Plant Regulator Label Claims, Including Plant Biostimulants**

**Bergeson & Campbell PC**

On March 25, 2019, the U.S. Environmental Protection Agency (EPA) finally weighed-in on the murky and often misunderstood topic of label claims for...

---

**New Life For A Dormant Defense: Do Proposition 65 Warnings Violate The First Amendment?**

**Buchalter**

Can you be forced to slap language on a product you sell that not only do you not agree with but which can be false or misleading - and scare your...

---

**Denial of Motion to Add Additional Defendants Found to be Dispensable Upheld**

**Colorado**

**Goldberg Segalla LLP**

The plaintiff filed suit against several defendants alleging exposure to asbestos caused their development of mesothelioma...

---

**Environmental Litigation Alert: Citizen Suits Challenge Rollbacks, Replacements and Project Approvals**

**Wilmer Cutler Pickering Hale and Dorr LLP**

Over the past two years the Trump Administration has initiated a fast-paced agenda of rolling back environmental regulations, while also reexamining...

---

**EPA Updates New RT25 Data to Help Beekeepers and Farmers Protect Pollinators**



### **Bergeson & Campbell PC**

On March 21, 2019, the U.S. Environmental Protection Agency (EPA) announced it was updating its Residual Time to 25% Bee Mortality (RT25) Data Table...

---

### **Commercial Real Estate and Climate Change**

#### **Dechert LLP**

God help me, I'm finally writing about climate change. This commentary assiduously avoids the obviously political (we take the view that complaining...

---

### **Regulatory Developments: House Subcommittees Hold Hearing on EPA's IRIS Program**

#### **Bergeson & Campbell PC**

On March 27, 2019, the House Science, Space, and Technology Subcommittee on Investigations and Oversight and Subcommittee on Environment held a...

---

### **Recent Vehicle Tampering Decision May Invite Citizen Enforcement for Mobile Source Emissions**

#### **Barnes & Thornburg LLP**

Earlier this month, the U.S. District Court for the District of Utah held that a nonprofit organization could pursue an aftermarket parts retailer, a...

---

### **Energy & Sustainability Washington Updates - March 2019**

#### **Mintz**

The Senate Energy and Natural Resources Committee recently held a number of energy-related hearings. On February 7, the committee held a hearing to...

---

### **Environmental Study of Glyphosate Raises Issues Beyond Personal Injury Litigation**

#### **Goldberg Segalla LLP**

Aside from toxic tort litigation pertaining to the use of glyphosate, a recent study has evaluated environmental issues pertaining to the world's most...

---

### **New Jersey Puts PFAS Manufacturers in the Cross-Hairs**

#### **Jenner & Block LLP**

New Jersey continues to take an aggressive stance with respect to per- and polyfluoralkyl (PFAS) contamination. On March 25, 2019, the New Jersey...

---

### **Friday Enforcement Wrap: University Settles for \$112.5 Million to Resolve Allegations of False Claims**

#### **Arent Fox LLP**

The US Department of Justice announced on March 25 that Duke University agreed to a settlement in the amount of \$112.5 million to resolve allegations...

---

### **Internet & Social Media**



### **Technology policies that protect your company and its IP**

#### **Harness, Dickey & Pierce, PLC**



A computer and technology policy is an important part of protecting and managing intellectual property. A business should consider establishing a...

---

### **TINA Seeks to Influence FTC on Social Media Influencers**

#### **Manatt Phelps & Phillips LLP**

Decrying the Federal Trade Commission's (FTC's) lack of action against social media influencers, Truth in Advertising, Inc. (TINA), filed a formal...

---

### **Digitalisation and innovation provide new fuel for M&A deals**

#### **Allen and Overy LLP**

Businesses across sectors are responding to the threat of digital disruption, looking to build, buy and/or collaborate to transform their...

---

### **¿A quién pertenecen las fotos que te hagas en el Vessel de Nueva York?** New

York

#### **Cuatrecasas**

En los últimos años, el barrio de Hudson Yards en Nueva York ha Estado sujeto a un Proyecto de desarrollo inmobiliario que incluye gran cantidad de...

---

### **Blockchain Games and Collectibles - Patents and Other Legal Issues**

#### **Sheppard Mullin Richter & Hampton LLP**

The use of blockchain (or distributed ledger) technology for games (a.k.a blockchain games) and token-based digital collectibles is on the rise. The...

---

### **In Groundbreaking Settlements, Attorneys General Find Fake Social Media Engagement Illegal**

#### **Proskauer Rose LLP**

On January 30, 2019, the Office of the New York Attorney General ("NY AG") and the Office of the Florida Attorney General ("Florida AG") announced...

---

### **"ADapt your Website": Key Takeaways from the Domino's Website Litigation**

#### **Proskauer Rose LLP**

The United States Court of Appeals for the Ninth Circuit recently issued a decision holding that the Americans with Disabilities Act ("ADA") applies...

---

### **FTC Releases 2018 Privacy and Data Security Update Report**

#### **Morrison & Foerster LLP**

With privacy and data security issues dominating headlines over the past year, the Federal Trade Commission - the Nation's top privacy watchdog - has...

---

### **Federal Bill Would Expand COPPA**

#### **Manatt Phelps & Phillips LLP**

Federal lawmakers have proposed a new bill (Senate Bill 748) that would amend the Children's Online Privacy Protection Act (COPPA) to prohibit...

---

### **FTC Seeks Information from ISPs on Privacy Procedures**

#### **Robinson & Cole LLP**

The Federal Trade Commission (FTC) issued an Order to File a Special Report to seven Internet broadband providers in the U.S., requesting information...

---

**As new prepaid rule takes effect, virtual currency wallet providers need to take notice**

**DLA Piper**

On April 1, 2019, the CFPB's new Prepaid Rule takes effect, which extends Regulation E's coverage to "prepaid accounts." While much of the focus has...

---

**Continued Progress in Developing the Digital Marketplace for Copyrighted Works**

**Squire Patton Boggs**

The Copyright Act often seems to lag behind technology, with infringements rampant on the Wild Internet. Not so, as was evidenced by the robust...

---

**Senate Armed Services Subcommittee on Cybersecurity Holds Hearing to Discuss the Responsibilities of the Defense Industrial Base**

**Covington & Burling LLP**

On March 26, 2019, the Senate Armed Services Subcommittee on Cybersecurity held a hearing to receive testimony assessing how the Department of...

---

**Financial Industry Regulator Issues Cybersecurity Guidance**

**Borden Ladner Gervais LLP**

In December 2018, the United States Financial Industry Regulatory Authority issued a Report on Selected Cybersecurity Practices - 2018 to help...

---

**The future of conveyancing - A new digital age?**

**Walker Morris LLP**

In a world that is becoming increasingly digitalised, it is likely that within the next few years we will see huge technological shifts in the way...

---

**Cybersecurity Alert: Lawmakers Draft Bi-Partisan Bill to Enhance Internet of Things Security**

**Brouse McDowell**

House and Senate lawmakers recently rolled out bipartisan legislation that sets cybersecurity standards for internet-connected devices that are...

---

**Supreme Court challenges privacy litigants to demonstrate Article III standing**

**Illinois**

**Thompson Coburn LLP**

The case stems from an appeal regarding the settlement of the plaintiff class' claims against Google for violation of the Stored Communications Act...

---

**CFIUS's Axe to Grind: China's Kunlun Forced to Divest Grindr on National Security Grounds**

**Morrison & Foerster LLP**

The Committee on Foreign Investment in the United States (CFIUS) is reportedly



forcing Beijing Kunlun Tech Co. Ltd. ("Kunlun") to divest Grindr LLC...

---

**Privacy Tip #183 - Apple Announces Privacy-Protecting Credit Card**

**Robinson & Cole LLP**

Apple has partnered with Goldman Sachs to offer a privacy-protected credit card that has no signature, card number or any other personal information...

---

**Retail fraud on the rise**

**Walker Morris LLP**

Walker Morris' Retail and Commercial Dispute Resolution specialists Gwendoline Davies and Tim Pickworth look at some of the latest fraud challenges...

---

**Third-Party Outsourcing: Disrupting the Consumer Layaway Market**

**Hunton Andrews Kurth LLP**

The Chief Marketing Officer is in the General Counsel's office and says she has to have this new payment tender - "Afterpay" - live on the website...

---

**California and European Privacy FAQs: Can a supervisory authority bring an enforcement action for a violation of the ePrivacy Directive?**

[California](#)

**Bryan Cave Leighton Paisner LLP**

The California Consumer Privacy Act ("CCPA") was enacted in early 2018 as a political compromise to stave off a poorly drafted, and plaintiff's...

---

**HUD says social media platform's advertising violates FHA**

**Buckley LLP**

On March 28, HUD announced that it charged a world-wide social media platform with violating the Fair Housing Act (FHA) by allowing advertisers to...

---

**Tech Brings Authentication Challenges In Ad And IP Cases**

**Drinker Biddle & Reath LLP**

The ability of any individual, without access to sophisticated technology, to decipher the "authenticity" of any experience is diminishing daily...

---

**Still open for discussion: venue based on presence of servers**

**McDermott Will & Emery**

The US Court of Appeals for the Federal Circuit elected not to decide en banc whether servers or similar equipment in third-party facilities...

---

**FTC settles deceptive practices allegations with office supply company, tech-support vendor**

**Buckley LLP**

On March 27, the FTC announced it had entered into two stipulated orders for permanent injunction and monetary judgment (see here and here) against...

---

**Study: Trends in Cybercrime Highlight the Growing Incidence of Mobile Device Attacks**

**Winston & Strawn LLP**

On March 6, 2019, ThreatMetrix released its latest CyberCrime Report. The Report analyzed 17 billion transactions, including cybercrime attacks...

---

### **Washington State Pushes Forward With Comprehensive Privacy Legislation**

Washington

#### **Holland & Knight LLP**

On Friday, March 22, 2019, the State of Washington continued efforts to move forward on new privacy legislation. The State House of Representative's...

---

### **Seventh Circuit Wades into Big Data Case Law**

#### **Crowell & Moring LLP**

As the country's new Congress settles into their terms, several technology issues are starting to come to the fore. Several Senators have recently...

---

### **Elizabeth Warren Wants to Break Up Big Data - Could She Do It?**

#### **Kelley Drye & Warren LLP**

Presidential Candidate Elizabeth Warren thinks Big Tech is too big and wants it—and, in particular, Amazon, Facebook and Google—broken up and their...

---

### **UK Data Protection Survey Reveals Mixed Compliance Progress**

#### **Ropes & Gray LLP**

The UK Information Commissioner's Office (ICO) is calling on UK data controllers and processors to be more accountable in the wake of the latest...

---

### **Is your online application process a risk?**

#### **Porter Wright Morris & Arthur LLP**

Do you solicit and accept employment applicants electronically? If so, assume a potential applicant has physical or other disabilities making it...

---

### **Clarifications and questions on Utah's new electronic privacy law**

#### **Freshfields Bruckhaus Deringer**

First, the statute isn't a comprehensive privacy law. Sure, it's titled the "Electronic Information or Data Privacy Act." (The presence of the...

---

### **FTC imposes unprecedented fine for violations of children's online privacy rules**

#### **Pearl Cohen Zedek Latzer Baratz**

Operators of the video social networking app Musical.ly have agreed to pay a record penalty of \$5.7 million to settle an enforcement lawsuit brought...

---

### **Privacy FAQs: If a data subject submits an access or deletion request directly to a service provider, is the service provider required to respond to the data subject?**

#### **Bryan Cave Leighton Paisner LLP**

The California Consumer Privacy Act ("CCPA") was enacted in early 2018 as a political compromise to stave off a poorly drafted, and plaintiff's...

---



## **K&L Gates**

There is a lot of buzz around blockchain technology, distributed energy resources (“DERs”), microgrids, and other technological innovations in the...

---

## **Booking.com is not generic: Fourth Circuit addresses protection for “.com” trademarks**

### **McDermott Will & Emery**

Affirming the district court's summary judgment ruling on the protectability of the trademark BOOKING.COM, the US Court of Appeals for the Fourth...

---

## **All for one and one for all - EU consumer remedies unite**

### **Cooley LLP**

Last week, EU Parliament approved a proposal for a new directive on the sale of goods (New SGD). The New SGD would enhance European...

---

## **Harden Your Organization's Domain Name System (DNS) Security to Protect Against Damaging Data Loss and Insider Threat**

### **Epstein Becker Green**

The importance of the Domain Name System (DNS) to your organization's cybersecurity cannot be understated. Communications between computers on the...

---

## **Social Media: A Defense Against Union Organizing?**

### **Fisher Phillips**

A company's website used to be the primary vehicle for communicating with its external audiences, its intranet for connecting with employees. Both...

---

## **What's Next? Recent Activity in Tech Legislation**

### **Manatt Phelps & Phillips LLP**

If the action from the 116th Congress matches only half of the noise it is making regarding the tech industry, the next few months are likely to see...

---

## **Legal Practice**



## **South Carolina High Court Allows Malpractice Claim by Insurer Against its Assigned Defense Counsel**

South Carolina

### **Goldberg Segalla LLP**

Early March, in a narrow, carefully worded opinion, a divided Supreme Court of South Carolina ruled that a liability insurer may sue an attorney it...

---

## **Improve Your Storytelling: Seven Ways**

### **Holland & Hart LLP**

So you have worked up your case for trial and, now the question is, what is the best way to convert all of that factual detail and law into...

---

## **International Arbitration Passport 2019**

### **HFW**



Our international arbitration experts tell you everything you need to know about each jurisdiction, with up-to-date information about local arbitral...

---

#### **In-House Tips on Brand Protection in China**

##### **Finnegan, Henderson, Farabow, Garrett & Dunner LLP**

Managing Intellectual Property invited intellectual property attorneys and in-house counsel for global brands to discuss the usefulness of...

---

#### **DPA penalty discount for self reporting: change recommended by House of Lords committee**

##### **Allen and Overy LLP**

The operation of the Bribery Act 2010 has been subjected to post-legislative scrutiny for the first time since it came into force. A House of Lords...

---

#### **Report: Only one-third of lawyers believe their organization is very prepared to keep pace with changes in the legal market**

##### **Legisway by WoltersKluwer**

Globally, the legal sector is poised for significant transformation. Increasing information complexity, client demands, economic forces, changing...

---

#### **Expect Science Views to Vary**

##### **Holland & Hart LLP**

Jurors sometimes need to grapple with science, and given the constraints of the trial process and the often-complex nature of the testimony...

---

#### **When Is Pre-Acquisition Analysis of Patents Protected from Discovery During Litigation?**

##### **Mintz**

A Discovery Master in Limestone Memory Systems LLC v. Micron Tech., Inc. pending in the Central District of California recently provided additional...

---

#### **Public Safety Depends on Juries Chosen Without Racial Discrimination**

Mississippi

##### **Wilmer Cutler Pickering Hale and Dorr LLP**

On March 20, the U.S. Supreme Court is set to hear a particularly consequential death penalty case in which a Mississippi district attorney...

---

#### **Why the rainmaker is dead: The new rules for winning work**

##### **Prodonovich Advisory**

This senior partner (almost invariably a white male) supposedly uses his fat book of contacts and force of personality to wine, dine and charm...

---

#### **Projects & Procurement**



#### **Renewable Energy in the USA**

##### **Hunton Andrews Kurth LLP**

A structured guide to renewable energy in the USA

---

---

## **The "Great Rebuilding of America's Crumbling Infrastructure"**

### **Jones Day**

From the start of his presidential campaign, President Donald J. Trump made America's "crumbling infrastructure" one of his top priorities, promising...

---

## **Fastest 5 Minutes: Overtime Pay, CAS and GAAP, OTA Use News (March 29)**

Audio

### **Crowell & Moring LLP**

This week's Episode covers overtime pay, CAS and GAAP, and OTA use news, and is hosted by partners David Robbins and Peter Eyre. Crowell & Moring's...

---

## **Saving Israel's National Outline Plan 38 for Urban Renewal**

### **Barnea**

The housing shortage in Israel and the issue of urban renewal are constantly on the public agenda. This past year, there have been many discussions...

---

## **Emerging Technologies Washington Update- Mar 28, 2019**

### **McGuireWoods Consulting LLC**

This Week: House Energy and Commerce Subcommittee advances net neutrality legislation, Senators unveil bipartisan legislation calling for federal...

---

## **VA Vendors Beware: Mind the Company You Keep; It's Time for a Compliance Checkup**

### **Sheppard Mullin Richter & Hampton LLP**

Department of Veterans Affairs (VA) acquisitions are about to get a lot more attention - from the VA Office of Inspector General (OIG), the U.S...

---

## **All Things Protest: Section 809 Panel Recommendations (March 2019)**

Audio

### **Crowell & Moring LLP**

Crowell & Moring's "All Things Protest" podcast keeps you up to date on major trends in bid protest litigation, key developments in high-profile...

---

## **April 3, 2019 European Public Procurement: CJEU Rules Utilities Directive Applicable to Public Railway Transportation Services**

### **Kilpatrick Townsend & Stockton LLP**

At the request of the Swedish Supreme Administrative Court, the Court of Justice of the European Union (CJEU) recently issued a preliminary ruling in...

---

## **UK Infrastructure - Spring growth at the grassroots?**

### **White & Case LLP**

Uncertainty remains over the infrastructure aspirations of the UK central government. As part of a series of articles on infrastructure, Caroline...

---

## **Did the Government Shutdown Delay Your Case?**

Virginia

### **Squire Patton Boggs**

The recent shutdown of the federal government was the longest ever. The



recovery may be slow, and there may still be another shutdown coming soon...

---

#### **OFCCP Announces FY2019 Audits**

##### **Morrison & Foerster LLP**

On March 25, 2019, the Office of Federal Contract Compliance Programs (OFCCP) published the list of contractors that are scheduled to receive...

---

#### **District Court Relies on Azar's Overruling of Overpayment Rule to Deliver Another Blow to DOJ's MA Enforcement Efforts**

California

##### **Sidley Austin LLP**

On March 29, 2019, the United States District Court for the Central District of California denied the Department of Justice's Motion for Partial...

---

#### **Recent Summary Judgment Decision Highlights Potential AKS Concerns Associated with Promotional Speakers Programs**

New York

##### **Sidley Austin LLP**

A recent decision from the Southern District of New York denying defendants' motion for summary judgment identified a number of characteristics of a...

---

#### **The future of DOD contracting**

##### **DLA Piper**

DLA Piper's Government Contracts practice recently hosted a panel discussion on developments and trends affecting the future of Department of Defense...

---

#### **Highlights from the USDA listening session on federal hemp regulations**

##### **Thompson Coburn LLP**

On March 13, 2019, the U.S. Department of Agriculture ("USDA") conducted a listening session to solicit comments from interested parties to aid in...

---

#### **A pesar de las dificultades en el camino, el modelo de entrega P3 comprueba su valor**

##### **Bilzin Sumberg**

A pesar de que las asociaciones público-privadas (P3) se han convertido en el método líder en entregas de infraestructura en varios países alrededor...

---

#### **March Comes in Like a Lion: New Verification Process and Focused Reviews for Government Contractors and Subcontractors**

##### **Dinsmore & Shohl LLP**

On March 25, 2019, the Office of Federal Contract Compliance Programs (OFCCP) released its Corporate Scheduling Announcement List (CSAL)...

---

#### **Immunities of international organisations after the surprise decision in Jam v IFC: A look ahead**

##### **20 Essex Street**

In the wake of the US Supreme Court's surprise ruling in Jam v IFC, the corridors of the World Bank echo with metaphors of alarm. Chief Justice...

---

## **Challenging the Relator's Standing to Bring a Qui Tam Can Open the Door to Jurisdictional Discovery**

### **Phelps Dunbar LLP**

Is a relator's release of claims valid and enforceable if she or he executed it prior to filing a False Claims Act qui tam against the same...

---

## **The Christian Doctrine: The Double-Secret Contract Clause**

### **Seyfarth Shaw LLP**

The typical government contract contains a laundry list of standard Federal Acquisition Regulation (FAR) or Defense Federal Regulation Acquisition...

---

## **FERC Opens Inquiry on Improvements to Electric Transmission Incentives Policy**

### **Sidley Austin LLP**

On March 21, 2019, the Federal Energy Regulatory Commission ("FERC" or "Commission") issued a notice of inquiry ("NOI") in which the Commission...

---

## **Bipartisan Support for Bill Authorizing Tax Exempt Financing of Public Buildings**

### **Nossaman LLP**

A pair of Senators from both sides of the aisle, Senator Todd Young (R-Ind.) and Senator Catherine Cortez Masto (D-Nev.), introduced the Public...

---

## **Self-Disclosure and the FCA Statute of Limitations: Cochise Consultancy, Inc. v. United States v. ex rel. Billy Joe Hunt**

### **Holland & Knight LLP**

The United States Supreme Court heard oral arguments in the case mentioned in our prior blog post, Cochise Consultancy v. United States, ex rel. Hunt...

---

## **FERC Issues Proposed Order Directing Wind Farms to Provide Transmission Service over Jointly-Owned Tie Line**

### **Troutman Sanders LLP**

On March 21, 2019, the Commission issued a proposed order directing two wind energy generators, Cedar Creek Wind Energy, LLC ("Cedar Creek") and Cedar...

---

## **FERC Permits Transmission-Only Public Power Entity to Use Same Formula Rate for Future Transmission Projects in Different PJM Zones Based on Cash-Flow Method**

### **Troutman Sanders LLP**

On March 26, 2019, FERC accepted, subject to condition, AMP Transmission, LLC's ("AMP") proposed formula rate template and implementation protocols...

---

## **Despite Bumps in the Road, the P3 Delivery Model Proves its Worth**

### **Bilzin Sumberg**

Although public-private partnerships (P3s) have become a leading method of delivering infrastructure in several countries throughout the world...

---

## **Fourth Circuit: Government Not Collaterally Estopped from Prosecuting Defendant After Declining to Intervene in Civil FCA Suit Against Him**



### **Arent Fox LLP**

As a matter of first impression, the US Court of Appeals for the Fourth Circuit recently held that the Government's decision to decline to intervene...

---

### **CAS Board Begins Statutorily-Mandated CAS/GAAP Conformance**

#### **Crowell & Moring LLP**

On March 13, 2019, the Cost Accounting Standards Board (CAS Board) released a Staff Discussion Paper (SDP) on conformance of the Cost Accounting...

---

### **"Lunch-n-Learns" Under Fire as Novartis Kickback Case Moves Closer to Trial**

#### **FisherBroyles LLP**

In a ruling released earlier this week, a federal district judge decreed that the U.S. Department of Justice (DOJ) has presented sufficient evidence...

---

### **A new target: The Antitrust Division focuses on criminal antitrust violations in public procurement**

#### **Hogan Lovells**

The Antitrust Division (Division) has recently prioritized the investigation and prosecution of criminal antitrust violations involving public...

---

### **Giving Credit Where Credit is Due: University's False Claims Act Settlement Highlights Importance of Proper Accounting Practices for Federal Award Recipients**

#### **Vinson & Elkins LLP**

On March 21, 2019, the Department of Justice ("DOJ") announced that the University of Wisconsin-Madison (the "University") agreed to pay \$1.5 million...

---

Public



### **Court Rules that Petition to Dissolve Fire District is Administrative in Nature and not Subject to Referendum Process**

#### **Miller Starr Regalia**

On March 7, 2019, the Fourth District Court of Appeal published Southcott v. Julian-Cuyamaca Fire Protection District, \_\_ Cal.App.5th \_\_ (Case No...

---

### **Nonprofits Impacted by Proposed Legislation Aimed at For-Profit Institutions**

#### **Cooley LLP**

Senator Maggie Hassan (D-NH) and Senate Minority Whip Dick Durbin (D-IL) have introduced legislation intended to "hold predatory institutions...

---

### **Could a Federal Data Privacy Law be a Reality in 2019?**

#### **Squire Patton Boggs**

From the continual evolution of the California Consumer Protection Act (CCPA) to the potential ramifications of a Brexit "no-deal" on data transfers...

---

### **The Weekly Hill Update**

#### **Baker & Hostetler LLP**



BakerHostetler on Tuesday will host our 30th Annual Legislative Seminar, with members of the House and Senate from both sides of the aisle...

---

**The Zoological Society of London goes high-tech in the fight against poaching**  
**White & Case LLP**

ZSL (the Zoological Society of London) both operates the highly successful London and Whipsnade Zoos and is a key player in promoting global Animal...

---

**Will Smartphones in Classrooms Be a Thing of the Past?** California

**Atkinson Andelson Loya Ruud & Romo**

Spend any amount of time in a middle school or high school classroom across California, and you will witness firsthand the impact of smartphones on...

---

**Can the NRA fund an Australian political party? What you need to know about our election donation laws**

**MARQUE Lawyers**

The recent Al Jazeera investigation into the NRA's covert lobbying showed how foreign money could influence Australian political processes. One...

---

**An Unlikely New Target for Consumer Protection Laws: Allegations of Sexual Abuse in Religious Education** Virginia

**Ellis & Winters LLP**

West Virginia made history last week when it filed a new lawsuit about the sexual-abuse scandal embroiling the Roman Catholic Church. The state...

---

**From RMBS to SLABS: Is History Repeating Itself?**

**Bilzin Sumberg**

The fallout from the last financial crisis and recession is far from over. More than a decade after the demise of Lehman and Bear Stearns, among...

---

**The Tangled Web of Global Approvals**

**Freshfields Bruckhaus Deringer**

Are you prepared to navigate the increasingly sophisticated process for national security approvals on your next merger or acquisition? The explosion...

---

**Schooled in law**

**White & Case LLP**

We added a new partnership with the Grunin Center for Law and Social Entrepreneurship at New York University School of Law to our growing roster of...

---

**4 Challenges For College GCs After Admissions Scandal**

**Brownstein Hyatt Farber Schreck LLP**

For some time now, the college admissions process for athletes and nonathletes alike has been the subject of considerable controversy...

---

**29 March 2019: Brexit Day Update**

**Greenberg Traurig LLP**

Today, 29 March 2019, was planned to be Brexit day: the UK would leave the EU at 23:00 GMT. That plan has had to be abandoned and Brexit day...

---

#### **Daily Brexit Update - 29 March 2019**

##### **Baker McKenzie**

MP's reject May's withdrawal agreement - what happens next...(BBC) May's deal was rejected by 344 votes to 286 and the Government has therefore lost the...

---

#### **Thank You for Attending Our Safety Act Webinar**

##### **LeClairRyan**

Thank you to those of you who joined us today for our ongoing Aviation Webinar Series, with this edition focusing on the Safety Act. Among the...

---

#### **Washington Tax Update: Congress, Treasury, Global - April 2019**

##### **Potomac Law Group PLLC**

The House failed to override the President's veto of a congressional resolution that would have prevented him from using a national emergency...

---

#### **Competition Law Enforcement Trends and Developments in the U.S., Europe and China: Looking Ahead to 2019**

##### **Covington & Burling LLP**

For the first time since its formation, the FTC was completely reconstituted due to five new commissioners being seated in 2018. The new slate...

---

#### **Blaney's appeals: Ontario Court of Appeal Summaries (March 25-29, 2019)**

Ontario

##### **Blaney McMurtry LLP**

There were only four substantive civil decisions released. In two of them, the Court continued to provide guidance on the Anti-SLAPP provisions of...

---

#### **Privacy & Cybersecurity Update**

##### **Skadden Arps Slate Meagher & Flom LLP**

In this month's edition of our Privacy & Cybersecurity Update, we examine new cybersecurity legislation in California and Massachusetts, the British...

---

#### **Navigating the Shifting Trade Landscape - Key Take-Aways from McCarthy Tétrault's 9th Annual Retail and Consumer Markets Summit (Series Part One)**

##### **McCarthy Tétrault LLP**

We recently hosted our 9th annual Retail and Consumer Markets Summit, our yearly client-focused event that canvasses the most timely and relevant...

---

#### **Update: Senate Version of TRACED Act Gains Yet More Bipartisan Support**

##### **Squire Patton Boggs**

The US Senate version of the TRACED Act, S.B. 151, gained eight more co-sponsors yesterday. Senators Jon Tester (D-MT), Todd Young (R-IN), Angus King...

---



**Change.org responds to The Independent Group new name, IPOS GI registry, and delays at IP Australia: news digest**

**World Trademark Review**

Every Tuesday and Friday, WTR presents a round-up of news, developments and insights from across the trademark sphere. In our latest edition, we look...

---

**North Carolina Legislative Update, March 29, 2019** [North Carolina](#)

**Brooks Pierce McLendon Humphrey & Leonard LLP**

Activity at the General Assembly continued to accelerate this week as joint appropriations committees held their final meetings and prepared to...

---

**Direct Purchases of Bonds By Banks: A Popular Alternative for Municipalities**

**Foster Swift Collins & Smith PC**

Traditionally, municipalities have sold bonds through competitive sales and negotiated sales. In a competitive sale, bids from interested buyers are...

---

**CFTC Passes Provision to Provide Greater Brexit-Related Market Certainty by Unanimous Vote**

**Katten Muchin Rosenman LLP**

On May 25, the Commodity Futures Trading Commission adopted an interim final rule designed to provide greater certainty to the global marketplace in...

---

**Traced Act Scheduled for Senate Commerce Committee Action**

**Squire Patton Boggs**

The U.S. Senate version of the TRACED Act, S.151, is on the schedule for a full Senate Commerce, Science and Transportation Committee markup tomorrow...

---

**2019 Session: Randy Henderson, Mayor, City of Fort Myers** [Video](#)

**GrayRobinson PA**

In this week's GRay Matters, Robert Stuart interviews Randy Henderson, Mayor of the City of Fort Myers, discussing their priorities for the 2019...

---

**NCGA Week in Review- Mar 29, 2019** [North Carolina](#)

**McGuireWoods Consulting LLC**

While North Carolina lawmakers were hard at work in committee meetings and holding floor vote sessions this week, the U.S. Supreme Court heard oral...

---

**Moving the needle** [Ohio](#)

**Graydon Head & Ritchey LLP**

The City of Cincinnati last week asked its employees to take immediate steps to preserve text messages that discuss public business, even those...

---

**Potential New Tax Law Would Allow NCAA Athletes to Profit From Their Image**

**Goldberg Segalla LLP**

On March 14, 2019, Rep. Mark Walker (R-N.C.) introduced a bill that would allow NCAA athletes to profit from their image and likeness. The...

---

## **What is the Status of Legislation to Expand New Jersey's Medical Marijuana Program**

New Jersey

### **Porzio Bromberg & Newman PC**

In New Jersey, most of the attention concerning cannabis has focused on the legalization of adult use cannabis. On March 12, Governor Phil Murphy...

---

## **NC Legislative Update: March 29, 2019**

North Carolina

### **Nexsen Pruet**

New legislation continued to be filed this week with the Senate's bill filing deadline approaching on Tuesday, April 2nd. The House has a few weeks...

---

## **Court Overturns Trump Administration Efforts to Revoke Withdrawal Status for Outer Continental Shelf Lands**

### **Wilmer Cutler Pickering Hale and Dorr LLP**

On March 29, 2019, the United States District Court for the District of Alaska issued its ruling in a case challenging a presidential executive order...

---

## **Affirm GC Manny Alvarez Appointed California DBO Commissioner**

### **McGuireWoods LLP**

On Thursday, March 28, California Governor Gavin Newsom announced that Manuel "Manny" Alvarez, 38, has been appointed Commissioner of the California...

---

## **NC Politics in the News- Apr 1, 2019**

North Carolina

### **McGuireWoods Consulting LLC**

Did you know North Carolina is the fourth-largest producer of strawberries in the nation? Farmers across the state are gearing up for one of their...

---

## **Hemp and CBD Sales Bill Cultivated in Ohio**

Ohio

### **Frost Brown Todd LLC**

Hemp is not marijuana - let us start there. This is a critical distinction the Ohio legislature has learned through the lobbying efforts of our firm's...

---

## **What Schools Need to Know About CFPB's Prepaid Accounts Regulation**

### **Womble Bond Dickinson (US) LLP**

Counsel at schools and universities understandably don't follow legal developments in financial services very closely, but recent changes in...

---

## **The role of the courts in public education**

Florida

### **White & Case LLP**

Following our court victory to obtain necessary and state-of-the-art medical screening for the children of Flint after the water crisis, we are now...

---

## **Virginia Exempts Financial Institutions from Debt Management Plan Agency Regulations**

Virginia

### **Hudson Cook LLP**



On March 8, 2019, Virginia enacted House Bill 2284, which amends Va. Code § 6.2-2001 to exempt any bank, savings institution or credit union from...

---

### **At Long Last...ED Issues Guidance Regarding Implementation of the 2016 Borrower Defense to Repayment Rules**

**Cooley LLP**

Following a court ruling in September 2018 making the delayed Obama-era Borrower Defense to Repayment regulations immediately effective, the...

---

### **Religious Organizations Legal Updates: Guns in Places of Worship? The Debate Continues.**

**Florida**

**GrayRobinson PA**

In the wake of multiple tragic shootings, the debate continues whether religious organizations should permit members to carry firearms when...

---

### **Recent Developments in State Authorization**

**Cooley LLP**

As outlined in our previous posts on proposed regulations in California, we are also tracking newly proposed laws introduced in Washington State...

---

### **Antitrust authorities maintain the pressure on dealmakers**

**Allen and Overy LLP**

The willingness of competition authorities to intervene in proposed mergers across the world remained undiminished in 2018, and there is every reason...

---

### **Corp Fin Director Highlights the Need for Tailored Brexit Disclosures and Principles-Based Sustainability Disclosures**

**White & Case LLP**

In his March 15, 2019 speech<sup>1</sup> at the 18th Annual Institute on Securities Regulation in Europe, William Hinman, Director of the Securities and...

---

### **Federal Budget 2019: A laser focus on re-election**

**Corrs Chambers Westgarth**

Federal Treasurer Josh Frydenberg's maiden Federal Budget, released on 2 April (with an election only a matter of weeks away) is laser-focussed on...

---

### **SEC advises on how to disclose complex, uncertain and evolving risks, including Brexit - Let investors see with management's eyes**

**Freshfields Bruckhaus Deringer**

At a recent conference in London, Bill Hinman, Director of the SEC's Division of Corporation Finance, spoke about crafting reliable and robust...

---

### **Brexit update: cross-country recognition of derivative trading and infrastructure**

**Macfarlanes LLP**

On a departure of the United Kingdom from the European Union on 29 March 2019 without a transition agreement (a hard Brexit), UK entities would...

---



## **ESMA Publishes Statement on Preparations Regarding Clearing and Settlement for a No-Deal Brexit**

### **Katten Muchin Rosenman LLP**

On March 28, the European Securities and Markets Association (ESMA) published a statement updating market participants on its preparations for the...



## **Global**

### **Employment & Labor**



#### **Sponsored business immigration in Austria**

##### **Oberhammer Rechtsanwälte**

A structured guide to employer-sponsored immigration in Austria

#### **Un-sponsored business immigration in Canada**

##### **Segal Immigration Law**

A structured guide to immigration routes for entrepreneurs, investors and highly skilled foreign professionals in Canada

#### **Global employee termination law: Indonesia**

##### **SSEK Indonesian Legal Consultants**

A structured guide to termination law in Indonesia, covering notice, redundancies, dismissal and protections.

#### **Managing the employment relationship in Morocco**

##### **DLA Piper**

A structured guide to country specific laws, misclassification, contracts and foreign workers in Morocco

#### **Un-sponsored business immigration in Luxembourg**

##### **Immigration Law Associates**

A structured guide to immigration routes for entrepreneurs, investors and highly skilled foreign professionals in Luxembourg

#### **Global employee termination law in Cyprus**

##### **Dr K Chrysostomides & Co**

A structured guide to termination law in Cyprus covering notice, redundancies, dismissal and protections

#### **Managing the employment relationship in Kenya**

##### **Munyao Muthama & Kashindi Advocates**

A structured guide to country specific laws, misclassification, contracts and foreign workers in Kenya

#### **Un-sponsored business immigration in Ireland**

### **Mason Hayes & Curran**

A structured guide to immigration routes for entrepreneurs, investors and highly skilled foreign professionals in Ireland

---

### **Overview and Q&A: Construction and Projects in Qatar**

#### **K&L Gates**

The Q&A is part of the global guide to construction and projects. Areas covered include trends and significant deals, the main parties, procurement...

---

### **The importance of inventing a way forward for women in IP**

#### **Phillips Ormonde Fitzpatrick**

Across the world, individuals, companies and firms have been celebrating women's achievements as part of International Women's Day, and Women's...

---

### **Delivering value and managing risks: how human rights are relevant for business**

#### **White & Case LLP**

Mounting pressure on businesses to gain clarity on their social and environmental footprint will challenge corporate operations in 2019. New risks...

---

### **I migliori consigli sul whistleblowing - I nostri migliori consigli per un sistema di whistleblowing efficiente e affidabile**

#### **WhistleB**

Poiché il whistleblowing è stato al centro delle notizie nel 2018, abbiamo deciso di iniziare il 2019 parlando con voi di tutto quello che, secondo...

---

### **Whistleblowing: a trusted channel in the organisational ethics toolkit**

#### **WhistleB**

This is the fourth annual customer study carried out by WhistleB. It was conducted in February 2019 and combines results from a questionnaire sent to...

---

### **Global - Comparing rates and types of minimum wage across the world**

#### **Ius Laboris**

Most countries have a national minimum wage in some form: in some it is regulated on a monthly basis, but in others a daily or hourly basis. Click to...

---

### **Adapting EU employment law to the new world of work**

#### **Freshfields Bruckhaus Deringer**

EU negotiators have been busy with employment matters recently, launching the European Labour Authority and agreeing on the details of a new...

---

## **Environment & Climate Change**



### **Oil and gas environmental protection laws in Lebanon**

#### **Kouatly & Associates**

A structured guide to oil and gas environmental protection laws in Lebanon

---



## **Pollution control regulations in the European Union**

### **White & Case LLP**

A structured guide to soil, air and water pollution regulations in the European Union

---

## **Oil and gas environmental protection laws in Venezuela**

### **InterJuris Abogados**

A structured guide to oil and gas environmental protection laws in Venezuela

---

## **Energy disputes regulation in Brazil**

### **FUX Advogados**

A structured guide to energy disputes regulation in Brazil

---

## **The path to a Global Pact for the Environment**

### **White & Case LLP**

In 2018, the United Nations adopted a resolution to explore the creation of a universal environmental charter based in international law—a Global...

---

## **A blueprint for financing climate action at scale**

### **White & Case LLP**

Our lawyers co-authored a White Paper with the G20 Sustainable Finance Study Group that calls for the creation of a sustainable collateralized loan...

---

## **Internet & Social Media**



## **Fintech financing, investment and government support in Jersey**

### **Ogier**

A structured guide to fintech financing, investment and government support in Jersey

---

## **Electronic contracts and signatures in Luxembourg**

### **NautaDutilh**

A structured guide to electronic contracts and signatures in Luxembourg

---

## **Data security and breach notification in Finland**

### **Dittmar & Indrenius**

A structured guide to data security and breach notification in Finland

---

## **Data security and breach notification in France**

### **ADSTO**

A structured guide to data security and breach notification in France

---

## **Electronic contracts and signatures in Belgium**

### **Lydian**

A structured guide to electronic contracts and signatures in Belgium

---

## **Electronic contracts and signatures in Brazil**

### **Pinheiro Neto Advogados**

A structured guide to electronic contracts and signatures in Brazil

---

### **Electronic payments in Germany**

#### **SKW Schwarz Rechtsanwälte**

A structured guide to electronic payments in Germany

---

### **Electronic contracts and signatures in Canada**

#### **Stikeman Elliott LLP**

A structured guide to electronic contracts and signatures in Canada

---

### **Electronic marketing and internet use in Colombia**

#### **Baker McKenzie**

A structured guide to electronic marketing and internet use in Colombia

---

### **Patent litigation in autotech markets: new technologies, new plaintiffs?**

#### **Taylor Wessing**

These are just a few of the points that automobile manufacturers and their suppliers are currently confronted with. In the past, automobile...

---

### **Policing the internet: aligning the internet with the real world**

#### **Macedo Vitorino & Associados**

The Internet is open to anyone with a mobile phone hiding behind an Internet 'identity', and this is where the real work is for Governments and...

---

### **Five ways IoT will change retail**

#### **Gowling WLG**

IoT is becoming increasingly prominent in our daily lives. According to Statista, the global IoT market is set to grow to \$8.9 trillion by 2020...

---

### **Sudan dissolves Appeal Committee, WIPO AI image search, and most admired Canadian brand: news digest**

#### **World Trademark Review**

Every Tuesday and Friday, WTR presents a round-up of news, developments and insights from across the trademark sphere. In our latest edition, we look...

---

### **Key Considerations When Contracting Cloud**

#### **Baker McKenzie**

The use of cloud systems raises questions on control over the equipment, software and most importantly... the data. This increases the need for a solid...

---

## **Projects & Procurement**



### **Construction project financing and payment in Russia**

#### **Clifford Chance**

A structured guide to construction project financing and payment in Russia

---



## **Driverless Cars**

### **Linklaters LLP**

The advent of driverless cars promises a fundamental transformation of the way we transport people and goods, how we spend time, and how we organise...

Public



## **Brexit - International Trade and WTO Rules**

### **Allen and Overy LLP**

At the heart of what Brexit will actually mean for business are the UK's terms of trade with the EU27 and the rest of the world after it leaves the...

## **Brexit - the UK and Free Trade**

### **Allen and Overy LLP**

At the heart of what Brexit could actually mean for businesses with a trading link to the UK will be the terms of trade agreed between the UK and its...

## **Is education a right for migrant children?**

### **White & Case LLP**

Our research forms the basis of ongoing advocacy work to expand access to education for migrants and provides insight into concrete actions that...

## **Brexit Update: What next for cross-border restructuring?**

### **DLA Piper**

Immediately following the results of the UK referendum on exiting the EU in June 2016, we wrote about the potential impact of Brexit on cross-border...

## **Global M&A Insights | Q1 2019**

### **Allen and Overy LLP**

Commentators have wondered for some time when the deal market would end its record-breaking bull run. The question is whether the latest data marks...

## **The Week Ahead in the European Parliament - Friday, March 29, 2019**

### **Covington & Burling LLP**

Next week will be a mixed week in the European Parliament with a mini Plenary and committee meetings. Members of the European Parliament ("MEPs")...

## **Asset Management & Investment Funds: EU & International Developments: March 2019**

### **A&L Goodbody**

In case of a no-deal Brexit, UK administrators included in the ESMA register of administrators and third-country benchmarks (ESMA register) before...

## **No deal Brexit - trading on the basis of WTO rules**

### **Allen and Overy LLP**

The protracted negotiations over the terms of the UK's withdrawal from the EU have brought into stark focus the prospects of a 'hard' Brexit. One of...



## Other top stories

Managing the employment relationship in Massachusetts

---

The Perils of Electing S Corporation Status

---

The California Consumer Privacy Act: Frequently Asked Questions

---

Cyber Quarterly - March 2019

---

Forcing Employee to Quit Second Job Is Not a Tangible Job Action?

---

Digital currency and DLT developments around the world - March 2019

---

12 Weeks is 12 Weeks: DOL Clamps Down on FMLA Leave

---

The Future of Work: Five Developing Trends for Technology, Media, and Telecommunications Employers

---

What would the perfect employee agreement look like?

---

The "dark overlord" strikes the practice of law: what law firms can do to protect themselves

---

## International developments

2019 Years a Slave

---

Al Jazeera's One Nation sting wasn't just legally solid, it was ethically responsible too

---

Episode 39: Can an Employer be Held Liable for the Deliberate Disclosure of 100,000 Employees' Data by a Rogue Employee? [Audio](#)

---

Ontario Labour Relations Board Sheds Light on Severance Pay Calculation Rules

---

Summary Judgment May Not Be Appropriate for Determining Reasonable Notice

---

A Business Deal Is a Business Deal... or Is It?

---

Denunciation by Whistleblowers: was the Ex-Employee's Defamation Suit Abusive?

---

BREXIT - Urgent measures for the operation of UK insurance undertakings and distributors in case of hard BREXIT - Law Decree n. 22 dated 25 March 2019

---

Expansion Of Time Recording Obligation In Spain

---

N.L. Supreme Court: Undue Hardship Can Arise from Inability to Measure Cannabis Impairment and Manage Workplace Risk

---

Proposed Changes to Canadian Stock Option Deduction

---

China reaffirms its prohibition on gender discrimination in employment recruiting

---

Dentro de dos meses, registro diario de jornada. ¿Para todos? [ES](#)

---

BREXIT - Pubblicato il Decreto Legge sull'operatività di compagnie e intermediari assicurativi e riassicurativi in caso di hard Brexit [IT](#)

---

**Massenentlassungsanzeige: Nicht jeder Fehler schadet** [DE](#)

---

**Brexit (Italy) Banking activities & investment services carried out by UK operators in case of no deal and the implementing measures issued by CONSOB and Bank of Italy**

---

**Social Licence and the Rule of Law**

---

**No todos los biocombustibles merecen la calificación de «combustibles verdes»** [ES](#)

---

**Cómputo de las faltas justificadas al trabajo a efectos de despido** [ES](#)

---

**Auskunftsanspruch nach Entgelttransparenzgesetz gilt nicht für freie Mitarbeiter** [DE](#)

---

**Voto por correo en elecciones sindicales. Modalidad establecida por acuerdo** [ES](#)

---

**Impugnación de oficio de una suspensión colectica. Dies a quo** [ES](#)

---

[Unsubscribe](#) | [Disclaimer](#) | [Privacy policy](#)

This email is being sent to you by Lexology on behalf of the Calbar Public Law

[Contact Lexology](#)

[About Lexology](#)



© 2006-2019 Globe Business Media Group

**From:** [US-CERT](#)  
**To:** [Tanner McGinnis](#)  
**Subject:** SB19-077: Vulnerability Summary for the Week of March 11, 2019  
**Date:** Monday, March 18, 2019 10:37:43 AM



National Cyber Awareness System:

## **[SB19-077: Vulnerability Summary for the Week of March 11, 2019](#)**

03/18/2019 09:07 AM EDT

Original release date: March 18, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- sourcetree	There was an argument injection vulnerability in Atlassian Sourcetree for macOS from version 1.2 before version 3.1.1 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for macOS is able to exploit this issue to gain code execution on the system.	2019-03-08	<a href="#">9.0</a>	<a href="#">CVE-2018-20234</a> <a href="#">CONFIRM</a>
atlassian -- sourcetree	There was an argument injection vulnerability in Atlassian Sourcetree for Windows from version 0.5a before version 3.0.15 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for Windows is able to exploit this issue to gain code execution on the system.	2019-03-08	<a href="#">9.0</a>	<a href="#">CVE-2018-20235</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
atlassian -- sourcetree	There was an command injection vulnerability in Sourcetree for Windows from version 0.5a before version 3.0.10 via URI handling. A remote attacker could send a malicious URI to a victim using Sourcetree for Windows to exploit this issue to gain code execution on the system.	2019-03-08	<a href="#">9.3</a>	<a href="#">CVE-2018-20236</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
cisco -- nx-os	A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to gain read and write access to a critical configuration file. The vulnerability is due to a failure to impose strict filesystem permissions on the targeted device. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow an attacker to use the content of this configuration file to bypass authentication and log in as any user of the device. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(3)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	<a href="#">7.2</a>	<a href="#">CVE-2019-1601</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the user account management interface of Cisco NX-OS Software could allow an authenticated, local attacker to gain elevated privileges on an affected device. The vulnerability is due to an incorrect authorization check of user accounts and their associated Group ID (GID). An attacker could exploit this vulnerability by taking advantage of a logic error that will permit the use of higher privileged commands than what is necessarily assigned. A successful exploit could allow an attacker to execute commands with elevated privileges on the underlying Linux shell of an affected device. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 8.2(3), and 8.3(2). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	<a href="#">7.2</a>	<a href="#">CVE-2019-1604</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary code as root. The vulnerability is due to incorrect input validation in the NX-API feature. An attacker could exploit this vulnerability by sending a crafted HTTP or HTTPS request to an internal service on an affected device that has the NX-API feature enabled. A successful exploit could allow the attacker to cause a buffer overflow and execute arbitrary code as root. Note: The NX-API feature is disabled by default. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.1(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(8) and 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(8). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and	2019-03-08	<a href="#">7.2</a>	<a href="#">CVE-2019-1605</a> <a href="#">B.D</a> <a href="#">CISCO</a>

	6000 Series Switches are affected in versions prior to 7 3(2)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 7 3(3)D1(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I4(8) and 7 0(3)I7(1). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).			
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3).	2019-03-08	7.2	<a href="#">CVE-2019-1607</a> B D CISCO
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7 3(3)D1(1), and 8.2(3).	2019-03-08	7.2	<a href="#">CVE-2019-1608</a> B D CISCO
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(2). Nexus 3500 Platform Switches are affected in versions prior to 7 0(3)I7(6). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7 0(3)I7(6). Nexus 3600 Platform Switches are affected in versions prior to 7 0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7 3(3)D1(1), 8 2(3), and 8.3(2). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7 0(3)I4(9) and 7.0(3)I7(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	7.2	<a href="#">CVE-2019-1609</a> B D CISCO
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 3500 Platform Switches and Nexus 3000 Series Switches software versions prior to 7 0(3)I7(4) are affected.	2019-03-11	7.2	<a href="#">CVE-2019-1610</a> B D CISCO
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software and Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Firepower 4100 Series Next-Generation Firewalls are affected running software versions prior to 2.2.2.91, 2.3.1.110, and 2.4.1.222. Firepower 9300 Security Appliance are affected running software versions prior to 2.2.2.91, 2.3.1.110, and 2.4.1.222. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(25) and 8.3(1). Nexus 3000 Series Switches are affected running software versions prior to 7 0(3)I4(9) and 7 0(3)I7(5). Nexus 3500 Platform Switches are affected running software versions prior to 7 0(3)I7(5). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected running software versions prior to 7.1(5)N1(1b) and 7 3(4)N1(1). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22), 7 3(3)D1(1), 8 2(3). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9) and 7 0(3)I7(5). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5).	2019-03-11	7.2	<a href="#">CVE-2019-1611</a> B D CISCO
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7 0(3)F3(5).	2019-03-11	7.2	<a href="#">CVE-2019-1612</a> B D CISCO
cisco -- nx-os	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The vulnerability is due to incorrect input validation of user-supplied data by the NX-API subsystem. An attacker could exploit this vulnerability by sending malicious HTTP or HTTPS packets to the management interface of an affected system that has the NX-API feature enabled. A successful exploit could allow the attacker to perform a command-injection attack and execute arbitrary commands with root privileges. Note: NX-API is disabled by default. MDS 9000 Series Multilayer Switches are affected running software versions prior to 8.1(1b) and 8 2(3). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)I7(4). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected running software versions prior to 7 3(4)N1(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 7000 and 7700 Series Switches are affected running	2019-03-11	9.0	<a href="#">CVE-2019-1614</a> B D CISCO



	software versions prior to 7.3(3)D1(1) and 8.2(3).			
cisco -- spa514g_firmware	A vulnerability in the implementation of Session Initiation Protocol (SIP) processing in Cisco Small Business SPA514G IP Phones could allow an unauthenticated, remote attacker to cause an affected device to become unresponsive, resulting in a denial of service (DoS) condition. The vulnerability is due to improper processing of S P request messages by an affected device. An attacker could exploit this vulnerability by sending crafted S P messages to an affected device. A successful exploit could allow the attacker to cause the affected device to become unresponsive, resulting in a DoS condition that persists until the device is restarted manually. Cisco has not released software updates that address this vulnerability. This vulnerability affects Cisco Small Business SPA514G IP Phones that are running firmware release 7.6.2SR2 or earlier.	2019-03-13	7.8	<a href="#">CVE-2018-0389</a> B D <a href="#">CISCO</a>
cobham -- satcom_sailor_800_firmware	Cobham Satcom Sailor 800 and 900 devices contained a vulnerability that allowed for arbitrary writing of content to the system's configuration file. This was exploitable via multiple attack vectors depending on the device's configuration. Further analysis also indicated this vulnerability could be leveraged to achieve a Denial of Service (DoS) condition, where the device would require a factory reset to return to normal operation.	2019-03-15	7.8	<a href="#">CVE-2018-19393</a> MISC MISC
ftpgetter -- ftpgetter	FTPGetter Standard v.5.97.0.177 allows remote code execution when a user initiates an FTP connection to an attacker-controlled machine that sends crafted responses. Long responses can also crash the FTP client with memory corruption.	2019-03-13	7.5	<a href="#">CVE-2019-9760</a> MISC <a href="#">EXPLOIT-DB</a>
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 154069.	2019-03-11	7.2	<a href="#">CVE-2018-1978</a> B D XF <a href="#">CONFIRM</a>
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 154078.	2019-03-11	7.2	<a href="#">CVE-2018-1980</a> B D XF <a href="#">CONFIRM</a>
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 155893.	2019-03-11	7.2	<a href="#">CVE-2019-4015</a> B D XF <a href="#">CONFIRM</a>
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 155894.	2019-03-11	7.2	<a href="#">CVE-2019-4016</a> B D XF <a href="#">CONFIRM</a>
ibm -- websphere_mq	BM WebSphere MQ 8.0.0.0 through 9.1.1 could allow a local user to inject code that could be executed with root privileges. This is due to an incomplete fix for CVE-2018-1792. IBM X-Force D: 154887.	2019-03-11	7.2	<a href="#">CVE-2018-1998</a> XF <a href="#">CONFIRM</a>
intel -- converged_security_management_engine_firmware	Bounds check in Kernel subsystem in Intel CSME before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20, or Intel(R) Server Platform Services before versions 4.00.04.383 or SPS 4.01.02.174, or Intel(R) TXE before versions 3.1.60 or 4.0.10 may allow an unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12191</a> <a href="#">CONFIRM</a>
intel -- converged_security_management_engine_firmware	Logic bug in Kernel subsystem in Intel CSME before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20, or Intel(R) Server Platform Services before version SPS_E5_04.00.04.393.0 may allow an unauthenticated user to potentially bypass MEBx authentication via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12192</a> <a href="#">CONFIRM</a>
intel -- converged_security_management_engine_firmware	Buffer overflow in an OS component in Intel CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 and Intel TXE version before 3.1.60 or 4.0.10 may allow a privileged user to potentially execute arbitrary code via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12199</a> <a href="#">CONFIRM</a>
intel -- graphics_driver	Potential memory corruption in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12214</a> <a href="#">CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12216</a> <a href="#">CONFIRM</a>
intel -- graphics_driver	Logic bug in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12220</a> <a href="#">CONFIRM</a>
intel -- platform_sample_firmware	Denial of service vulnerability in Platform Sample/ Silicon Reference firmware for 8th Generation Intel Core Processor, 7th Generation Intel Core Processor may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12203</a> <a href="#">CONFIRM</a>
intel -- platform_sample_firmware	Privilege escalation vulnerability in Platform Sample/ Silicon Reference firmware Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12204</a> <a href="#">CONFIRM</a>
intel -- platform_sample_firmware	Privilege escalation vulnerability in Platform Sample/ Silicon Reference firmware for 8th Generation Intel(R) Core Processor, 7th Generation Intel(R) Core Processor may allow unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12205</a> <a href="#">CONFIRM</a>
microvirt -- memu	An issue was discovered in Microvirt MEmu 6.0.6. The MemuService.exe service binary is vulnerable to local privilege escalation through binary planting due to insecure permissions set at install time. This allows code to be run as NT AUTHORITY\SYSTEM.	2019-03-13	7.2	<a href="#">CVE-2018-20621</a> MISC
nablarch_project -- nablarch	Nablarch 5 (5, and 5u1 to 5u13) allows remote attackers to conduct XML External Entity (XXE) attacks via unspecified vectors.	2019-03-12	8.5	<a href="#">CVE-2019-5918</a> JVN MISC
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_FD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.	2019-03-08	7.5	<a href="#">CVE-2019-9638</a> MISC DEBIAN
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_FD_in_MAKERNOTE because of mishandling the data_len variable.	2019-03-08	7.5	<a href="#">CVE-2019-9639</a> MISC DEBIAN
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.	2019-03-08	7.5	<a href="#">CVE-2019-9640</a> MISC DEBIAN
	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before			<a href="#">CVE-2019-9641</a>



php -- php	7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in <code>exif_process_FD_in_TFF</code> .	2019-03-08	7.5	MISC DEBIAN
phpshe -- phpshe	A SQL Injection was discovered in PHPSHE 1.7 in <code>include/plugin/payment/alipay/pay.php</code> with the parameter <code>id</code> . The vulnerability does not need any authentication.	2019-03-13	7.5	CVE-2019-9762 MISC
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	7.2	CVE-2018-4054 MISC
pixar -- renderman	A local privilege escalation vulnerability exists in the Mac OS X version of Pixar Renderman 22.3.0's Install Helper helper tool. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine for a successful exploit.	2019-03-08	7.2	CVE-2019-5015 MISC
podofoproject -- podofoproject	PoDoFo 0.9.6 has a heap-based buffer overflow in <code>PdfString::ConvertUTF16toUTF8</code> in <code>base/PdfString.cpp</code> .	2019-03-11	7.5	CVE-2019-9687 MISC
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Overflow that leads to a Heap-Based Buffer Overflow in the function <code>rdp_in_unistr()</code> and results in memory corruption and possibly even a remote code execution.	2019-03-15	7.5	CVE-2018-20177 MISC CONFIRM
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Underflow that leads to a Heap-Based Buffer Overflow in the function <code>lspci_process()</code> and results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20179 MISC CONFIRM
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Underflow that leads to a Heap-Based Buffer Overflow in the function <code>rdpsnddbg_process()</code> and results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20180 MISC CONFIRM
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Underflow that leads to a Heap-Based Buffer Overflow in the function <code>seamless_process()</code> and results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20181 B.D MISC MLIST CONFIRM GENTOO DEBIAN
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain a Buffer Overflow over the global variables in the function <code>seamless_process_line()</code> that results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20182 B.D MISC MLIST CONFIRM GENTOO DEBIAN
sdcms -- sdcms	An issue was discovered in SDCMS V1.7. In the <code>\app\admin\controller\themecontroller.php</code> file, the <code>check_bad()</code> function's filtering is not strict, resulting in PHP code execution. This occurs because some dangerous PHP functions (such as "eval") are blocked but others (such as "system") are not, and because "php" is blocked but ".PHP" is not blocked.	2019-03-10	7.5	CVE-2019-9651 MISC
shanda -- maplestory_online	In Shanda MapleStory Online V160, the <code>SdoKeyCrypt.sys</code> driver allows privilege escalation to NT AUTHORITY\SYSTEM because of not validating the IOCTL <code>0x8000c01c</code> input value, leading to an integer signedness error and a heap-based buffer underflow.	2019-03-12	7.2	CVE-2019-9729 MISC
tinysvcmdnsproject -- tinysvcmdns	In <code>tinysvcmdns</code> through 2018-01-16, an mDNS server processing a crafted packet can perform arbitrary data read operations up to 16383 bytes from the start of the buffer. This can lead to a segmentation fault in <code>uncompress_nlabel</code> in <code>mdns.c</code> and a crash of the server (depending on the memory protection of the CPU and the operating system), or disclosure of memory content via error messages or a server response. NOTE: the product's web site states "This project is un-maintained, and has been since 2013. ... There are known vulnerabilities ... You are advised to NOT use this library for any new projects / products."	2019-03-13	9.4	CVE-2019-9748 MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1024tools -- 1024tools	DOM-based XSS exists in 1024Tools Markdown 1.0 via vectors involving the <code>'&lt;EMBED SRC="data:image/svg+xml'"</code> substring.	2019-03-12	4.3	CVE-2019-9736 MISC
apache -- solr	Server Side Request Forgery in Apache Solr, versions 1.3 until 7.6 (inclusive). Since the "shards" parameter does not have a corresponding whitelist mechanism, a remote attacker with access to the server could make Solr perform an HTTP GET request to any reachable URL.	2019-03-08	5.0	CVE-2017-3164 MLIST B.D
blog_miniproject -- blog_miniproject	In <code>Blog_mini</code> 1.0, XSS exists via the author name of a comment reply in the <code>app/main/views.py</code> <code>articleDetails()</code> function, related to <code>app/templates/_article_comments.html</code> .	2019-03-14	4.3	CVE-2019-9765 MISC
botanproject -- botan	A side-channel issue was discovered in Botan before 2.9.0. An attacker capable of precisely measuring the time taken for ECC key generation may be able to derive information about the high bits of the secret key, as the function to derive the public point from the secret scalar uses an unblinded Montgomery ladder whose loop iteration count depends on the bitlength of the secret. This issue affects only key generation, not ECDSA signatures or ECDH key agreement.	2019-03-08	4.3	CVE-2018-20187 MISC MISC
checkstyle -- checkstyle	Checkstyle before 8.18 loads external DTDs by default.	2019-03-11	5.0	CVE-2019-9658 MISC MISC MISC
chuango -- a11_pstn/lcd/rfid_touch_alarm_system_firmware	The Chuango 433 MHz burglar-alarm product line uses static codes in the RF remote control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay attacks, as demonstrated by Chuango branded products, and non-Chuango branded products such as the Eminent EM8617 OV2 Wifi Alarm System.	2019-03-11	6.4	CVE-2019-9659 MISC
	Multiple vulnerabilities in the web-based management interface of Cisco Enterprise Chat			

cisco -- enterprise_chat_and_email	and Email could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit these vulnerabilities either by injecting malicious code in a chat window or by sending a crafted link to a user of the interface. In both cases, the attacker must persuade the user to click the crafted link or open the chat window that contains the attacker's code. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Version 11.6(1) is affected.	2019-03-11	4.3	<a href="#">CVE-2019-1702</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to escalate lower-level privileges to the administrator level. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow an attacker to make configuration changes to the system as administrator. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	4.6	<a href="#">CVE-2019-1603</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(27) and 8.2(3). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(6). Nexus 3500 Platform Switches are affected running software versions prior to 6.0(2)A8(11) and 7.0(3)I7(6). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9), 7.0(3)I7(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22) and 8.2(3).	2019-03-11	4.6	<a href="#">CVE-2019-1613</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the Image Signature Verification feature of Cisco NX-OS Software could allow an authenticated, local attacker with administrator-level credentials to install a malicious software image on an affected device. The vulnerability is due to improper verification of digital signatures for software images. An attacker could exploit this vulnerability by loading an unsigned software image on an affected device. A successful exploit could allow the attacker to boot a malicious software image. Note: The fix for this vulnerability requires a BIOS upgrade as part of the software upgrade. For additional information, see the Details section of this advisory. Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I7(5). Nexus 9000 Series Fabric Switches in ACI Mode are affected running software versions prior to 13.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I7(5). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5).	2019-03-11	4.6	<a href="#">CVE-2019-1615</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the Cisco Fabric Services component of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Cisco Fabric Services packets. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow, resulting in process crashes and a DoS condition on the device. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(25), 8.1(1b), 8.3(1). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected running software versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22) and 8.2(3). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5). UCS 6200, 6300, and 6400 Fabric Interconnects are affected running software versions prior to 3.2(3) and 4.0(2a).	2019-03-11	5.0	<a href="#">CVE-2019-1616</a> <a href="#">B D</a> <a href="#">CISCO</a>
cleansoft -- free_mp3_cd_ripper	Stack-based buffer overflow in Free MP3 CD Ripper 2.6, when converting a file, allows user-assisted remote attackers to execute arbitrary code via a crafted mp3 file.	2019-03-14	6.8	<a href="#">CVE-2019-9766</a> <a href="#">EXPLOIT-DB</a>
cleansoft -- free_mp3_cd_ripper	Stack-based buffer overflow in Free MP3 CD Ripper 2.6, when converting a file, allows user-assisted remote attackers to execute arbitrary code via a crafted .wma file.	2019-03-14	6.8	<a href="#">CVE-2019-9767</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
cmsmadesimple -- cms_made_simple	class.showtime2_image.php in CMS Made Simple (CMSMS) before 2.2.10 does not ensure that a watermark file has a standard image file extension (G F, JPG, JPEG, or PNG).	2019-03-11	5.0	<a href="#">CVE-2019-9692</a> <a href="#">MISC</a> <a href="#">MISC</a>
cmsmadesimple -- cms_made_simple	In CMS Made Simple (CMSMS) before 2.2.10, an authenticated user can achieve SQL Injection in class.showtime2_data.php via the functions _updateshow (parameter show_id), _inputshow (parameter show_id), _Getshowinfo (parameter show_id), _Getpictureinfo (parameter picture_id), _AdjustNameSeq (parameter shownumber), _Updatepicture (parameter picture_id), and _Deletepicture (parameter picture_id).	2019-03-11	6.5	<a href="#">CVE-2019-9693</a> <a href="#">MISC</a> <a href="#">MISC</a>
codecrafters -- ability_mail_server	Ability Mail Server 4.2.6 has Persistent Cross Site Scripting (XSS) via the body e-mail body. To exploit the vulnerability, the victim must open an email with malicious Javascript inserted into the body of the email as an iframe.	2019-03-12	4.3	<a href="#">CVE-2019-9557</a> <a href="#">MISC</a>
cyberark -- endpoint_privilege_manager	A buffer overflow in the kernel driver CybKernelTracker.sys in CyberArk Endpoint Privilege Manager versions prior to 10.7 allows an attacker (without Administrator privileges) to escalate privileges or crash the machine by loading an image, such as a DLL, with a long path.	2019-03-08	6.9	<a href="#">CVE-2019-9627</a> <a href="#">B D</a> <a href="#">MISC</a>
editor md_project -- editor.md	Editor md 1.5.0 has DOM-based XSS via vectors involving the '<EMBED SRC="data:image/svg+xml" subtring.	2019-03-12	4.3	<a href="#">CVE-2019-9737</a>

				<a href="#">MISC</a>
esafenet -- electronic_document_security_management_system	ESAFENET CDG V3 and V5 has an arbitrary file download vulnerability via the fileName parameter in download.jsp because the InstallationPack parameter is mishandled in a /CDGServer3/ClientAjax request.	2019-03-08	<a href="#">5.0</a>	<a href="#">CVE-2019-9632</a> <a href="#">MISC</a>
ffmpeg -- ffmpeg	In Ffmpeg 4.1, a denial of service in the subtitle decoder allows attackers to hog the CPU via a crafted video file in Matroska format, because ff_htmlmarkup_to_ass in libavcodec/htmlsubtitles.c has a complex format argument to sscanf.	2019-03-12	<a href="#">4.3</a>	<a href="#">CVE-2019-9718</a> <a href="#">B.D</a> <a href="#">MISC</a>
ffmpeg -- ffmpeg	A denial of service in the subtitle decoder in Ffmpeg 4.1 allows attackers to hog the CPU via a crafted video file in Matroska format, because handle_open_brace in libavcodec/htmlsubtitles.c has a complex format argument to sscanf.	2019-03-12	<a href="#">4.3</a>	<a href="#">CVE-2019-9721</a> <a href="#">B.D</a> <a href="#">MISC</a>
gitnoteapp -- gitnote	gitnote 3.1.0 allows remote attackers to execute arbitrary code via a crafted Markdown file, as demonstrated by a javascript:window.parent.top.require('child_process') execFile substring in the onerror attribute of an MG element.	2019-03-14	<a href="#">6.8</a>	<a href="#">CVE-2019-9785</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- glib	gio/gsocketclient.c in GNOME GLib 2.59.2 does not ensure that a parent GTask remains alive during the execution of a connection-attempting enumeration, which allows remote attackers to cause a denial of service (g_socket_client_connected_callback mishandling and application crash) via a crafted web site, as demonstrated by GNOME Web (aka Epiphany).	2019-03-08	<a href="#">4.3</a>	<a href="#">CVE-2019-9633</a> <a href="#">B.D</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer overflow in the function dwg_decode_eed_data at decode.c for the y dimension.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9770</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function bit_convert_TU at bits.c.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9771</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LEADER at dwg.spec.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9772</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer overflow in the function dwg_decode_eed_data at decode.c for the z dimension.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9773</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is an out-of-bounds read in the function bit_read_B at bits.c.	2019-03-14	<a href="#">6.4</a>	<a href="#">CVE-2019-9774</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is an out-of-bounds read in the function dwg_dxf_BLOCK_CONTROL at dwg.spec.	2019-03-14	<a href="#">6.4</a>	<a href="#">CVE-2019-9775</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LTYPE at dwg.spec (later than CVE-2019-9779).	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9776</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer over-read in the function dxf_header_write at header_variables_dxf.spec.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9777</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer over-read in the function dwg_dxf_LTYPE at dwg.spec.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9778</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LTYPE at dwg.spec (earlier than CVE-2019-9776).	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9779</a> <a href="#">MISC</a> <a href="#">MISC</a>
golang -- go	An issue was discovered in net/http in Go 1.11.5. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the second argument to http.NewRequest with '\r\n' followed by an HTTP header or a Redis command.	2019-03-13	<a href="#">4.3</a>	<a href="#">CVE-2019-9741</a> <a href="#">MISC</a>
golangtc -- gopher	jimmykuu Gopher 2.0 has DOM-based XSS via vectors involving the '<EMBED SRC="data:image/svg+xml"' substring.	2019-03-12	<a href="#">4.3</a>	<a href="#">CVE-2019-9738</a> <a href="#">MISC</a>
gpsd_project -- gpsd	gpsd versions 2.90 to 3.17 and microjson versions 1.0 to 1.3, an open source project, allow a stack-based buffer overflow, which may allow remote attackers to execute arbitrary code on embedded platforms via traffic on Port 2947/TCP or crafted JSON inputs.	2019-03-13	<a href="#">5.8</a>	<a href="#">CVE-2018-17937</a> <a href="#">B.D</a> <a href="#">MISC</a>
ibm -- api_connect	IBM API Connect v2018.1 and 2018.4.1 is affected by an information disclosure vulnerability in the consumer API. Any registered user can obtain a list of all other users in all other orgs, including email id/names, etc. IBM X-Force ID: 155148.	2019-03-11	<a href="#">4.0</a>	<a href="#">CVE-2018-2009</a> <a href="#">B.D</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-</a>

ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152858.	2019-03-11	4.6	<a href="#">CVE-2018-1922</a> <a href="#">B.D</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152859.	2019-03-11	4.6	<a href="#">CVE-2018-1923</a> <a href="#">B.D</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>
ibm -- rational_engineering_lifecycle_manager	IBM Rational Engineering Lifecycle Manager 5.0 through 6.0.6 could allow a malicious user to be allowed to view any view if he knows the URL link of a the view, and access information that should not be able to see. BM X-Force ID: 153120.	2019-03-14	4.0	<a href="#">CVE-2018-1929</a> <a href="#">CONFIRM</a> <a href="#">X.F</a>
ibm -- sdk	IBM SDK, Java Technology Edition Version 8 on the AIX platform uses absolute RPATHs which may facilitate code injection and privilege elevation by local users. BM X-Force ID: 152081.	2019-03-11	4.6	<a href="#">CVE-2018-1890</a> <a href="#">X.F</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to spoof connection information which could be used to launch further attacks against the system. IBM X-Force ID: 152531.	2019-03-11	4.0	<a href="#">CVE-2018-1902</a> <a href="#">B.D</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>
ibm -- websphere_mq	IBM WebSphere 8.0.0.0 through 9.1.1 could allow an authenticated attacker to escalate their privileges when using multiplexed channels. BM X-Force ID: 153915.	2019-03-11	6.0	<a href="#">CVE-2018-1974</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>
ichain -- insurance_wallet	Directory traversal vulnerability in iChain Insurance Wallet App for iOS Version 1.3.0 and earlier allows remote attackers to read arbitrary files via unspecified vectors.	2019-03-12	5.0	<a href="#">CVE-2019-5923</a> <a href="#">J.V.N</a> <a href="#">MISC</a>
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel(R) AMT in Intel(R) CSME before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20 may allow an unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	4.6	<a href="#">CVE-2018-12185</a> <a href="#">CONFIRM</a>
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel CSME subsystem before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 or Intel TXE before 3.1.60 or 4.0.10 may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12190</a> <a href="#">CONFIRM</a>
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel(R) AMT in Intel(R) CSME before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20 may allow a privileged user to potentially execute arbitrary code via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12196</a> <a href="#">CONFIRM</a>
intel -- converged_security_management_engine_firmware	Buffer overflow in HECI subsystem in Intel(R) CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 and Intel(R) TXE version before 3.1.60 or 4.0.10, or Intel(R) Server Platform Services before version 5.00.04.012 may allow an unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	4.6	<a href="#">CVE-2018-12208</a> <a href="#">CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause an integer overflow via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12221</a> <a href="#">CONFIRM</a>
intel -- graphics_driver	Insufficient access control in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to escape from a virtual machine guest-to-host via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12223</a> <a href="#">CONFIRM</a>
intel -- rapid_storage_technology_enterprise	Improper permissions in the installer for Intel(R) Accelerated Storage Manager in RSTe v5.5 and before may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-03-14	4.6	<a href="#">CVE-2019-0135</a> <a href="#">CONFIRM</a>
intel -- usb_3.0_creator_utility	Improper permissions for Intel(R) USB 3.0 Creator Utility all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-03-14	4.6	<a href="#">CVE-2019-0129</a> <a href="#">CONFIRM</a>
iotivity -- iotivity	In IoTivity through 1.3.1, the CoAP server interface can be used for Distributed Denial of Service attacks using source IP address spoofing and UDP-based traffic amplification. The reflected traffic is 6 times bigger than spoofed requests. This occurs because the construction of a "4.01 Unauthorized" response is mishandled. NOTE: the vendor states "While this is an interesting attack, there is no plan for maintainer to fix, as we are migrating to IoTivity Lite."	2019-03-13	6.4	<a href="#">CVE-2019-9750</a> <a href="#">MISC</a>
jenkins -- appdynamics	An insufficiently protected credentials vulnerability exists in JenkinsAppDynamics Dashboard Plugin 1.0.14 and earlier in src/main/java/nl/codecentric/jenkins/appd/AppDynamicsResultsPublisher.java that allows attackers without permission to obtain passwords configured in jobs to obtain them.	2019-03-08	4.0	<a href="#">CVE-2019-1003039</a> <a href="#">CONFIRM</a>
jenkins -- azure_vm_agents	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgentTemplate.java, src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to perform the 'verify configuration' form validation action, thereby obtaining limited information about the Azure configuration.	2019-03-08	4.0	<a href="#">CVE-2019-1003035</a> <a href="#">CONFIRM</a>
jenkins -- azure_vm_agents	A data modification vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgent.java that allows attackers with Overall/Read permission to attach a public IP address to an Azure VM agent.	2019-03-08	4.0	<a href="#">CVE-2019-1003036</a> <a href="#">CONFIRM</a>
jenkins -- azure_vm_agents	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2019-03-08	4.0	<a href="#">CVE-2019-1003037</a> <a href="#">CONFIRM</a>

jenkins -- email_extension	A sandbox bypass vulnerability exists in Jenkins Email Extension Plugin 2.64 and earlier in pom.xml, src/main/java/hudson/plugins/emailext/ExtendedEmailPublisher.java, src/main/java/hudson/plugins/emailext/plugins/content/EmailExtScript.java, src/main/java/hudson/plugins/emailext/plugins/content/ScriptContent.java, src/main/java/hudson/plugins/emailext/plugins/trigger/AbstractScriptTrigger.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003032</a> <a href="#">CONF RM</a>
jenkins -- groovy	A sandbox bypass vulnerability exists in Jenkins Groovy Plugin 2.1 and earlier in pom.xml, src/main/java/hudson/plugins/groovy/StringScriptSource.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003033</a> <a href="#">CONF RM</a>
jenkins -- job_dsl	A sandbox bypass vulnerability exists in Jenkins Job DSL Plugin 1.71 and earlier in job-dsl-core/src/main/groovy/javaposse/jobdsl/dsl/AbstractDslScriptLoader.groovy, job-dsl-plugin/build.gradle, job-dsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/JobDslWhitelist.groovy, job-dsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/SandboxDslScriptLoader.groovy that allows attackers with control over Job DSL definitions to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003034</a> <a href="#">CONF RM</a>
jenkins -- matrix_project	A sandbox bypass vulnerability exists in Jenkins Matrix Project Plugin 1.13 and earlier in pom.xml, src/main/java/hudson/matrix/FilterScript.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003031</a> <a href="#">CONF RM</a>
jenkins -- pipeline:_groovy	A sandbox bypass vulnerability exists in Jenkins Pipeline: Groovy Plugin 2.63 and earlier in pom.xml, src/main/java/org/jenkinsci/plugins/workflow/cps/CpsGroovyShell.java that allows attackers able to control pipeline scripts to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003030</a> <a href="#">CONF RM</a>
jenkins -- script_security	A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.53 and earlier in src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/GroovySandbox.java, src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/SecureGroovyScript.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003029</a> <a href="#">CONF RM</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The item_title layout in edit views lacks escaping, leading to XSS.	2019-03-12	4.3	<a href="#">CVE-2019-9711</a> <a href="#">B D</a> <a href="#">MISC</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The JSON handler in com_config lacks input validation, leading to XSS.	2019-03-12	4.3	<a href="#">CVE-2019-9712</a> <a href="#">B D</a> <a href="#">MISC</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The sample data plugins lack ACL checks, allowing unauthorized access.	2019-03-12	5.0	<a href="#">CVE-2019-9713</a> <a href="#">B D</a> <a href="#">MISC</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The media form field lacks escaping, leading to XSS.	2019-03-12	4.3	<a href="#">CVE-2019-9714</a> <a href="#">B D</a> <a href="#">MISC</a>
jtbcc -- jtbcc_php	An issue was discovered in JTBC(PHP) 3.0.1.8. Its cache management module is flawed. An arbitrary file ending in ".inc.php" can be deleted via a console/cache/manage.php?type=action&action=batch&batch=delete&ids=../ substring.	2019-03-11	6.4	<a href="#">CVE-2019-9662</a> <a href="#">MISC</a>
kartatopia -- piluscart	PilusCart 1.4.1 is vulnerable to index.php?module=users&action=newUser CSRF, leading to the addition of a new user as administrator.	2019-03-14	6.8	<a href="#">CVE-2019-9769</a> <a href="#">EXPLOIT-DB</a>
korenix -- jetport_web_manager	The Web manager (aka Commander) on Korenix JetPort 5601 and 5601f devices has Persistent XSS via the Port Alias field under Serial Setting.	2019-03-12	4.3	<a href="#">CVE-2019-9725</a> <a href="#">MISC</a>
lexmark -- cx725h_firmware	On certain Lexmark devices that communicate with an LDAP or SMTP server, a malicious administrator can discover LDAP or SMTP credentials by changing that server's hostname to one that they control, and then capturing the credentials that are sent there. This occurs because stored credentials are not automatically deleted upon that type of hostname change.	2019-03-12	4.0	<a href="#">CVE-2018-17944</a> <a href="#">CONF RM</a>
libofx_project -- libofx	An issue was discovered in LibOFX 0.9.14. There is a NULL pointer dereference in the function OFXApplication::startElement in the file lib/ofx_sgml.cpp, as demonstrated by ofxdump.	2019-03-11	6.8	<a href="#">CVE-2019-9656</a> <a href="#">MISC</a>
maccms -- maccms	Maccms 10 allows remote attackers to execute arbitrary PHP code by entering this code in a template/default_pc/html/art Edit action. This occurs because template rendering uses an include operation on a cache file, which bypasses the prohibition of .php files as templates.	2019-03-14	6.5	<a href="#">CVE-2019-9829</a> <a href="#">MISC</a>
mailtraq -- webmail	Mailtraq WebMail version 2.17.7.3550 has Persistent Cross Site Scripting (XSS) via the body of an e-mail message. To exploit the vulnerability, the victim must open an email with malicious Javascript inserted into the body of the email as an iframe.	2019-03-12	4.3	<a href="#">CVE-2019-9558</a> <a href="#">MISC</a>
microsoft -- teams	Untrusted search path vulnerability in The installer of Microsoft Teams allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-03-12	6.8	<a href="#">CVE-2019-5922</a> <a href="#">JVN</a> <a href="#">B D</a>
microsoft -- windows_7	Untrusted search path vulnerability in Windows 7 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-03-12	6.8	<a href="#">CVE-2019-5921</a> <a href="#">JVN</a> <a href="#">B D</a>
nablarch_project -- nablarch	An incomplete cryptography of the data store function by using hidden tag in Nablarch 5 (5, and 5u1 to 5u13) allows remote attackers to obtain information of the stored data, to register invalid value, or alter the value via unspecified vectors.	2019-03-12	6.4	<a href="#">CVE-2019-5919</a> <a href="#">JVN</a>



				<a href="#">MISC</a>
nrcrafts -- formcraft	Cross-site request forgery (CSRF) vulnerability in FormCraft 1 2.1 and earlier allows remote attackers to hijack the authentication of administrators via a specially crafted page.	2019-03-12	6.8	<a href="#">CVE-2019-5920</a> <a href="#">JVN</a> <a href="#">MISC</a> <a href="#">MISC</a>
openstack -- neutron	An issue was discovered in the iptables firewall module in OpenStack Neutron before 10.0.8, 11.x before 11.0.7, 12.x before 12.0.6, and 13.x before 13.0.3. By setting a destination port in a security group rule along with a protocol that doesn't support that option (for example, VRRP), an authenticated user may block further application of security group rules for instances from any project/tenant on the compute hosts to which it's applied. (Only deployments using the iptables security group driver are affected.)	2019-03-12	4.0	<a href="#">CVE-2019-9735</a> <a href="#">B D</a> <a href="#">MISC</a>
openwsman_project -- openwsman	Openwsman, versions up to and including 2.6.9, are vulnerable to arbitrary file disclosure because the working directory of openwsmand daemon was set to root directory. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to openwsman server.	2019-03-14	5.0	<a href="#">CVE-2019-3816</a> <a href="#">CONF RM</a> <a href="#">B D</a> <a href="#">CONF RM</a>
openwsman_project -- openwsman	Openwsman, versions up to and including 2.6.9, are vulnerable to infinite loop in process_connection() when parsing specially crafted HTTP requests. A remote, unauthenticated attacker can exploit this vulnerability by sending malicious HTTP request to cause denial of service to openwsman server.	2019-03-14	5.0	<a href="#">CVE-2019-3833</a> <a href="#">CONF RM</a> <a href="#">B D</a> <a href="#">CONF RM</a>
php -- php	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.	2019-03-08	5.0	<a href="#">CVE-2019-9637</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
php -- php	<b>** DISPUTED **</b> An issue was discovered in PHP 7.x before 7.1.27 and 7.3.x before 7.3.3. phar_tar_writeheaders_int in ext/phar/tar.c has a buffer overflow via a long link value. NOTE: The vendor indicates that the link value is used only when an archive contains a symlink, which currently cannot happen: "This issue allows theoretical compromise of security, but a practical attack is usually impossible."	2019-03-11	6.8	<a href="#">CVE-2019-9675</a> <a href="#">MISC</a> <a href="#">MISC</a>
phpshe -- phpshe	An XXE issue was discovered in PHPSHE 1.7, which can be used to read any file in the system or scan the internal network without authentication. This occurs because of the call to wechat_getxml in include/plugin/payment/wechat/notify_url.php.	2019-03-13	5.0	<a href="#">CVE-2019-9761</a> <a href="#">MISC</a>
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to read any root file from the file system. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	4.9	<a href="#">CVE-2018-4055</a> <a href="#">MISC</a>
python -- python	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	2019-03-08	5.0	<a href="#">CVE-2019-9636</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
python -- python	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with '\r\n' followed by an HTTP header or a Redis command.	2019-03-12	4.3	<a href="#">CVE-2019-9740</a> <a href="#">MISC</a>
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Out-Of-Bounds Read in the function ui_clip_handle_data() that results in an information leak.	2019-03-15	5.0	<a href="#">CVE-2018-20174</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contains several Integer Signedness errors that lead to Out-Of-Bounds Reads in the file mcs.c and result in a Denial of Service (segfault).	2019-03-15	5.0	<a href="#">CVE-2018-20175</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">CONF RM</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain several Out-Of-Bounds Reads in the file secure.c that result in a Denial of Service (segfault).	2019-03-15	5.0	<a href="#">CVE-2018-20176</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Out-Of-Bounds Read in the function process_demand_active() that results in a Denial of Service (segfault).	2019-03-15	5.0	<a href="#">CVE-2018-20178</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MLIST</a> <a href="#">CONF RM</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
rednao -- smart_forms	Cross-site request forgery (CSRF) vulnerability in Smart Forms 2 6.15 and earlier allows remote attackers to hijack the authentication of administrators via a specially crafted page.	2019-03-12	6.8	<a href="#">CVE-2019-5924</a> <a href="#">JVN</a> <a href="#">MISC</a>
sap -- advanced_business_application_programming_platform_kernel	ABAP Server of SAP NetWeaver and ABAP Platform fail to perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has been corrected in the following versions: KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.74, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, 7.74, 8.04, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, 7.74, 7.75, 8.04.	2019-03-12	6.5	<a href="#">CVE-2019-0270</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- banking_services_from_sap	Banking services from SAP 9.0 (FSAPPL version 5) and SAP S/4HANA Financial Products Subledger (S4FPSL, version 1) performs an inadequate authorization check for	2019-03-	6.5	<a href="#">CVE-2019-0276</a>

	an authenticated user, potentially resulting in escalation of privileges.	12		<a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- businessobjects_business_intelligence	SAP BusinessObjects Business Intelligence Platform (CMC Module), versions 4.10. 4.20 and 4.30, does not sufficiently validate an XML document accepted from an untrusted source.	2019-03-12	5.5	<a href="#">CVE-2019-0268</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- hana_extended_application_services	SAP HANA extended application services, version 1, advanced does not sufficiently validate an XML document accepted from an authenticated developer with privileges to the SAP space (XML External Entity vulnerability).	2019-03-12	5.5	<a href="#">CVE-2019-0277</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- mobile_platform_sdk	SAP Mobile Platform SDK allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service (i.e. denial of service). Fixed in versions 3.1 SP03 PL02, SDK 3.1 SP04, or later.	2019-03-12	5.0	<a href="#">CVE-2019-0274</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sdcms -- sdcms	There is a CSRF in SDCMS V1.7 via an m=admin&c=theme&a=edit request. t allows PHP code injection by providing a filename in the file parameter, and providing file content in the t2 parameter.	2019-03-10	6.8	<a href="#">CVE-2019-9652</a> <a href="#">MISC</a>
sftnow -- sftnow	sftnow through 2018-12-29 allows index.php?g=Admin&m=User&a=add_post CSRF to add an admin account.	2019-03-11	6.8	<a href="#">CVE-2019-9688</a> <a href="#">MISC</a>
stackstorm -- stackstorm	In st2web in StackStorm Web UI before 2.9.3 and 2.10.x before 2.10.3, it is possible to bypass the CORS protection mechanism via a "null" origin value, potentially leading to XSS.	2019-03-08	4.3	<a href="#">CVE-2019-9580</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
thinkst -- canarytokens	Thinkst Canarytokens through 2019-03-01 relies on limited variation in size, metadata, and timestamp, which makes it easier for attackers to estimate whether a Word document contains a token.	2019-03-14	5.0	<a href="#">CVE-2019-9768</a> <a href="#">MISC</a>
tinyc -- tinyc	An issue was discovered in Tiny C Compiler (aka TinyCC or TCC) 0.9.27. Compiling a crafted source file leads to an 1 byte out of bounds write in the end_macro function in tccpp.c.	2019-03-13	4.3	<a href="#">CVE-2019-9754</a> <a href="#">MISC</a>
tinysvcmDNS -- tinysvcmDNS	In tinysvcmDNS through 2018-01-16, a maliciously crafted mDNS (Multicast DNS) packet triggers an infinite loop while parsing an mDNS query. When mDNS compressed labels point to each other, the function uncompress_nlabel goes into an infinite loop trying to analyze the packet with an mDNS query. As a result, the mDNS server hangs after receiving the malicious mDNS packet. NOTE: the product's web site states "This project is un-maintained, and has been since 2013. ... There are known vulnerabilities ... You are advised to NOT use this library for any new projects / products."	2019-03-13	5.0	<a href="#">CVE-2019-9747</a> <a href="#">MISC</a>
treasuredata -- fluent_bit	An issue was discovered in the MQTT input plugin in Fluent Bit through 1.0.4. When this plugin acts as an MQTT broker (server), it mishandles incoming network messages. After processing a crafted packet, the plugin's mqtt_packet_drop function (in /plugins/in_mqtt/mqtt_prot.c) executes the memmove() function with a negative size parameter. That leads to a crash of the whole Fluent Bit server via a SIGSEGV signal.	2019-03-13	5.0	<a href="#">CVE-2019-9749</a> <a href="#">MISC</a>
webmproject -- libwebm	In libwebm before 2019-03-08, a NULL pointer dereference caused by the functions OutputCluster and OutputTracks in webm_info.cc will trigger an abort, which allows a DoS attack, a similar issue to CVE-2018-19212.	2019-03-13	5.0	<a href="#">CVE-2019-9746</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to .php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php.	2019-03-14	6.8	<a href="#">CVE-2019-9787</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- application_policy_infrastructure_controller	A vulnerability in the management interface of Cisco Application Policy Infrastructure Controller (APIC) software could allow an unauthenticated, adjacent attacker to gain unauthorized access on an affected device. The vulnerability is due to a lack of proper access control mechanisms for IPv6 link-local connectivity imposed on the management interface of an affected device. An attacker on the same physical network could exploit this vulnerability by attempting to connect to the IPv6 link-local address on the affected device. A successful exploit could allow the attacker to bypass default access control restrictions on an affected device. Cisco Application Policy Infrastructure Controller (APIC) devices running versions prior to 4.2(0.21c) are affected.	2019-03-11	3.3	<a href="#">CVE-2019-1690</a> <a href="#">BID</a> <a href="#">CISCO</a>
cobham -- satcom_sailor_800_firmware	Cobham Satcom Sailor 800 and 900 devices contained persistent XSS, which required administrative access to exploit. The vulnerability was exploitable by acquiring a copy of the device's configuration file, inserting an XSS payload into a relevant field (e.g., Satellite name), and then restoring the malicious configuration file.	2019-03-15	3.5	<a href="#">CVE-2018-19394</a> <a href="#">MISC</a> <a href="#">MISC</a>
dradisframework -- dradis	Cross-site scripting vulnerability in Dradis Community Edition Dradis Community Edition v3.11 and earlier and Dradis Professional Edition v3.1.1 and earlier allow remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-03-12	3.5	<a href="#">CVE-2019-5925</a> <a href="#">JVN</a> <a href="#">MISC</a>
	BM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 5.0 through			

ibm -- rational_collaborative_lifecycle_management	6.0.6) is vulnerable to HTTP header injection, caused by improper validation of input. By persuading a victim to visit a specially-crafted Web page, a remote attacker could exploit this vulnerability to inject arbitrary HTTP headers, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. BM X-Force ID: 144884.	2019-03-14	3.5	<a href="#">CVE-2018-1658</a> CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	BM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 5.0 through 6.0.6) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 145509.	2019-03-14	3.5	<a href="#">CVE-2018-1688</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Rational Engineering Lifecycle Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152734.	2019-03-14	3.5	<a href="#">CVE-2018-1910</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Rational Engineering Lifecycle Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152738.	2019-03-14	3.5	<a href="#">CVE-2018-1914</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Jazz Foundation (IBM Rational Engineering Lifecycle Manager 5.0 through 6.0.6) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152740.	2019-03-14	3.5	<a href="#">CVE-2018-1916</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Jazz Foundation (IBM Rational Engineering Lifecycle Manager 5.0 through 6.0.6) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153495.	2019-03-14	3.5	<a href="#">CVE-2018-1952</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148613.	2019-03-14	3.5	<a href="#">CVE-2018-1759</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148617.	2019-03-14	3.5	<a href="#">CVE-2018-1763</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148618.	2019-03-14	3.5	<a href="#">CVE-2018-1764</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150426.	2019-03-14	3.5	<a href="#">CVE-2018-1823</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150427.	2019-03-14	3.5	<a href="#">CVE-2018-1824</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150428.	2019-03-14	3.5	<a href="#">CVE-2018-1825</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150432.	2019-03-14	3.5	<a href="#">CVE-2018-1829</a> CONFIRM XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148615.	2019-03-14	3.5	<a href="#">CVE-2018-1761</a> CONFIRM BID XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 154135.	2019-03-14	3.5	<a href="#">CVE-2018-1982</a> CONFIRM BID XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 154136.	2019-03-14	3.5	<a href="#">CVE-2018-1983</a> CONFIRM XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 154137.	2019-03-14	3.5	<a href="#">CVE-2018-1984</a> CONFIRM BID XF
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 or Intel TXE before version 3.1.60 or 4.0.10 may allow an unauthenticated user to potentially modify data via physical access.	2019-03-14	2.1	<a href="#">CVE-2018-12188</a> CONFIRM
intel -- converged_security_management_engine_firmware	Unhandled exception in Content Protection subsystem in Intel CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 or Intel TXE before 3.1.60 or 4.0.10 may allow privileged user to potentially modify data via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12189</a> CONFIRM
intel -- graphics_driver	Insufficient access control in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to read device configuration information via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12209</a> CONFIRM
intel -- graphics_driver	Multiple pointer dereferences in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12210</a> CONFIRM
intel -- graphics_driver	Insufficient input validation in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12211</a> CONFIRM
	Buffer overflow in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057),			

intel -- graphics_driver	20.19.x.5063 (aka 15.40.x.5063) 21 20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12212 CONFIRM</a>
intel -- graphics_driver	Potential memory corruption in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12213 CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12215 CONFIRM</a>
intel -- graphics_driver	Insufficient access control in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to read device configuration information via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12217 CONFIRM</a>
intel -- graphics_driver	Unhandled exception in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a memory leak via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12218 CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to read memory via local access via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12219 CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause an out of bound memory read via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12222 CONFIRM</a>
intel -- graphics_driver	Buffer leakage in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable information disclosure via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12224 CONFIRM</a>
intel -- graphics_driver	Multiple out of bounds read in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable information disclosure via local access.	2019-03-14	2.1	<a href="#">CVE-2018-18089 CONFIRM</a>
intel -- graphics_driver	Out of bounds read in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-18090 CONFIRM</a>
intel -- graphics_driver	Use after free in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an unprivileged user to potentially enable a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-18091 CONFIRM</a>
jenkins -- repository_connector	An insufficiently protected credentials vulnerability exists in Jenkins Repository Connector Plugin 1.2.4 and earlier in src/main/java/org/jvnet/hudson/plugins/repositoryconnector/ArtifactDeployer.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/Repository.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/UserPwd.java that allows an attacker with local file system access or control of a Jenkins administrator's web browser (e.g. malicious extension) to retrieve the password stored in the plugin configuration.	2019-03-08	2.1	<a href="#">CVE-2019-1003038 CONFIRM</a>
mcafee -- database_security	Data Leakage Attacks vulnerability in the web interface in McAfee Database Security prior to the 4.6.6 March 2019 update allows local users to expose passwords via incorrectly auto completing password fields in the admin browser login screen.	2019-03-12	2.1	<a href="#">CVE-2019-3615 BID CONFIRM</a>
rsa -- archer_grc_platform	RSA Archer versions, prior to 6.5 SP1, contain an information exposure vulnerability. Users' session information is logged in plain text in the RSA Archer log files. An authenticated malicious local user with access to the log files may obtain the exposed information to use it in further attacks.	2019-03-13	2.1	<a href="#">CVE-2019-3715 FULLDISC</a>
rsa -- archer_grc_platform	RSA Archer versions, prior to 6.5 SP2, contain an information exposure vulnerability. The database connection password may get logged in plain text in the RSA Archer log files. An authenticated malicious local user with access to the log files may obtain the exposed password to use it in further attacks.	2019-03-13	2.1	<a href="#">CVE-2019-3716 BID FULLDISC</a>
sap -- businessobjects_business_intelligence	SAP BusinessObjects Business Intelligence Platform (BI Workspace), versions 4.10 and 4.20, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-03-12	3.5	<a href="#">CVE-2019-0269 BID MISC MISC</a>
sap -- netweaver_java_application_server	SAML 1.1 SSO Demo Application in SAP NetWeaver Java Application Server (J2EE-APPS), versions 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40 and 7.50, does not sufficiently encode user-controlled inputs, which results in cross-site scripting (XSS) vulnerability.	2019-03-12	3.5	<a href="#">CVE-2019-0275 BID MISC MISC</a>
yzmcms -- yzmcms	Stored XSS exists in YzmCMS 5.2 via the admin/category/edit.html "catname" parameter.	2019-03-11	3.5	<a href="#">CVE-2019-9660 MISC</a>
yzmcms -- yzmcms	Stored XSS exists in YzmCMS 5.2 via the admin/system_manage/user_config_edit.html "value" parameter,	2019-03-11	3.5	<a href="#">CVE-2019-9661 MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	ABAP Server (used in NetWeaver and Suite/ERP) and ABAP Platform does not sufficiently validate an XML document accepted from an untrusted source,		not yet	<a href="#">CVE-2019-0271 B D</a>

abap -- server_and_platform	leading to an XML External Entity (XEE) vulnerability. Fixed in Kernel 7.21 or 7.22, that is ABAP Server 7.00 to 7.31 and Kernel 7.45, 7.49 or 7.53, that is ABAP Server 7.40 to 7.52 or ABAP Platform.	2019-03-12	calculated	<a href="#">MISC</a> <a href="#">MISC</a>
airmore -- airmore	The AirMore application through 1.6.1 for Android allows remote attackers to cause a denial of service (system hang) via many simultaneous /? Key=PhoneRequestAuthorization requests.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9831</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a>
azure-umqtt-c -- azure-umqtt-c	azure-umqtt-c (available through GitHub prior to 2017 October 6) allows remote attackers to cause a denial of service via unspecified vectors.	2019-03-12	not yet calculated	<a href="#">CVE-2019-5917</a> <a href="#">JVN</a> <a href="#">B D</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. The client applications of AccessManagerCoreService.exe communicate with this server through named pipes. A user can initiate communication with the server by creating a named pipe and sending commands to achieve elevated privileges.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18255</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. A regular user can obtain local administrator privileges if they run any whitelisted application through the Custom App Launcher.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18256</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. CALRunElevated.exe provides "NT AUTHORITY\SYSTEM" access to unprivileged users via the --system option.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18252</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. CALRunElevated.exe attempts to enforce access control by adding an unprivileged user to the local Administrators group for a very short time to execute a single command. However, the user is left in that group if the command crashes, and there is also a race condition in all cases.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18253</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. An unprivileged user can read the cal_whitelist table in the Custom App Launcher (CAL) database, and potentially gain privileges by placing a Trojan horse program at an app pathname.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18254</a> <a href="#">MISC</a>
circuitwerkes -- sicon-8	CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a web-based front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's web browser.	2019-03-15	not yet calculated	<a href="#">CVE-2019-5616</a> <a href="#">MISC</a>
cisco -- common_services_platform_collector	A vulnerability in the Cisco Common Services Platform Collector (CSPC) could allow an unauthenticated, remote attacker to access an affected device by using an account that has a default, static password. This account does not have administrator privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to the affected system using this account. A successful exploit could allow the attacker to log in to the CSPC using the default account. For Cisco CSPC 2.7.x, Cisco fixed this vulnerability in Release 2.7.4.6. For Cisco CSPC 2.8.x, Cisco fixed this vulnerability in Release 2.8.1.2.	2019-03-13	not yet calculated	<a href="#">CVE-2019-1723</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- dna_center	A vulnerability in the web-based management interface of Cisco DNA Center could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. Cisco DNA Center versions prior to 1.2.5 are affected.	2019-03-11	not yet calculated	<a href="#">CVE-2019-1707</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid user credentials to exploit this vulnerability. Nexus 3000, 3500, and Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1606</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to access sensitive data that could be used to elevate their privileges to administrator. The vulnerability is due to improper implementation of filesystem permissions. An attacker could exploit this vulnerability by logging in to the CLI of an affected device, accessing a specific file, and leveraging this information to authenticate to the NX-API server. A successful exploit could allow an attacker to make configuration changes as administrator. Note: NX-API is disabled by default. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1602</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the Fibre Channel over Ethernet (FCoE) N-port Virtualization (NPV) protocol implementation in Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to an incorrect processing of FCoE packets when the coe-npv feature is uninstalled. An attacker could exploit this vulnerability by sending a stream of FCoE frames from an adjacent host to an affected device. An exploit could allow the attacker to cause packet amplification to occur, resulting in the saturation of interfaces and a DoS condition. Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I7(5) and 9.2(2).	2019-03-11	not yet calculated	<a href="#">CVE-2019-1617</a> <a href="#">B D</a> <a href="#">CISCO</a>
cloud_foundry_foundation -- cloud_controller	Cloud Foundry Cloud Controller, versions prior to 1.78.0, contain an endpoint with improper authorization. A remote authenticated malicious user with read permissions can request package information and receive a signed bit-service url that grants the user write permissions to the bit-service.	2019-03-13	not yet calculated	<a href="#">CVE-2019-3785</a> <a href="#">CONFIRM</a>
cloud_foundry_foundation -- container_runtime	Cloud Foundry Container Runtime, versions prior to 0.28.0, deploys K8s worker nodes that contains a configuration file with IAAS credentials. A malicious user with access to the k8s nodes can obtain IAAS credentials allowing the user to escalate privileges to gain access to the IAAS account.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3780</a> <a href="#">CONFIRM</a>
cloud_foundry_foundation -- container_runtime	Cloud Foundry Container Runtime, versions prior to 0.29.0, deploys Kubernetes clusters utilize the same CA (Certificate Authority) to sign and trust certs for ETCD as used by the Kubernetes API. This could allow a user authenticated with a cluster to request a signed certificate leveraging the Kubernetes CSR capability to obtain a credential that could escalate privilege access to ETCD.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3779</a> <a href="#">CONFIRM</a>



cobham -- satcom_sailor_250_and_500_devices	Cobham Satcom Sailor 250 and 500 devices before 1.25 contained persistent XSS, which could be exploited by an unauthenticated threat actor via the index.lua?pageID=Phone%20book name field.	2019-03-15	not yet calculated	<a href="#">CVE-2018-19391</a> MISC
cobham -- satcom_sailor_250_and_500_devices	Cobham Satcom Sailor 250 and 500 devices before 1.25 contained an unauthenticated password reset vulnerability. This could allow modification of any user account's password (including the default "admin" account), without prior knowledge of their password. All that is required is knowledge of the username and attack vector (/index.lua?pageID=Administration usernameAdmChange, passwordAdmChange1, and passwordAdmChange2 fields).	2019-03-15	not yet calculated	<a href="#">CVE-2018-19392</a> MISC
ethereum -- cryptobotsbattle_token	An Integer overflow vulnerability exists in the batchTransfer function of a smart contract implementation for CryptoBotsBattle (CBTB), an Ethereum token. This vulnerability could be used by an attacker to create an arbitrary amount of tokens or any user.	2019-03-15	not yet calculated	<a href="#">CVE-2018-17882</a> MISC
f5 -- big-ip	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6597</a> CONFIRM
f5 -- big-ip	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to perform the attack.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6598</a> CONFIRM
f5 -- big-ip	In BIG-IP 11.6.1-11.6.3.2 or 11.5.1-11.5.8, or Enterprise Manager 3.1.1, improper escaping of values in an undisclosed page of the configuration utility may result with an improper handling on the JSON response when it is injected by a malicious script via a remote cross-site scripting (XSS) attack.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6599</a> B D CONFIRM
f5 -- big-ip	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6600</a> CONFIRM
f5 -- big-ip	In BIG-IP 13.0.0, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, the Application Acceleration Manager (AAM) wand process used in processing of mages and PDFs fails to drop group permissions when executing helper scripts.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6601</a> CONFIRM
f5 -- big-ip_apm	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.1, 12.1.0-12.1.3.6, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when processing fragmented ClientHello messages in a DTLS session TMM may corrupt memory eventually leading to a crash. Only systems offering DTLS connections via APM are impacted.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6596</a> B D CONFIRM
feifeicms -- feifeicms	FeiFeiCMS 4.1.190209 allows remote attackers to upload and execute arbitrary PHP code by visiting index.php?s=Admin-Index to modify the set of allowable file extensions, as demonstrated by adding php to the default jpg,gif,png,jpeg setting, and then using the "add article" feature.	2019-03-14	not yet calculated	<a href="#">CVE-2019-9825</a> MISC
fujitsu -- wireless_keyboard_set	The receiver (aka bridge) component of Fujitsu Wireless Keyboard Set LX901 GK900 devices allows Keystroke Injection. This occurs because it accepts unencrypted 2.4 GHz packets, even though all legitimate communication uses AES encryption.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9835</a> MISC
g_data_software -- total_security	gdwfpd.sys in G Data Total Security before 2019-02-22 allows an attacker to bypass ACLs because Interpreted Device Characteristics lacks F LE_DEVICE_SECURE_OPEN and therefore files and directories "inside" the \gdwfpd device are not properly protected, leading to unintended impersonation or object creation.	2019-03-13	not yet calculated	<a href="#">CVE-2019-9742</a> MISC
google -- android	The Screen Stream application through 3.0.15 for Android allows remote attackers to cause a denial of service via many simultaneous /start-stop requests.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9833</a> EXPLOIT-DB
google -- android	The AirDrop application through 2.0 for Android allows remote attackers to cause a denial of service via a client that makes many socket connections through a configured port.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9832</a> EXPLOIT-DB
highcharts_js -- highcharts_js	In js/parts/SvgRenderer.js in Highcharts JS before 6.1.0, the use of backtracking regular expressions permitted an attacker to conduct a denial of service attack against the SVGRenderer component, aka ReDoS.	2019-03-14	not yet calculated	<a href="#">CVE-2018-20801</a> MISC
huawei -- oceanstor_uds_devices	Huawei OceanStor UDS devices with software before V100R002C01SPC102 might allow remote attackers to capture and change patch loading information resulting in the deletion of directory files and compromise of system functions when loading a patch.	2019-03-13	not yet calculated	<a href="#">CVE-2015-2254</a> CONFIRM
ibm -- content_navigator	IBM Content Navigator 3.0CD is could allow an attacker to execute arbitrary code on a user's workstation. When editing an executable file in ICN with Edit service, it will be executed on the user's workstation. BM X-Force ID: 156000.	2019-03-14	not yet calculated	<a href="#">CVE-2019-4034</a> B D XF CONFIRM
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 152671.	2019-03-14	not yet calculated	<a href="#">CVE-2018-1908</a> CONFIRM XF
intel -- active_management_technology	Insufficient input validation in Intel(R) Active Management Technology (Intel(R) AMT) before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20 may allow an unauthenticated user to potentially cause a denial of service via network access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12187</a> CONFIRM
intel -- capability_licensing_service	Insufficient access control in Intel(R) Capability Licensing Service before version 1.50.638.1 may allow an unprivileged user to potentially escalate privileges via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12200</a> CONFIRM
intel -- matrix_storage_manager	Improper permissions in Intel(R) Matrix Storage Manager 8.9.0.1023 and before may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2019-0121</a> CONFIRM
intel -- multiple_products	Privilege escalation vulnerability in Platform Sample/ Silicon Reference firmware or 8th Generation Intel(R) Core Processor, 7th Generation Intel(R) Core Processor may allow privileged user to potentially leverage existing features via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12202</a> CONFIRM
intel -- multiple_products	Buffer overflow vulnerability in Platform Sample / Silicon Reference firmware for 8th Generation Intel(R) Core Processor, 7th Generation Intel(R) Core Processor, Intel(R) Pentium(R) Silver J5005 Processor, Intel(R) Pentium(R) Silver N5000 Processor, Intel(R) Celeron(R) J4105 Processor, Intel(R) Celeron(R) J4005 Processor, Intel Celeron(R) N4100 Processor and Intel(R) Celeron N4000 Processor may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12201</a> CONFIRM

intel -- server_platform_services_heci_subsystem	Insufficient input validation in Intel(R) Server Platform Services HECI subsystem before version SPS_E5_04.00.04.393.0 may allow privileged user to potentially cause a denial of service via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12198 CONFIRM</a>
intel -- sgx_sdk_for_linux_and_sgx_sdk_for_windows	Double free in Intel(R) SGX SDK for Linux before version 2.2 and Intel(R) SGX SDK for Windows before version 2.1 may allow an authenticated user to potentially enable information disclosure or denial of service via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2019-0122 CONFIRM</a>
jupyter -- notebook	An XSSI (cross-site inclusion) vulnerability in Jupyter Notebook before 5.7.6 allows inclusion of resources on malicious pages when visited by users who are authenticated with a Jupyter server. Access to the content of resources has been demonstrated with Internet Explorer through capturing of error messages, though not reproduced with other browsers. This occurs because Internet Explorer's error messages can include the content of any invalid JavaScript that was encountered.	2019-03-12	not yet calculated	<a href="#">CVE-2019-9644 MISC</a>
mybb -- mybb	An XSS issue was discovered in upcoming_events.php in the Upcoming Events plugin before 1.33 for MyBB via a crafted name for an event.	2019-03-10	not yet calculated	<a href="#">CVE-2019-9650 MISC MISC</a>
netdata -- netdata	The Netdata web application through 1.13.0 allows remote attackers to inject their own malicious HTML code into an imported snapshot, aka HTML Injection. Successful exploitation will allow attacker-supplied HTML to run in the context of the affected browser, potentially allowing the attacker to steal authentication credentials or to control how the site is rendered to the user.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9834 EXPLOIT-DB MISC</a>
nexus -- 9000_series_switches_in_standalone_nx-os_mode	A vulnerability in the Tetration Analytics agent for Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an authenticated, local attacker to execute arbitrary code as root. The vulnerability is due to an incorrect permissions setting. An attacker could exploit this vulnerability by replacing valid agent files with malicious code. A successful exploit could result in the execution of code supplied by the attacker. Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running versions prior to 7.0(3)I7(5).	2019-03-11	not yet calculated	<a href="#">CVE-2019-1618 B D CISCO</a>
open_ticket_request_system -- open_ticket_request_system	An issue was discovered in Open Ticket Request System (OTRS) 6.x before 6.0.17 and 7.x before 7.0.5. An attacker who is logged into OTRS as an admin user may manipulate the URL to cause execution of JavaScript in the context of OTRS. This is related to Kernel/Output/Template/Document.pm.	2019-03-13	not yet calculated	<a href="#">CVE-2019-9751 MISC</a>
open_ticket_request_system -- open_ticket_request_system	An issue was discovered in Open Ticket Request System (OTRS) 5.x before 5.0.34, 6.x before 6.0.16, and 7.x before 7.0.4. An attacker who is logged into OTRS as an agent or a customer user may upload a carefully crafted resource in order to cause execution of JavaScript in the context of OTRS. This is related to Content-type mishandling in Kernel/Modules/PictureUpload.pm.	2019-03-13	not yet calculated	<a href="#">CVE-2019-9752 MISC</a>
open_ticket_request_system -- open_ticket_request_system	An issue was discovered in Open Ticket Request System (OTRS) 5.0.31 and 6.0.13. Users updating to 6.0.13 (also patchlevel updates) or 5.0.31 (only major updates) will experience data loss in their agent preferences table.	2019-03-13	not yet calculated	<a href="#">CVE-2018-20800 MISC</a>
opensuse -- yast2-multipath	In yast2-multipath before version 4.1.1 a static temporary filename allows local attackers to overwrite files on systems without symlink protection	2019-03-15	not yet calculated	<a href="#">CVE-2018-17955 CONFIRM</a>
opensuse -- yast2-printer	In yast2-printer up to and including version 4.0.2 the SMB printer settings don't escape characters in passwords properly. If a password with backticks or similar characters is supplied this allows for executing code as root. This requires ricking root to enter such a password in yast.	2019-03-15	not yet calculated	<a href="#">CVE-2018-20106 CONFIRM</a>
opensuse -- yast2-samba-provision	In yast2-samba-provision up to and including version 1.0.1 the password for samba shares was provided on the command line to tools used by yast2-samba-provision, allowing local attackers to read them in the process list	2019-03-15	not yet calculated	<a href="#">CVE-2018-17956 CONFIRM</a>
pacman -- pacman	pacman before 5.1.3 allows directory traversal when installing a remote package via a specified URL "pacman -U <url>" due to an unsanitized file name received from a Content-Disposition header. pacman renames the downloaded package file to match the name given in this header. However, pacman did not sanitize his name, which may contain slashes, before calling rename(). A malicious server (or a network MitM if downloading over HTTP) can send a Content-Disposition header to make pacman place the file anywhere in the filesystem, potentially leading to arbitrary root code execution. Notably, this bypasses pacman's package signature checking. This occurs in curl_download_internal in lib/libalpm/download.c.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9686 MISC MISC MISC</a>
paul_vixie -- vixie_cron	Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (use-after-free and daemon crash) because of a orce_rescan_user error.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9706 MISC MISC MISC</a>
paul_vixie -- vixie_cron	Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (memory consumption) via a large crontab file because an unlimited number of lines is accepted.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9705 B D MISC</a>
paul_vixie -- vixie_cron	Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (daemon crash) via a large crontab file because the calloc return value is not checked.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9704 B D MISC</a>
rsa -- authentication_manager	RSA Authentication Manager versions prior to 8.4 P1 contain an Insecure Credential Management Vulnerability. A malicious Operations Console administrator may be able to obtain the value of a domain password that another Operations Console administrator had set previously and use it for attacks.	2019-03-13	not yet calculated	<a href="#">CVE-2019-3711 B D FULLDISC</a>
topvision -- cc8800_cmmts_c-e_devices	Topvision CC8800 CMTS C-E devices allow remote attackers to obtain sensitive information via a direct request for /WebContent/startup tar.gz with userName=admin in a cookie.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18205 MISC MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has out-of-bounds read vulnerability in VNC client code inside TextChat module, which results in a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8267 MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple off-by-one vulnerabilities in VNC server code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8272 MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1206 has multiple off-by-one vulnerabilities in VNC client code connected with improper usage of ClientConnection::ReadString function, which can potentially result code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8268 MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of SETPIXELS macro in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8265 MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside RAW decoder, which can potentially result code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been	2019-03-08	not yet calculated	<a href="#">CVE-2019-8280 MISC</a>

	fixed in revision 1204.			
ultravnc -- ultravnc	UltraVNC revision 1211 contains multiple memory leaks (CWE-655) in VNC server code, which allows an attacker to read stack memory and can be abused or information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8277</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a stack buffer overflow vulnerability in VNC server code inside file transfer request handler, which can result in Denial of Service (DoS). This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8276</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple improper null termination vulnerabilities in VNC server code, which result in out-of-bound data being accessed by remote users. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8275</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer request handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8274</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer request handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8273</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of ClientConnection::Copybuffer function in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. User interaction is required to trigger these vulnerabilities. These vulnerabilities have been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8266</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8271</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1210 has out-of-bounds read vulnerability in VNC client code inside Ultra decoder, which results in a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1211.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8270</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1206 has stack-based Buffer overflow vulnerability in VNC client code inside FileTransfer module, which leads to a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8269</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client code inside Ultra2 decoder, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8264</a> <a href="#">MISC</a>
webargs -- webargs	An issue was discovered in webargs before 5.1.3, as used with mosh and other products. JSON parsing uses a short-lived cache to store the parsed JSON body. This cache is not thread-safe, meaning that incorrect JSON payloads could have been parsed for concurrent requests.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9710</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Contact Form Email plugin before 1.2.66 for WordPress allows wp-admin/admin.php item XSS, related to cp_admin_int_edition.inc.php in the "custom edition area."	2019-03-10	not yet calculated	<a href="#">CVE-2019-9646</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nca.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to tmcginnis@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20508 · (888) 282-0870



From: [US-CERT](mailto:US-CERT)  
To: [woufarte@ci.sunnyside.ca.us](mailto:woufarte@ci.sunnyside.ca.us)  
Subject: SB19-077: Vulnerability Summary for the Week of March 11, 2019  
Date: Monday, March 18, 2019 9:41:59 AM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

### **[SB19-077: Vulnerability Summary for the Week of March 11, 2019](#)**

03/18/2019 09:07 AM EDT

Original release date: March 18, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
atlassian -- sourcetree	There was an argument injection vulnerability in Atlassian Sourcetree for macOS from version 1.2 before version 3.1.1 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for macOS is able to exploit this issue to gain code execution on the system.	2019-03-08	9.0	<a href="#">CVE-2018-20234</a> <a href="#">CONFIRM</a>
atlassian -- sourcetree	There was an argument injection vulnerability in Atlassian Sourcetree for Windows from version 0.5a before version 3.0.15 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for Windows is able to exploit this issue to gain code execution on the system.	2019-03-08	9.0	<a href="#">CVE-2018-20235</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
atlassian -- sourcetree	There was a command injection vulnerability in Sourcetree for Windows from version 0.5a before version 3.0.10 via URI handling. A remote attacker could send a malicious URI to a victim using Sourcetree for Windows to exploit this issue to gain code execution on the system.	2019-03-08	9.3	<a href="#">CVE-2018-20236</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
cisco -- nx-os	A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to gain read and write access to a critical configuration file. The vulnerability is due to a failure to impose strict filesystem permissions on the targeted device. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow an attacker to use the content of this configuration file to bypass authentication and log in as any user of the device. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(3)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	7.2	<a href="#">CVE-2019-1601</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the user account management interface of Cisco NX-OS Software could allow an authenticated, local attacker to gain elevated privileges on an affected device. The vulnerability is due to an incorrect authorization check of user accounts and their associated Group ID (GID). An attacker could exploit this vulnerability by taking advantage of a logic error that will permit the use of higher privileged commands than what is necessarily assigned. A successful exploit could allow an attacker to execute commands with elevated privileges on the underlying Linux shell of an affected device. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 8.2(3), and 8.3(2). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	7.2	<a href="#">CVE-2019-1604</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary code as root. The vulnerability is due to incorrect input validation in the NX-API feature. An attacker could exploit this vulnerability by sending a crafted HTTP or HTTPS request to an internal service on an affected device that has the NX-API feature enabled. A successful exploit could allow the attacker to cause a buffer overflow and execute arbitrary code as root. Note: The NX-API feature is disabled by default. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.1(1). Nexus 3000 Series Switches are	2019-03-08	7.2	<a href="#">CVE-2019-1605</a> <a href="#">B.D</a>

	affected in versions prior to 7.0(3)4(8) and 7.0(3)17(1). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(8). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.3(2)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 7.3(3)D1(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)4(8) and 7.0(3)17(1). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).			<a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3).	2019-03-08	7.2	<a href="#">CVE-2019-1607</a> B D <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3).	2019-03-08	7.2	<a href="#">CVE-2019-1608</a> B D <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(2). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)17(6). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)4(9) and 7.0(3)17(6). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), 8.2(3), and 8.3(2). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)4(9) and 7.0(3)17(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	7.2	<a href="#">CVE-2019-1609</a> B D <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 3500 Platform Switches and Nexus 3000 Series Switches software versions prior to 7.0(3)17(4) are affected.	2019-03-11	7.2	<a href="#">CVE-2019-1610</a> B D <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software and Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Firepower 4100 Series Next-Generation Firewalls are affected running software versions prior to 2.2.2.91, 2.3.1.110, and 2.4.1.222. Firepower 9300 Security Appliance are affected running software versions prior to 2.2.2.91, 2.3.1.110, and 2.4.1.222. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(25) and 8.3(1). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)4(9) and 7.0(3)17(5). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)17(5). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected running software versions prior to 7.1(5)N1(1b) and 7.3(4)N1(1). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22), 7.3(3)D1(1), 8.2(3). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)4(9) and 7.0(3)17(5). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5).	2019-03-11	7.2	<a href="#">CVE-2019-1611</a> B D <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)4(9) and 7.0(3)17(4). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)17(4). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)F3(5).	2019-03-11	7.2	<a href="#">CVE-2019-1612</a> B D <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The vulnerability is due to incorrect input validation of user-supplied data by the NX-API subsystem. An attacker could exploit this vulnerability by sending malicious HTTP or HTTPS packets to the management interface of an affected system that has the NX-API feature enabled. A successful exploit could allow the attacker to perform a command-injection attack and execute arbitrary commands with root privileges. Note: NX-API is disabled by default. MDS 9000 Series Multilayer Switches are affected running software versions prior to 8.1(1b) and 8.2(3). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)4(9) and 7.0(3)17(4). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)17(4). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected	2019-03-11	9.0	<a href="#">CVE-2019-1614</a> B D <a href="#">CISCO</a>



	running software versions prior to 7 3(4)N1(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 7 3(3)D1(1) and 8 2(3).			
cisco -- spa514g_firmware	A vulnerability in the implementation of Session Initiation Protocol (SIP) processing in Cisco Small Business SPA514G IP Phones could allow an unauthenticated, remote attacker to cause an affected device to become unresponsive, resulting in a denial of service (DoS) condition. The vulnerability is due to improper processing of S P request messages by an affected device. An attacker could exploit this vulnerability by sending crafted S P messages to an affected device. A successful exploit could allow the attacker to cause the affected device to become unresponsive, resulting in a DoS condition that persists until the device is restarted manually. Cisco has not released software updates that address this vulnerability. This vulnerability affects Cisco Small Business SPA514G IP Phones that are running firmware release 7.6.2SR2 or earlier.	2019-03-13	7.8	<a href="#">CVE-2018-0389</a> B.D CISCO
cobham -- satcom_sailor_800_firmware	Cobham Satcom Sailor 800 and 900 devices contained a vulnerability that allowed for arbitrary writing of content to the system's configuration file. This was exploitable via multiple attack vectors depending on the device's configuration. Further analysis also indicated this vulnerability could be leveraged to achieve a Denial of Service (DoS) condition, where the device would require a factory reset to return to normal operation.	2019-03-15	7.8	<a href="#">CVE-2018-19393</a> MISC MISC
ftpgetter -- ftpgetter	FTPGetter Standard v.5 97 0.177 allows remote code execution when a user initiates an FTP connection to an attacker-controlled machine that sends crafted responses. Long responses can also crash the FTP client with memory corruption.	2019-03-13	7.5	<a href="#">CVE-2019-9760</a> MISC EXPLOIT-DB
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 154069.	2019-03-11	7.2	<a href="#">CVE-2018-1978</a> B.D XF CONFIRM
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 154078.	2019-03-11	7.2	<a href="#">CVE-2018-1980</a> B.D XF CONFIRM
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 155893.	2019-03-11	7.2	<a href="#">CVE-2019-4015</a> B.D XF CONFIRM
ibm -- db2	BM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force D: 155894.	2019-03-11	7.2	<a href="#">CVE-2019-4016</a> B.D XF CONFIRM
ibm -- websphere_mq	BM WebSphere MQ 8 0.0.0 through 9.1.1 could allow a local user to inject code that could be executed with root privileges. This is due to an incomplete fix for CVE-2018-1792. IBM X-Force D: 154887.	2019-03-11	7.2	<a href="#">CVE-2018-1998</a> XF CONFIRM
intel -- converged_security_management_engine_firmware	Bounds check in Kernel subsystem in Intel CSME before version 11 8.60, 11.11.60, 11.22.60 or 12.0.20, or Intel(R) Server Platform Services before versions 4.00 04 383 or SPS 4 01 02.174, or Intel(R) TXE before versions 3.1 60 or 4 0.10 may allow an unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12191</a> CONFIRM
intel -- converged_security_management_engine_firmware	Logic bug in Kernel subsystem in Intel CSME before version 11 8.60, 11.11 60, 11.22.60 or 12.0.20, or Intel(R) Server Platform Services before version SPS_E5_04 00.04.393.0 may allow an unauthenticated user to potentially bypass MEBx authentication via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12192</a> CONFIRM
intel -- converged_security_management_engine_firmware	Buffer overflow in an OS component in Intel CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 and Intel TXE version before 3.1.60 or 4.0.10 may allow a privileged user to potentially execute arbitrary code via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12199</a> CONFIRM
intel -- graphics_driver	Potential memory corruption in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18 x.5059 (aka 15 33.x 5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19 x.5063 (aka 15.40.x 5063) 21.20.x 5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12214</a> CONFIRM
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18 x.5059 (aka 15 33.x 5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19 x.5063 (aka 15.40.x 5063) 21.20.x 5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12216</a> CONFIRM
intel -- graphics_driver	Logic bug in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions before versions 10.18 x.5059 (aka 15.33.x 5059), 10.18 x.5057 (aka 15.36.x.5057), 20.19 x.5063 (aka 15.40.x 5063) 21.20.x 5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12220</a> CONFIRM
intel -- platform_sample_firmware	Denial of service vulnerability in Platform Sample/ Silicon Reference firmware for 8th Generation Intel Core Processor, 7th Generation Intel Core Processor may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12203</a> CONFIRM
intel -- platform_sample_firmware	Privilege escalation vulnerability in Platform Sample/ Silicon Reference firmware Intel(R) Server Board, Intel(R) Server System and Intel(R) Compute Module may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	7.2	<a href="#">CVE-2018-12204</a> CONFIRM
intel -- platform_sample_firmware	Privilege escalation vulnerability in Platform Sample/ Silicon Reference firmware for 8th Generation Intel(R) Core Processor, 7th Generation Intel(R) Core Processor may allow unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	7.2	<a href="#">CVE-2018-12205</a> CONFIRM
microvirt -- memu	An issue was discovered in Microvirt MEmu 6.0.6. The MemuService.exe service binary is vulnerable to local privilege escalation through binary planting due to insecure permissions set at install time. This allows code to be run as NT AUTHORITY\SYSTEM.	2019-03-13	7.2	<a href="#">CVE-2018-20621</a> MISC
nablarch_project -- nablarch	Nablarch 5 (5, and 5u1 to 5u13) allows remote attackers to conduct XML External Entity (XXE) attacks via unspecified vectors.	2019-03-12	8.5	<a href="#">CVE-2019-5918</a> JVN MISC
php -- php	An issue was discovered in the EXIF component in PHP before 7.1 27, 7 2 x before 7.2.16, and 7 3 x before 7.3 3. There is an uninitialized read in exif_process_FD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.	2019-03-08	7.5	<a href="#">CVE-2019-9638</a> MISC DEBIAN
php -- php	An issue was discovered in the EXIF component in PHP before 7.1 27, 7 2 x before 7.2.16, and 7 3 x before 7.3 3. There is an uninitialized read in exif_process_FD_in_MAKERNOTE because of mishandling the data_len variable.	2019-03-08	7.5	<a href="#">CVE-2019-9639</a> MISC DEBIAN
				<a href="#">CVE-2019-9640</a>

php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.	2019-03-08	7.5	MISC DEBIAN
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_FD_in_TFF.	2019-03-08	7.5	CVE-2019-9641 MISC DEBIAN
phpshe -- phpshe	A SQL Injection was discovered in PHPSHE 1.7 in include/plugin/payment/alipay/pay.php with the parameter id. The vulnerability does not need any authentication.	2019-03-13	7.5	CVE-2019-9762 MISC
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	7.2	CVE-2018-4054 MISC
pixar -- renderman	A local privilege escalation vulnerability exists in the Mac OS X version of Pixar Renderman 22.3.0's Install Helper helper tool. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine for a successful exploit.	2019-03-08	7.2	CVE-2019-5015 MISC
podof project -- podof	PoDoFo 0.9.6 has a heap-based buffer overflow in PdfString::ConvertUTF16toUTF8 in base/PdfString.cpp.	2019-03-11	7.5	CVE-2019-9687 MISC
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Overflow that leads to a Heap-Based Buffer Overflow in the function rdp_in_unistr() and results in memory corruption and possibly even a remote code execution.	2019-03-15	7.5	CVE-2018-20177 MISC CONFIRM
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Underflow that leads to a Heap-Based Buffer Overflow in the function lspci_process() and results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20179 MISC CONFIRM
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Underflow that leads to a Heap-Based Buffer Overflow in the function rdpnsdbg_process() and results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20180 MISC CONFIRM
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain an Integer Underflow that leads to a Heap-Based Buffer Overflow in the function seamless_process() and results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20181 B.D MISC MLIST CONFIRM GENTOO DEBIAN
rdesktop -- rdesktop	rdesktop versions up to and including v1.8.3 contain a Buffer Overflow over the global variables in the function seamless_process_line() that results in memory corruption and probably even a remote code execution.	2019-03-15	7.5	CVE-2018-20182 B.D MISC MLIST CONFIRM GENTOO DEBIAN
sdcms -- sdcms	An issue was discovered in SDCMS V1.7. In the \app\admin\controller\themecontroller.php file, the check_bad() function's filtering is not strict, resulting in PHP code execution. This occurs because some dangerous PHP functions (such as "eval") are blocked but others (such as "system") are not, and because "php" is blocked but ".PHP" is not blocked.	2019-03-10	7.5	CVE-2019-9651 MISC
shanda -- maplestory_online	In Shanda MapleStory Online V160, the SdoKeyCrypt.sys driver allows privilege escalation to NT AUTHORITY\SYSTEM because of not validating the IOCTL 0x8000c01c input value, leading to an integer signedness error and a heap-based buffer underflow.	2019-03-12	7.2	CVE-2019-9729 MISC
tinysvcmdns_project -- tinysvcmdns	In tinysvcmdns through 2018-01-16, an mDNS server processing a crafted packet can perform arbitrary data read operations up to 16383 bytes from the start of the buffer. This can lead to a segmentation fault in uncompress_nlabel in mdns.c and a crash of the server (depending on the memory protection of the CPU and the operating system), or disclosure of memory content via error messages or a server response. NOTE: the product's web site states "This project is un-maintained, and has been since 2013. .... There are known vulnerabilities ... You are advised to NOT use this library for any new projects / products."	2019-03-13	9.4	CVE-2019-9748 MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1024tools -- 1024tools	DOM-based XSS exists in 1024Tools Markdown 1.0 via vectors involving the '<EMBED SRC=""data:image/svg+xml' substring.	2019-03-12	4.3	CVE-2019-9736 MISC
apache -- solr	Server Side Request Forgery in Apache Solr, versions 1.3 until 7.6 (inclusive). Since the "shards" parameter does not have a corresponding whitelist mechanism, a remote attacker with access to the server could make Solr perform an HTTP GET request to any reachable URL.	2019-03-08	5.0	CVE-2017-3164 MLIST B.D
blog_mini_project -- blog_mini	In Blog_mini 1.0, XSS exists via the author name of a comment reply in the app/main/views.py articleDetails() function, related to app/templates/_article_comments.html.	2019-03-14	4.3	CVE-2019-9765 MISC
botan_project -- botan	A side-channel issue was discovered in Botan before 2.9.0. An attacker capable of precisely measuring the time taken for ECC key generation may be able to derive information about the high bits of the secret key, as the function to derive the public point from the secret scalar uses an unblinded Montgomery ladder whose loop iteration count depends on the bitlength of the secret. This issue affects only key generation, not ECDSA signatures or ECDH key agreement.	2019-03-08	4.3	CVE-2018-20187 MISC MISC
checkstyle -- checkstyle	Checkstyle before 8.18 loads external DTDs by default.	2019-03-11	5.0	CVE-2019-9658 MISC MISC MISC
	The Chuango 433 MHz burglar-alarm product line uses static codes in the RF remote			CVE-

chuango -- a11_pstn/lcd/rfid_touch_alarm_system_firmware	control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay attacks, as demonstrated by Chuango branded products, and non-Chuango branded products such as the Eminent EM8617 OV2 Wifi Alarm System.	2019-03-11	6.4	2019-9659 MISC
cisco -- enterprise_chat_and_email	Multiple vulnerabilities in the web-based management interface of Cisco Enterprise Chat and Email could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit these vulnerabilities either by injecting malicious code in a chat window or by sending a crafted link to a user of the interface. In both cases, the attacker must persuade the user to click the crafted link or open the chat window that contains the attacker's code. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Version 11.6(1) is affected.	2019-03-11	4.3	CVE-2019-1702 B.D CISCO
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to escalate lower-level privileges to the administrator level. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow an attacker to make configuration changes to the system as administrator. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	4.6	CVE-2019-1603 B.D CISCO
cisco -- nx-os	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(27) and 8.2(3). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(6). Nexus 3500 Platform Switches are affected running software versions prior to 6.0(2)A8(11) and 7.0(3)I7(6). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9), 7.0(3)I7(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22) and 8.2(3).	2019-03-11	4.6	CVE-2019-1613 B.D CISCO
cisco -- nx-os	A vulnerability in the Image Signature Verification feature of Cisco NX-OS Software could allow an authenticated, local attacker with administrator-level credentials to install a malicious software image on an affected device. The vulnerability is due to improper verification of digital signatures for software images. An attacker could exploit this vulnerability by loading an unsigned software image on an affected device. A successful exploit could allow the attacker to boot a malicious software image. Note: The fix for this vulnerability requires a BIOS upgrade as part of the software upgrade. For additional information, see the Details section of this advisory. Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I7(5). Nexus 9000 Series Fabric Switches in ACI Mode are affected running software versions prior to 13.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I7(5). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5).	2019-03-11	4.6	CVE-2019-1615 B.D CISCO
cisco -- nx-os	A vulnerability in the Cisco Fabric Services component of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Cisco Fabric Services packets. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow, resulting in process crashes and a DoS condition on the device. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(25), 8.1(1b), 8.3(1). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected running software versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22) and 8.2(3). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5). UCS 6200, 6300, and 6400 Fabric Interconnects are affected running software versions prior to 3.2(3j) and 4.0(2a).	2019-03-11	5.0	CVE-2019-1616 B.D CISCO
cleanersoft -- free_mp3_cd_ripper	Stack-based buffer overflow in Free MP3 CD Ripper 2.6, when converting a file, allows user-assisted remote attackers to execute arbitrary code via a crafted .mp3 file.	2019-03-14	6.8	CVE-2019-9766 EXPLOIT-DB
cleanersoft -- free_mp3_cd_ripper	Stack-based buffer overflow in Free MP3 CD Ripper 2.6, when converting a file, allows user-assisted remote attackers to execute arbitrary code via a crafted .wma file.	2019-03-14	6.8	CVE-2019-9767 MISC EXPLOIT-DB
cmsmadesimple -- cms_made_simple	class.showtime2_image.php in CMS Made Simple (CMSMS) before 2.2.10 does not ensure that a watermark file has a standard image file extension (G F, JPG, JPEG, or PNG).	2019-03-11	5.0	CVE-2019-9692 MISC MISC
cmsmadesimple -- cms_made_simple	In CMS Made Simple (CMSMS) before 2.2.10, an authenticated user can achieve SQL Injection in class.showtime2_data.php via the functions _updateshow (parameter show_id), _inputshow (parameter show_id), _Getshowinfo (parameter show_id), _Getpictureinfo (parameter picture_id), _AdjustNameSeq (parameter shownumber), _Updatepicture (parameter picture_id), and _Deletepicture (parameter picture_id).	2019-03-11	6.5	CVE-2019-9693 MISC MISC
codecrafters -- ability_mail_server	Ability Mail Server 4.2.6 has Persistent Cross Site Scripting (XSS) via the body e-mail body. To exploit the vulnerability, the victim must open an email with malicious Javascript inserted into the body of the email as an iframe.	2019-03-12	4.3	CVE-2019-9557 MISC
cyberark -- endpoint_privilege_manager	A buffer overflow in the kernel driver CybKernelTracker.sys in CyberArk Endpoint Privilege Manager versions prior to 10.7 allows an attacker (without Administrator privileges) to escalate privileges or crash the machine by loading an image, such as a DLL, with a long path.	2019-03-08	6.9	CVE-2019-9627 B.D

				<a href="#">MISC</a>
editor md_project -- editor.md	Editor md 1.5.0 has DOM-based XSS via vectors involving the '<EMBED SRC="data:image/svg+xml" subtring.	2019-03-12	<a href="#">4.3</a>	<a href="#">CVE-2019-9737</a> <a href="#">MISC</a>
esafenet -- electronic_document_security_management_system	ESAFENET CDG V3 and V5 has an arbitrary file download vulnerability via the fileName parameter in download.jsp because the InstallationPack parameter is mishandled in a /CDGServer3/ClientAjax request.	2019-03-08	<a href="#">5.0</a>	<a href="#">CVE-2019-9632</a> <a href="#">MISC</a>
ffmpeg -- ffmpeg	In FFmpeg 4.1, a denial of service in the subtitle decoder allows attackers to hog the CPU via a crafted video file in Matroska format, because ff_htmlmarkup_to_ass in libavcodec/htmlsubtitles.c has a complex format argument to sscanf.	2019-03-12	<a href="#">4.3</a>	<a href="#">CVE-2019-9718</a> <a href="#">B D</a> <a href="#">MISC</a>
ffmpeg -- ffmpeg	A denial of service in the subtitle decoder in FFmpeg 4.1 allows attackers to hog the CPU via a crafted video file in Matroska format, because handle_open_brace in libavcodec/htmlsubtitles.c has a complex format argument to sscanf.	2019-03-12	<a href="#">4.3</a>	<a href="#">CVE-2019-9721</a> <a href="#">B D</a> <a href="#">MISC</a>
gitnoteapp -- gitnote	gitnote 3.1.0 allows remote attackers to execute arbitrary code via a crafted Markdown file, as demonstrated by a javascript:window.parent.top.require('child_process') execFile subtring in the onerror attribute of an MG element.	2019-03-14	<a href="#">6.8</a>	<a href="#">CVE-2019-9785</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- glib	gio/gsocketclient.c in GNOME GLib 2.59.2 does not ensure that a parent GTask remains alive during the execution of a connection-attempting enumeration, which allows remote attackers to cause a denial of service (g_socket_client_connected_callback mishandling and application crash) via a crafted web site, as demonstrated by GNOME Web (aka Epiphany).	2019-03-08	<a href="#">4.3</a>	<a href="#">CVE-2019-9633</a> <a href="#">B D</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer overflow in the function dwg_decode_eed_data at decode.c for the y dimension.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9770</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function bit_convert_TU at bits.c.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9771</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LEADER at dwg.spec.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9772</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer overflow in the function dwg_decode_eed_data at decode.c for the z dimension.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9773</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is an out-of-bounds read in the function bit_read_B at bits.c.	2019-03-14	<a href="#">6.4</a>	<a href="#">CVE-2019-9774</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is an out-of-bounds read in the function dwg_dxf_BLOCK_CONTROL at dwg.spec.	2019-03-14	<a href="#">6.4</a>	<a href="#">CVE-2019-9775</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LTYPE at dwg.spec (later than CVE-2019-9779).	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9776</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer over-read in the function dxf_header_write at header_variables_dxf.spec.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9777</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer over-read in the function dwg_dxf_LTYPE at dwg.spec.	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9778</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- libredwg	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LTYPE at dwg.spec (earlier than CVE-2019-9776).	2019-03-14	<a href="#">5.0</a>	<a href="#">CVE-2019-9779</a> <a href="#">MISC</a> <a href="#">MISC</a>
golang -- go	An issue was discovered in net/http in Go 1.11.5. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the second argument to http.NewRequest with \r\n followed by an HTTP header or a Redis command.	2019-03-13	<a href="#">4.3</a>	<a href="#">CVE-2019-9741</a> <a href="#">MISC</a>
golangtc -- gopher	jimmykuu Gopher 2.0 has DOM-based XSS via vectors involving the '<EMBED SRC="data:image/svg+xml" subtring.	2019-03-12	<a href="#">4.3</a>	<a href="#">CVE-2019-9738</a> <a href="#">MISC</a>
gpsd_project -- gpsd	gpsd versions 2.90 to 3.17 and microjson versions 1.0 to 1.3, an open source project, allow a stack-based buffer overflow, which may allow remote attackers to execute arbitrary code on embedded platforms via traffic on Port 2947/TCP or crafted JSON inputs.	2019-03-13	<a href="#">5.8</a>	<a href="#">CVE-2018-17937</a> <a href="#">B D</a> <a href="#">MISC</a>
ibm -- api_connect	IBM API Connect v2018.1 and 2018.4.1 is affected by an information disclosure vulnerability in the consumer API. Any registered user can obtain a list of all other users in	2019-03-	<a href="#">4.0</a>	<a href="#">CVE-2018-2009</a>

	all other orgs, including email id/names, etc. IBM X-Force D: 155148.	11		<a href="#">B D</a> <a href="#">XF</a> <a href="#">CONF RM</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152858.	2019-03-11	4.6	<a href="#">CVE-2018-1922</a> <a href="#">B D</a> <a href="#">XF</a> <a href="#">CONF RM</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152859.	2019-03-11	4.6	<a href="#">CVE-2018-1923</a> <a href="#">B D</a> <a href="#">XF</a> <a href="#">CONF RM</a>
ibm -- rational_engineering_lifecycle_manager	IBM Rational Engineering Lifecycle Manager 5.0 through 6.0 6 could allow a malicious user to be allowed to view any view if he knows the URL link of a the view, and access information that should not be able to see. BM X-Force D: 153120.	2019-03-14	4.0	<a href="#">CVE-2018-1929</a> <a href="#">CONF RM</a> <a href="#">XF</a>
ibm -- sdk	IBM SDK, Java Technology Edition Version 8 on the AIX platform uses absolute RPATHs which may facilitate code injection and privilege elevation by local users. BM X-Force ID: 152081.	2019-03-11	4.6	<a href="#">CVE-2018-1890</a> <a href="#">XF</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to spoof connection information which could be used to launch further attacks against the system. IBM X-Force ID: 152531.	2019-03-11	4.0	<a href="#">CVE-2018-1902</a> <a href="#">B D</a> <a href="#">XF</a> <a href="#">CONF RM</a>
ibm -- websphere_mq	IBM WebSphere 8.0 0 0 through 9.1.1 could allow an authenticated attacker to escalate their privileges when using multiplexed channels. BM X-Force ID: 153915.	2019-03-11	6.0	<a href="#">CVE-2018-1974</a> <a href="#">XF</a> <a href="#">CONF RM</a>
ichain -- insurance_wallet	Directory traversal vulnerability in iChain Insurance Wallet App for iOS Version 1.3.0 and earlier allows remote attackers to read arbitrary files via unspecified vectors.	2019-03-12	5.0	<a href="#">CVE-2019-5923</a> <a href="#">JVN</a> <a href="#">MISC</a>
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel(R) AMT in Intel(R) CSME before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20 may allow an unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	4.6	<a href="#">CVE-2018-12185</a> <a href="#">CONF RM</a>
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel CSME subsystem before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 or Intel TXE before 3.1.60 or 4.0.10 may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12190</a> <a href="#">CONF RM</a>
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel(R) AMT in Intel(R) CSME before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20 may allow a privileged user to potentially execute arbitrary code via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12196</a> <a href="#">CONF RM</a>
intel -- converged_security_management_engine_firmware	Buffer overflow in HECI subsystem in Intel(R) CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 and Intel(R) TXE version before 3.1.60 or 4.0.10, or Intel(R) Server Platform Services before version 5.00.04 012 may allow an unauthenticated user to potentially execute arbitrary code via physical access.	2019-03-14	4.6	<a href="#">CVE-2018-12208</a> <a href="#">CONF RM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x 5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x 5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100 6373 potentially enables an unprivileged user to cause an integer overflow via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12221</a> <a href="#">CONF RM</a>
intel -- graphics_driver	Insufficient access control in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x 5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x 5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100 6373 potentially enables an unprivileged user to escape from a virtual machine guest-to-host via local access.	2019-03-14	4.6	<a href="#">CVE-2018-12223</a> <a href="#">CONF RM</a>
intel -- rapid_storage_technology_enterprise	Improper permissions in the installer for Intel(R) Accelerated Storage Manager in RSTe v5.5 and before may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-03-14	4.6	<a href="#">CVE-2019-0135</a> <a href="#">CONF RM</a>
intel -- usb_3.0_creator_utility	Improper permissions for Intel(R) USB 3.0 Creator Utility all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-03-14	4.6	<a href="#">CVE-2019-0129</a> <a href="#">CONF RM</a>
iotivity -- iotivity	In IoTivity through 1.3.1, the CoAP server interface can be used for Distributed Denial of Service attacks using source IP address spoofing and UDP-based traffic amplification. The reflected traffic is 6 times bigger than spoofed requests. This occurs because the construction of a "4.01 Unauthorized" response is mishandled. NOTE: the vendor states "While this is an interesting attack, there is no plan for maintainer to fix, as we are migrating to IoTivity Lite."	2019-03-13	6.4	<a href="#">CVE-2019-9750</a> <a href="#">MISC</a>
jenkins -- appdynamics	An insufficiently protected credentials vulnerability exists in JenkinsAppDynamics Dashboard Plugin 1.0.14 and earlier in src/main/java/nl/codecentric/jenkins/appd/AppDynamicsResultsPublisher.java that allows attackers without permission to obtain passwords configured in jobs to obtain them.	2019-03-08	4.0	<a href="#">CVE-2019-1003039</a> <a href="#">CONF RM</a>
jenkins -- azure_vm_agents	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgentTemplate.java, src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to perform the 'verify configuration' form validation action, thereby obtaining limited information about the Azure configuration.	2019-03-08	4.0	<a href="#">CVE-2019-1003035</a> <a href="#">CONF RM</a>
jenkins -- azure_vm_agents	A data modification vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgent.java that allows attackers with Overall/Read permission to attach a public P address to an Azure VM agent.	2019-03-08	4.0	<a href="#">CVE-2019-1003036</a> <a href="#">CONF RM</a>



jenkins -- azure_vm_agents	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2019-03-08	4.0	<a href="#">CVE-2019-1003037</a> <a href="#">CONF RM</a>
jenkins -- email_extension	A sandbox bypass vulnerability exists in Jenkins Email Extension Plugin 2.64 and earlier in pom.xml, src/main/java/hudson/plugins/emailext/ExtendedEmailPublisher.java, src/main/java/hudson/plugins/emailext/plugins/content/EmailExtScript.java, src/main/java/hudson/plugins/emailext/plugins/content/ScriptContent.java, src/main/java/hudson/plugins/emailext/plugins/trigger/AbstractScriptTrigger.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003032</a> <a href="#">CONF RM</a>
jenkins -- groovy	A sandbox bypass vulnerability exists in Jenkins Groovy Plugin 2.1 and earlier in pom.xml, src/main/java/hudson/plugins/groovy/StringScriptSource.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003033</a> <a href="#">CONF RM</a>
jenkins -- job_dsl	A sandbox bypass vulnerability exists in Jenkins Job DSL Plugin 1.71 and earlier in job-dsl-core/src/main/groovy/javaposse/jobdsl/dsl/AbstractDslScriptLoader.groovy, job-dsl-plugin/build.gradle, job-dsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/JobDslWhitelist.groovy, job-dsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/SandboxDslScriptLoader.groovy that allows attackers with control over Job DSL definitions to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003034</a> <a href="#">CONF RM</a>
jenkins -- matrix_project	A sandbox bypass vulnerability exists in Jenkins Matrix Project Plugin 1.13 and earlier in pom.xml, src/main/java/hudson/matrix/FilterScript.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003031</a> <a href="#">CONF RM</a>
jenkins -- pipeline_groovy	A sandbox bypass vulnerability exists in Jenkins Pipeline: Groovy Plugin 2.63 and earlier in pom.xml, src/main/java/org/jenkinsci/plugins/workflow/cps/CpsGroovyShell.java that allows attackers able to control pipeline scripts to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003030</a> <a href="#">CONF RM</a>
jenkins -- script_security	A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.53 and earlier in src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/GroovySandbox.java, src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/SecureGroovyScript.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	6.5	<a href="#">CVE-2019-1003029</a> <a href="#">CONF RM</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The item_title layout in edit views lacks escaping, leading to XSS.	2019-03-12	4.3	<a href="#">CVE-2019-9711</a> <a href="#">B D</a> <a href="#">MISC</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The JSON handler in com_config lacks input validation, leading to XSS.	2019-03-12	4.3	<a href="#">CVE-2019-9712</a> <a href="#">B D</a> <a href="#">MISC</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The sample data plugins lack ACL checks, allowing unauthorized access.	2019-03-12	5.0	<a href="#">CVE-2019-9713</a> <a href="#">B D</a> <a href="#">MISC</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.4. The media form field lacks escaping, leading to XSS.	2019-03-12	4.3	<a href="#">CVE-2019-9714</a> <a href="#">B D</a> <a href="#">MISC</a>
jtbc -- jtbc_php	An issue was discovered in JTBC(PHP) 3.0.1.8. Its cache management module is flawed. An arbitrary file ending in ".inc.php" can be deleted via a console/cache/manage.php?type=action&action=batch&batch=delete&ids=../ substring.	2019-03-11	6.4	<a href="#">CVE-2019-9662</a> <a href="#">MISC</a>
kartatopia -- piluscart	PilusCart 1.4.1 is vulnerable to index.php?module=users&action=newUser CSRF, leading to the addition of a new user as administrator.	2019-03-14	6.8	<a href="#">CVE-2019-9769</a> <a href="#">EXPLOIT-DB</a>
korenix -- jetport_web_manager	The Web manager (aka Commander) on Korenix JetPort 5601 and 5601f devices has Persistent XSS via the Port Alias field under Serial Setting.	2019-03-12	4.3	<a href="#">CVE-2019-9725</a> <a href="#">MISC</a>
lexmark -- cx725h_firmware	On certain Lexmark devices that communicate with an LDAP or SMTP server, a malicious administrator can discover LDAP or SMTP credentials by changing that server's hostname to one that they control, and then capturing the credentials that are sent there. This occurs because stored credentials are not automatically deleted upon that type of hostname change.	2019-03-12	4.0	<a href="#">CVE-2018-17944</a> <a href="#">CONF RM</a>
libofx_project -- libofx	An issue was discovered in LibOFX 0.9.14. There is a NULL pointer dereference in the function OFXApplication::startElement in the file lib/ofx_sgml.cpp, as demonstrated by ofxdump.	2019-03-11	6.8	<a href="#">CVE-2019-9656</a> <a href="#">MISC</a> <a href="#">MISC</a>
maccms -- maccms	Maccms 10 allows remote attackers to execute arbitrary PHP code by entering this code in a template/default_pc/html/art Edit action. This occurs because template rendering uses an include operation on a cache file, which bypasses the prohibition of .php files as templates.	2019-03-14	6.5	<a href="#">CVE-2019-9829</a> <a href="#">MISC</a>
mailtraq -- webmail	Mailtraq WebMail version 2.17.7.3550 has Persistent Cross Site Scripting (XSS) via the body of an e-mail message. To exploit the vulnerability, the victim must open an email with malicious Javascript inserted into the body of the email as an iframe.	2019-03-12	4.3	<a href="#">CVE-2019-9558</a> <a href="#">MISC</a>
microsoft -- teams	Untrusted search path vulnerability in The installer of Microsoft Teams allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-03-12	6.8	<a href="#">CVE-2019-5922</a> <a href="#">JVN</a> <a href="#">B D</a>
microsoft -- windows_7	Untrusted search path vulnerability in Windows 7 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-03-12	6.8	<a href="#">CVE-2019-5921</a> <a href="#">JVN</a> <a href="#">B D</a>

nablarch_project -- nablarch	An incomplete cryptography of the data store function by using hidden tag in Nablarch 5 (5, and 5u1 to 5u13) allows remote attackers to obtain information of the stored data, to register invalid value, or alter the value via unspecified vectors.	2019-03-12	6.4	CVE-2019-5919 JVN MISC
ncrafts -- formcraft	Cross-site request forgery (CSRF) vulnerability in FormCraft 1 2.1 and earlier allows remote attackers to hijack the authentication of administrators via a specially crafted page.	2019-03-12	6.8	CVE-2019-5920 JVN MISC MISC
openstack -- neutron	An issue was discovered in the iptables firewall module in OpenStack Neutron before 10.0.8, 11.x before 11.0.7, 12.x before 12.0.6, and 13.x before 13.0.3. By setting a destination port in a security group rule along with a protocol that doesn't support that option (for example, VRRP), an authenticated user may block further application of security group rules for instances from any project/tenant on the compute hosts to which it's applied. (Only deployments using the iptables security group driver are affected.)	2019-03-12	4.0	CVE-2019-9735 B.D MISC
openwsman_project -- openwsman	Openwsman, versions up to and including 2.6.9, are vulnerable to arbitrary file disclosure because the working directory of openwsmand daemon was set to root directory. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to openwsman server.	2019-03-14	5.0	CVE-2019-3816 CONF.RM B.D CONF.RM
openwsman_project -- openwsman	Openwsman, versions up to and including 2.6.9, are vulnerable to infinite loop in process_connection() when parsing specially crafted HTTP requests. A remote, unauthenticated attacker can exploit this vulnerability by sending malicious HTTP request to cause denial of service to openwsman server.	2019-03-14	5.0	CVE-2019-3833 CONF.RM B.D CONF.RM
php -- php	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.	2019-03-08	5.0	CVE-2019-9637 MISC DEBIAN
php -- php	** DISPUTED ** An issue was discovered in PHP 7.x before 7.1.27 and 7.3.x before 7.3.3. phar_tar_writeheaders_int in ext/phar/tar.c has a buffer overflow via a long link value. NOTE: The vendor indicates that the link value is used only when an archive contains a symlink, which currently cannot happen: "This issue allows theoretical compromise of security, but a practical attack is usually impossible."	2019-03-11	6.8	CVE-2019-9675 MISC MISC
phpshe -- phpshe	An XXE issue was discovered in PHPSHE 1.7, which can be used to read any file in the system or scan the internal network without authentication. This occurs because of the call to wechat_getxml in include/plugin/payment/wechat/notify_url.php.	2019-03-13	5.0	CVE-2019-9761 MISC
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to read any root file from the file system. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	4.9	CVE-2018-4055 MISC
python -- python	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	2019-03-08	5.0	CVE-2019-9636 B.D MISC MISC
python -- python	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with '\r\n' followed by an HTTP header or a Redis command.	2019-03-12	4.3	CVE-2019-9740 MISC
rdesktop -- rdesktop	rdesktop versions up to and including v1 8.3 contain an Out-Of-Bounds Read in the function ui_clip_handle_data() that results in an information leak.	2019-03-15	5.0	CVE-2018-20174 MISC CONF.RM
rdesktop -- rdesktop	rdesktop versions up to and including v1 8.3 contains several Integer Signedness errors that lead to Out-Of-Bounds Reads in the file mcs.c and result in a Denial of Service (segfault).	2019-03-15	5.0	CVE-2018-20175 B.D MISC MLIST CONF.RM GENTOO DEBIAN
rdesktop -- rdesktop	rdesktop versions up to and including v1 8.3 contain several Out-Of-Bounds Reads in the file secure.c that result in a Denial of Service (segfault).	2019-03-15	5.0	CVE-2018-20176 MISC CONF.RM
rdesktop -- rdesktop	rdesktop versions up to and including v1 8.3 contain an Out-Of-Bounds Read in the function process_demand_active() that results in a Denial of Service (segfault).	2019-03-15	5.0	CVE-2018-20178 B.D MISC MLIST CONF.RM GENTOO DEBIAN
rednao -- smart_forms	Cross-site request forgery (CSRF) vulnerability in Smart Forms 2 6.15 and earlier allows remote attackers to hijack the authentication of administrators via a specially crafted page.	2019-03-12	6.8	CVE-2019-5924 JVN MISC
sap -- advanced_business_application_programming_platform_kernel	ABAP Server of SAP NetWeaver and ABAP Platform fail to perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has been corrected in the following versions: KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.74, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, 7.74, 8.04, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, 7.74, 7.75, 8.04.	2019-03-12	6.5	CVE-2019-0270 B.D MISC MISC

sap -- banking_services_from_sap	Banking services from SAP 9.0 (FSAPPL version 5) and SAP S/4HANA Financial Products Subledger (S4FPSL, version 1) performs an inadequate authorization check for an authenticated user, potentially resulting in escalation of privileges.	2019-03-12	6.5	<a href="#">CVE-2019-0276</a> <a href="#">B D</a> <a href="#">MISC</a>
sap -- businessobjects_business_intelligence	SAP BusinessObjects Business Intelligence Platform (CMC Module), versions 4.10, 4.20 and 4.30, does not sufficiently validate an XML document accepted from an untrusted source.	2019-03-12	5.5	<a href="#">CVE-2019-0268</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- hana_extended_application_services	SAP HANA extended application services, version 1, advanced does not sufficiently validate an XML document accepted from an authenticated developer with privileges to the SAP space (XML External Entity vulnerability).	2019-03-12	5.5	<a href="#">CVE-2019-0277</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- mobile_platform_sdk	SAP Mobile Platform SDK allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service (i.e. denial of service). Fixed in versions 3.1 SP03 PL02, SDK 3.1 SP04, or later.	2019-03-12	5.0	<a href="#">CVE-2019-0274</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sdcms -- sdcms	There is a CSRF in SDCMS V1.7 via an m=admin&c=theme&a=edit request. t allows PHP code injection by providing a filename in the file parameter, and providing file content in the t2 parameter.	2019-03-10	6.8	<a href="#">CVE-2019-9652</a> <a href="#">MISC</a>
sftnow -- sftnow	sftnow through 2018-12-29 allows index.php?g=Admin&m=User&a=add_post CSRF to add an admin account.	2019-03-11	6.8	<a href="#">CVE-2019-9688</a> <a href="#">MISC</a>
stackstorm -- stackstorm	In st2web in StackStorm Web UI before 2.9.3 and 2.10.x before 2.10.3, it is possible to bypass the CORS protection mechanism via a "null" origin value, potentially leading to XSS.	2019-03-08	4.3	<a href="#">CVE-2019-9580</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
thinkst -- canarytokens	Thinkst Canarytokens through 2019-03-01 relies on limited variation in size, metadata, and timestamp, which makes it easier for attackers to estimate whether a Word document contains a token.	2019-03-14	5.0	<a href="#">CVE-2019-9768</a> <a href="#">MISC</a>
tinyc -- tinyc	An issue was discovered in Tiny C Compiler (aka TinyCC or TCC) 0.9.27. Compiling a crafted source file leads to an 1 byte out of bounds write in the end_macro function in tccpp.c.	2019-03-13	4.3	<a href="#">CVE-2019-9754</a> <a href="#">MISC</a>
tinysvcdns_project -- tinysvcdns	In tinysvcdns through 2018-01-16, a maliciously crafted mDNS (Multicast DNS) packet triggers an infinite loop while parsing an mDNS query. When mDNS compressed labels point to each other, the function uncompress_nlabel goes into an infinite loop trying to analyze the packet with an mDNS query. As a result, the mDNS server hangs after receiving the malicious mDNS packet. NOTE: the product's web site states "This project is un-maintained, and has been since 2013. ... There are known vulnerabilities ... You are advised to NOT use this library for any new projects / products."	2019-03-13	5.0	<a href="#">CVE-2019-9747</a> <a href="#">MISC</a>
treasuredata -- fluent_bit	An issue was discovered in the MQTT input plugin in Fluent Bit through 1.0.4. When this plugin acts as an MQTT broker (server), it mishandles incoming network messages. After processing a crafted packet, the plugin's mqtt_packet_drop function (in /plugins/in_mqtt/mqtt_prot.c) executes the memmove() function with a negative size parameter. That leads to a crash of the whole Fluent Bit server via a SIGSEGV signal.	2019-03-13	5.0	<a href="#">CVE-2019-9749</a> <a href="#">MISC</a>
webmproject -- libwebm	In libwebm before 2019-03-08, a NULL pointer dereference caused by the functions OutputCluster and OutputTracks in webm_info.cc will trigger an abort, which allows a DoS attack, a similar issue to CVE-2018-19212.	2019-03-13	5.0	<a href="#">CVE-2019-9746</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php.	2019-03-14	6.8	<a href="#">CVE-2019-9787</a> <a href="#">B D</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- application_policy_infrastructure_controller	A vulnerability in the management interface of Cisco Application Policy Infrastructure Controller (APIC) software could allow an unauthenticated, adjacent attacker to gain unauthorized access on an affected device. The vulnerability is due to a lack of proper access control mechanisms for Pv6 link-local connectivity imposed on the management interface of an affected device. An attacker on the same physical network could exploit this vulnerability by attempting to connect to the IPv6 link-local address on the affected device. A successful exploit could allow the attacker to bypass default access control restrictions on an affected device. Cisco Application Policy Infrastructure Controller (APIC) devices running versions prior to 4.2(0.21c) are affected.	2019-03-11	3.3	<a href="#">CVE-2019-1690</a> <a href="#">BID</a> <a href="#">CISCO</a>
cobham -- satcom_sailor_800_firmware	Cobham Satcom Sailor 800 and 900 devices contained persistent XSS, which required administrative access to exploit. The vulnerability was exploitable by acquiring a copy of the device's configuration file, inserting an XSS payload into a relevant field (e.g., Satellite name), and then restoring the malicious configuration file.	2019-03-15	3.5	<a href="#">CVE-2018-19394</a> <a href="#">MISC</a> <a href="#">MISC</a>
	Cross-site scripting vulnerability in Dradis Community Edition Dradis Community Edition v3.11 and earlier and Dradis Professional Edition v3.1.1 and earlier allow			<a href="#">CVE-2019-5925</a>

dradisframework -- dradis	remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-03-12	3.5	JVN MISC
ibm -- rational_collaborative_lifecycle_management	BM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 5.0 through 6.0.6) is vulnerable to HTTP header injection, caused by improper validation of input. By persuading a victim to visit a specially-crafted Web page, a remote attacker could exploit this vulnerability to inject arbitrary HTTP headers, which will allow the attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. BM X-Force ID: 144884.	2019-03-14	3.5	<a href="#">CVE-2018-1658</a> CONFIRM XF
ibm -- rational_collaborative_lifecycle_management	BM Jazz Foundation (IBM Rational Collaborative Lifecycle Management 5.0 through 6.0.6) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 145509.	2019-03-14	3.5	<a href="#">CVE-2018-1688</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Rational Engineering Lifecycle Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152734.	2019-03-14	3.5	<a href="#">CVE-2018-1910</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Rational Engineering Lifecycle Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152738.	2019-03-14	3.5	<a href="#">CVE-2018-1914</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Jazz Foundation (IBM Rational Engineering Lifecycle Manager 5.0 through 6.0.6) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152740.	2019-03-14	3.5	<a href="#">CVE-2018-1916</a> CONFIRM XF
ibm -- rational_engineering_lifecycle_manager	BM Jazz Foundation (IBM Rational Engineering Lifecycle Manager 5.0 through 6.0.6) is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153495.	2019-03-14	3.5	<a href="#">CVE-2018-1952</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148613.	2019-03-14	3.5	<a href="#">CVE-2018-1759</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148617.	2019-03-14	3.5	<a href="#">CVE-2018-1763</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148618.	2019-03-14	3.5	<a href="#">CVE-2018-1764</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150426.	2019-03-14	3.5	<a href="#">CVE-2018-1823</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150427.	2019-03-14	3.5	<a href="#">CVE-2018-1824</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150428.	2019-03-14	3.5	<a href="#">CVE-2018-1825</a> CONFIRM XF
ibm -- rational_quality_manager	BM Rational Quality Manager 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 150432.	2019-03-14	3.5	<a href="#">CVE-2018-1829</a> CONFIRM XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 148615.	2019-03-14	3.5	<a href="#">CVE-2018-1761</a> CONFIRM BID XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 154135.	2019-03-14	3.5	<a href="#">CVE-2018-1982</a> CONFIRM BID XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 154136.	2019-03-14	3.5	<a href="#">CVE-2018-1983</a> CONFIRM XF
ibm -- rational_team_concert	BM Rational Team Concert 5.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 154137.	2019-03-14	3.5	<a href="#">CVE-2018-1984</a> CONFIRM BID XF
intel -- converged_security_management_engine_firmware	Insufficient input validation in Intel CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 or Intel TXE before version 3.1.60 or 4.0.10 may allow an unauthenticated user to potentially modify data via physical access.	2019-03-14	2.1	<a href="#">CVE-2018-12188</a> CONFIRM
intel -- converged_security_management_engine_firmware	Unhandled exception in Content Protection subsystem in Intel CSME before versions 11.8.60, 11.11.60, 11.22.60 or 12.0.20 or Intel TXE before 3.1.60 or 4.0.10 may allow privileged user to potentially modify data via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12189</a> CONFIRM
intel -- graphics_driver	Insufficient access control in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to read device configuration information via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12209</a> CONFIRM
intel -- graphics_driver	Multiple pointer dereferences in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12210</a> CONFIRM
intel -- graphics_driver	Insufficient input validation in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064)	2019-03-14	2.1	<a href="#">CVE-2018-12211</a> CONFIRM

	and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.			
intel -- graphics_driver	Buffer overflow in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12212 CONFIRM</a>
intel -- graphics_driver	Potential memory corruption in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12213 CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to cause a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12215 CONFIRM</a>
intel -- graphics_driver	Insufficient access control in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables a privileged user to read device configuration information via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12217 CONFIRM</a>
intel -- graphics_driver	Unhandled exception in User Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause a memory leak via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12218 CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to read memory via local access via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12219 CONFIRM</a>
intel -- graphics_driver	Insufficient input validation in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 potentially enables an unprivileged user to cause an out of bound memory read via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12222 CONFIRM</a>
intel -- graphics_driver	Buffer leakage in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable information disclosure via local access.	2019-03-14	2.1	<a href="#">CVE-2018-12224 CONFIRM</a>
intel -- graphics_driver	Multiple out of bounds read in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable information disclosure via local access.	2019-03-14	2.1	<a href="#">CVE-2018-18089 CONFIRM</a>
intel -- graphics_driver	Out of bounds read in igdkm64.sys in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an authenticated user to potentially enable denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-18090 CONFIRM</a>
intel -- graphics_driver	Use after free in Kernel Mode Driver in Intel(R) Graphics Driver for Windows* before versions 10.18.x.5059 (aka 15.33.x.5059), 10.18.x.5057 (aka 15.36.x.5057), 20.19.x.5063 (aka 15.40.x.5063) 21.20.x.5064 (aka 15.45.x.5064) and 24.20.100.6373 may allow an unprivileged user to potentially enable a denial of service via local access.	2019-03-14	2.1	<a href="#">CVE-2018-18091 CONFIRM</a>
jenkins -- repository_connector	An insufficiently protected credentials vulnerability exists in Jenkins Repository Connector Plugin 1.2.4 and earlier in src/main/java/org/jvnet/hudson/plugins/repositoryconnector/ArtifactDeployer.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/Repository.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/UserPwd.java that allows an attacker with local file system access or control of a Jenkins administrator's web browser (e.g. malicious extension) to retrieve the password stored in the plugin configuration.	2019-03-08	2.1	<a href="#">CVE-2019-1003038 CONFIRM</a>
mcafee -- database_security	Data Leakage Attacks vulnerability in the web interface in McAfee Database Security prior to the 4.6.6 March 2019 update allows local users to expose passwords via incorrectly auto completing password fields in the admin browser login screen.	2019-03-12	2.1	<a href="#">CVE-2019-3615 BID CONFIRM</a>
rsa -- archer_grc_platform	RSA Archer versions, prior to 6.5 SP1, contain an information exposure vulnerability. Users' session information is logged in plain text in the RSA Archer log files. An authenticated malicious local user with access to the log files may obtain the exposed information to use it in further attacks.	2019-03-13	2.1	<a href="#">CVE-2019-3715 FULLDISC</a>
rsa -- archer_grc_platform	RSA Archer versions, prior to 6.5 SP2, contain an information exposure vulnerability. The database connection password may get logged in plain text in the RSA Archer log files. An authenticated malicious local user with access to the log files may obtain the exposed password to use it in further attacks.	2019-03-13	2.1	<a href="#">CVE-2019-3716 BID FULLDISC</a>
sap -- businessobjects_business_intelligence	SAP BusinessObjects Business Intelligence Platform (BI Workspace), versions 4.10 and 4.20, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-03-12	3.5	<a href="#">CVE-2019-0269 BID MISC MISC</a>
sap -- netweaver_java_application_server	SAML 1.1 SSO Demo Application in SAP NetWeaver Java Application Server (J2EE-APPS), versions 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40 and 7.50, does not sufficiently encode user-controlled inputs, which results in cross-site scripting (XSS) vulnerability.	2019-03-12	3.5	<a href="#">CVE-2019-0275 BID MISC MISC</a>
yzmcms -- yzmcms	Stored XSS exists in YzmCMS 5.2 via the admin/category/edit.html "catname" parameter.	2019-03-11	3.5	<a href="#">CVE-2019-9660 MISC</a>
yzmcms -- yzmcms	Stored XSS exists in YzmCMS 5.2 via the admin/system_manage/user_config_edit.html "value" parameter,	2019-03-11	3.5	<a href="#">CVE-2019-9661 MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary		CVSS	Source & Patch
---------	--	------	----------------



Vendor -- Product	Description	Published	Score	Info
abap -- server_and_platform	ABAP Server (used in NetWeaver and Suite/ERP) and ABAP Platform does not sufficiently validate an XML document accepted from an untrusted source, leading to an XML External Entity (XEE) vulnerability. Fixed in Kernel 7.21 or 7.22, that is ABAP Server 7.00 to 7.31 and Kernel 7.45, 7.49 or 7.53, that is ABAP Server 7.40 to 7.52 or ABAP Platform.	2019-03-12	not yet calculated	<a href="#">CVE-2019-0271</a> B D <a href="#">MISC</a> <a href="#">MISC</a>
airmore -- airmore	The AirMore application through 1.6.1 for Android allows remote attackers to cause a denial of service (system hang) via many simultaneous /? Key=PhoneRequestAuthorization requests.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9831</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a>
azure-umqtt-c -- azure-umqtt-c	azure-umqtt-c (available through GitHub prior to 2017 October 6) allows remote attackers to cause a denial of service via unspecified vectors.	2019-03-12	not yet calculated	<a href="#">CVE-2019-5917</a> JVN B D <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. The client applications of AccessManagerCoreService.exe communicate with this server through named pipes. A user can initiate communication with the server by creating a named pipe and sending commands to achieve elevated privileges.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18255</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. A regular user can obtain local administrator privileges if they run any whitelisted application through the Custom App Launcher.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18256</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. CALRunElevated.exe provides "NT AUTHORITY\SYSTEM" access to unprivileged users via the --system option.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18252</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. CALRunElevated.exe attempts to enforce access control by adding an unprivileged user to the local Administrators group for a very short time to execute a single command. However, the user is left in that group if the command crashes, and there is also a race condition in all cases.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18253</a> <a href="#">MISC</a>
capmon -- access_manager	An issue was discovered in CapMon Access Manager 5.4.1.1005. An unprivileged user can read the cal_whitelist table in the Custom App Launcher (CAL) database, and potentially gain privileges by placing a Trojan horse program at an app pathname.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18254</a> <a href="#">MISC</a>
circuitwerkes -- sicon-8	CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a web-based front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's web browser.	2019-03-15	not yet calculated	<a href="#">CVE-2019-5616</a> <a href="#">MISC</a>
cisco -- common_services_platform_collector	A vulnerability in the Cisco Common Services Platform Collector (CSPC) could allow an unauthenticated, remote attacker to access an affected device by using an account that has a default, static password. This account does not have administrator privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to the affected system using this account. A successful exploit could allow the attacker to log in to the CSPC using the default account. For Cisco CSPC 2.7.x, Cisco fixed this vulnerability in Release 2.7.4.6. For Cisco CSPC 2.8.x, Cisco fixed this vulnerability in Release 2.8.1.2.	2019-03-13	not yet calculated	<a href="#">CVE-2019-1723</a> B D <a href="#">CISCO</a>
cisco -- dna_center	A vulnerability in the web-based management interface of Cisco DNA Center could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. Cisco DNA Center versions prior to 1.2.5 are affected.	2019-03-11	not yet calculated	<a href="#">CVE-2019-1707</a> B D <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid user credentials to exploit this vulnerability. Nexus 3000, 3500, and Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1606</a> B D <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to access sensitive data that could be used to elevate their privileges to administrator. The vulnerability is due to improper implementation of filesystem permissions. An attacker could exploit this vulnerability by logging in to the CLI of an affected device, accessing a specific file, and leveraging this information to authenticate to the NX-API server. A successful exploit could allow an attacker to make configuration changes as administrator. Note: NX-API is disabled by default. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1602</a> B D <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the Fibre Channel over Ethernet (FCoE) N-port Virtualization (NPV) protocol implementation in Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to an incorrect processing of FCoE packets when the coe-npv feature is uninstalled. An attacker could exploit this vulnerability by sending a stream of FCoE frames from an adjacent host to an affected device. An exploit could allow the attacker to cause packet amplification to occur, resulting in the saturation of interfaces and a DoS condition. Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I7(5) and 9.2(2).	2019-03-11	not yet calculated	<a href="#">CVE-2019-1617</a> B D <a href="#">CISCO</a>
cloud_foundry_foundation -- cloud_controller	Cloud Foundry Cloud Controller, versions prior to 1.78.0, contain an endpoint with improper authorization. A remote authenticated malicious user with read permissions can request package information and receive a signed bit-service url that grants the user write permissions to the bit-service.	2019-03-13	not yet calculated	<a href="#">CVE-2019-3785</a> <a href="#">CONFIRM</a>
cloud_foundry_foundation -- container_runtime	Cloud Foundry Container Runtime, versions prior to 0.28.0, deploys K8s worker nodes that contains a configuration file with IAAS credentials. A malicious user with access to the k8s nodes can obtain IAAS credentials allowing the user to escalate privileges to gain access to the IAAS account.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3780</a> <a href="#">CONFIRM</a>
	Cloud Foundry Container Runtime, versions prior to 0.29.0, deploys Kubernetes			

cloud_foundry_foundation -- container_runtime	clusters utilize the same CA (Certificate Authority) to sign and trust certs for ETCD as used by the Kubernetes API. This could allow a user authenticated with a cluster to request a signed certificate leveraging the Kubernetes CSR capability to obtain a credential that could escalate privilege access to ETCD.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3779</a> CONFIRM
cobham -- satcom_sailor_250_and_500_devices	Cobham Satcom Sailor 250 and 500 devices before 1.25 contained persistent XSS, which could be exploited by an unauthenticated threat actor via the index.lua?pageID=Phone%20book name field.	2019-03-15	not yet calculated	<a href="#">CVE-2018-19391</a> MISC MISC
cobham -- satcom_sailor_250_and_500_devices	Cobham Satcom Sailor 250 and 500 devices before 1.25 contained an unauthenticated password reset vulnerability. This could allow modification of any user account's password (including the default "admin" account), without prior knowledge of their password. All that is required is knowledge of the username and attack vector (/index.lua?pageID=Administration usernameAdmChange, passwordAdmChange1, and passwordAdmChange2 fields).	2019-03-15	not yet calculated	<a href="#">CVE-2018-19392</a> MISC MISC
ethereum -- cryptobotsbattle_token	An Integer overflow vulnerability exists in the batchTransfer function of a smart contract implementation for CryptoBotsBattle (CBTB), an Ethereum token. This vulnerability could be used by an attacker to create an arbitrary amount of tokens or any user.	2019-03-15	not yet calculated	<a href="#">CVE-2018-17882</a> MISC MISC
f5 -- big-ip	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6597</a> CONFIRM
f5 -- big-ip	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to perform the attack.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6598</a> CONFIRM
f5 -- big-ip	In BIG-IP 11.6.1-11.6.3.2 or 11.5.1-11.5.8, or Enterprise Manager 3.1.1, improper escaping of values in an undisclosed page of the configuration utility may result with an improper handling on the JSON response when it is injected by a malicious script via a remote cross-site scripting (XSS) attack.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6599</a> B D CONFIRM
f5 -- big-ip	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be effected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6600</a> CONFIRM
f5 -- big-ip	In BIG-IP 13.0.0, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, the Application Acceleration Manager (AAM) wamd process used in processing of images and PDFs fails to drop group permissions when executing helper scripts.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6601</a> CONFIRM
f5 -- big-ip_apm	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.1, 12.1.0-12.1.3.6, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when processing fragmented ClientHello messages in a DTLS session TMM may corrupt memory eventually leading to a crash. Only systems offering DTLS connections via APM are impacted.	2019-03-13	not yet calculated	<a href="#">CVE-2019-6596</a> B D CONFIRM
feifeicms -- feifeicms	FeiFeiCMS 4.1.190209 allows remote attackers to upload and execute arbitrary PHP code by visiting index.php?s=Admin-Index to modify the set of allowable file extensions, as demonstrated by adding php to the default jpg,gif,png,jpeg setting, and then using the "add article" feature.	2019-03-14	not yet calculated	<a href="#">CVE-2019-9825</a> MISC MISC
fujitsu -- wireless_keyboard_set	The receiver (aka bridge) component of Fujitsu Wireless Keyboard Set LX901 GK900 devices allows Keystroke Injection. This occurs because it accepts unencrypted 2.4 GHz packets, even though all legitimate communication uses AES encryption.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9835</a> MISC
g_data_software -- total_security	gdwfpd.sys in G Data Total Security before 2019-02-22 allows an attacker to bypass ACLs because Interpreted Device Characteristics lacks FILE_DEVICE_SECURE_OPEN and therefore files and directories "inside" the \gdwfpd device are not properly protected, leading to unintended impersonation or object creation.	2019-03-13	not yet calculated	<a href="#">CVE-2019-9742</a> MISC MISC
google -- android	The Screen Stream application through 3.0.15 for Android allows remote attackers to cause a denial of service via many simultaneous /start-stop requests.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9833</a> EXPLOIT-DB
google -- android	The AirDrop application through 2.0 for Android allows remote attackers to cause a denial of service via a client that makes many socket connections through a configured port.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9832</a> EXPLOIT-DB MISC
highcharts_js -- highcharts_js	In js/parts/SvgRenderer.js in Highcharts JS before 6.1.0, the use of backtracking regular expressions permitted an attacker to conduct a denial of service attack against the SVGRenderer component, aka ReDoS.	2019-03-14	not yet calculated	<a href="#">CVE-2018-20801</a> MISC MISC
huawei -- oceanstor_uds_devices	Huawei OceanStor UDS devices with software before V100R002C01SPC102 might allow remote attackers to capture and change patch loading information resulting in the deletion of directory files and compromise of system functions when loading a patch.	2019-03-13	not yet calculated	<a href="#">CVE-2015-2254</a> CONFIRM
ibm -- content_navigator	IBM Content Navigator 3.0CD could allow an attacker to execute arbitrary code on a user's workstation. When editing an executable file in ICN with Edit service, it will be executed on the user's workstation. BM X-Force ID: 156000.	2019-03-14	not yet calculated	<a href="#">CVE-2019-4034</a> B D X E CONFIRM
ibm -- robotic_process_automation_with_automation_anywhere	IBM Robotic Process Automation with Automation Anywhere 11 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 152671.	2019-03-14	not yet calculated	<a href="#">CVE-2018-1908</a> CONFIRM X E
intel -- active_management_technology	Insufficient input validation in Intel(R) Active Management Technology (Intel(R) AMT) before version 11.8.60, 11.11.60, 11.22.60 or 12.0.20 may allow an unauthenticated user to potentially cause a denial of service via network access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12187</a> CONFIRM
intel -- capability_licensing_service	Insufficient access control in Intel(R) Capability Licensing Service before version 1.50.638.1 may allow an unprivileged user to potentially escalate privileges via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12200</a> CONFIRM
intel -- matrix_storage_manager	Improper permissions in Intel(R) Matrix Storage Manager 8.9.0.1023 and before may allow an authenticated user to potentially enable escalation of privilege via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2019-0121</a> CONFIRM
intel -- multiple_products	Privilege escalation vulnerability in Platform Sample/ Silicon Reference firmware or 8th Generation Intel(R) Core Processor, 7th Generation Intel(R) Core Processor may allow privileged user to potentially leverage existing features via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12202</a> CONFIRM
	Buffer overflow vulnerability in Platform Sample/ Silicon Reference firmware for 8th Generation Intel(R) Core Processor, 7th Generation Intel(R) Core Processor, Intel(R) Pentium(R) Silver J5005 Processor, Intel(R) Pentium(R) Silver N5000			

intel -- multiple_products	Processor, Intel(R) Celeron(R) J4105 Processor, Intel(R) Celeron(R) J4005 Processor, Intel Celeron(R) N4100 Processor and Intel(R) Celeron N4000 Processor may allow privileged user to potentially execute arbitrary code via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12201 CONFIRM</a>
intel -- server_platform_services_heci_subsystem	Insufficient input validation in Intel(R) Server Platform Services HECI subsystem before version SPS_E5_04.00.04.393.0 may allow privileged user to potentially cause a denial of service via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2018-12198 CONFIRM</a>
intel -- sgx_sdk_for_linux_and_sgx_sdk_for_windows	Double free in Intel(R) SGX SDK for Linux before version 2.2 and Intel(R) SGX SDK for Windows before version 2.1 may allow an authenticated user to potentially enable information disclosure or denial of service via local access.	2019-03-14	not yet calculated	<a href="#">CVE-2019-0122 CONFIRM</a>
jupyter -- notebook	An XSSI (cross-site inclusion) vulnerability in Jupyter Notebook before 5.7.6 allows inclusion of resources on malicious pages when visited by users who are authenticated with a Jupyter server. Access to the content of resources has been demonstrated with Internet Explorer through capturing of error messages, though not reproduced with other browsers. This occurs because Internet Explorer's error messages can include the content of any invalid JavaScript that was encountered.	2019-03-12	not yet calculated	<a href="#">CVE-2019-9644 MISC</a>
mybb -- mybb	An XSS issue was discovered in upcoming_events.php in the Upcoming Events plugin before 1.33 for MyBB via a crafted name for an event.	2019-03-10	not yet calculated	<a href="#">CVE-2019-9650 MISC MISC</a>
netdata -- netdata	The Netdata web application through 1.13.0 allows remote attackers to inject their own malicious HTML code into an imported snapshot, aka HTML Injection. Successful exploitation will allow attacker-supplied HTML to run in the context of the affected browser, potentially allowing the attacker to steal authentication credentials or to control how the site is rendered to the user.	2019-03-15	not yet calculated	<a href="#">CVE-2019-9834 EXPLOIT-DB MISC</a>
nexus -- 9000_series_switches_in_standalone_nx-os_mode	A vulnerability in the Tetration Analytics agent for Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an authenticated, local attacker to execute arbitrary code as root. The vulnerability is due to an incorrect permissions setting. An attacker could exploit this vulnerability by replacing valid agent files with malicious code. A successful exploit could result in the execution of code supplied by the attacker. Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running versions prior to 7.0(3)I7(5).	2019-03-11	not yet calculated	<a href="#">CVE-2019-1618 B D CISCO</a>
open_ticket_request_system -- open_ticket_request_system	An issue was discovered in Open Ticket Request System (OTRS) 6.x before 6.0.17 and 7.x before 7.0.5. An attacker who is logged into OTRS as an admin user may manipulate the URL to cause execution of JavaScript in the context of OTRS. This is related to Kernel/Output/Template/Document.pm.	2019-03-13	not yet calculated	<a href="#">CVE-2019-9751 MISC</a>
open_ticket_request_system -- open_ticket_request_system	An issue was discovered in Open Ticket Request System (OTRS) 5.x before 5.0.34, 6.x before 6.0.16, and 7.x before 7.0.4. An attacker who is logged into OTRS as an agent or a customer user may upload a carefully crafted resource in order to cause execution of JavaScript in the context of OTRS. This is related to Content-type mishandling in Kernel/Modules/PictureUpload.pm.	2019-03-13	not yet calculated	<a href="#">CVE-2019-9752 MISC</a>
open_ticket_request_system -- open_ticket_request_system	An issue was discovered in Open Ticket Request System (OTRS) 5.0.31 and 6.0.13. Users updating to 6.0.13 (also patchlevel updates) or 5.0.31 (only major updates) will experience data loss in their agent preferences table.	2019-03-13	not yet calculated	<a href="#">CVE-2018-20800 MISC</a>
opensuse -- yast2-multipath	In yast2-multipath before version 4.1.1 a static temporary filename allows local attackers to overwrite files on systems without symlink protection	2019-03-15	not yet calculated	<a href="#">CVE-2018-17955 CONFIRM</a>
opensuse -- yast2-printer	In yast2-printer up to and including version 4.0.2 the SMB printer settings don't escape characters in passwords properly. If a password with backticks or similar characters is supplied this allows for executing code as root. This requires ricking root to enter such a password in yast.	2019-03-15	not yet calculated	<a href="#">CVE-2018-20106 CONFIRM</a>
opensuse -- yast2-samba-provision	In yast2-samba-provision up to and including version 1.0.1 the password for samba shares was provided on the command line to tools used by yast2-samba-provision, allowing local attackers to read them in the process list	2019-03-15	not yet calculated	<a href="#">CVE-2018-17956 CONFIRM</a>
pacman -- pacman	pacman before 5.1.3 allows directory traversal when installing a remote package via a specified URL "pacman -U <url>" due to an unsanitized file name received from a Content-Disposition header. pacman renames the downloaded package file to match the name given in this header. However, pacman did not sanitize his name, which may contain slashes, before calling rename(). A malicious server (or a network MitM if downloading over HTTP) can send a Content-Disposition header to make pacman place the file anywhere in the filesystem, potentially leading to arbitrary root code execution. Notably, this bypasses pacman's package signature checking. This occurs in curl_download_internal in lib/libalpm/dload.c.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9686 MISC MISC MISC</a>
paul_vixie -- vixie_cron	Vixie Cron before the 3.0p11-133 Debian package allows local users to cause a denial of service (use-after-free and daemon crash) because of a orce_rescan_user error.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9706 MISC MISC MISC</a>
paul_vixie -- vixie_cron	Vixie Cron before the 3.0p11-133 Debian package allows local users to cause a denial of service (memory consumption) via a large crontab file because an unlimited number of lines is accepted.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9705 B D MISC</a>
paul_vixie -- vixie_cron	Vixie Cron before the 3.0p11-133 Debian package allows local users to cause a denial of service (daemon crash) via a large crontab file because the calloc return value is not checked.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9704 B D MISC</a>
rsa -- authentication_manager	RSA Authentication Manager versions prior to 8.4 P1 contain an Insecure Credential Management Vulnerability. A malicious Operations Console administrator may be able to obtain the value of a domain password that another Operations Console administrator had set previously and use it for attacks.	2019-03-13	not yet calculated	<a href="#">CVE-2019-3711 FULLDISC</a>
topvision -- cc8800_cmts_c-e_devices	Topvision CC8800 CMTS C-E devices allow remote attackers to obtain sensitive information via a direct request for /WebContent/startup tar.gz with userName=admin in a cookie.	2019-03-15	not yet calculated	<a href="#">CVE-2018-18205 MISC MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has out-of-bounds read vulnerability in VNC client code inside TextChat module, which results in a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8267 MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple off-by-one vulnerabilities in VNC server code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8272 MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1206 has multiple off-by-one vulnerabilities in VNC client code connected with improper usage of ClientConnection::ReadString function, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8268 MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of SETPIXELS macro in VNC client code, which	2019-03-08	not yet	<a href="#">CVE-2019-8265</a>

	can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1208.		calculated	<a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside RAW decoder, which can potentially result code execution. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8280</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 contains multiple memory leaks (CWE-655) in VNC server code, which allows an attacker to read stack memory and can be abused or information disclosure. Combined with another vulnerability, it can be used to eak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8277</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a stack buffer overflow vulnerability in VNC server code inside file transfer request handler, which can result in Denial of Service (DoS). This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8276</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple improper null termination vulnerabilities in VNC server code, which result in out-of-bound data being accessed by remote users. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8275</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer offer handler, which can potentially in result code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8274</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer request handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8273</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of ClientConnection::Copybuffer function in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. User interaction is required to trigger these vulnerabilities. These vulnerabilities have been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8266</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer handler, which can potentially result code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8271</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1210 has out-of-bounds read vulnerability in VNC client code inside Ultra decoder, which results in a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1211.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8270</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1206 has stack-based Buffer overflow vulnerability in VNC client code inside FileTransfer module, which leads to a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8269</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside Ultra2 decoder, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8264</a> <a href="#">MISC</a>
webargs -- webargs	An issue was discovered in webargs before 5.1.3, as used with marshmallow and other products. JSON parsing uses a short-lived cache to store the parsed JSON body. This cache is not thread-safe, meaning that incorrect JSON payloads could have been parsed for concurrent requests.	2019-03-11	not yet calculated	<a href="#">CVE-2019-9710</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The Contact Form Email plugin before 1.2.66 for WordPress allows wp-admin/admin.php item XSS, related to cp_admin_int_edition.inc.php in the "custom edition area."	2019-03-10	not yet calculated	<a href="#">CVE-2019-9646</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nrcas.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



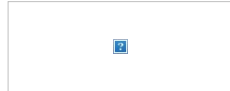
#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to wguilarte@ci.sunnyvale.ca.us using GovDelivery Communications Cloud on behalf of United States Computer Emergency Readiness Team (US-CERT) - 245 Murray Lane SW Bldg 410 - Washington, DC 20598 - (888) 282-0870



From: [US-CERT](#)  
To: [Tanner McGinnis](#)  
Subject: SB19-070: Vulnerability Summary for the Week of March 4 2019  
Date: Monday, March 11, 2019 1:14:14 PM



National Cyber Awareness System:

## SB19-070 Vulnerability Summary for the Week of March 4 2019

03/11/2019 04:14 AM EDT

Original release date: March 11, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology \(NIST\) National Vulnerability Database \(NVD\)](#) in the past week. The NVD is sponsored by the [Department of Homeland Security \(DHS\) National Cybersecurity and Communications Integration Center \(NCCIC\)](#) / [United States Computer Emergency Readiness Team \(US-CERT\)](#). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System \(CVSS\)](#) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database \(NVD\)](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
airdroid -- airdroid	The Airdroid application through 4.2.1.6 for Android allows remote attackers to cause a denial of service (service crash) via many simultaneous sdctl/comm/lite_auth/ requests.	2019-03-06	7.8	<a href="#">CVE-2019-9599</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a>
apache -- jmeter	Unauthenticated RCE is possible when JMeter is used in distributed mode (-r or -R command line options). Attacker can establish a RMI connection to a jmeter-server using RemoteJMeterEngine and proceed with an attack using untrusted data deserialization. This only affects tests running in Distributed mode. Note that versions before 4.0 are not able to encrypt traffic between the nodes, nor authenticate the participating nodes so upgrade to JMeter 5.1 is also advised.	2019-03-06	7.5	<a href="#">CVE-2019-0187</a> <a href="#">MLIST</a> <a href="#">BID</a>
apache -- solr	In Apache Solr versions 5.0.0 to 5.5.5 and 6.0.0 to 6.6.5, the Config API allows to configure the JMX server via an HTTP POST request. By pointing it to a malicious RMI server, an attacker could take advantage of Solr's unsafe deserialization to trigger remote code execution on the Solr side.	2019-03-07	7.5	<a href="#">CVE-2019-0192</a> <a href="#">MLIST</a> <a href="#">BID</a>
apple -- iphone_os	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. An application may be able to execute arbitrary code with kernel privileges.	2019-03-05	9.3	<a href="#">CVE-2019-6213</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">EXPLOIT-DB</a>
apple -- iphone_os	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may be able to execute arbitrary code with kernel privileges.	2019-03-05	9.3	<a href="#">CVE-2019-6218</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">EXPLOIT-DB</a>
apple -- iphone_os	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3, iTunes 12.9.3 for Windows. A sandboxed process may be able to circumvent sandbox restrictions.	2019-03-04	7.5	<a href="#">CVE-2019-6235</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
bluecms_project -- bluecms	BlueCMS 1.6 allows SQL Injection via the user_id parameter in an uploads/admin/user.php? act=edit request.	2019-03-06	7.5	<a href="#">CVE-2019-9594</a> <a href="#">MISC</a>
checkpoint -- zonealarm	Check Point ZoneAlarm version 15.3.064.17729 and below expose a WCF service that can allow a local low privileged user to execute arbitrary code as SYSTEM.	2019-03-01	7.2	<a href="#">CVE-2018-8790</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- nx-os	A vulnerability in a specific CLI command implementation of Cisco Nexus 9000 Series ACI Mode Switch Software could allow an authenticated, local attacker to escape a restricted shell on an affected device. The vulnerability is due to insufficient sanitization of user-supplied input when issuing a specific CLI command with parameters on an affected device. An attacker could exploit this vulnerability by authenticating to the device CLI and issuing certain commands. A successful exploit could allow the attacker to escape the restricted shell and execute arbitrary commands with root-level privileges on the affected device. This vulnerability only affects Cisco Nexus 9000 Series ACI Mode Switches that are running a release prior to 14.0(3d).	2019-03-06	7.2	<a href="#">CVE-2019-1591</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the Bash shell implementation for Cisco NX-OS Software could allow an authenticated, local attacker to escalate their privilege level by executing commands authorized to other user roles. The attacker must authenticate with valid user credentials. The vulnerability is due to the incorrect implementation of a Bash shell command that allows role-based access control (RBAC) to be bypassed. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the Bash prompt. A successful exploit could allow the attacker to escalate their privilege level by executing commands that should be restricted to other roles. For example, a dev-ops user could escalate their privilege level to admin with a successful exploit of this vulnerability.	2019-03-06	7.2	<a href="#">CVE-2019-1593</a> <a href="#">BID</a> <a href="#">CISCO</a>
	A vulnerability in the Bash shell implementation for Cisco NX-OS Software could allow an authenticated, local attacker to escalate their privilege level to root. The attacker must			



cisco -- nx-os	authenticate with valid user credentials. The vulnerability is due to incorrect permissions of a system executable. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the Bash prompt. A successful exploit could allow the attacker to escalate their privilege level to root. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-07	7.2	<a href="#">CVE-2019-1596</a> <a href="#">CISCO</a>
dolbarr -- dolbarr	An issue was discovered in Dolbarr through 7.0.0. expensereport/card.php in the expense reports module allows SQL injection via the integer parameters qty and value_unit.	2019-03-07	7.5	<a href="#">CVE-2018-16809</a> <a href="#">MISC</a>
fengoffice -- feng_office	Feng Office 3.7.0.5 allows remote attackers to execute arbitrary code via "<!--#exec cmd=" in a .shtml file to ck_upload_handler.php.	2019-03-07	7.5	<a href="#">CVE-2019-9623</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
flarumchina -- flarumchina	FlarumChina v0.1.0-beta.7C has SQL injection via a /?q= request.	2019-03-04	7.5	<a href="#">CVE-2019-9566</a> <a href="#">MISC</a>
freedesktop -- poppler	Poppler 0.74.0 has a heap-based buffer over-read in the CairoRescaleBox.cc downsample_row_box_filter function.	2019-03-08	7.5	<a href="#">CVE-2019-9631</a> <a href="#">MISC</a>
ibm -- financial_transaction_manager	BM Financial Transaction Manager for Digital Payments for Multi-Platform 3.1.0 is vulnerable o SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-ForceID: 155998.	2019-03-05	7.5	<a href="#">CVE-2019-4032</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
layerbb -- layerbb	LayerBB 1.1.1 has SQL Injection via the search.php search_query parameter.	2019-03-07	7.5	<a href="#">CVE-2018-17988</a> <a href="#">EXPLOIT-DB</a>
microsoft -- .net_framework	A remote code execution vulnerability exists in .NET Framework and Visual Studio software when the software fails to check the source markup of a file.An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka '.NET Framework and Visual Studio Remote Code Execution Vulnerability'.	2019-03-05	9.3	<a href="#">CVE-2019-0613</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0590</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0591</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0593</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0605</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0607</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0610</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0640</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0642</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0644</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0651</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0652</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0655</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0645, CVE-2019-0650.	2019-03-05	7.6	<a href="#">CVE-2019-0634</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0650.	2019-03-05	7.6	<a href="#">CVE-2019-0645</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0645.	2019-03-05	7.6	<a href="#">CVE-2019-0650</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- exchange_server	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0686.	2019-03-05	9.3	<a href="#">CVE-2019-0724</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	2019-03-05	7.6	<a href="#">CVE-2019-0806</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0672, CVE-2019-0673, CVE-2019-0674, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0671</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0673, CVE-2019-0674, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0672</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0674, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0673</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0673, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0674</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0673, CVE-2019-0674.	2019-03-05	9.3	<a href="#">CVE-2019-0675</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint_enterprise_server	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails o check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0604.	2019-03-05	9.3	<a href="#">CVE-2019-0594</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint_enterprise_server	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails o check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0594.	2019-03-05	9.3	<a href="#">CVE-2019-0604</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- visual_studio_code	A remote code execution vulnerability exists in Visual Studio Code when it process environment variables after opening a project, aka 'Visual Studio Code Remote Code Execution Vulnerability'.	2019-03-05	9.3	<a href="#">CVE-2019-0728</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine mproperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0595</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine mproperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0596</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine mproperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0597</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine mproperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0598</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine mproperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0599</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Windows Graphics Device nterface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0662.	2019-03-05	9.3	<a href="#">CVE-2019-0618</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'.	2019-03-05	7.2	<a href="#">CVE-2019-0623</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine mproperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599.	2019-03-05	9.3	<a href="#">CVE-2019-0625</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'.	2019-03-05	7.5	<a href="#">CVE-2019-0626</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633.	2019-03-05	9.0	<a href="#">CVE-2019-0630</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630.	2019-03-05	9.0	<a href="#">CVE-2019-0633</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Windows Graphics Device nterface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618.	2019-03-05	9.3	<a href="#">CVE-2019-0662</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetNetworkTomographySettings API function, as demonstrated by shell metacharacters in the tomography_ping_number field.	2019-03-07	10.0	<a href="#">CVE-2019-9117</a> <a href="#">MISC</a>
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetNTPServerSettings API function, as demonstrated by shell metacharacters in he system_time_timezone field.	2019-03-07	10.0	<a href="#">CVE-2019-9118</a> <a href="#">MISC</a>
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetStaticRouteSettings API function, as demonstrated by shell metacharacters in he staticroute_list field.	2019-03-07	10.0	<a href="#">CVE-2019-9119</a> <a href="#">MISC</a>
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request	2019-03-07	10.0	<a href="#">CVE-2019-9120</a> <a href="#">MISC</a>

	body for the SetWLANACLSettings API function, as demonstrated by shell metacharacters in he wi(0),(0)_maclist field.			
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetSmartQoSSettings API function, as demonstrated by shell metacharacters in he smartqos_priority_devices field.	2019-03-07	10.0	<a href="#">CVE-2019-9121</a> MISC
moxa -- eds-405a_firmware	Moxa IKS and EDS fails to properly check array bounds which may allow an attacker to read device memory on arbitrary addresses, and may allow an attacker to retrieve sensitive data or cause device reboot.	2019-03-05	8.5	<a href="#">CVE-2019-6522</a> BID MISC
moxa -- eds-405a_firmware	Several buffer overflow vulnerabilities have been identified in Moxa IKS and EDS, which may allow remote code execution.	2019-03-05	7.5	<a href="#">CVE-2019-6557</a> BID MISC
moxa -- eds-405a_firmware	Moxa IKS and EDS generate a predictable cookie calculated with an MD5 hash, allowing an attacker to capture the administrator's password, which could lead to a full compromise of the device.	2019-03-05	10.0	<a href="#">CVE-2019-6563</a> BID MISC
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 contains multiple hard coded credentials for the Telnet and SSH interfaces.	2019-03-05	10.0	<a href="#">CVE-2019-3918</a> MISC
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to a stack buffer overflow via crafted HTTP POST request sent by a remote, unauthenticated attacker to /GponForm/fsetup_Form. An attacker can leverage this vulnerability to potentially execute arbitrary code.	2019-03-05	7.5	<a href="#">CVE-2019-3922</a> MISC
phpshe -- phpshe	PHPSHE 1.7 allows module/index/cart.php pintuan_id SQL Injection to index.php.	2019-03-07	7.5	<a href="#">CVE-2019-9626</a> MISC
solarwinds -- orion_platform	SolarWinds Orion Platform before 2018.4 Hotfix 2 allows privilege escalation through the RabbitMQ service.	2019-03-01	7.5	<a href="#">CVE-2019-9546</a> CONFIRM
twinkletoesoftware -- booked	phpscheduleit Booked Scheduler 2.7.5 allows arbitrary file upload via the Favicon field, eading to execution of arbitrary Web/custom-favicon.php PHP code, because Presenters/Admin/ManageThemePresenter.php does not ensure an image file extension.	2019-03-05	7.5	<a href="#">CVE-2019-9581</a> MISC MISC EXPLOIT-DB
zzcms -- zzcms	zzcms v8.3 contains a SQL Injection vulnerability in /user/logincheck.php via an X-Forwarded-For HTTP header.	2019-03-07	7.5	<a href="#">CVE-2018-17412</a> MISC

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	MiniCMS 1.10 allows mc-admin/post.php?state=publish&delete= CSRF to delete articles, a different vulnerability than CVE-2018-18891.	2019-03-06	5.8	<a href="#">CVE-2019-9603</a> MISC
apache -- mesos	When parsing a JSON payload with deeply nested JSON structures, the parser in Apache Mesos versions pre-1.4.x, 1.4.0 to 1.4.2, 1.5.0 to 1.5.1, 1.6.0 to 1.6.1, and 1.7.0 might overflow the stack due to unbounded recursion. A malicious actor can therefore cause a denial of service of Mesos masters rendering the Mesos-controlled cluster inoperable.	2019-03-05	5.0	<a href="#">CVE-2018-11793</a> BID MISC
apache -- qpid_broker-j	A Denial of Service vulnerability was found in Apache Qpid Broker-J versions 6.0.0-7.0.6 (inclusive) and 7.1.0 which allows an unauthenticated attacker to crash the broker instance by sending specially crafted commands using AMQP protocol versions below 1.0 (AMQP 0-8, 0-9, 0-91 and 0-10). Users of Apache Qpid Broker-J versions 6.0.0-7.0.6 (inclusive) and 7.1.0 utilizing AMQP protocols 0-8, 0-9, 0-91, 0-10 must upgrade to Qpid Broker-J versions 7.0.7 or 7.1.1 or later.	2019-03-06	5.0	<a href="#">CVE-2019-0200</a> BID MLIST
apowersoft -- apowermanager	The ApowerManager application through 3.1.7 for Android allows remote attackers to cause a denial of service via many simultaneous /?Key=PhoneRequestAuthorization requests.	2019-03-06	5.0	<a href="#">CVE-2019-9601</a> EXPLOIT-DB MISC
appcms -- appcms	AppCMS 2.0.101 allows XSS via the upload/callback.php params parameter.	2019-03-06	4.3	<a href="#">CVE-2019-9595</a> MISC
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6212</a> BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM UBUNTU
apple -- icloud	A type confusion issue was addressed with improved memory handling. This issue is fixed in OS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6215</a> BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM UBUNTU EXPLOIT-DB
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6216</a> BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6217</a> BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6226</a> BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM

apple -- icloud	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, Cloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6227</a> BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-03-05	4.3	<a href="#">CVE-2019-6229</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6233</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6234</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An out-of-bounds read was addressed with improved input validation. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3. An attacker in a privileged network position may be able to execute arbitrary code.	2019-03-05	5.8	<a href="#">CVE-2019-6200</a> BID CONFIRM CONFIRM
apple -- iphone_os	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, watchOS 5.1.3. A malicious application may be able to elevate privileges.	2019-03-05	6.8	<a href="#">CVE-2019-6202</a> BID CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An issue existed with autofill resuming after it was canceled. The issue was addressed with improved state management. This issue is fixed in iOS 12.1.3. Password autofill may fill in passwords after they were manually cleared.	2019-03-04	5.0	<a href="#">CVE-2019-6206</a> BID CONFIRM
apple -- iphone_os	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in memory shared between processes.	2019-03-05	4.3	<a href="#">CVE-2019-6208</a> BID CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to determine kernel memory layout.	2019-03-05	4.3	<a href="#">CVE-2019-6209</a> BID CONFIRM CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6211</a> CONFIRM CONFIRM
apple -- iphone_os	A type confusion issue was addressed with improved memory handling. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to break out of its sandbox.	2019-03-05	6.8	<a href="#">CVE-2019-6214</a> BID CONFIRM CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, watchOS 5.1.3. Processing a maliciously crafted message may lead to a denial of service.	2019-03-05	5.0	<a href="#">CVE-2019-6219</a> BID CONFIRM CONFIRM CONFIRM
apple -- iphone_os	A logic issue existed in the handling of Group FaceTime calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.1.4, macOS Mojave 10.14.3 Supplemental Update. The initiator of a Group FaceTime call may be able to cause the recipient to answer.	2019-03-05	5.0	<a href="#">CVE-2019-6223</a> CONFIRM CONFIRM
apple -- iphone_os	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A remote attacker may be able to initiate a FaceTime call causing arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6224</a> BID CONFIRM CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to break out of its sandbox.	2019-03-05	6.8	<a href="#">CVE-2019-6230</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to read restricted memory.	2019-03-05	4.3	<a href="#">CVE-2019-6231</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- itunes	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, iTunes 12.9.3 for Windows. A malicious application may be able to elevate privileges.	2019-03-05	6.8	<a href="#">CVE-2019-6221</a> BID CONFIRM CONFIRM CONFIRM
apple -- mac_os_x	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.3. An application may be able to read restricted memory.	2019-03-05	4.3	<a href="#">CVE-2019-6220</a> BID CONFIRM
apple -- safari	A cross-site scripting issue existed in Safari. This issue was addressed with improved URL validation. This issue is fixed in iOS 12.1.3, Safari 12.0.3. Processing maliciously crafted web	2019-03-05	4.3	<a href="#">CVE-2019-6228</a> BID

	content may lead to a cross site scripting attack.			<a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
axiosys -- bento4	An issue was discovered in Bento4 1.5.1-628. An out of bounds write occurs in AP4_CttsTableEntry::AP4_CttsTableEntry() located in Core/AP4Array.h. It can be triggered by sending a crafted file to (for example) the mp42hls binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.	2019-03-01	<a href="#">6.8</a>	<a href="#">CVE-2019-9544</a> <a href="#">MISC</a> <a href="#">MISC</a>
bluemind -- bluemind	n BlueMind 3.5.x before 3.5.11 Hotfix 7 and 4.x before 4.0-beta3, the contact application mishandles temporary uploads.	2019-03-04	<a href="#">5.0</a>	<a href="#">CVE-2019-9563</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bolt -- bolt	Controller/Async/FileManager.php in the filemanager in Bolt before 3.6.5 allows remote attackers to execute arbitrary PHP code by renaming a previously uploaded file to have a .php extension.	2019-03-07	<a href="#">6.5</a>	<a href="#">CVE-2019-9185</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chshcms -- cscms	An issue was discovered in Cscms 4.1.0. There is an admin.php/pay CSRF vulnerability that can change the payment account to redirect funds.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2019-9598</a> <a href="#">MISC</a>
cisco -- nx-os	A vulnerability in the 802.1X implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation of Extensible Authentication Protocol over LAN (EAPOL) frames. An attacker could exploit this vulnerability by sending a crafted EAPOL frame to an interface on the targeted device. A successful exploit could allow the attacker to cause the Layer 2 (L2) forwarding process to restart multiple times, leading to a system-level restart of the device and a DoS condition. Note: This vulnerability affects only NX-OS devices configured with 802.1X functionality. Cisco Nexus 1000V Switch for VMware vSphere devices are affected in versions prior to 5.2(1)SV3(1.4b). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.3(5)N1(1) and 7.1(5)N1(1b). Nexus 7000 and 7700 Series Switches are affected in versions prior to 8.2(3). Nexus 9000 Series Fabric Switches in ACI Mode are affected in versions prior to 13.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4).	2019-03-06	<a href="#">6.1</a>	<a href="#">CVE-2019-1594</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the Fibre Channel over Ethernet (FCoE) protocol implementation in Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an incorrect allocation of an internal interface index. An adjacent attacker with the ability to submit a crafted FCoE packet that crosses affected interfaces could trigger this vulnerability. A successful exploit could allow the attacker to cause a packet loop and high throughput on the affected interfaces, resulting in a DoS condition. This vulnerability has been fixed in version 7.3(5)N1(1).	2019-03-06	<a href="#">6.1</a>	<a href="#">CVE-2019-1595</a> <a href="#">BID</a> <a href="#">CISCO</a>
directadmin -- directadmin	JBMC DirectAdmin 1.55 allows CSRF via the /CMD_ACCOUNT_ADMIN URI to create a new admin account.	2019-03-07	<a href="#">6.8</a>	<a href="#">CVE-2019-9625</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
dolbarr -- dolbarr	An issue was discovered in Dolbarr through 7.0.0. There is Stored XSS in expensereport/card.php in the expense reports plugin via the comments parameter, or a public or private note.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2018-16808</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.0.2 has open redirects via the html/common/forward_js.jsp FORWARD_URL parameter or the html/portlet/ext/common/page_preview_popup.jsp hostname parameter.	2019-03-07	<a href="#">5.8</a>	<a href="#">CVE-2018-17422</a> <a href="#">MISC</a>
ebrigade -- ebrigade	eBrigade through 4.5 allows Arbitrary File Download via ../ directory traversal in the showfile.php file parameter, as demonstrated by reading the user-data/save/backup.sql file.	2019-03-07	<a href="#">4.0</a>	<a href="#">CVE-2019-9622</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
freedesktop -- poppler	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readGenericBitmap() located in JBIG2Stream.cc, can be triggered by sending a crafted pdf file to (for example) the pdfseparate binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to JArithmeticDecoder::decodeBit.	2019-03-01	<a href="#">6.8</a>	<a href="#">CVE-2019-9543</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
freedesktop -- poppler	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readTextRegion() located in JBIG2Stream.cc, can be triggered by sending a crafted pdf file to (for example) the pdftimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to JBIG2Bitmap::clearToZero.	2019-03-01	<a href="#">6.8</a>	<a href="#">CVE-2019-9545</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	There is a stack consumption issue in md5Round1() located in Decrypt.cc in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to Catalog::countPageTree.	2019-03-06	<a href="#">6.8</a>	<a href="#">CVE-2019-9587</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	There is an invalid memory access in gAtomicIncrement() located at GMutex.h in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.	2019-03-06	<a href="#">6.8</a>	<a href="#">CVE-2019-9588</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	There is a NULL pointer dereference vulnerability in PSOutputDev::setupResources() located in PSOutputDev.cc in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.	2019-03-06	<a href="#">6.8</a>	<a href="#">CVE-2019-9589</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- gdk-pixbuf	GdkPixBuf (aka gdk-pixbuf), possibly 2.32.2, as used by GNOME Nautilus 3.14.3 on Ubuntu 16.04, allows attackers to cause a denial of service (stack corruption) or possibly have unspecified other impact via a crafted file folder.	2019-03-07	<a href="#">6.8</a>	<a href="#">CVE-2017-12447</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- binutils	The aout_32_swap_std_reloc_out function in aout.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils before 2.31, allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted file, as demonstrated by objcopy.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2018-14038</a> <a href="#">MISC</a> <a href="#">MISC</a>
golang -- go	Go through 1.12 on Windows misuses certain LoadLibrary functionality, leading to DLL njection.	2019-03-08	<a href="#">6.8</a>	<a href="#">CVE-2019-9634</a> <a href="#">MISC</a>
hyphp -- hybbs	An issue was found in HYBBS through 2016-03-08. There is an XSS vulnerability via an article title to post.html.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2018-14499</a> <a href="#">MISC</a>
ibm -- cloud_private	BM Cloud Private 3.1.1 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 153319.	2019-03-05	<a href="#">5.8</a>	<a href="#">CVE-2018-1939</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- infosphere_information_governance_catalog	BM InfoSphere Information Governance Catalog 11.3, 11.5, and 11.7 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 151639.	2019-03-05	<a href="#">5.8</a>	<a href="#">CVE-2018-1875</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 Standard Edition could allow highly sensitive information to be transmitted in plain text. An attacker could obtain this information using man in the middle techniques. IBM X-ForceID: 157008.	2019-03-05	<a href="#">4.3</a>	<a href="#">CVE-2019-4063</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>



imagemagick -- imagemagick	n ImageMagick before 7.0.8-25, some memory leaks exist in DecodeImage in coders/pcd.c.	2019-03-07	5.0	<a href="#">CVE-2019-7175</a> MISC
jtbc -- jtbc	console/account/manage.php?type=action&action=add in JTBC v3.0(C) has CSRF for adding an administrator account.	2019-03-07	6.8	<a href="#">CVE-2018-17429</a> MISC
libjpeg-turbo -- libjpeg-turbo	get_8bit_row in rdbmp.c in libjpeg-turbo through 1.5.90 and MozJPEG through 3.3.1 allows attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the color indices is out of range for the number of palette entries.	2019-03-07	4.3	<a href="#">CVE-2018-14498</a> MISC MISC MISC
linux -- linux_kernel	n the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, which makes it easier for attackers to exploit kernel NULL pointer dereferences on non-SMAP platforms. This is related to a capability check for the wrong task.	2019-03-05	4.9	<a href="#">CVE-2019-9213</a> MISC MISC MISC MISC MISC MISC EXPLOIT-DB
medical_store_script_project -- medical_store_script	PHP Scripts Mall Medical Store Script 3.0.3 allows Path Traversal by navigating to the parent directory of a jpg or png file.	2019-03-06	5.0	<a href="#">CVE-2019-9607</a> MISC
microsoft -- .net_core	A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's, aka '.NET Framework and Visual Studio Spoofing Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0657</a> MISC REDHAT CONFIRM
microsoft -- chakracore	A vulnerability exists in Microsoft Chakra JIT server, aka 'Scripting Engine Elevation of Privileged Vulnerability'.	2019-03-05	6.8	<a href="#">CVE-2019-0649</a> MISC CONFIRM
microsoft -- chakracore	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0648.	2019-03-05	4.3	<a href="#">CVE-2019-0658</a> MISC CONFIRM
microsoft -- edge	A security feature bypass vulnerability exists in Microsoft Edge handles whitelisting, aka 'Microsoft Edge Security Feature Bypass Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0641</a> MISC CONFIRM
microsoft -- edge	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0643</a> MISC CONFIRM
microsoft -- edge	An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the user's computer or data. To exploit the vulnerability, an attacker must know the memory address of where the object was created. The update addresses the vulnerability by changing the way certain functions handle objects in memory, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0658.	2019-03-05	4.3	<a href="#">CVE-2019-0648</a> MISC CONFIRM
microsoft -- edge	A spoofing vulnerability exists when Microsoft browsers improperly handles specific redirects, aka 'Microsoft Browser Spoofing Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0654</a> MISC CONFIRM
microsoft -- excel	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0669</a> MISC CONFIRM
microsoft -- excel_viewer	A security feature bypass vulnerability exists when Microsoft Office does not validate URLs. An attacker could send a victim a specially crafted file, which could trick the victim into entering credentials, aka 'Microsoft Office Security Feature Bypass Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0540</a> MISC CONFIRM
microsoft -- exchange_server	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0724.	2019-03-05	5.8	<a href="#">CVE-2019-0686</a> MISC CONFIRM
microsoft -- internet_explorer	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory. An attacker who successfully exploited this vulnerability could test for the presence of files on disk, aka 'Internet Explorer Information Disclosure Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0676</a> MISC CONFIRM
microsoft -- java_software_development_kit	An information disclosure vulnerability exists in the way Azure IoT Java SDK logs sensitive information, aka 'Azure IoT Java SDK Information Disclosure Vulnerability'.	2019-03-05	5.0	<a href="#">CVE-2019-0741</a> MISC CONFIRM
microsoft -- powershell_core	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0631, CVE-2019-0632.	2019-03-05	4.6	<a href="#">CVE-2019-0627</a> MISC CONFIRM
microsoft -- powershell_core	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0632.	2019-03-05	4.6	<a href="#">CVE-2019-0631</a> MISC CONFIRM
microsoft -- powershell_core	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0631.	2019-03-05	4.6	<a href="#">CVE-2019-0632</a> MISC CONFIRM
microsoft -- sharepoint_enterprise_server	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'.	2019-03-05	6.5	<a href="#">CVE-2019-0668</a> MISC CONFIRM
microsoft -- sharepoint_enterprise_server	A spoofing vulnerability exists in Microsoft SharePoint when the application does not properly parse HTTP content, aka 'Microsoft SharePoint Spoofing Vulnerability'.	2019-03-05	5.8	<a href="#">CVE-2019-0670</a> MISC CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0602</a> MISC CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0615</a> MISC CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0616</a> MISC CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0660, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0619</a> MISC CONFIRM
microsoft -- windows_10	A security feature bypass vulnerability exists when Windows Defender Firewall incorrectly applies firewall profiles to cellular network connections, aka 'Windows Defender Firewall Security Feature Bypass Vulnerability'.	2019-03-05	5.0	<a href="#">CVE-2019-0637</a> MISC CONFIRM
microsoft -- windows_10	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'.	2019-03-05	6.9	<a href="#">CVE-2019-0656</a> MISC CONFIRM
				<a href="#">CVE-2019-0659</a>

microsoft -- windows_10	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka "Windows Storage Service Elevation of Privilege Vulnerability".	2019-03-05	4.4	<a href="#">BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability". This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0660 BID CONFIRM</a>
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability". This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660.	2019-03-05	4.3	<a href="#">CVE-2019-0664 BID CONFIRM</a>
mitel -- connect_onsite	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE before 19.49.1500.0 allows remote attackers to inject arbitrary web script or HTML via the brandUrl parameter.	2019-03-06	4.3	<a href="#">CVE-2019-9591 MISC</a>
mitel -- connect_onsite	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE 19.45.1602.0 allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2019-03-06	4.3	<a href="#">CVE-2019-9592 MISC</a>
mitel -- connect_onsite	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE 18.82.2000.0 allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2019-03-06	4.3	<a href="#">CVE-2019-9593 MISC</a>
monstra -- monstra	Monstra CMS 3.0.4 allows remote attackers to execute arbitrary PHP code via a mixed-case file extension, as demonstrated by the 123.Php filename, because plugins/box/filesmanager/filesmanager.admin.php mishandles the forbidden_types variable.	2019-03-07	6.5	<a href="#">CVE-2018-17418 MISC</a>
moxa -- eds-405a_firmware	Moxa IKS and EDS store plaintext passwords, which may allow sensitive information to be read by someone with access to the device.	2019-03-05	5.0	<a href="#">CVE-2019-6518 BID MISC</a>
moxa -- eds-405a_firmware	Moxa IKS and EDS does not properly check authority on server side, which results in a read-only user being able to perform arbitrary configuration changes.	2019-03-05	5.0	<a href="#">CVE-2019-6520 BID MISC</a>
moxa -- eds-405a_firmware	Moxa IKS and EDS do not implement sufficient measures to prevent multiple failed authentication attempts, which may allow an attacker to discover passwords via brute force attack.	2019-03-05	5.0	<a href="#">CVE-2019-6524 BID MISC</a>
moxa -- eds-405a_firmware	Moxa IKS and EDS allow remote authenticated users to cause a denial of service via a specially crafted packet, which may cause the switch to crash.	2019-03-05	4.0	<a href="#">CVE-2019-6559 BID MISC</a>
moxa -- eds-405a_firmware	Cross-site request forgery has been identified in Moxa IKS and EDS, which may allow for the execution of unauthorized actions on the device.	2019-03-05	6.8	<a href="#">CVE-2019-6561 BID MISC</a>
moxa -- eds-405a_firmware	Moxa IKS and EDS fails to properly validate user input, giving unauthenticated and authenticated attackers the ability to perform XSS attacks, which may be used to send a malicious script.	2019-03-05	4.3	<a href="#">CVE-2019-6565 BID MISC</a>
netgate -- pfsense	n pfSense 2.4.4_1, blocking of source IP addresses on the basis of failed HTTPS authentication is inconsistent with blocking of source IP addresses on the basis of failed SSH authentication (the behavior does not match the sshguard documentation), which might make it easier for attackers to bypass intended access restrictions.	2019-03-01	5.0	<a href="#">CVE-2018-20799 MISC</a>
njandancms -- njandancms	njandancms through 2013-05-23 has index.php/admin/user_new CSRF to add an administrator.	2019-03-07	6.8	<a href="#">CVE-2019-8437 MISC</a>
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 allows a remote, unauthenticated attacker to enable telnetd on the router via a crafted HTTP request.	2019-03-05	5.0	<a href="#">CVE-2019-3917 MISC</a>
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to command injection via crafted HTTP request sent by a remote, authenticated attacker to /GponForm/usb_restore_Form?script/.	2019-03-05	6.5	<a href="#">CVE-2019-3919 MISC</a>
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to authenticated command injection via crafted HTTP request sent by a remote, authenticated attacker to /GponForm/device_Form?script/.	2019-03-05	6.5	<a href="#">CVE-2019-3920 MISC</a>
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to a stack buffer overflow via crafted HTTP POST request sent by a remote, authenticated attacker to /GponForm/usb_Form?script/. An attacker can leverage this vulnerability to potentially execute arbitrary code.	2019-03-05	6.5	<a href="#">CVE-2019-3921 EXPLOIT-DB MISC</a>
phome -- empirecms	EmpireCMS 7.5 allows CSRF for adding a user account via an enews=AddUser action to e/admin/user/ListUser.php, a similar issue to CVE-2018-16339.	2019-03-07	6.8	<a href="#">CVE-2018-18449 MISC</a>
phpmywind -- phpmywind	An issue was discovered in PHPMyWind 5.5. The username parameter of the install/index.php page has a stored Cross-site Scripting (XSS) vulnerability, as demonstrated by admin/login.php.	2019-03-07	4.3	<a href="#">CVE-2019-7660 MISC</a>
phpmywind -- phpmywind	An issue was discovered in PHPMyWind 5.5. The method parameter of the data/api/oauth/connect.php page has a reflected Cross-site Scripting (XSS) vulnerability.	2019-03-07	4.3	<a href="#">CVE-2019-7661 MISC</a>
popojicms -- popojicms	An issue was discovered in PopojiCMS v2.0.1. It has CSRF via the po-admin/route.php?mod=user&act=adnewn URI, as demonstrated by adding a level=1 account, a similar issue to CVE-2018-18935.	2019-03-03	6.8	<a href="#">CVE-2019-9549 MISC</a>
psigriconnect -- iec104_security_proxy_firmware	PSI GridConnect GmbH Telecontrol Gateway and Smart Telecontrol Unit family, IEC104 Security Proxy versions Telecontrol Gateway 3G Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway XS-MU Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway VM Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Smart Telecontrol Unit TCG Versions 5.0.27, 5.1.19, 6.0.16 and prior, and IEC104 Security Proxy Version 2.2.10 and prior The web application browser interprets input as active HTML, JavaScript, or VBScript, which could allow an attacker to execute arbitrary code.	2019-03-05	6.5	<a href="#">CVE-2019-6528 BID MISC</a>
quizandsurveymaster -- quiz_and_survey_master	The Quiz And Survey Master plugin 6.0.4 for WordPress allows wp-admin/admin.php?page=mlw_quiz_results quiz_id XSS.	2019-03-05	4.3	<a href="#">CVE-2019-9575 MISC MISC MISC MISC</a>
sagemcom -- f@st_5260_firmware	Sagemcom F@st 5260 routers using firmware version 0.4.39, in WPA mode, default to using a PSK that is generated from a 2-part wordlist of known values and a nonce with insufficient entropy. The number of possible PSKs is about 1.78 billion, which is too small.	2019-03-05	5.0	<a href="#">CVE-2019-9555 MISC</a>
samba -- samba	A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.	2019-03-06	4.0	<a href="#">CVE-2019-3824 CONFIRM MISC MLIST CONFIRM UBUNTU DEBIAN</a>
schoolcms -- schoolcms	SchoolCMS version 2.3.1 allows file upload via the theme upload feature at admin.php?m=admin&c=theme&a=upload by using the .zip extension along with the .Static substring, changing the Content-Type to application/zip, and placing PHP code after the ZIP header. This ultimately allows execution of arbitrary PHP code in PublicHome_Static.php because of mishandling in the Application\Admin\Controller\ThemeController.class.php Upload() function.	2019-03-05	6.5	<a href="#">CVE-2019-9572 MISC</a>
simplemachines -- simple_machines_forum	Simple Machines Forum (SMF) 2.0.4 allows XSS via the index.php?action=pm;sa=settings;save sa parameter.	2019-03-07	4.3	<a href="#">CVE-2013-7467 MISC</a>
simplemachines -- simple_machines_forum	Simple Machines Forum (SMF) 2.0.4 allows PHP Code Injection via the index.php?action=admin;area=languages;sa=editlang dictionary parameter.	2019-03-07	6.8	<a href="#">CVE-2013-7468 MISC</a>
	n Storage Performance Development Kit (SPDK) before 19.01, a malicious vhost client (i.e.,			

spdk -- storage_performance_development_kit	virtual machine) could carefully construct a circular descriptor chain that would result in a partial denial of service in the SPDK vhost target, because the vhost target did not properly detect such chains.	2019-03-01	5.0	<a href="#">CVE-2019-9547</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
tengcon -- t-920_plc_firmware	An issue was discovered on TENGCONTROL T-920 PLC v5.5 devices. It allows remote attackers to cause a denial of service (persistent failure mode) by sending a series of x191xb2x00x00x00x06x43x01x00xaccx00 (aka UID 0x43) requests to TCP port 502.	2019-03-06	5.0	<a href="#">CVE-2019-9590</a> <a href="#">MISC</a>
theolivetree -- ftp_server	The Olive Tree FTP Server (aka com.theolivetree.ftpsrvr) application through 1.32 for Android allows remote attackers to cause a denial of service via a client that makes many connection attempts and drops certain packets.	2019-03-06	5.0	<a href="#">CVE-2019-9600</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a>
ucms_project -- ucms	An issue was discovered in UCMS 1.4.6. There is XSS in the title bar, as demonstrated by a do=list request.	2019-03-07	4.3	<a href="#">CVE-2018-16804</a> <a href="#">MISC</a>
webmin -- webmin	Webmin 1.900 allows remote attackers to execute arbitrary code by leveraging the "Java file manager" and "Upload and Download" privileges to upload a crafted .cgi file via the updown/upload.cgi URI.	2019-03-07	6.8	<a href="#">CVE-2019-9624</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
yaml-cpp_project -- yaml-cpp	The SingleDocParser::HandleFlowSequence function in yaml-cpp (aka LibYaml-C++) 0.6.2 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted YAML file.	2019-03-07	4.3	<a href="#">CVE-2018-20710</a> <a href="#">MISC</a>
zrlog -- zrlog	An issue was discovered in ZrLog 2.0.3. There is a SQL injection vulnerability in the article management search box via the keywords parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17420</a> <a href="#">MISC</a>
zrlog -- zrlog	An issue was discovered in ZrLog 2.0.3. There is stored XSS in the file upload area via a crafted attached/file/ pathname.	2019-03-07	4.3	<a href="#">CVE-2018-17421</a> <a href="#">MISC</a>
zyxel -- nbg-418n_firmware	Zyxel NBG-418N v2 v1.00(AAXM.4)C0 devices allow login.cgi CSRF.	2019-03-07	6.8	<a href="#">CVE-2019-6710</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
zzcms -- zzcms	XSS exists in zzcms v8.3 via the /uploadimg_form.php noshuiyin parameter.	2019-03-07	4.3	<a href="#">CVE-2018-17413</a> <a href="#">MISC</a>
zzcms -- zzcms	zzcms v8.3 has a SQL injection in /user/jobmanage.php via the bigclass parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17414</a> <a href="#">MISC</a>
zzcms -- zzcms	zzcms V8.3 has a SQL injection in /user/zs_elite.php via the id parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17415</a> <a href="#">MISC</a>
zzcms -- zzcms	A SQL injection vulnerability exists in zzcms v8.3 via the /admin/adclass.php bigclassid parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17416</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- nx-os	A vulnerability in the Cisco Nexus 9000 Series Fabric Switches running in Application-Centric Infrastructure (ACI) mode could allow an authenticated, local attacker to read arbitrary files on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms of user-supplied input sent to an affected device. A successful exploit could allow the attacker unauthorized access to read arbitrary files on an affected device. This vulnerability has been fixed in version 14.0(1h).	2019-03-06	2.1	<a href="#">CVE-2019-1588</a> <a href="#">BID</a> <a href="#">CISCO</a>
dhcms_project -- dhcms	DhCms through 2017-09-18 has admin.php?r=admin/Index/index XSS.	2019-03-03	3.5	<a href="#">CVE-2019-9550</a> <a href="#">MISC</a>
dllicms -- dllicms	An issue was discovered in DiliCMS 2.4.0. There is a Stored XSS Vulnerability in the first extbox of "System setting->site setting" of admin/index.php, aka site_name.	2019-03-07	3.5	<a href="#">CVE-2019-8438</a> <a href="#">MISC</a>
dllicms -- dllicms	An issue was discovered in DiliCMS 2.4.0. There is a Stored XSS Vulnerability in the second extbox of "System setting->site setting" of admin/index.php, aka site_domain.	2019-03-07	3.5	<a href="#">CVE-2019-8439</a> <a href="#">MISC</a>
dllicms -- dllicms	An issue was discovered in DiliCMS 2.4.0. There is a Stored XSS Vulnerability in the third extbox (aka site logo) of "System setting->site setting" of admin/index.php, aka site_logo.	2019-03-07	3.5	<a href="#">CVE-2019-8440</a> <a href="#">MISC</a>
ibm -- cloud_private	BM Cloud Private 3.1.1 could allow a local user with administrator privileges to intercept highly sensitive unencrypted data. IBM X-Force ID: 153317.	2019-03-05	2.1	<a href="#">CVE-2018-1937</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- cloud_private	BM Cloud Private 3.1.1 could allow a local user with administrator privileges to intercept highly sensitive unencrypted data. IBM X-Force ID: 153318.	2019-03-05	2.1	<a href="#">CVE-2018-1938</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- infosphere_information_governance_catalog	BM InfoSphere Information Server 11.3, 11.5, and 11.7 could allow an attacker to change one of the settings related to InfoSphere Business Glossary Anywhere due to improper access control. IBM X-Force ID: 152528.	2019-03-05	3.3	<a href="#">CVE-2018-1899</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- rational_doors_next_generation	BM DOORS Next Generation (DNG/RR) 5.0 through 5.0.2 and 6.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152735.	2019-03-06	3.5	<a href="#">CVE-2018-1911</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- rational_doors_next_generation	BM DOORS Next Generation (DNG/RR) 6.0.2 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152736.	2019-03-06	3.5	<a href="#">CVE-2018-1912</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 155905.	2019-03-05	3.5	<a href="#">CVE-2019-4027</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 155906.	2019-03-05	3.5	<a href="#">CVE-2019-4028</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-force ID: 155907.	2019-03-05	3.5	<a href="#">CVE-2019-4029</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	BM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 155946.	2019-03-06	3.5	<a href="#">CVE-2019-4030</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
microsoft -- team_foundation_server	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0743.	2019-03-05	3.5	<a href="#">CVE-2019-0742</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- team_foundation_server	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0742.	2019-03-05	3.5	<a href="#">CVE-2019-0743</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
	An information disclosure vulnerability exists when the Human Interface Devices (HID)			<a href="#">CVE-2019-0600</a>

microsoft -- windows_10	component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0601.	2019-03-05	1.9	<a href="#">BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0600.	2019-03-05	1.9	<a href="#">CVE-2019-0601</a> <a href="#">BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661, CVE-2019-0663.	2019-03-05	2.1	<a href="#">CVE-2019-0621</a> <a href="#">BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	2019-03-05	2.1	<a href="#">CVE-2019-0628</a> <a href="#">BID CONFIRM</a>
microsoft -- windows_10	An information vulnerability exists when Windows improperly discloses file information, aka 'Windows Information Disclosure Vulnerability'.	2019-03-05	2.1	<a href="#">CVE-2019-0636</a> <a href="#">BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0661.	2019-03-05	2.1	<a href="#">CVE-2019-0663</a> <a href="#">BID CONFIRM</a>
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663.	2019-03-05	2.1	<a href="#">CVE-2019-0661</a> <a href="#">BID CONFIRM</a>
personal_video_collection_script_project -- personal_video_collection_script	PHP Scripts Mail Personal Video Collection Script 4.0.4 has Stored XSS via the "Update profile" feature.	2019-03-06	3.5	<a href="#">CVE-2019-9606</a> <a href="#">MISC</a>
pivotal_software -- operations_manager	Pivotal Operations Manager, 2.1.x versions prior to 2.1.20, 2.2.x versions prior to 2.2.16, 2.3.x versions prior to 2.3.10, 2.4.x versions prior to 2.4.3, contains a reflected cross site scripting vulnerability. A remote user that is able to convince an Operations Manager user to interact with malicious content could execute arbitrary JavaScript in the user's browser.	2019-03-07	3.5	<a href="#">CVE-2019-3776</a> <a href="#">CONFIRM</a>
vanillaforums -- vanilla_forums	Multiple stored XSS in Vanilla Forums before 2.5 allow remote attackers to inject arbitrary JavaScript code into any message on forum.	2019-03-01	3.5	<a href="#">CVE-2019-8279</a> <a href="#">MISC</a>
wdoyo -- doyocms	An issue was discovered in DOYO (aka doyocms) 2.3 through 2015-05-06. It has admin.php XSS.	2019-03-03	3.5	<a href="#">CVE-2019-9551</a> <a href="#">MISC</a>
wuzhicms -- wuzhi_cms	WUZHI CMS 4.1.0 has stored XSS via the "Membership Center" "I want to ask" "detailed description" field under the index.php?m=member URI.	2019-03-07	3.5	<a href="#">CVE-2018-17425</a> <a href="#">MISC</a>
wuzhicms -- wuzhi_cms	WUZHI CMS 4.1.0 has stored XSS via the "Extension module" "SMS in station" field under the index.php?m=core URI.	2019-03-07	3.5	<a href="#">CVE-2018-17426</a> <a href="#">MISC</a>
yzmcms -- yzmcms	An issue was discovered in YzmCMS 5.2.0. It has XSS via the bottom text field to the admin/system_manage/save.html URI, related to the site_code parameter.	2019-03-05	3.5	<a href="#">CVE-2019-9570</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- solr	Server Side Request Forgery in Apache Solr, versions 1.3 until 7.6 (inclusive). Since the "shards" parameter does not have a corresponding whitelist mechanism, a remote attacker with access to the server could make Solr perform an HTTP GET request to any reachable URL.	2019-03-08	not yet calculated	<a href="#">CVE-2017-3164</a> <a href="#">MLIST BID</a>
apple -- multiple_products	A memory corruption issue was addressed with improved lock state checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in memory shared between processes.	2019-03-05	not yet calculated	<a href="#">CVE-2019-6205</a> <a href="#">BID CONFIRM CONFIRM CONFIRM EXPLOIT-DB</a>
apple -- multiple_products	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may be able to elevate privileges.	2019-03-05	not yet calculated	<a href="#">CVE-2019-6225</a> <a href="#">BID CONFIRM CONFIRM CONFIRM EXPLOIT-DB</a>
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to execute arbitrary code with kernel privileges.	2019-03-05	not yet calculated	<a href="#">CVE-2019-6210</a> <a href="#">BID CONFIRM CONFIRM CONFIRM CONFIRM</a>
atlassian -- sourcetree_for_macos	There was an argument injection vulnerability in Atlassian Sourcetree for macOS from version 1.2 before version 3.1.1 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for macOS is able to exploit this issue to gain code execution on the system.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20234</a> <a href="#">CONFIRM</a>
atlassian -- sourcetree_for_windows	There was an argument injection vulnerability in Atlassian Sourcetree for Windows from version 0.5a before version 3.0.15 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for Windows is able to exploit this issue to gain code execution on the system.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20235</a> <a href="#">CONFIRM</a>
atlassian -- sourcetree_for_windows	There was a command injection vulnerability in Sourcetree for Windows from version 0.5a before version 3.0.10 via URI handling. A remote attacker could send a malicious URI to a victim using Sourcetree for Windows to exploit this issue to gain code execution on the system.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20236</a> <a href="#">CONFIRM</a>
botan -- botan	A side-channel issue was discovered in Botan before 2.9.0. An attacker capable of precisely measuring the time taken for ECC key generation may be able to derive information about the high bits of the secret key, as the function to derive the public point from the secret scalar uses an unblinded Montgomery ladder whose loop iteration count depends on the bitlength of the secret. This issue affects only key generation, not ECDSA signatures or ECDH key agreement.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20187</a> <a href="#">MISC MISC MISC</a>
	Multiple vulnerabilities in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets by an affected device. An attacker could exploit these vulnerabilities by			

cisco -- fxos_and_cisco_nx_os_software	<p>sending an LDAP packet crafted using Basic Encoding Rules (BER) to an affected device. The LDAP packet must have a source IP address of an LDAP server configured on the targeted device. A successful exploit could cause the affected device to reload, resulting in a DoS condition. Firepower 4100 Series Next-Generation Firewalls are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. Firepower 9300 Security Appliances are affected in versions prior to 2.0.1.201, 2.2.2.54 and 2.3.1.75. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.2(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(2). Nexus 7000 and 7700 Series Switches are affected in versions prior to 8.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(1). Cisco UCS 6200 and 6300 Fabric Interconnect devices are affected in versions prior to 3.2(2b).</p>	2019-03-07	not yet calculated	<a href="#">CVE-2019-1597</a> <a href="#">CISCO</a>
cisco -- fxos_software_and_cisco_nx_os_software	<p>Multiple vulnerabilities in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets by an affected device. An attacker could exploit these vulnerabilities by sending an LDAP packet crafted using Basic Encoding Rules (BER) to an affected device. The LDAP packet must have a source IP address of an LDAP server configured on the targeted device. A successful exploit could cause the affected device to reload, resulting in a DoS condition. Firepower 4100 Series Next-Generation Firewalls are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. Firepower 9300 Security Appliances are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.2(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(2). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(20), 7.3(2)D1(1), and 8.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(1). UCS 6200 and 6300 Fabric Interconnect are affected in versions prior to 3.2(2b).</p>	2019-03-07	not yet calculated	<a href="#">CVE-2019-1598</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_aci_mode_switch_software	<p>A vulnerability in the controller authorization functionality of Cisco Nexus 9000 Series ACI Mode Switch Software could allow an authenticated, local attacker to escalate standard users with root privilege on an affected device. The vulnerability is due to a misconfiguration of certain sudoers files for the bashroot component on an affected device. An attacker could exploit this vulnerability by authenticating to the affected device with a crafted user ID, which may allow temporary administrative access to escalate privileges. A successful exploit could allow the attacker to escalate privileges on an affected device. This Vulnerability has been fixed in version 4.0(1h)</p>	2019-03-06	not yet calculated	<a href="#">CVE-2019-1585</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	<p>A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(2). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(6). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(6). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), 8.2(3), and 8.3(2). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).</p>	2019-03-08	not yet calculated	<a href="#">CVE-2019-1609</a> <a href="#">CISCO</a>
cisco -- nx-os_software	<p>A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid user credentials to exploit this vulnerability. Nexus 3000, 3500, and Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4).</p>	2019-03-08	not yet calculated	<a href="#">CVE-2019-1606</a> <a href="#">CISCO</a>
cisco -- nx-os_software	<p>A vulnerability in the network stack of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. The vulnerability is due to an issue with allocating and freeing memory buffers in the network stack. An attacker could exploit this vulnerability by sending crafted TCP streams to an affected device in a sustained way. A successful exploit could cause the network stack of an affected device to run out of available buffers, impairing operations of control plane and management plane protocols, resulting in a DoS condition. Note: This vulnerability can be triggered only by traffic that is destined to an affected device and cannot be exploited using traffic that transits an affected device. Nexus 1000V Switch for Microsoft Hyper-V is affected in versions prior to 5.2(1)SM3(2.1). Nexus 1000V Switch for VMware vSphere is affected in versions prior to 5.2(1)SV3(4.1a). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(6) and 9.2(2). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(11), 7.0(3)I7(6), and 9.2(2). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5) and 9.2(2). Nexus 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(5)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5) and 9.2(2). UCS 6200 and 6300 Series Fabric Interconnect are affected in versions prior to 3.2(3j) and 4.0(2a). UCS 6400 Series Fabric Interconnect are affected in versions prior to 4.0(2a).</p>	2019-03-07	not yet calculated	<a href="#">CVE-2019-1599</a> <a href="#">CISCO</a>
cisco -- nx-os_software	<p>A vulnerability in the file system permissions of Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to access sensitive information that is stored in the file system of an affected system. The vulnerability is due to improper implementation of file system permissions. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow the attacker to access sensitive and critical files. Firepower 4100 Series Next-Generation Firewalls are affected in versions prior to 2.2.2.91 and 2.3.1.110. Firepower 9300 Series Next-Generation Firewalls are affected in versions prior to 2.2.2.91 and 2.3.1.110. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(3)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). Nexus 9000 Series Switches- Standalone are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).</p>	2019-03-07	not yet calculated	<a href="#">CVE-2019-1600</a> <a href="#">CISCO</a>
cisco -- nx-os_software	<p>A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to gain read and write access to a critical configuration file. The vulnerability is due to a failure to impose strict filesystem permissions on the targeted device. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow an attacker to use the content of this configuration file to bypass authentication and log in as any user of the device. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus</p>	2019-03-	not yet	<a href="#">CVE-2019-</a>



	3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(3)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	08	calculated	<a href="#">1601</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to access sensitive data that could be used to elevate their privileges to administrator. The vulnerability is due to improper implementation of filesystem permissions. An attacker could exploit this vulnerability by logging in to the CLI of an affected device, accessing a specific file, and leveraging this information to authenticate to the NX-API server. A successful exploit could allow an attacker to make configuration changes as administrator. Note: NX-API is disabled by default. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1602</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to escalate lower-level privileges to the administrator level. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow an attacker to make configuration changes to the system as administrator. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1603</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the user account management interface of Cisco NX-OS Software could allow an authenticated, local attacker to gain elevated privileges on an affected device. The vulnerability is due to an incorrect authorization check of user accounts and their associated Group ID (GID). An attacker could exploit this vulnerability by taking advantage of a logic error that will permit the use of higher privileged commands than what is necessarily assigned. A successful exploit could allow an attacker to execute commands with elevated privileges on the underlying Linux shell of an affected device. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 8.2(3), and 8.3(2). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1604</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary code as root. The vulnerability is due to incorrect input validation in the NX-API feature. An attacker could exploit this vulnerability by sending a crafted HTTP or HTTPS request to an internal service on an affected device that has the NX-API feature enabled. A successful exploit could allow the attacker to cause a buffer overflow and execute arbitrary code as root. Note: The NX-API feature is disabled by default. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.1(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(8) and 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(8). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.3(2)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 7.3(3)D1(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I4(8) and 7.0(3)I7(1). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1605</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1608</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1607</a> <a href="#">CISCO</a>
cloud_foundry -- cli	Cloud Foundry CLI, versions prior to v6.43.0, improperly exposes passwords when verbose/trace/debugging is turned on. A local unauthenticated or remote authenticated malicious user with access to logs may gain part or all of a users password.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3781</a> <a href="#">CONFIRM</a>
cloud_foundry -- container_runtime	Cloud Foundry Container Runtime, versions prior to 0.28.0, deploys K8s worker nodes that contains a configuration file with IAAS credentials. A malicious user with access to the k8s nodes can obtain IAAS credentials allowing the user to escalate privileges to gain access to the IAAS account.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3780</a> <a href="#">CONFIRM</a>
cloud_foundry -- container_runtime	Cloud Foundry Container Runtime, versions prior to 0.29.0, deploys Kubernetes clusters utilize the same CA (Certificate Authority) to sign and trust certs for ETCD as used by the Kubernetes API. This could allow a user authenticated with a cluster to request a signed certificate leveraging the Kubernetes CSR capability to obtain a credential that could escalate privilege access to ETCD.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3779</a> <a href="#">CONFIRM</a>
cloud_foundry -- stratos	Cloud Foundry Stratos, versions prior to 2.3.0, contains an insecure session that can be spoofed. When deployed on cloud foundry with multiple instances using the default embedded SQLite database, a remote authenticated malicious user can switch sessions to another user with the same session id.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3784</a> <a href="#">CONFIRM</a>
cloud_foundry -- stratos	Cloud Foundry Stratos, versions prior to 2.3.0, deploys with a public default session store secret. A malicious user with default session store secret can brute force another user's current Stratos session, and act on behalf of that user.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3783</a> <a href="#">CONFIRM</a>
cloud_foundry -- uaa	Cloud Foundry UAA, versions prior to v70.0, allows a user to update their own email address. A remote authenticated user can impersonate a different user by changing their email address to that of a different user.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3775</a> <a href="#">CONFIRM</a>
cyberark -- endpoint_privilege_manager	A buffer overflow in the kernel driver CybKernelTracker.sys in CyberArk Endpoint Privilege Manager versions prior to 10.7 allows an attacker (without Administrator privileges) to	2019-03-	not yet	<a href="#">CVE-2019-</a>

	escalate privileges or crash the machine by loading an image, such as a DLL, with a long path.	08	calculated	<a href="#">9627</a> <a href="#">MISC</a>
dell -- wes_wyse_device_agent_and_wyse_thinlinux_hagent	Dell WES Wyse Device Agent versions prior to 14.1.2.9 and Dell Wyse ThinLinux HAgent versions prior to 5.4.55.00.10 contain a buffer overflow vulnerability. An unauthenticated attacker may potentially exploit this vulnerability to execute arbitrary code on the system with privileges of the FTP client by sending specially crafted input data to the affected system. The FTP code that contained the vulnerability has been removed.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3712</a> <a href="#">MISC</a>
druide -- antidote_rx_and_hd	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.	2019-03-04	not yet calculated	<a href="#">CVE-2019-9565</a> <a href="#">MISC</a> <a href="#">MISC</a>
eloan -- eloan	Eloan V3.0 through 2018-09-20 allows remote attackers to list files via a direct request to the p2p/api/ or p2p/lib/ or p2p/images/ URI.	2019-03-03	not yet calculated	<a href="#">CVE-2019-9552</a> <a href="#">MISC</a>
esafenet -- cdg	ESAFENET CDG V3 and V5 has an arbitrary file download vulnerability via the fileName parameter in download.jsp because the InstallationPack parameter is mishandled in a /CDGServer3/ClientAjax request.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9632</a> <a href="#">MISC</a>
gnome -- glib	gio/socketclient.c in GNOME GLib 2.59.2 does not ensure that a parent GTask remains alive during the execution of a connection-attempting enumeration, which allows remote attackers to cause a denial of service (g_socket_client_connected_callback mishandling and application crash) via a crafted web site, as demonstrated by GNOME Web (aka Epiphany).	2019-03-08	not yet calculated	<a href="#">CVE-2019-9633</a> <a href="#">MISC</a>
golang -- go	An issue was discovered in setTA in scan_rr.go in the Miek Gieben DNS library before 1.0.10 for Go. A dns.ParseZone() parsing error causes a segmentation violation, leading to denial of service.	2019-03-07	not yet calculated	<a href="#">CVE-2018-17419</a> <a href="#">MISC</a>
hashicorp -- consul	HashiCorp Consul (and Consul Enterprise) 1.4.x before 1.4.3 allows a client to bypass intended access restrictions and obtain the privileges of one other arbitrary token within secondary datacenters, because a token with literally "<hidden>" as its secret is used in unusual circumstances.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8336</a> <a href="#">MISC</a>
invision -- power_board	Stored XSS in Invision Power Board versions 3.3.1 - 3.4.8 leads to Remote Code Execution.	2019-03-01	not yet calculated	<a href="#">CVE-2019-8278</a> <a href="#">BID</a> <a href="#">MISC</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Repository Connector Plugin 1.2.4 and earlier in src/main/java/org/jvnet/hudson/plugins/repositoryconnector/ArtifactDeployer.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/Repository.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/UserPwd.java that allows an attacker with local file system access or control of a Jenkins administrator's web browser (e.g. malicious extension) to retrieve the password stored in the plugin configuration.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003038</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Email Extension Plugin 2.64 and earlier in pom.xml, src/main/java/hudson/plugins/emailext/ExtendedEmailPublisher.java, src/main/java/hudson/plugins/emailext/plugins/content/EmailExtScript.java, src/main/java/hudson/plugins/emailext/plugins/content/ScriptContent.java, src/main/java/hudson/plugins/emailext/plugins/trigger/AbstractScriptTrigger.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003032</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in JenkinsAppDynamics Dashboard Plugin 1.0.14 and earlier in src/main/java/nl/codecentric/jenkins/appd/AppDynamicsResultsPublisher.java that allows attackers without permission to obtain passwords configured in jobs to obtain them.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003039</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.53 and earlier in src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/GroovySandbox.java, src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/SecureGroovyScript.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003029</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Pipeline: Groovy Plugin 2.63 and earlier in pom.xml, src/main/java/org/jenkinsci/plugins/workflow/cps/CpsGroovyShell.java that allows attackers able to control pipeline scripts to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003030</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Matrix Project Plugin 1.13 and earlier in pom.xml, src/main/java/hudson/matrix/FilterScript.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003031</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Groovy Plugin 2.1 and earlier in pom.xml, src/main/java/hudson/plugins/groovy/StringScriptSource.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003033</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Job DSL Plugin 1.71 and earlier in job-dsl-core/src/main/groovy/javaposse/jobdsl/dsl/AbstractDslScriptLoader.groovy, job-dsl-plugin/build.gradle, job-dsl-plugin/src/main/groovy/jobdsl/plugin/JobDslWhitelist.groovy, job-dsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/SandboxDslScriptLoader.groovy that allows attackers with control over Job DSL definitions to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003034</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgentTemplate.java, src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to perform the 'verify configuration' form validation action, thereby obtaining limited information about the Azure configuration.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003035</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A data modification vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgent.java that allows attackers with Overall/Read permission to attach a public IP address to an Azure VM agent.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003036</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003037</a> <a href="#">CONFIRM</a>
microsoft -- azure_iot_java_sdk	An Elevation of Privilege vulnerability exists in the way Azure IoT Java SDK generates symmetric keys for encryption, allowing an attacker to predict the randomness of the key, aka 'Azure IoT Java SDK Elevation of Privilege Vulnerability'.	2019-03-05	not yet calculated	<a href="#">CVE-2019-0729</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
	An information disclosure vulnerability exists when Windows Hyper-V on a host operating	2019-03-	not yet	<a href="#">CVE-2019-</a>

microsoft -- windows_hyber-v	system fails to properly validate input from an authenticated user on a guest operating system, aka "Windows Hyper-V Information Disclosure Vulnerability".	05	calculated	<a href="#">0635 BID CONFIRM</a>
netapp -- snapcenter	NetApp SnapCenter Server prior to 4.1 does not set the secure flag for a sensitive cookie in an HTTPS session which can allow the transmission of the cookie in plain text over an unencrypted channel.	2019-03-04	not yet calculated	<a href="#">CVE-2018-5482 BID CONFIRM</a>
netapp -- snapcenter_server	NetApp SnapCenter Server prior to 4.0 is susceptible to cross site scripting vulnerability that could allow a privileged user to inject arbitrary scripts into the custom secondary policy label field.	2019-03-04	not yet calculated	<a href="#">CVE-2017-15515 BID CONFIRM</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. It allows admin/system/generate/create?sql= SQL injection, related to SystemGenerateController.java.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9615 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadFile URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9617 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadScrawl URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9616 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. It allows admin/cms/template/getTemplates.html?res_path=res directory traversal, with ../ in the dir parameter, to write arbitrary content (in the file_content parameter) into an arbitrary file (specified by the file_name parameter). This is related to the save function in TemplateController.java.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9611 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. A command execution vulnerability exists via a template file with '<#assign ex="freemarker.template.utility.Execute"?new(>\${ ex(" followed by the command.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9614 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadVideo URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9613 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/comn/service/upload URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9612 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/comn/service/editUploadImage URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9609 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. It has admin/cms/template/getTemplates.html?res_path=res&up_dir=../ directory traversal, related to the getTemplates function in TemplateController.java.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9610 MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadImage URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9608 MISC</a>
openssl -- openssl	ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 specifies that the nonce value (IV) should be 96 bits (12 bytes). OpenSSL allows a variable nonce length and front pads the nonce with 0 bytes if it is less than 12 bytes. However it also incorrectly allows a nonce to be set of up to 16 bytes. In this case only the last 12 bytes are significant and any additional leading bytes are ignored. It is a requirement of using this cipher that nonce values are unique. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. If an application changes the default nonce length to be longer than 12 bytes and then makes a change to the leading bytes of the nonce expecting the new value to be a new unique nonce then such an application could inadvertently encrypt messages with a reused nonce. Additionally the ignored bytes in a long nonce are not covered by the integrity guarantee of this cipher. Any application that relies on the integrity of these ignored leading bytes of a long nonce may be further affected. Any OpenSSL internal use of this cipher, including in SSL/TLS, is safe because no such use sets such a long nonce value. However user applications that use this cipher directly and set a non-default nonce length to be longer than 12 bytes may be vulnerable. OpenSSL versions 1.1.1 and 1.1.0 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1c-dev (Affected 1.1.1-1.1.1b). Fixed in OpenSSL 1.1.0k-dev (Affected 1.1.0-1.1.0j).	2019-03-06	not yet calculated	<a href="#">CVE-2019-1543 CONFIRM CONFIRM CONFIRM</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9638 MISC</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9639 MISC</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9640 MISC</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9641 MISC</a>
php -- php	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9637 MISC</a>
pivotal -- application_service	Pivotal Application Service (PAS), versions 2.2.x prior to 2.2.12, 2.3.x prior to 2.3.7 and 2.4.x prior to 2.4.3, contain apps manager that uses a cloud controller proxy that fails to verify SSL certs. A remote unauthenticated attacker that could hijack the Cloud Controller's DNS record could intercept access tokens sent to the Cloud Controller, giving the attacker access to the user's resources in the Cloud Controller	2019-03-07	not yet calculated	<a href="#">CVE-2019-3777 BID CONFIRM</a>
	Spring Security OAuth, versions 2.3 prior to 2.3.5, and 2.2 prior to 2.2.4, and 2.1 prior to 2.1.4, and 2.0 prior to 2.0.17, and older unsupported versions could be susceptible to an			

pivotal -- spring_security_oauth	open redirector attack that can leak an authorization code. A malicious user or attacker can craft a request to the authorization endpoint using the authorization code grant type, and specify a manipulated redirection URI via the "redirect_uri" parameter. This can cause the authorization server to redirect the resource owner user-agent to a URI under the control of the attacker with the leaked authorization code. This vulnerability exposes applications that meet all of the following requirements: Act in the role of an Authorization Server (e.g. @EnableAuthorizationServer) and uses the DefaultRedirectResolver in the AuthorizationEndpoint. This vulnerability does not expose applications that: Act in the role of an Authorization Server and uses a different RedirectResolver implementation other than DefaultRedirectResolver, act in the role of a Resource Server only (e.g. @EnableResourceServer), act in the role of a Client only (e.g. @EnableOAuthClient).	2019-03-07	not yet calculated	<a href="#">CVE-2019-3778</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	not yet calculated	<a href="#">CVE-2018-4054</a> <a href="#">MISC</a>
pixar -- renderman	A local privilege escalation vulnerability exists in the Mac OS X version of Pixar Renderman 22.3.0's Install Helper tool. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine for a successful exploit.	2019-03-08	not yet calculated	<a href="#">CVE-2019-5015</a> <a href="#">MISC</a>
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to read any root file from the file system. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	not yet calculated	<a href="#">CVE-2018-4055</a> <a href="#">MISC</a>
python -- python	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9636</a> <a href="#">MISC</a> <a href="#">MISC</a>
rainbow_pdf -- office_server_document_converter	A heap overflow vulnerability exists in the PowerPoint document conversion function of Rainbow PDF Office Server Document Converter V7.0 Pro R1 (7.0.2018.1113). While parsing Document Summary Property Set stream, the getSummaryInformation function is incorrectly checking the correlation between size and the number of properties in PropertySet packets, causing an out-of-bounds write that leads to heap corruption and consequent code execution.	2019-03-07	not yet calculated	<a href="#">CVE-2019-5019</a> <a href="#">MISC</a>
simple_machines -- simple_machines_forum	Simple Machines Forum (SMF) 2.0.4 allows local file inclusion, with resultant remote code execution, in install.php via ../ directory traversal in the db_type parameter if install.php remains present after installation.	2019-03-07	not yet calculated	<a href="#">CVE-2013-7466</a> <a href="#">MISC</a>
sslheaders -- sslheaders	sslheaders plugin extracts information from the client certificate and sets headers in the request based on the configuration of the plugin. The plugin doesn't strip the headers from the request in some scenarios. This problem was discovered in versions 6.0.0 to 6.0.3, 7.0.0 to 7.1.5, and 8.0.0 to 8.0.1.	2019-03-07	not yet calculated	<a href="#">CVE-2018-11783</a> <a href="#">BID</a> <a href="#">MLIST</a>
stackstorm -- web_ui	In st2web in StackStorm Web UI before 2.9.3 and 2.10.x before 2.10.3, it is possible to bypass the CORS protection mechanism via a "null" origin value, potentially leading to XSS.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9580</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
suse -- supportutils	Supportutils, before version 3.1-5.7.1, when run with command line argument -A searched the file system for a ndspath binary. If an attacker provides one at an arbitrary location it is executed with root privileges	2019-03-05	not yet calculated	<a href="#">CVE-2018-19636</a> <a href="#">CONFIRM</a>
suse -- supportutils	In supportutils, before version 3.1-5.7.1 and if pacemaker is installed on the system, an unprivileged user could have overwritten arbitrary files in the directory that is used by supportutils to collect the log files.	2019-03-05	not yet calculated	<a href="#">CVE-2018-19638</a> <a href="#">CONFIRM</a>
suse -- supportutils	If supportutils before version 3.1-5.7.1 is run with -v to perform rpm verification and the attacker manages to manipulate the rpm listing (e.g. with CVE-2018-19638) he can execute arbitrary commands as root.	2019-03-05	not yet calculated	<a href="#">CVE-2018-19639</a> <a href="#">CONFIRM</a>
suse -- supportutils	If the attacker manages to create files in the directory used to collect log files in supportutils before version 3.1-5.7.1 (e.g. with CVE-2018-19638) he can kill arbitrary processes on the local machine.	2019-03-05	not yet calculated	<a href="#">CVE-2018-19640</a> <a href="#">CONFIRM</a>
suse -- supportutils	Supportutils, before version 3.1-5.7.1, wrote data to static file /tmp/supp_log, allowing local attackers to overwrite files on systems without symlink protection	2019-03-05	not yet calculated	<a href="#">CVE-2018-19637</a> <a href="#">CONFIRM</a>
tibco -- jasperreports_server_and_jasperreports_server_for_activematrix_bpm	The SOAP API component vulnerability of TIBCO Software Inc.'s TIBCO JasperReports Server, and TIBCO JasperReports Server for ActiveMatrix BPM contains a vulnerability that may allow a malicious authenticated user to copy text files from the host operating system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3. TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3.	2019-03-07	not yet calculated	<a href="#">CVE-2019-8986</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- multiple_products	The repository component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, TIBCO Jaspersoft Reporting and Analytics for AWS contains a persistent cross site scripting vulnerability. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, and TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18816</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- multiple_products	The REST API component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, and TIBCO Jaspersoft Reporting and Analytics for AWS contains a vulnerability that theoretically allows unauthenticated users to bypass authorization checks for portions of the HTTP interface to the JasperReports Server. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, and TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18815</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
	The default server implementation of TIBCO Software Inc.'s TIBCO JasperReports Library, TIBCO JasperReports Library Community Edition, TIBCO JasperReports Library for ActiveMatrix BPM, TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO			

tibco -- multiple_products	Jaspersoft for AWS with Multi-Tenancy, and TIBCO Jaspersoft Reporting and Analytics for AWS contains a directory-traversal vulnerability that may theoretically allow web server users to access contents of the host system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Library: versions up to and including 6.3.4; 6.4.1; 6.4.2; 6.4.21; 7.1.0; 7.2.0, TIBCO JasperReports Library Community Edition: versions up to and including 6.7.0, TIBCO JasperReports Library for ActiveMatrix BPM: versions up to and including 6.4.21, TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 6.4.3; 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18809</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- multiple_products	The domain management component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, and TIBCO Jaspersoft Reporting and Analytics for AWS contains a race-condition vulnerability that may allow any users with domain save privileges to gain superuser privileges. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, and TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18808</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has multiple heap buffer overflow vulnerabilities in VNC client code inside Ultra decoder, which results in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1204.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8262</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1198 has a buffer underflow vulnerability in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1199.	2019-03-05	not yet calculated	<a href="#">CVE-2018-15361</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1199 has a out-of-bounds read vulnerability in VNC code inside client CoRRE decoder, caused by multiplication overflow. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1200.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8261</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer offer handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8274</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a stack buffer overflow vulnerability in VNC server code inside file transfer request handler, which can result in Denial of Service (DoS). This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8276</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1206 has stack-based Buffer overflow vulnerability in VNC client code inside FileTransfer module, which leads to a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8269</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1210 has out-of-bounds read vulnerability in VNC client code inside Ultra decoder, which results in a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1211.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8270</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8271</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple off-by-one vulnerabilities in VNC server code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8272</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer request handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8273</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of ClientConnection::Copybuffer function in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. User interaction is required to trigger these vulnerabilities. These vulnerabilities have been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8266</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple improper null termination vulnerabilities in VNC server code, which result in out-of-bound data being accessed by remote users. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8275</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 contains multiple memory leaks (CWE-655) in VNC server code, which allows an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8277</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has out-of-bounds read vulnerability in VNC client code inside TextChat module, which results in a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8267</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1199 has a out-of-bounds read vulnerability in VNC client RRE decoder code, caused by multiplication overflow. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1200.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8260</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside RAW decoder, which can potentially result code execution. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8280</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1198 contains multiple memory leaks (CWE-655) in VNC client code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1199.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8259</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1198 has a heap buffer overflow vulnerability in VNC client code which results code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1199.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8258</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of SETPIXELS macro in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These	2019-03-08	not yet calculated	<a href="#">CVE-2019-8265</a>



	vulnerabilities have been fixed in revision 1208.			MISC
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside Ultra2 decoder, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8264</a> MISC
ultravnc -- ultravnc	UltraVNC revision 1205 has stack-based buffer overflow vulnerability in VNC client code inside ShowConnInfo routine, which leads to a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. User interaction is required to trigger this vulnerability. This vulnerability has been fixed in revision 1206.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8263</a> MISC
ultravnc -- ultravnc	UltraVNC revision 1206 has multiple off-by-one vulnerabilities in VNC client code connected with improper usage of ClientConnection::ReadString function, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8268</a> MISC
wordpress -- wordpress	The "Forminator Contact Form, Poll & Quiz Builder" plugin before 1.6 for WordPress has SQL Injection via the wp-admin/admin.php?page=forminator-entries entry[] parameter if the attacker has the delete permission.	2019-03-04	not yet calculated	<a href="#">CVE-2019-9568</a> MISC
wordpress -- wordpress	The WP Human Resource Management plugin before 2.2.6 for WordPress mishandles leave applications.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9573</a> MISC
wordpress -- wordpress	The Blog2Social plugin before 5.0.3 for WordPress allows wp-admin/admin.php?page=blog2social-ship XSS.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9576</a> MISC
wordpress -- wordpress	The WP Human Resource Management plugin before 2.2.6 for WordPress does not ensure that a leave modification occurs in the context of the Administrator or HR Manager role.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9574</a> MISC
wordpress -- wordpress	The "Forminator Contact Form, Poll & Quiz Builder" plugin before 1.6 for WordPress has XSS via a custom input field of a poll.	2019-03-04	not yet calculated	<a href="#">CVE-2019-9567</a> MISC
yubico -- libu2f-host	In devs.c in Yubico libu2f-host before 1.1.8, the response to init is misparsed, leaking uninitialized stack memory back to the device.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9578</a> MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to tmcginnis@sunnyvale.ca.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) - 25 Murray Lane SW Bldg 10 - Washington, DC 20598 - (888) 282-0870



From: [US-CERT](mailto:US-CERT)  
To: [wgularte@cissummyva.e.ca.us](mailto:wgularte@cissummyva.e.ca.us)  
Subject: SB19-070: Vulnerability Summary for the Week of March 4 2019  
Date: Monday March 11 2019 12:08:39 PM

ATTN: Email is from an external source; Stop, Look, and Think before opening attachments or links.



National Cyber Awareness System:

## SB19-070 Vulnerability Summary for the Week of March 4 2019

03/11/2019 04:14 AM EDT

Original release date: March 11, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology \(NIST\) National Vulnerability Database \(NVD\)](#) in the past week. The NVD is sponsored by the [Department of Homeland Security \(DHS\) National Cybersecurity and Communications Integration Center \(NCCIC\)](#) / [United States Computer Emergency Readiness Team \(US-CERT\)](#). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System \(CVSS\)](#) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database \(NVD\)](#). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
airdroid -- airdroid	The AirDroid application through 4.2.1.6 for Android allows remote attackers to cause a denial of service (service crash) via many simultaneous sdctl/comm/lite_auth/ requests.	2019-03-06	7.8	<a href="#">CVE-2019-9599</a> <a href="#">EXPLOIT-DB</a> <a href="#">MISC</a>
apache -- jmeter	Unauthenticated RCE is possible when JMeter is used in distributed mode (-r or -R command line options). Attacker can establish a RMI connection to a jmeter-server using RemoteJMeterEngine and proceed with an attack using untrusted data deserialization. This only affect tests running in Distributed mode. Note that versions before 4.0 are not able to encrypt traffic between the nodes, nor authenticate the participating nodes so upgrade to JMeter 5.1 is also advised.	2019-03-06	7.5	<a href="#">CVE-2019-0187</a> <a href="#">MLIST</a> <a href="#">BID</a>
apache -- solr	In Apache Solr versions 5.0.0 to 5.5.5 and 6.0.0 to 6.6.5, the Config API allows to configure the JMX server via an HTTP POST request. By pointing it to a malicious RMI server, an attacker could take advantage of Solr's unsafe deserialization to trigger remote code execution on the Solr side.	2019-03-07	7.5	<a href="#">CVE-2019-0192</a> <a href="#">MLIST</a> <a href="#">BID</a>
apple -- iphone_os	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. An application may be able to execute arbitrary code with kernel privileges.	2019-03-05	9.3	<a href="#">CVE-2019-6213</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">EXPLOIT-DB</a>
apple -- iphone_os	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may be able to execute arbitrary code with kernel privileges.	2019-03-05	9.3	<a href="#">CVE-2019-6218</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">EXPLOIT-DB</a>
apple -- iphone_os	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3, iTunes 12.9.3 for Windows. A sandboxed process may be able to circumvent sandbox restrictions.	2019-03-04	7.5	<a href="#">CVE-2019-6235</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
bluecms_project -- bluecms	BlueCMS 1.6 allows SQL Injection via the user_id parameter in an uploads/admin/user.php?act=edit request.	2019-03-06	7.5	<a href="#">CVE-2019-9594</a> <a href="#">MISC</a>
checkpoint -- zonealarm	Check Point ZoneAlarm version 15.3.064.17729 and below expose a WCF service that can allow a local low privileged user to execute arbitrary code as SYSTEM.	2019-03-01	7.2	<a href="#">CVE-2018-8790</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- nx-os	A vulnerability in a specific CLI command implementation of Cisco Nexus 9000 Series ACI Mode Switch Software could allow an authenticated, local attacker to escape a restricted shell on an affected device. The vulnerability is due to insufficient sanitization of user-supplied input when issuing a specific CLI command with parameters on an affected device. An attacker could exploit this vulnerability by authenticating to the device CLI and issuing certain commands. A successful exploit could allow the attacker to escape the restricted shell and execute arbitrary commands with root-level privileges on the affected device. This vulnerability only affects Cisco Nexus 9000 Series ACI Mode Switches that are running a release prior to 14.0(3d).	2019-03-06	7.2	<a href="#">CVE-2019-1591</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the Bash shell implementation for Cisco NX-OS Software could allow an authenticated, local attacker to escalate their privilege level by executing commands authorized to other user roles. The attacker must authenticate with valid user credentials. The vulnerability is due to the incorrect implementation of a Bash shell command that allows role-based access control (RBAC) to be bypassed. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the Bash prompt. A successful exploit could allow the attacker to escalate their privilege level by executing commands that should be restricted to other roles. For example, a dev-ops user could	2019-03-06	7.2	<a href="#">CVE-2019-1593</a> <a href="#">BID</a> <a href="#">CISCO</a>

	escalate their privilege level to admin with a successful exploit of this vulnerability.			
cisco -- nx-os	A vulnerability in the Bash shell implementation for Cisco NX-OS Software could allow an authenticated, local attacker to escalate their privilege level to root. The attacker must authenticate with valid user credentials. The vulnerability is due to incorrect permissions of a system executable. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the Bash prompt. A successful exploit could allow the attacker to escalate their privilege level to root. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-07	7.2	<a href="#">CVE-2019-1596</a> <a href="#">CISCO</a>
dolibarr -- dolibarr	An issue was discovered in Dolibarr through 7.0.0. expensereport/card.php in the expense reports module allows SQL injection via the integer parameters qty and value_unit.	2019-03-07	7.5	<a href="#">CVE-2018-16809</a> <a href="#">MISC</a>
fengoffice -- feng_office	Feng Office 3.7.0.5 allows remote attackers to execute arbitrary code via "<!--#exec cmd=" in a .shtml file to ck_upload_handler.php.	2019-03-07	7.5	<a href="#">CVE-2019-9623</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
flarumchina -- flarumchina	FlarumChina v0.1.0-beta.7C has SQL injection via a /?q= request.	2019-03-04	7.5	<a href="#">CVE-2019-9566</a> <a href="#">MISC</a>
freedesktop -- poppler	Poppler 0.74.0 has a heap-based buffer over-read in the CairoRescaleBox.cc downsample_row_box_filter function.	2019-03-08	7.5	<a href="#">CVE-2019-9631</a> <a href="#">MISC</a>
ibm -- financial_transaction_manager	BM Financial Transaction Manager for Digital Payments for Multi-Platform 3.1.0 is vulnerable o SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-ForceID: 155998.	2019-03-05	7.5	<a href="#">CVE-2019-4032</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
layerbb -- layerbb	LayerBB 1.1.1 has SQL Injection via the search.php search_query parameter.	2019-03-07	7.5	<a href="#">CVE-2018-17988</a> <a href="#">EXPLOIT-DB</a>
microsoft -- .net_framework	A remote code execution vulnerability exists in .NET Framework and Visual Studio software when the software fails to check the source markup of a file.An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka '.NET Framework and Visual Studio Remote Code Execution Vulnerability'.	2019-03-05	9.3	<a href="#">CVE-2019-0613</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0590</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0591</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0593</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0605</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0607</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0610</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0640</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0642</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0644</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0651</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0652</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- chakracore	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655.	2019-03-05	7.6	<a href="#">CVE-2019-0655</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0645, CVE-2019-0650.	2019-03-05	7.6	<a href="#">CVE-2019-0634</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0650.	2019-03-05	7.6	<a href="#">CVE-2019-0645</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0645.	2019-03-05	7.6	<a href="#">CVE-2019-0650</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

microsoft -- exchange_server	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0686.	2019-03-05	9.3	<a href="#">CVE-2019-0724</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'.	2019-03-05	7.6	<a href="#">CVE-2019-0806</a> BID CONFIRM
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0672, CVE-2019-0673, CVE-2019-0674, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0671</a> BID CONFIRM
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0673, CVE-2019-0674, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0672</a> BID CONFIRM
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0674, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0673</a> BID CONFIRM
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0673, CVE-2019-0675.	2019-03-05	9.3	<a href="#">CVE-2019-0674</a> BID CONFIRM
microsoft -- office	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0673, CVE-2019-0674.	2019-03-05	9.3	<a href="#">CVE-2019-0675</a> BID CONFIRM
microsoft -- sharepoint_enterprise_server	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0604.	2019-03-05	9.3	<a href="#">CVE-2019-0594</a> BID CONFIRM
microsoft -- sharepoint_enterprise_server	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0594.	2019-03-05	9.3	<a href="#">CVE-2019-0604</a> BID CONFIRM
microsoft -- visual_studio_code	A remote code execution vulnerability exists in Visual Studio Code when it process environment variables after opening a project, aka 'Visual Studio Code Remote Code Execution Vulnerability'.	2019-03-05	9.3	<a href="#">CVE-2019-0728</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0595</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0596</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0597</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0599, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0598</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625.	2019-03-05	9.3	<a href="#">CVE-2019-0599</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0662.	2019-03-05	9.3	<a href="#">CVE-2019-0618</a> BID CONFIRM
microsoft -- windows_10	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'.	2019-03-05	7.2	<a href="#">CVE-2019-0623</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599.	2019-03-05	9.3	<a href="#">CVE-2019-0625</a> BID CONFIRM
microsoft -- windows_10	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'.	2019-03-05	7.5	<a href="#">CVE-2019-0626</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633.	2019-03-05	9.0	<a href="#">CVE-2019-0630</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630.	2019-03-05	9.0	<a href="#">CVE-2019-0633</a> BID CONFIRM
microsoft -- windows_10	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618.	2019-03-05	9.3	<a href="#">CVE-2019-0662</a> BID CONFIRM
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetNetworkTomographySettings API function, as demonstrated by shell metacharacters in the tomography_ping_number field.	2019-03-07	10.0	<a href="#">CVE-2019-9117</a> MISC
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetNTPServerSettings API function, as demonstrated by shell metacharacters in the system_time_timezone field.	2019-03-07	10.0	<a href="#">CVE-2019-9118</a> MISC
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetStaticRouteSettings API function, as demonstrated by shell metacharacters in the staticroute_list field.	2019-03-07	10.0	<a href="#">CVE-2019-9119</a> MISC
	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute			

motorola -- c1_firmware	arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetWLANACLSettings API function, as demonstrated by shell metacharacters in he wl(0).(0)_maclist field.	2019-03-07	<a href="#">10.0</a>	<a href="#">CVE-2019-9120 MISC</a>
motorola -- c1_firmware	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetSmartQoSSettings API function, as demonstrated by shell metacharacters in he smartqos_priority_devices field.	2019-03-07	<a href="#">10.0</a>	<a href="#">CVE-2019-9121 MISC</a>
moxa -- eds-405a_firmware	Moxa IKS and EDS fails to properly check array bounds which may allow an attacker to read device memory on arbitrary addresses, and may allow an attacker to retrieve sensitive data or cause device reboot.	2019-03-05	<a href="#">8.5</a>	<a href="#">CVE-2019-6522 BID MISC</a>
moxa -- eds-405a_firmware	Several buffer overflow vulnerabilities have been identified in Moxa IKS and EDS, which may allow remote code execution.	2019-03-05	<a href="#">7.5</a>	<a href="#">CVE-2019-6557 BID MISC</a>
moxa -- eds-405a_firmware	Moxa IKS and EDS generate a predictable cookie calculated with an MD5 hash, allowing an attacker to capture the administrator's password, which could lead to a full compromise of the device.	2019-03-05	<a href="#">10.0</a>	<a href="#">CVE-2019-6563 BID MISC</a>
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 contains multiple hard coded credentials for the Telnet and SSH interfaces.	2019-03-05	<a href="#">10.0</a>	<a href="#">CVE-2019-3918 MISC</a>
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to a stack buffer overflow via crafted HTTP POST request sent by a remote, unauthenticated attacker to /GponForm/setup_Form. An attacker can leverage this vulnerability to potentially execute arbitrary code.	2019-03-05	<a href="#">7.5</a>	<a href="#">CVE-2019-3922 MISC</a>
phpshe -- phpshe	PHPSHE 1.7 allows module/index/cart.php pintuan_id SQL Injection to index.php.	2019-03-07	<a href="#">7.5</a>	<a href="#">CVE-2019-9626 MISC</a>
solarwinds -- orion_platform	SolarWinds Orion Platform before 2018.4 Hotfix 2 allows privilege escalation through the RabbitMQ service.	2019-03-01	<a href="#">7.5</a>	<a href="#">CVE-2019-9546 CONFIRM</a>
twinkltoessoftware -- booked	phpscheduleit Booked Scheduler 2.7.5 allows arbitrary file upload via the Favicon field, leading to execution of arbitrary Web/custom-favicon.php PHP code, because Presenters/Admin/ManageThemePresenter.php does not ensure an image file extension.	2019-03-05	<a href="#">7.5</a>	<a href="#">CVE-2019-9581 MISC MISC EXPLOIT-DB</a>
zscms -- zscms	zscms v8.3 contains a SQL Injection vulnerability in /user/logincheck.php via an X-Forwarded-For HTTP header.	2019-03-07	<a href="#">7.5</a>	<a href="#">CVE-2018-17412 MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
1234n -- minicms	MiniCMS 1.10 allows mc-admin/post.php?state=publish&delete= CSRF to delete articles, a different vulnerability than CVE-2018-18891.	2019-03-06	<a href="#">5.8</a>	<a href="#">CVE-2019-9603 MISC</a>
apache -- mesos	When parsing a JSON payload with deeply nested JSON structures, the parser in Apache Mesos versions pre-1.4.x, 1.4.0 to 1.4.2, 1.5.0 to 1.5.1, 1.6.0 to 1.6.1, and 1.7.0 might overflow the stack due to unbounded recursion. A malicious actor can therefore cause a denial of service of Mesos masters rendering the Mesos-controlled cluster inoperable.	2019-03-05	<a href="#">5.0</a>	<a href="#">CVE-2018-11793 BID MISC</a>
apache -- qpid_broker-j	A Denial of Service vulnerability was found in Apache Qpid Broker-J versions 6.0.0-7.0.6 (inclusive) and 7.1.0 which allows an unauthenticated attacker to crash the broker instance by sending specially crafted commands using AMQP protocol versions below 1.0 (AMQP 0-8, 0-9, 0-91 and 0-10). Users of Apache Qpid Broker-J versions 6.0.0-7.0.6 (inclusive) and 7.1.0 utilizing AMQP protocols 0-8, 0-9, 0-91, 0-10 must upgrade to Qpid Broker-J versions 7.0.7 or 7.1.1 or later.	2019-03-06	<a href="#">5.0</a>	<a href="#">CVE-2019-0200 BID MLIST</a>
apowersoft -- apowermanager	The ApowerManager application through 3.1.7 for Android allows remote attackers to cause a denial of service via many simultaneous /?Key=PhoneRequestAuthorization requests.	2019-03-06	<a href="#">5.0</a>	<a href="#">CVE-2019-9601 EXPLOIT-DB MISC</a>
apccms -- apccms	AppCMS 2.0.101 allows XSS via the upload/callback.php params parameter.	2019-03-06	<a href="#">4.3</a>	<a href="#">CVE-2019-9595 MISC</a>
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	<a href="#">6.8</a>	<a href="#">CVE-2019-6212 BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM UBUGNTU</a>
apple -- icloud	A type confusion issue was addressed with improved memory handling. This issue is fixed in OS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	<a href="#">6.8</a>	<a href="#">CVE-2019-6215 BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM UBUGNTU EXPLOIT-DB</a>
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	<a href="#">6.8</a>	<a href="#">CVE-2019-6216 BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM</a>
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	<a href="#">6.8</a>	<a href="#">CVE-2019-6217 BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM</a>
apple -- icloud	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	<a href="#">6.8</a>	<a href="#">CVE-2019-6226 BID CONFIRM CONFIRM CONFIRM</a>



	arbitrary code execution.			CONFIRM CONFIRM CONFIRM
apple -- icloud	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, Cloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6227</a> BID CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to universal cross site scripting.	2019-03-05	4.3	<a href="#">CVE-2019-6229</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6233</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- icloud	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6234</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An out-of-bounds read was addressed with improved input validation. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3. An attacker in a privileged network position may be able to execute arbitrary code.	2019-03-05	5.8	<a href="#">CVE-2019-6200</a> BID CONFIRM CONFIRM
apple -- iphone_os	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, watchOS 5.1.3. A malicious application may be able to elevate privileges.	2019-03-05	6.8	<a href="#">CVE-2019-6202</a> BID CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An issue existed with autofill resuming after it was canceled. The issue was addressed with improved state management. This issue is fixed in iOS 12.1.3. Password autofill may fill in passwords after they were manually cleared.	2019-03-04	5.0	<a href="#">CVE-2019-6206</a> BID CONFIRM
apple -- iphone_os	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in memory shared between processes.	2019-03-05	4.3	<a href="#">CVE-2019-6208</a> BID CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to determine kernel memory layout.	2019-03-05	4.3	<a href="#">CVE-2019-6209</a> BID CONFIRM CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3. Processing maliciously crafted web content may lead to arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6211</a> CONFIRM CONFIRM
apple -- iphone_os	A type confusion issue was addressed with improved memory handling. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to break out of its sandbox.	2019-03-05	6.8	<a href="#">CVE-2019-6214</a> BID CONFIRM CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, watchOS 5.1.3. Processing a maliciously crafted message may lead to a denial of service.	2019-03-05	5.0	<a href="#">CVE-2019-6219</a> BID CONFIRM CONFIRM CONFIRM
apple -- iphone_os	A logic issue existed in the handling of Group FaceTime calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.1.4, macOS Mojave 10.14.3 Supplemental Update. The initiator of a Group FaceTime call may be able to cause the recipient to answer.	2019-03-05	5.0	<a href="#">CVE-2019-6223</a> CONFIRM CONFIRM
apple -- iphone_os	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A remote attacker may be able to initiate a FaceTime call causing arbitrary code execution.	2019-03-05	6.8	<a href="#">CVE-2019-6224</a> BID CONFIRM CONFIRM CONFIRM CONFIRM EXPLOIT-DB
apple -- iphone_os	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to break out of its sandbox.	2019-03-05	6.8	<a href="#">CVE-2019-6230</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to read restricted memory.	2019-03-05	4.3	<a href="#">CVE-2019-6231</a> BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- itunes	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in OS 12.1.3, macOS Mojave 10.14.3, iTunes 12.9.3 for Windows. A malicious application may be able to elevate privileges.	2019-03-05	6.8	<a href="#">CVE-2019-6221</a> BID CONFIRM CONFIRM CONFIRM
apple -- mac_os_x	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.3. An application may be able to read restricted memory.	2019-03-05	4.3	<a href="#">CVE-2019-6220</a> BID

				<a href="#">CONFIRM</a>
apple -- safari	A cross-site scripting issue existed in Safari. This issue was addressed with improved URL validation. This issue is fixed in iOS 12.1.3, Safari 12.0.3. Processing maliciously crafted web content may lead to a cross site scripting attack.	2019-03-05	<a href="#">4.3</a>	<a href="#">CVE-2019-6228</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
axiosys -- bento4	An issue was discovered in Bento4 1.5.1-628. An out of bounds write occurs in AP4_CttsTableEntry::AP4_CttsTableEntry() located in Core/AP4Array.h. It can be triggered by sending a crafted file to (for example) the mp42hls binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.	2019-03-01	<a href="#">6.8</a>	<a href="#">CVE-2019-9544</a> <a href="#">MISC</a> <a href="#">MISC</a>
bluemind -- bluemind	n BlueMind 3.5.x before 3.5.11 Hotfix 7 and 4.x before 4.0-beta3, the contact application mishandles temporary uploads.	2019-03-04	<a href="#">5.0</a>	<a href="#">CVE-2019-9563</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bolt -- bolt	Controller/Async/FileManager.php in the filemanager in Bolt before 3.6.5 allows remote attackers to execute arbitrary PHP code by renaming a previously uploaded file to have a .php extension.	2019-03-07	<a href="#">6.5</a>	<a href="#">CVE-2019-9185</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
chshcms -- cscms	An issue was discovered in Cscms 4.1.0. There is an admin.php/pay CSRF vulnerability that can change the payment account to redirect funds.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2019-9598</a> <a href="#">MISC</a>
cisco -- nx-os	A vulnerability in the 802.1X implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation of Extensible Authentication Protocol over LAN (EAPOL) frames. An attacker could exploit this vulnerability by sending a crafted EAPOL frame to an interface on the targeted device. A successful exploit could allow the attacker to cause the Layer 2 (L2) forwarding process to restart multiple times, leading to a system-level restart of the device and a DoS condition. Note: This vulnerability affects only NX-OS devices configured with 802.1X functionality. Cisco Nexus 1000V Switch for VMware vSphere devices are affected in versions prior to 5.2(1)SV3(1.4b). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.3(5)N1(1) and 7.1(5)N1(1b). Nexus 7000 and 7700 Series Switches are affected in versions prior to 8.2(3). Nexus 9000 Series Fabric Switches in ACI Mode are affected in versions prior to 13.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4).	2019-03-06	<a href="#">6.1</a>	<a href="#">CVE-2019-1594</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os	A vulnerability in the Fibre Channel over Ethernet (FCoE) protocol implementation in Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an incorrect allocation of an internal interface index. An adjacent attacker with the ability to submit a crafted FCoE packet that crosses affected interfaces could trigger this vulnerability. A successful exploit could allow the attacker to cause a packet loop and high throughput on the affected interfaces, resulting in a DoS condition. This vulnerability has been fixed in version 7.3(5)N1(1).	2019-03-06	<a href="#">6.1</a>	<a href="#">CVE-2019-1595</a> <a href="#">BID</a> <a href="#">CISCO</a>
directadmin -- directadmin	JBMC DirectAdmin 1.55 allows CSRF via the /CMD_ACCOUNT_ADMIN URI to create a new admin account.	2019-03-07	<a href="#">6.8</a>	<a href="#">CVE-2019-9625</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
dolbarr -- dolbarr	An issue was discovered in Dolbarr through 7.0.0. There is Stored XSS in expensereport/card.php in the expense reports plugin via the comments parameter, or a public or private note.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2018-16808</a> <a href="#">MISC</a>
dotcms -- dotcms	dotCMS before 5.0.2 has open redirects via the html/common/forward_js.jsp FORWARD_URL parameter or the html/portlet/ext/common/page_preview_popup.jsp hostname parameter.	2019-03-07	<a href="#">5.8</a>	<a href="#">CVE-2018-17422</a> <a href="#">MISC</a>
ebrigade -- ebrigade	eBrigade through 4.5 allows Arbitrary File Download via ./ directory traversal in the showfile.php file parameter, as demonstrated by reading the user-data/save/backup.sql file.	2019-03-07	<a href="#">4.0</a>	<a href="#">CVE-2019-9622</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
freedesktop -- poppler	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readGenericBitmap() located in JBIG2Stream.cc, can be triggered by sending a crafted pdf file to (for example) the pdfseparate binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to JArithmeticDecoder::decodeBit.	2019-03-01	<a href="#">6.8</a>	<a href="#">CVE-2019-9543</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
freedesktop -- poppler	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readTextRegion() located in JBIG2Stream.cc, can be triggered by sending a crafted pdf file to (for example) the pdftimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to JBIG2Bitmap::clearToZero.	2019-03-01	<a href="#">6.8</a>	<a href="#">CVE-2019-9545</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	There is a stack consumption issue in md5Round1() located in Decrypt.cc in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to Catalog::countPageTree.	2019-03-06	<a href="#">6.8</a>	<a href="#">CVE-2019-9587</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	There is an Invalid memory access in gAtomicIncrement() located at GMutex.h in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.	2019-03-06	<a href="#">6.8</a>	<a href="#">CVE-2019-9588</a> <a href="#">MISC</a> <a href="#">MISC</a>
glyphandcog -- xpdfreader	There is a NULL pointer dereference vulnerability in PSOutputDev::setupResources() located in PSOutputDev.cc in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.	2019-03-06	<a href="#">6.8</a>	<a href="#">CVE-2019-9589</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnome -- gdk-pixbuf	GdkPixBuf (aka gdk-pixbuf), possibly 2.32.2, as used by GNOME Nautilus 3.14.3 on Ubuntu 16.04, allows attackers to cause a denial of service (stack corruption) or possibly have unspecified other impact via a crafted file folder.	2019-03-07	<a href="#">6.8</a>	<a href="#">CVE-2017-12447</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- binutils	The aout_32_swap_std_reloc_out function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils before 2.31, allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted file, as demonstrated by objcopy.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2018-14038</a> <a href="#">MISC</a> <a href="#">MISC</a>
golang -- go	Go through 1.12 on Windows misuses certain LoadLibrary functionality, leading to DLL njection.	2019-03-08	<a href="#">6.8</a>	<a href="#">CVE-2019-9634</a> <a href="#">MISC</a>
hyphp -- hybbs	An issue was found in HYBBS through 2016-03-08. There is an XSS vulnerability via an article title to post.html.	2019-03-07	<a href="#">4.3</a>	<a href="#">CVE-2018-14499</a> <a href="#">MISC</a>
ibm -- cloud_private	BM Cloud Private 3.1.1 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 153319.	2019-03-05	<a href="#">5.8</a>	<a href="#">CVE-2018-1939</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- infosphere_information_governance_catalog	BM InfoSphere Information Governance Catalog 11.3, 11.5, and 11.7 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 151639.	2019-03-05	<a href="#">5.8</a>	<a href="#">CVE-2018-1875</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
				<a href="#">CVE-2019-4063</a>

ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 Standard Edition could allow highly sensitive information to be transmitted in plain text. An attacker could obtain this information using man in the middle techniques. IBM X-ForceID: 157008.	2019-03-05	4.3	<a href="#">CVE-2019-17175</a> MISC
imagemagick -- imagemagick	n ImageMagick before 7.0.8-25, some memory leaks exist in DecodeImage in coders/pcd.c.	2019-03-07	5.0	<a href="#">CVE-2018-17429</a> MISC
jtbc -- jtbc	console/account/manage.php?type=action&action=add in JTBC v3.0(C) has CSRF for adding an administrator account.	2019-03-07	6.8	<a href="#">CVE-2018-14498</a> MISC
libjpeg-turbo -- libjpeg-turbo	get_8bit_row in rdbmp.c in libjpeg-turbo through 1.5.90 and MozJPEG through 3.3.1 allows attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the color indices is out of range for the number of palette entries.	2019-03-07	4.3	<a href="#">CVE-2019-9213</a> MISC
linux -- linux_kernel	n the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, which makes it easier for attackers to exploit kernel NULL pointer dereferences on non-SMAP platforms. This is related to a capability check for the wrong task.	2019-03-05	4.9	<a href="#">CVE-2019-0657</a> MISC
medical_store_script_project -- medical_store_script	PHP Scripts Mall Medical Store Script 3.0.3 allows Path Traversal by navigating to the parent directory of a jpg or png file.	2019-03-06	5.0	<a href="#">CVE-2019-0649</a> MISC
microsoft -- .net_core	A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's, aka '.NET Framework and Visual Studio Spoofing Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0658</a> MISC
microsoft -- chakracore	A vulnerability exists in Microsoft Chakra JIT server, aka 'Scripting Engine Elevation of Privileged Vulnerability'.	2019-03-05	6.8	<a href="#">CVE-2019-0641</a> MISC
microsoft -- chakracore	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0648.	2019-03-05	4.3	<a href="#">CVE-2019-0643</a> MISC
microsoft -- edge	A security feature bypass vulnerability exists in Microsoft Edge handles whitelisting, aka Microsoft Edge Security Feature Bypass Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0654</a> MISC
microsoft -- edge	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0669</a> MISC
microsoft -- edge	An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the user's computer or data.To exploit the vulnerability, an attacker must know the memory address of where the object was created.The update addresses the vulnerability by changing he way certain functions handle objects in memory, aka Scripting Engine Information Disclosure Vulnerability. This CVE ID is unique from CVE-2019-0658.	2019-03-05	4.3	<a href="#">CVE-2019-0676</a> MISC
microsoft -- edge	A spoofing vulnerability exists when Microsoft browsers improperly handles specific redirects, aka 'Microsoft Browser Spoofing Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0741</a> MISC
microsoft -- excel	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0627</a> MISC
microsoft -- excel_viewer	A security feature bypass vulnerability exists when Microsoft Office does not validate URLs.An attacker could send a victim a specially crafted file, which could trick the victim into entering credentials, aka 'Microsoft Office Security Feature Bypass Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0631</a> MISC
microsoft -- exchange_server	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0724.	2019-03-05	5.8	<a href="#">CVE-2019-0632</a> MISC
microsoft -- internet_explorer	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory.An attacker who successfully exploited this vulnerability could test for the presence of files on disk, aka 'Internet Explorer Information Disclosure Vulnerability'.	2019-03-05	4.3	<a href="#">CVE-2019-0668</a> MISC
microsoft -- java_software_development_kit	An information disclosure vulnerability exists in the way Azure IoT Java SDK logs sensitive nformation, aka 'Azure IoT Java SDK Information Disclosure Vulnerability'.	2019-03-05	5.0	<a href="#">CVE-2019-0670</a> MISC
microsoft -- powershell_core	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0631, CVE-2019-0632.	2019-03-05	4.6	<a href="#">CVE-2019-0602</a> MISC
microsoft -- powershell_core	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0632.	2019-03-05	4.6	<a href="#">CVE-2019-0615</a> MISC
microsoft -- powershell_core	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0631.	2019-03-05	4.6	<a href="#">CVE-2019-0616</a> MISC
microsoft -- sharepoint_enterprise_server	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'.	2019-03-05	6.5	<a href="#">CVE-2019-0637</a> MISC
microsoft -- sharepoint_enterprise_server	A spoofing vulnerability exists in Microsoft SharePoint when the application does not properly parse HTTP content, aka 'Microsoft SharePoint Spoofing Vulnerability'.	2019-03-05	5.8	<a href="#">CVE-2019-0602</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0615</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0616</a> MISC
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0619</a> MISC
microsoft -- windows_10	A security feature bypass vulnerability exists when Windows Defender Firewall incorrectly applies firewall profiles to cellular network connections, aka 'Windows Defender Firewall Security Feature Bypass Vulnerability'.	2019-03-05	5.0	<a href="#">CVE-2019-0637</a> MISC

microsoft -- windows_10	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'.	2019-03-05	6.9	<a href="#">CVE-2019-0656</a> BID CONFIRM
microsoft -- windows_10	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'.	2019-03-05	4.4	<a href="#">CVE-2019-0659</a> BID CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0664.	2019-03-05	4.3	<a href="#">CVE-2019-0660</a> BID CONFIRM
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660.	2019-03-05	4.3	<a href="#">CVE-2019-0664</a> BID CONFIRM
mitel -- connect_onsite	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE before 19.49.1500.0 allows remote attackers to inject arbitrary web script or HTML via the brandUrl parameter.	2019-03-06	4.3	<a href="#">CVE-2019-9591</a> MISC
mitel -- connect_onsite	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE 19.45.1602.0 allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2019-03-06	4.3	<a href="#">CVE-2019-9592</a> MISC
mitel -- connect_onsite	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE 18.82.2000.0 allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2019-03-06	4.3	<a href="#">CVE-2019-9593</a> MISC
monstra -- monstra	Monstra CMS 3.0.4 allows remote attackers to execute arbitrary PHP code via a mixed-case file extension, as demonstrated by the 123.Php filename, because plugins/box/filesmanager/filesmanager.admin.php mishandles the forbidden_types variable.	2019-03-07	6.5	<a href="#">CVE-2018-17418</a> MISC
moxa -- eds-405a_firmware	Moxa IKS and EDS store plaintext passwords, which may allow sensitive information to be read by someone with access to the device.	2019-03-05	5.0	<a href="#">CVE-2019-6518</a> BID MISC
moxa -- eds-405a_firmware	Moxa IKS and EDS does not properly check authority on server side, which results in a read-only user being able to perform arbitrary configuration changes.	2019-03-05	5.0	<a href="#">CVE-2019-6520</a> BID MISC
moxa -- eds-405a_firmware	Moxa IKS and EDS do not implement sufficient measures to prevent multiple failed authentication attempts, which may allow an attacker to discover passwords via brute force attack.	2019-03-05	5.0	<a href="#">CVE-2019-6524</a> BID MISC
moxa -- eds-405a_firmware	Moxa IKS and EDS allow remote authenticated users to cause a denial of service via a specially crafted packet, which may cause the switch to crash.	2019-03-05	4.0	<a href="#">CVE-2019-6559</a> BID MISC
moxa -- eds-405a_firmware	Cross-site request forgery has been identified in Moxa IKS and EDS, which may allow for the execution of unauthorized actions on the device.	2019-03-05	6.8	<a href="#">CVE-2019-6561</a> BID MISC
moxa -- eds-405a_firmware	Moxa IKS and EDS fails to properly validate user input, giving unauthenticated and authenticated attackers the ability to perform XSS attacks, which may be used to send a malicious script.	2019-03-05	4.3	<a href="#">CVE-2019-6565</a> BID MISC
netgate -- pfsense	n pfSense 2.4.4_1, blocking of source IP addresses on the basis of failed HTTPS authentication is inconsistent with blocking of source IP addresses on the basis of failed SSH authentication (the behavior does not match the sshguard documentation), which might make it easier for attackers to bypass intended access restrictions.	2019-03-01	5.0	<a href="#">CVE-2018-20799</a> MISC
njiandan-cms_project -- njiandan-cms	njiandan-cms through 2013-05-23 has index.php/admin/user_new CSRF to add an administrator.	2019-03-07	6.8	<a href="#">CVE-2019-8437</a> MISC
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 allows a remote, unauthenticated attacker to enable telnetd on the router via a crafted HTTP request.	2019-03-05	5.0	<a href="#">CVE-2019-3917</a> MISC
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to command injection via crafted HTTP request sent by a remote, authenticated attacker to /GponForm/usb_restore_Form?script/.	2019-03-05	6.5	<a href="#">CVE-2019-3919</a> MISC
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to authenticated command injection via crafted HTTP request sent by a remote, authenticated attacker to /GponForm/device_Form?script/.	2019-03-05	6.5	<a href="#">CVE-2019-3920</a> MISC
nokia -- i-240w-q_gpon_ont_firmware	The Alcatel Lucent I-240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to a stack buffer overflow via crafted HTTP POST request sent by a remote, authenticated attacker to /GponForm/usb_Form?script/. An attacker can leverage this vulnerability to potentially execute arbitrary code.	2019-03-05	6.5	<a href="#">CVE-2019-3921</a> EXPLOIT-DB MISC
phome -- empirecms	EmpireCMS 7.5 allows CSRF for adding a user account via an enews=AddUser action to e/admin/user/ListUser.php, a similar issue to CVE-2018-16339.	2019-03-07	6.8	<a href="#">CVE-2018-18449</a> MISC
phpmywind -- phpmywind	An issue was discovered in PHPMyWind 5.5. The username parameter of the install/index.php page has a stored Cross-site Scripting (XSS) vulnerability, as demonstrated by admin/login.php.	2019-03-07	4.3	<a href="#">CVE-2019-7660</a> MISC
phpmywind -- phpmywind	An issue was discovered in PHPMyWind 5.5. The method parameter of the data/api/oauth/connect.php page has a reflected Cross-site Scripting (XSS) vulnerability.	2019-03-07	4.3	<a href="#">CVE-2019-7661</a> MISC
popojicms -- popojicms	An issue was discovered in PopojiCMS v2.0.1. It has CSRF via the po-admin/route.php?mod=user&act=addnew URI, as demonstrated by adding a level=1 account, a similar issue to CVE-2018-18935.	2019-03-03	6.8	<a href="#">CVE-2019-9549</a> MISC
psigridconnect -- iec104_security_proxy_firmware	PSI GridConnect GmbH Telecontrol Gateway and Smart Telecontrol Unit family, IEC104 Security Proxy versions Telecontrol Gateway 3G Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway XS-MU Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway VM Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Smart Telecontrol Unit TCG Versions 5.0.27, 5.1.19, 6.0.16 and prior, and IEC104 Security Proxy Version 2.2.10 and prior The web application browser interprets input as active HTML, JavaScript, or VBScript, which could allow an attacker to execute arbitrary code.	2019-03-05	6.5	<a href="#">CVE-2019-6528</a> BID MISC
quizandsurveymaster -- quiz_and_survey_master	The Quiz And Survey Master plugin 6.0.4 for WordPress allows wp-admin/admin.php?page=mlw_quiz_results quiz_id XSS.	2019-03-05	4.3	<a href="#">CVE-2019-9575</a> MISC MISC MISC MISC
sagemcom -- f@st_5260_firmware	Sagemcom F@st 5260 routers using firmware version 0.4.39, in WPA mode, default to using a PSK that is generated from a 2-part wordlist of known values and a nonce with insufficient entropy. The number of possible PSKs is about 1.78 billion, which is too small.	2019-03-05	5.0	<a href="#">CVE-2019-9555</a> MISC
samba -- samba	A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.	2019-03-06	4.0	<a href="#">CVE-2019-3824</a> CONFIRM MISC MLIST CONFIRM UBUNTU DEBIAN
schoolcms -- schoolcms	SchoolCMS version 2.3.1 allows file upload via the theme upload feature at admin.php?m=admin&c=theme&a=upload by using the .zip extension along with the .Static substring, changing the Content-Type to application/zip, and placing PHP code after the ZIP header. This ultimately allows execution of arbitrary PHP code in PublicHome_Static.php because of mishandling in the Application\Admin\Controller\ThemeController.class.php Upload() function.	2019-03-05	6.5	<a href="#">CVE-2019-9572</a> MISC
simplemachines -- simple_machines_forum	Simple Machines Forum (SMF) 2.0.4 allows XSS via the index.php?action=pm;sa=settings;save sa parameter.	2019-03-07	4.3	<a href="#">CVE-2013-7467</a> MISC

simplemachines -- simple_machines_forum	Simple Machines Forum (SMF) 2.0.4 allows PHP Code Injection via the index.php? action=admin;area=languages;sa=editlang dictionary parameter.	2019-03-07	6.8	<a href="#">CVE-2013-7468</a> MISC
spdk -- storage_performance_development_kit	n Storage Performance Development Kit (SPDK) before 19.01, a malicious vhost client (i.e., virtual machine) could carefully construct a circular descriptor chain that would result in a partial denial of service in the SPDK vhost target, because the vhost target did not properly detect such chains.	2019-03-01	5.0	<a href="#">CVE-2019-9547</a> CONFIRM CONFIRM
tengcon -- t-920_plc_firmware	An issue was discovered on TENGCONTROL T-920 PLC v5.5 devices. It allows remote attackers to cause a denial of service (persistent failure mode) by sending a series of x19\x00\x00\x00\x06\x43\x01\x00\xac\xff\x00 (aka UID 0x43) requests to TCP port 502.	2019-03-06	5.0	<a href="#">CVE-2019-9590</a> MISC
theolivetree -- ftp_server	The Olive Tree FTP Server (aka com.theolivetree.ftpsrv) application through 1.32 for Android allows remote attackers to cause a denial of service via a client that makes many connection attempts and drops certain packets.	2019-03-06	5.0	<a href="#">CVE-2019-9600</a> EXPLOIT-DB MISC
ucms_project -- ucms	An issue was discovered in UCMS 1.4.6. There is XSS in the title bar, as demonstrated by a do=list request.	2019-03-07	4.3	<a href="#">CVE-2018-16804</a> MISC
webmin -- webmin	Webmin 1.900 allows remote attackers to execute arbitrary code by leveraging the "Java file manager" and "Upload and Download" privileges to upload a crafted .cgi file via the updown/upload.cgi URI.	2019-03-07	6.8	<a href="#">CVE-2019-9624</a> MISC EXPLOIT-DB
yaml-cpp_project -- yaml-cpp	The SingleDocParser::HandleFlowSequence function in yaml-cpp (aka LibYaml-C++) 0.6.2 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted YAML file.	2019-03-07	4.3	<a href="#">CVE-2018-20710</a> MISC
zrlog -- zrlog	An issue was discovered in ZrLog 2.0.3. There is a SQL injection vulnerability in the article management search box via the keywords parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17420</a> MISC
zrlog -- zrlog	An issue was discovered in ZrLog 2.0.3. There is stored XSS in the file upload area via a crafted attached/file/ pathname.	2019-03-07	4.3	<a href="#">CVE-2018-17421</a> MISC
zyxel -- nbg-418n_firmware	Zyxel NBG-418N v2 v1.00(AAXM.4)C0 devices allow login.cgi CSRF.	2019-03-07	6.8	<a href="#">CVE-2019-6710</a> MISC MISC EXPLOIT-DB
zzcms -- zzcms	XSS exists in zzcms v8.3 via the /uploadimg_form.php noshuiyin parameter.	2019-03-07	4.3	<a href="#">CVE-2018-17413</a> MISC
zzcms -- zzcms	zzcms v8.3 has a SQL injection in /user/jobmanage.php via the bigclass parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17414</a> MISC
zzcms -- zzcms	zzcms V8.3 has a SQL injection in /user/zs_elite.php via the id parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17415</a> MISC
zzcms -- zzcms	A SQL injection vulnerability exists in zzcms v8.3 via the /admin/adclass.php bigclassid parameter.	2019-03-07	6.5	<a href="#">CVE-2018-17416</a> MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cisco -- nx-os	A vulnerability in the Cisco Nexus 9000 Series Fabric Switches running in Application-Centric Infrastructure (ACI) mode could allow an authenticated, local attacker to read arbitrary files on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms of user-supplied input sent to an affected device. A successful exploit could allow the attacker unauthorized access to read arbitrary files on an affected device. This vulnerability has been fixed in version 14.0(1h).	2019-03-06	2.1	<a href="#">CVE-2019-1588</a> BID CISCO
dhcms_project -- dhcms	DhCms through 2017-09-18 has admin.php?r=admin/Index/index XSS.	2019-03-03	3.5	<a href="#">CVE-2019-9550</a> MISC
dilicms -- dilicms	An issue was discovered in DilicMS 2.4.0. There is a Stored XSS Vulnerability in the first extbox of "System setting->site setting" of admin/index.php, aka site_name.	2019-03-07	3.5	<a href="#">CVE-2019-8438</a> MISC
dilicms -- dilicms	An issue was discovered in DilicMS 2.4.0. There is a Stored XSS Vulnerability in the second extbox of "System setting->site setting" of admin/index.php, aka site_domain.	2019-03-07	3.5	<a href="#">CVE-2019-8439</a> MISC
dilicms -- dilicms	An issue was discovered in DilicMS 2.4.0. There is a Stored XSS Vulnerability in the third extbox (aka site logo) of "System setting->site setting" of admin/index.php, aka site_logo.	2019-03-07	3.5	<a href="#">CVE-2019-8440</a> MISC
ibm -- cloud_private	BM Cloud Private 3.1.1 could allow a local user with administrator privileges to intercept highly sensitive unencrypted data. IBM X-Force ID: 153317.	2019-03-05	2.1	<a href="#">CVE-2018-1937</a> BID XF CONFIRM
ibm -- cloud_private	BM Cloud Private 3.1.1 could allow a local user with administrator privileges to intercept highly sensitive unencrypted data. IBM X-Force ID: 153318.	2019-03-05	2.1	<a href="#">CVE-2018-1938</a> BID XF CONFIRM
ibm -- infosphere_information_governance_catalog	BM InfoSphere Information Server 11.3, 11.5, and 11.7 could allow an attacker to change one of the settings related to InfoSphere Business Glossary Anywhere due to improper access control. IBM X-Force ID: 152528.	2019-03-05	3.3	<a href="#">CVE-2018-1899</a> CONFIRM XF
ibm -- rational_doors_next_generation	BM DOORS Next Generation (DNG/RR) 5.0 through 5.0.2 and 6.0 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152735.	2019-03-06	3.5	<a href="#">CVE-2018-1911</a> CONFIRM XF
ibm -- rational_doors_next_generation	BM DOORS Next Generation (DNG/RR) 6.0.2 through 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152736.	2019-03-06	3.5	<a href="#">CVE-2018-1912</a> CONFIRM XF
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-ForceID: 155905.	2019-03-05	3.5	<a href="#">CVE-2019-4027</a> BID XF CONFIRM
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 155906.	2019-03-05	3.5	<a href="#">CVE-2019-4028</a> BID XF CONFIRM
ibm -- sterling_b2b_integrator	BM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 155907.	2019-03-05	3.5	<a href="#">CVE-2019-4029</a> BID XF CONFIRM
ibm -- websphere_application_server	BM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. BM X-Force ID: 155946.	2019-03-06	3.5	<a href="#">CVE-2019-4030</a> CONFIRM XF
microsoft -- team_foundation_server	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0743.	2019-03-05	3.5	<a href="#">CVE-2019-0742</a> BID CONFIRM
	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not			<a href="#">CVE-2019-0743</a>



microsoft -- team_foundation_server	properly sanitize user provided input, aka 'Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0742.	2019-03-05	3.5	<a href="#">BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0601.	2019-03-05	1.9	<a href="#">CVE-2019-0600 BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0600.	2019-03-05	1.9	<a href="#">CVE-2019-0601 BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661, CVE-2019-0663.	2019-03-05	2.1	<a href="#">CVE-2019-0621 BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'.	2019-03-05	2.1	<a href="#">CVE-2019-0628 BID CONFIRM</a>
microsoft -- windows_10	An information vulnerability exists when Windows improperly discloses file information, aka 'Windows Information Disclosure Vulnerability'.	2019-03-05	2.1	<a href="#">CVE-2019-0636 BID CONFIRM</a>
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0661.	2019-03-05	2.1	<a href="#">CVE-2019-0663 BID CONFIRM</a>
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663.	2019-03-05	2.1	<a href="#">CVE-2019-0661 BID CONFIRM</a>
personal_video_collection_script_project -- personal_video_collection_script	PHP Scripts Mall Personal Video Collection Script 4.0.4 has Stored XSS via the "Update profile" feature.	2019-03-06	3.5	<a href="#">CVE-2019-9806 MISC</a>
pivotal_software -- operations_manager	Pivotal Operations Manager, 2.1.x versions prior to 2.1.20, 2.2.x versions prior to 2.2.16, 2.3.x versions prior to 2.3.10, 2.4.x versions prior to 2.4.3, contains a reflected cross site scripting vulnerability. A remote user that is able to convince an Operations Manager user to interact with malicious content could execute arbitrary JavaScript in the user's browser.	2019-03-07	3.5	<a href="#">CVE-2019-3776 CONFIRM</a>
vanillaforums -- vanilla_forums	Multiple stored XSS in Vanilla Forums before 2.5 allow remote attackers to inject arbitrary JavaScript code into any message on forum.	2019-03-01	3.5	<a href="#">CVE-2019-8279 MISC</a>
wdoyo -- doyocms	An issue was discovered in DOYO (aka doyocms) 2.3 through 2015-05-06. It has admin.php XSS.	2019-03-03	3.5	<a href="#">CVE-2019-9551 MISC</a>
wuzhicms -- wuzhi_cms	WUZHI CMS 4.1.0 has stored XSS via the "Membership Center" "I want to ask" "detailed description" field under the index.php?m=member URI.	2019-03-07	3.5	<a href="#">CVE-2018-17425 MISC</a>
wuzhicms -- wuzhi_cms	WUZHI CMS 4.1.0 has stored XSS via the "Extension module" "SMS in station" field under the index.php?m=core URI.	2019-03-07	3.5	<a href="#">CVE-2018-17426 MISC</a>
yzmcms -- yzmcms	An issue was discovered in YzmCMS 5.2.0. It has XSS via the bottom text field to the admin/system_manage/save.html URI, related to the site_code parameter.	2019-03-05	3.5	<a href="#">CVE-2019-9570 MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- solr	Server Side Request Forgery in Apache Solr, versions 1.3 until 7.6 (inclusive). Since the "shards" parameter does not have a corresponding whitelist mechanism, a remote attacker with access to the server could make Solr perform an HTTP GET request to any reachable URL.	2019-03-08	not yet calculated	<a href="#">CVE-2017-3164 MLIST BID</a>
apple -- multiple_products	A memory corruption issue was addressed with improved lock state checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in memory shared between processes.	2019-03-05	not yet calculated	<a href="#">CVE-2019-6205 BID CONFIRM CONFIRM EXPLOIT-DB</a>
apple -- multiple_products	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may be able to elevate privileges.	2019-03-05	not yet calculated	<a href="#">CVE-2019-6225 BID CONFIRM CONFIRM EXPLOIT-DB</a>
apple -- multiple_products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to execute arbitrary code with kernel privileges.	2019-03-05	not yet calculated	<a href="#">CVE-2019-6210 BID CONFIRM CONFIRM CONFIRM</a>
atlassian -- sourcetree_for_macos	There was an argument injection vulnerability in Atlassian Sourcetree for macOS from version 1.2 before version 3.1.1 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for macOS is able to exploit this issue to gain code execution on the system.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20234 CONFIRM</a>
atlassian -- sourcetree_for_windows	There was an argument injection vulnerability in Atlassian Sourcetree for Windows from version 0.5a before version 3.0.15 via filenames in Mercurial repositories. A remote attacker with permission to commit to a Mercurial repository linked in Sourcetree for Windows is able to exploit this issue to gain code execution on the system.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20235 CONFIRM</a>
atlassian -- sourcetree_for_windows	There was a command injection vulnerability in Sourcetree for Windows from version 0.5a before version 3.0.10 via URI handling. A remote attacker could send a malicious URI to a victim using Sourcetree for Windows to exploit this issue to gain code execution on the system.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20236 CONFIRM</a>
botan -- botan	A side-channel issue was discovered in Botan before 2.9.0. An attacker capable of precisely measuring the time taken for ECC key generation may be able to derive information about the high bits of the secret key, as the function to derive the public point from the secret scalar uses an unblinded Montgomery ladder whose loop iteration count depends on the bitlength of the secret. This issue affects only key generation, not ECDSA signatures or ECDH key agreement.	2019-03-08	not yet calculated	<a href="#">CVE-2018-20187 MISC MISC MISC</a>
	Multiple vulnerabilities in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco FXOS Software and Cisco NX-OS Software could allow an			

cisco -- fxos_and_cisco_nx_os_software	unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets by an affected device. An attacker could exploit these vulnerabilities by sending an LDAP packet crafted using Basic Encoding Rules (BER) to an affected device. The LDAP packet must have a source IP address of an LDAP server configured on the targeted device. A successful exploit could cause the affected device to reload, resulting in a DoS condition. Firepower 4100 Series Next-Generation Firewalls are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. Firepower 9300 Security Appliances are affected in versions prior to 2.0.1.201, 2.2.2.54 and 2.3.1.75. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.2(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(2). Nexus 7000 and 7700 Series Switches are affected in versions prior to 8.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(1). Cisco UCS 6200 and 6300 Fabric Interconnect devices are affected in versions prior to 3.2(2b).	2019-03-07	not yet calculated	<a href="#">CVE-2019-1597</a> <a href="#">CISCO</a>
cisco -- fxos_software_and_cisco_nx_os_software	Multiple vulnerabilities in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets by an affected device. An attacker could exploit these vulnerabilities by sending an LDAP packet crafted using Basic Encoding Rules (BER) to an affected device. The LDAP packet must have a source IP address of an LDAP server configured on the targeted device. A successful exploit could cause the affected device to reload, resulting in a DoS condition. Firepower 4100 Series Next-Generation Firewalls are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. Firepower 9300 Security Appliances are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.2(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(2). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(20), 7.3(2)D1(1), and 8.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(1). UCS 6200 and 6300 Fabric Interconnect are affected in versions prior to 3.2(2b).	2019-03-07	not yet calculated	<a href="#">CVE-2019-1598</a> <a href="#">CISCO</a>
cisco -- nexus_9000_series_aci_mode_switch_software	A vulnerability in the controller authorization functionality of Cisco Nexus 9000 Series ACI Mode Switch Software could allow an authenticated, local attacker to escalate standard users with root privilege on an affected device. The vulnerability is due to a misconfiguration of certain sudoers files for the bashroot component on an affected device. An attacker could exploit this vulnerability by authenticating to the affected device with a crafted user ID, which may allow temporary administrative access to escalate privileges. A successful exploit could allow the attacker to escalate privileges on an affected device. This Vulnerability has been fixed in version 4.0(1h)	2019-03-06	not yet calculated	<a href="#">CVE-2019-1585</a> <a href="#">BJD</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(2). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(6). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(6). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), 8.2(3), and 8.3(2). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1609</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid user credentials to exploit this vulnerability. Nexus 3000, 3500, and Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1606</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the network stack of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. The vulnerability is due to an issue with allocating and freeing memory buffers in the network stack. An attacker could exploit this vulnerability by sending crafted TCP streams to an affected device in a sustained way. A successful exploit could cause the network stack of an affected device to run out of available buffers, impairing operations of control plane and management plane protocols, resulting in a DoS condition. Note: This vulnerability can be triggered only by traffic that is destined to an affected device and cannot be exploited using traffic that transits an affected device. Nexus 1000V Switch for Microsoft Hyper-V is affected in versions prior to 5.2(1)SM3(2.1). Nexus 1000V Switch for VMware vSphere is affected in versions prior to 5.2(1)SV3(4.1a). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(6) and 9.2(2). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(11), 7.0(3)I7(6), and 9.2(2). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5) and 9.2(2). Nexus 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(5)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5) and 9.2(2). UCS 6200 and 6300 Series Fabric Interconnect are affected in versions prior to 3.2(3j) and 4.0(2a). UCS 6400 Series Fabric Interconnect are affected in versions prior to 4.0(2a).	2019-03-07	not yet calculated	<a href="#">CVE-2019-1599</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the file system permissions of Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to access sensitive information that is stored in the file system of an affected system. The vulnerability is due to improper implementation of file system permissions. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow the attacker to access sensitive and critical files. Firepower 4100 Series Next-Generation Firewalls are affected in versions prior to 2.2.2.91 and 2.3.1.110. Firepower 9300 Series Next-Generation Firewalls are affected in versions prior to 2.2.2.91 and 2.3.1.110. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(3)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). Nexus 9000 Series Switches- Standalone are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-07	not yet calculated	<a href="#">CVE-2019-1600</a> <a href="#">CISCO</a>
	A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to gain read and write access to a critical configuration file. The vulnerability is due to a failure to impose strict filesystem permissions on the targeted device. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow an attacker to use the content of this configuration			

cisco -- nx-os_software	file to bypass authentication and log in as any user of the device. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(3)D1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1601</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to access sensitive data that could be used to elevate their privileges to administrator. The vulnerability is due to improper implementation of filesystem permissions. An attacker could exploit this vulnerability by logging in to the CLI of an affected device, accessing a specific file, and leveraging this information to authenticate to the NX-API server. A successful exploit could allow an attacker to make configuration changes as administrator. Note: NX-API is disabled by default. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1602</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to escalate lower-level privileges to the administrator level. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated privileges. A successful exploit could allow an attacker to make configuration changes to the system as administrator. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1603</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the user account management interface of Cisco NX-OS Software could allow an authenticated, local attacker to gain elevated privileges on an affected device. The vulnerability is due to an incorrect authorization check of user accounts and their associated Group ID (GID). An attacker could exploit this vulnerability by taking advantage of a logic error that will permit the use of higher privileged commands than what is necessarily assigned. A successful exploit could allow an attacker to execute commands with elevated privileges on the underlying Linux shell of an affected device. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 8.2(3), and 8.3(2). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1604</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary code as root. The vulnerability is due to incorrect input validation in the NX-API feature. An attacker could exploit this vulnerability by sending a crafted HTTP or HTTPS request to an internal service on an affected device that has the NX-API feature enabled. A successful exploit could allow the attacker to cause a buffer overflow and execute arbitrary code as root. Note: The NX-API feature is disabled by default. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.1(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(8) and 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(8). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.3(2)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 7.3(3)D1(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I4(8) and 7.0(3)I7(1). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1605</a> <a href="#">BID</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1608</a> <a href="#">CISCO</a>
cisco -- nx-os_software	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3).	2019-03-08	not yet calculated	<a href="#">CVE-2019-1607</a> <a href="#">CISCO</a>
cloud_foundry -- cli	Cloud Foundry CLI, versions prior to v6.43.0, improperly exposes passwords when verbose/trace/debugging is turned on. A local unauthenticated or remote authenticated malicious user with access to logs may gain part or all of a users password.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3781</a> <a href="#">CONFIRM</a>
cloud_foundry -- container_runtime	Cloud Foundry Container Runtime, versions prior to 0.28.0, deploys K8s worker nodes that contains a configuration file with IAAS credentials. A malicious user with access to the k8s nodes can obtain IAAS credentials allowing the user to escalate privileges to gain access to the IAAS account.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3780</a> <a href="#">CONFIRM</a>
cloud_foundry -- container_runtime	Cloud Foundry Container Runtime, versions prior to 0.29.0, deploys Kubernetes clusters utilize the same CA (Certificate Authority) to sign and trust certs for ETCD as used by the Kubernetes API. This could allow a user authenticated with a cluster to request a signed certificate leveraging the Kubernetes CSR capability to obtain a credential that could escalate privilege access to ETCD.	2019-03-08	not yet calculated	<a href="#">CVE-2019-3779</a> <a href="#">CONFIRM</a>
cloud_foundry -- stratos	Cloud Foundry Stratos, versions prior to 2.3.0, contains an insecure session that can be spoofed. When deployed on cloud foundry with multiple instances using the default embedded SQLite database, a remote authenticated malicious user can switch sessions to another user with the same session id.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3784</a> <a href="#">CONFIRM</a>
cloud_foundry -- stratos	Cloud Foundry Stratos, versions prior to 2.3.0, deploys with a public default session store secret. A malicious user with default session store secret can brute force another user's current Stratos session, and act on behalf of that user.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3783</a> <a href="#">CONFIRM</a>
cloud_foundry -- uaa	Cloud Foundry UAA, versions prior to v70.0, allows a user to update their own email address. A remote authenticated user can impersonate a different user by changing their email address to that of a different user.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3775</a> <a href="#">CONFIRM</a>

cyberark -- endpoint_privilege_manager	A buffer overflow in the kernel driver CybKernelTracker.sys in CyberArk Endpoint Privilege Manager versions prior to 10.7 allows an attacker (without Administrator privileges) to escalate privileges or crash the machine by loading an image, such as a DLL, with a long path.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9627</a> <a href="#">MISC</a>
dell -- wes_wyse_device_agent_and_wyse_thinlinux_hagent	Dell WES Wyse Device Agent versions prior to 14.1.2.9 and Dell Wyse ThinLinux HAgent versions prior to 5.4.55.00.10 contain a buffer overflow vulnerability. An unauthenticated attacker may potentially exploit this vulnerability to execute arbitrary code on the system with privileges of the FTP client by sending specially crafted input data to the affected system. The FTP code that contained the vulnerability has been removed.	2019-03-07	not yet calculated	<a href="#">CVE-2019-3712</a> <a href="#">MISC</a>
druide -- antidote_rx_and_hd	Druide Antidote RX, HD, 8 before 8.05.2287, 9 before 9.5.3937 and 10 before 10.1.2147 allows remote attackers to steal NTLM hashes or perform SMB relay attacks upon a direct launch of the product, or upon an indirect launch via an integration such as Chrome, Firefox, Word, Outlook, etc. This occurs because the product attempts to access a share with the PLUG-INS subdomain name; an attacker may be able to use Active Directory Domain Services to register that name.	2019-03-04	not yet calculated	<a href="#">CVE-2019-9565</a> <a href="#">MISC</a> <a href="#">MISC</a>
eloan -- eloan	Eloan V3.0 through 2018-09-20 allows remote attackers to list files via a direct request to the p2p/api/ or p2p/lib/ or p2p/images/ URI.	2019-03-03	not yet calculated	<a href="#">CVE-2019-9552</a> <a href="#">MISC</a>
esafenet -- cdg	ESAFENET CDG V3 and V5 has an arbitrary file download vulnerability via the fileName parameter in download.jsp because the InstallationPack parameter is mishandled in a /CDGServer3/ClientAjax request.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9632</a> <a href="#">MISC</a>
gnome -- glib	gio/gsocketclient.c in GNOME GLib 2.59.2 does not ensure that a parent GTask remains alive during the execution of a connection-attempting enumeration, which allows remote attackers to cause a denial of service (g_socket_client_connected_callback mishandling and application crash) via a crafted web site, as demonstrated by GNOME Web (aka Epiphany).	2019-03-08	not yet calculated	<a href="#">CVE-2019-9633</a> <a href="#">MISC</a>
golang -- go	An issue was discovered in setTA in scan_rr.go in the Miek Gieben DNS library before 1.0.10 for Go. A dns.ParseZone() parsing error causes a segmentation violation, leading to denial of service.	2019-03-07	not yet calculated	<a href="#">CVE-2018-17419</a> <a href="#">MISC</a>
hashicorp -- consul	HashiCorp Consul (and Consul Enterprise) 1.4.x before 1.4.3 allows a client to bypass intended access restrictions and obtain the privileges of one other arbitrary token within secondary datacenters, because a token with literally "<hidden>" as its secret is used in unusual circumstances.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8336</a> <a href="#">MISC</a>
invision -- power_board	Stored XSS in Invision Power Board versions 3.3.1 - 3.4.8 leads to Remote Code Execution.	2019-03-01	not yet calculated	<a href="#">CVE-2019-8278</a> <a href="#">BID</a> <a href="#">MISC</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Repository Connector Plugin 1.2.4 and earlier in src/main/java/org/jvnet/hudson/plugins/repositoryconnector/ArtifactDeployer.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/Repository.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/UserPwd.java that allows an attacker with local file system access or control of a Jenkins administrator's web browser (e.g. malicious extension) to retrieve the password stored in the plugin configuration.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003038</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Email Extension Plugin 2.64 and earlier in pom.xml, src/main/java/hudson/plugins/emailext/ExtendedEmailPublisher.java, src/main/java/hudson/plugins/emailext/plugins/content/EmailExtScript.java, src/main/java/hudson/plugins/emailext/plugins/content/ScriptContent.java, src/main/java/hudson/plugins/emailext/plugins/trigger/AbstractScriptTrigger.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003032</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in JenkinsAppDynamics Dashboard Plugin 1.0.14 and earlier in src/main/java/nl/codecentric/jenkins/appd/AppDynamicsResultsPublisher.java that allows attackers without permission to obtain passwords configured in jobs to obtain them.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003039</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.53 and earlier in src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/GroovySandbox.java, src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/SecureGroovyScript.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003029</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Pipeline: Groovy Plugin 2.63 and earlier in pom.xml, src/main/java/org/jenkinsci/plugins/workflow/cps/CpsGroovyShell.java that allows attackers able to control pipeline scripts to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003030</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Matrix Project Plugin 1.13 and earlier in pom.xml, src/main/java/hudson/matrix/FilterScript.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003031</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Groovy Plugin 2.1 and earlier in pom.xml, src/main/java/hudson/plugins/groovy/StringScriptSource.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003033</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Jenkins Job DSL Plugin 1.71 and earlier in jobdsl-core/src/main/groovy/javaposse/jobdsl/dsl/AbstractDslScriptLoader.groovy, jobdsl-plugin/build.gradle, jobdsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/JobDslWhitelist.groovy, jobdsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/SandboxDslScriptLoader.groovy that allows attackers with control over Job DSL definitions to execute arbitrary code on the Jenkins master JVM.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003034</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgentTemplate.java, src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to perform the 'verify configuration' form validation action, thereby obtaining limited information about the Azure configuration.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003035</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A data modification vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMAgent.java that allows attackers with Overall/Read permission to attach a public IP address to an Azure VM agent.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003036</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2019-03-08	not yet calculated	<a href="#">CVE-2019-1003037</a> <a href="#">CONFIRM</a>
microsoft -- azure_iot_java_sdk	An Elevation of Privilege vulnerability exists in the way Azure IoT Java SDK generates symmetric keys for encryption, allowing an attacker to predict the randomness of the key, aka 'Azure IoT Java SDK Elevation of Privilege Vulnerability'.	2019-03-05	not yet calculated	<a href="#">CVE-2019-0729</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

microsoft -- windows_hyber-v	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka "Windows Hyper-V Information Disclosure Vulnerability".	2019-03-05	not yet calculated	<a href="#">CVE-2019-0635</a> <a href="#">BID CONFIRM</a>
netapp -- snapcenter	NetApp SnapCenter Server prior to 4.1 does not set the secure flag for a sensitive cookie in an HTTPS session which can allow the transmission of the cookie in plain text over an unencrypted channel.	2019-03-04	not yet calculated	<a href="#">CVE-2018-5482</a> <a href="#">BID CONFIRM</a>
netapp -- snapcenter_server	NetApp SnapCenter Server prior to 4.0 is susceptible to cross site scripting vulnerability that could allow a privileged user to inject arbitrary scripts into the custom secondary policy label field.	2019-03-04	not yet calculated	<a href="#">CVE-2017-15515</a> <a href="#">BID CONFIRM</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. It allows admin/system/generate/create?sql= SQL injection, related to SystemGenerateController.java.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9615</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadFile URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9617</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadScrawl URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9616</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. It allows admin/cms/template/getTemplates.html?res_path=res directory traversal, with ../ in the dir parameter, to write arbitrary content (in the file_content parameter) into an arbitrary file (specified by the file_name parameter). This is related to the save function in TemplateController.java.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9611</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. A command execution vulnerability exists via a template file with <#assign ex="freemarker.template.utility.Execute"?new(> \${ ex(" followed by the command.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9614</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadVideo URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9613</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/conn/service/upload URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9612</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/conn/service/editUploadImage URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9609</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. It has admin/cms/template/getTemplates.html?res_path=res&up_dir=../ directory traversal, related to the getTemplates function in TemplateController.java.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9610</a> <a href="#">MISC</a>
ofcms -- ofcms	An issue was discovered in OFCMS before 1.1.3. Remote attackers can execute arbitrary code because blocking of .jsp and .jspx files does not consider (for example) file.jsp::\$DATA to the admin/ueditor/uploadImage URI.	2019-03-06	not yet calculated	<a href="#">CVE-2019-9608</a> <a href="#">MISC</a>
openssl -- openssl	ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539 specifies that the nonce value (IV) should be 96 bits (12 bytes). OpenSSL allows a variable nonce length and front pads the nonce with 0 bytes if it is less than 12 bytes. However it also incorrectly allows a nonce to be set of up to 16 bytes. In this case only the last 12 bytes are significant and any additional leading bytes are ignored. It is a requirement of using this cipher that nonce values are unique. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. If an application changes the default nonce length to be longer than 12 bytes and then makes a change to the leading bytes of the nonce expecting the new value to be a new unique nonce then such an application could inadvertently encrypt messages with a reused nonce. Additionally the ignored bytes in a long nonce are not covered by the integrity guarantee of this cipher. Any application that relies on the integrity of these ignored leading bytes of a long nonce may be further affected. Any OpenSSL internal use of this cipher, including in SSL/TLS, is safe because no such use sets such a long nonce value. However user applications that use this cipher directly and set a non-default nonce length to be longer than 12 bytes may be vulnerable. OpenSSL versions 1.1.1 and 1.1.0 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1c-dev (Affected 1.1.1-1.1.1b). Fixed in OpenSSL 1.1.0k-dev (Affected 1.1.0-1.1.0j).	2019-03-06	not yet calculated	<a href="#">CVE-2019-1543</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9638</a> <a href="#">MISC</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9639</a> <a href="#">MISC</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9640</a> <a href="#">MISC</a>
php -- php	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9641</a> <a href="#">MISC</a>
php -- php	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9637</a> <a href="#">MISC</a>
pivotal -- application_service	Pivotal Application Service (PAS), versions 2.2.x prior to 2.2.12, 2.3.x prior to 2.3.7 and 2.4.x prior to 2.4.3, contain apps manager that uses a cloud controller proxy that fails to verify SSL certs. A remote unauthenticated attacker that could hijack the Cloud Controller's DNS record could intercept access tokens sent to the Cloud Controller, giving the attacker access to the user's resources in the Cloud Controller	2019-03-07	not yet calculated	<a href="#">CVE-2019-3777</a> <a href="#">BID CONFIRM</a>



pivotal -- spring_security_oauth	Spring Security OAuth, versions 2.3 prior to 2.3.5, and 2.2 prior to 2.2.4, and 2.1 prior to 2.1.4, and 2.0 prior to 2.0.17, and older unsupported versions could be susceptible to an open redirector attack that can leak an authorization code. A malicious user or attacker can craft a request to the authorization endpoint using the authorization code grant type, and specify a manipulated redirection URI via the "redirect_uri" parameter. This can cause the authorization server to redirect the resource owner user-agent to a URI under the control of the attacker with the leaked authorization code. This vulnerability exposes applications that meet all of the following requirements: Act in the role of an Authorization Server (e.g. @EnableAuthorizationServer) and uses the DefaultRedirectResolver in the AuthorizationEndpoint. This vulnerability does not expose applications that: Act in the role of an Authorization Server and uses a different RedirectResolver implementation other than DefaultRedirectResolver, act in the role of a Resource Server only (e.g. @EnableResourceServer), act in the role of a Client only (e.g. @EnableOAuthClient).	2019-03-07	not yet calculated	<a href="#">CVE-2019-3778</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	not yet calculated	<a href="#">CVE-2018-4054</a> <a href="#">MISC</a>
pixar -- renderman	A local privilege escalation vulnerability exists in the Mac OS X version of Pixar Renderman 22.3.0's Install Helper helper tool. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine for a successful exploit.	2019-03-08	not yet calculated	<a href="#">CVE-2019-5015</a> <a href="#">MISC</a>
pixar -- renderman	A local privilege escalation vulnerability exists in the install helper tool of the Mac OS X version of Pixar Renderman, version 22.2.0. A user with local access can use this vulnerability to read any root file from the file system. An attacker would need local access to the machine to successfully exploit this flaw.	2019-03-08	not yet calculated	<a href="#">CVE-2018-4055</a> <a href="#">MISC</a>
python -- python	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9636</a> <a href="#">MISC</a> <a href="#">MISC</a>
rainbow_pdf -- office_server_document_converter	A heap overflow vulnerability exists in the PowerPoint document conversion function of Rainbow PDF Office Server Document Converter V7.0 Pro R1 (7.0.2018.1113). While parsing Document Summary Property Set stream, the getSummaryInformation function is incorrectly checking the correlation between size and the number of properties in PropertySet packets, causing an out-of-bounds write that leads to heap corruption and consequent code execution.	2019-03-07	not yet calculated	<a href="#">CVE-2019-5019</a> <a href="#">MISC</a>
simple_machines -- simple_machines_forum	Simple Machines Forum (SMF) 2.0.4 allows local file inclusion, with resultant remote code execution, in install.php via ../directory traversal in the db_type parameter if install.php remains present after installation.	2019-03-07	not yet calculated	<a href="#">CVE-2013-7466</a> <a href="#">MISC</a>
sslheaders -- sslheaders	sslheaders plugin extracts information from the client certificate and sets headers in the request based on the configuration of the plugin. The plugin doesn't strip the headers from the request in some scenarios. This problem was discovered in versions 6.0.0 to 6.0.3, 7.0.0 to 7.1.5, and 8.0.0 to 8.0.1.	2019-03-07	not yet calculated	<a href="#">CVE-2018-11783</a> <a href="#">BID</a> <a href="#">MLIST</a>
stackstorm -- web_ui	In st2web in StackStorm Web UI before 2.9.3 and 2.10.x before 2.10.3, it is possible to bypass the CORS protection mechanism via a "null" origin value, potentially leading to XSS.	2019-03-08	not yet calculated	<a href="#">CVE-2019-9580</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
suse -- supportutils	Supportutils, before version 3.1-5.7.1, when run with command line argument -A searched the file system for a ndspath binary. If an attacker provides one at an arbitrary location it is executed with root privileges	2019-03-05	not yet calculated	<a href="#">CVE-2018-19636</a> <a href="#">CONFIRM</a>
suse -- supportutils	In supportutils, before version 3.1-5.7.1 and if pacemaker is installed on the system, an unprivileged user could have overwritten arbitrary files in the directory that is used by supportutils to collect the log files.	2019-03-05	not yet calculated	<a href="#">CVE-2018-19638</a> <a href="#">CONFIRM</a>
suse -- supportutils	If supportutils before version 3.1-5.7.1 is run with -v to perform rpm verification and the attacker manages to manipulate the rpm listing (e.g. with CVE-2018-19638) he can execute arbitrary commands as root.	2019-03-05	not yet calculated	<a href="#">CVE-2018-19639</a> <a href="#">CONFIRM</a>
suse -- supportutils	If the attacker manages to create files in the directory used to collect log files in supportutils before version 3.1-5.7.1 (e.g. with CVE-2018-19638) he can kill arbitrary processes on the local machine.	2019-03-05	not yet calculated	<a href="#">CVE-2018-19640</a> <a href="#">CONFIRM</a>
suse -- supportutils	Supportutils, before version 3.1-5.7.1, wrote data to static file /tmp/supp_log, allowing local attackers to overwrite files on systems without symlink protection	2019-03-05	not yet calculated	<a href="#">CVE-2018-19637</a> <a href="#">CONFIRM</a>
tibco -- jasperreports_server_and_jasperreports_server_for_activematrix_bpm	The SOAP API component vulnerability of TIBCO Software Inc.'s TIBCO JasperReports Server, and TIBCO JasperReports Server for ActiveMatrix BPM contains a vulnerability that may allow a malicious authenticated user to copy text files from the host operating system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3.	2019-03-07	not yet calculated	<a href="#">CVE-2019-8986</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- multiple_products	The repository component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, TIBCO Jaspersoft Reporting and Analytics for AWS contains a persistent cross site scripting vulnerability. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, and TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18816</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- multiple_products	The REST API component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, and TIBCO Jaspersoft Reporting and Analytics for AWS contains a vulnerability that theoretically allows unauthenticated users to bypass authorization checks for portions of the HTTP interface to the JasperReports Server. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, and TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18815</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
	The default server implementation of TIBCO Software Inc.'s TIBCO JasperReports Library, TIBCO JasperReports Library Community Edition, TIBCO JasperReports Library			

tibco -- multiple_products	for ActiveMatrix BPM, TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, and TIBCO Jaspersoft Reporting and Analytics for AWS contains a directory-traversal vulnerability that may theoretically allow web server users to access contents of the host system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Library: versions up to and including 6.3.4; 6.4.1; 6.4.2; 6.4.21; 7.1.0; 7.2.0, TIBCO JasperReports Library Community Edition: versions up to and including 6.7.0, TIBCO JasperReports Library for ActiveMatrix BPM: versions up to and including 6.4.21, TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 6.4.3; 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18809</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- multiple_products	The domain management component of TIBCO Software Inc.'s TIBCO JasperReports Server, TIBCO JasperReports Server Community Edition, TIBCO JasperReports Server for ActiveMatrix BPM, TIBCO Jaspersoft for AWS with Multi-Tenancy, and TIBCO Jaspersoft Reporting and Analytics for AWS contains a race-condition vulnerability that may allow any users with domain save privileges to gain superuser privileges. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0; 6.4.1; 6.4.2; 6.4.3; 7.1.0, TIBCO JasperReports Server Community Edition: versions up to and including 7.1.0, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3, TIBCO Jaspersoft for AWS with Multi-Tenancy: versions up to and including 7.1.0, and TIBCO Jaspersoft Reporting and Analytics for AWS: versions up to and including 7.1.0.	2019-03-07	not yet calculated	<a href="#">CVE-2018-18808</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has multiple heap buffer overflow vulnerabilities in VNC client code inside Ultra decoder, which results in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1204.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8262</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1198 has a buffer underflow vulnerability in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1199.	2019-03-05	not yet calculated	<a href="#">CVE-2018-15361</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1199 has a out-of-bounds read vulnerability in VNC code inside client CoRRE decoder, caused by multiplication overflow. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1200.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8261</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer offer handler, which can potentially result code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8274</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a stack buffer overflow vulnerability in VNC server code inside file transfer request handler, which can result in Denial of Service (DoS). This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8276</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1206 has stack-based Buffer overflow vulnerability in VNC client code inside FileTransfer module, which leads to a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8269</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1210 has out-of-bounds read vulnerability in VNC client code inside Ultra decoder, which results in a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1211.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8270</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer handler, which can potentially result code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8271</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple off-by-one vulnerabilities in VNC server code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8272</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer request handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8273</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of ClientConnection::Copybuffer function in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. User interaction is required to trigger these vulnerabilities. These vulnerabilities have been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8266</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 has multiple improper null termination vulnerabilities in VNC server code, which result in out-of-bound data being accessed by remote users. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8275</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1211 contains multiple memory leaks (CWE-655) in VNC server code, which allows an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8277</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1207 has out-of-bounds read vulnerability in VNC client code inside TextChat module, which results in a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8267</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1199 has a out-of-bounds read vulnerability in VNC client RRE decoder code, caused by multiplication overflow. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1200.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8260</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside RAW decoder, which can potentially result code execution. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8280</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1198 contains multiple memory leaks (CWE-655) in VNC client code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1199.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8259</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1198 has a heap buffer overflow vulnerability in VNC client code which results code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1199.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8258</a> <a href="#">MISC</a>
	UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with			<a href="#">CVE-</a>

ultravnc -- ultravnc	improper usage of SETPIXELS macro in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1208.	2019-03-08	not yet calculated	<a href="#">2019-8265</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside Ultra2 decoder, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8264</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1205 has stack-based buffer overflow vulnerability in VNC client code inside ShowConnInfo routine, which leads to a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. User interaction is required to trigger this vulnerability. This vulnerability has been fixed in revision 1206.	2019-03-05	not yet calculated	<a href="#">CVE-2019-8263</a> <a href="#">MISC</a>
ultravnc -- ultravnc	UltraVNC revision 1206 has multiple off-by-one vulnerabilities in VNC client code connected with improper usage of ClientConnection::ReadString function, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1207.	2019-03-08	not yet calculated	<a href="#">CVE-2019-8268</a> <a href="#">MISC</a>
wordpress -- wordpress	The "Forminator Contact Form, Poll & Quiz Builder" plugin before 1.6 for WordPress has SQL Injection via the wp-admin/admin.php?page=forminator-entries entry[] parameter if the attacker has the delete permission.	2019-03-04	not yet calculated	<a href="#">CVE-2019-9568</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Human Resource Management plugin before 2.2.6 for WordPress mishandles leave applications.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9573</a> <a href="#">MISC</a>
wordpress -- wordpress	The Blog2Social plugin before 5.0.3 for WordPress allows wp-admin/admin.php?page=blog2social-ship XSS.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9576</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Human Resource Management plugin before 2.2.6 for WordPress does not ensure that a leave modification occurs in the context of the Administrator or HR Manager role.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9574</a> <a href="#">MISC</a>
wordpress -- wordpress	The "Forminator Contact Form, Poll & Quiz Builder" plugin before 1.6 for WordPress has XSS via a custom input field of a poll.	2019-03-04	not yet calculated	<a href="#">CVE-2019-9567</a> <a href="#">MISC</a>
yubico -- libu2f-host	In devs.c in Yubico libu2f-host before 1.1.8, the response to init is misparsed, leaking uninitialized stack memory back to the device.	2019-03-05	not yet calculated	<a href="#">CVE-2019-9578</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [US-CERT](#). If you need help or have questions, please send an email to [US-CERT@ncsc.us-cert.gov](mailto:US-CERT@ncsc.us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncsc.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

**From:** [CyberheistNews](#)  
**To:** [blu@ci.sunnyvale.ca.us](mailto:blu@ci.sunnyvale.ca.us)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:49:45 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**



Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and



%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian



## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to



SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **blu@ci.sunnyvale.ca.us** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [etrujillo@sunnyvale.ca.gov](mailto:etrujillo@sunnyvale.ca.gov)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:48:36 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.



- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.



“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:



<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.flixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.flixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.flixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.flixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to [etrujillo@sunnyvale.ca.gov](mailto:etrujillo@sunnyvale.ca.gov) by  
[DoNotReply@CyberheistNews.knowbe4.com](mailto:DoNotReply@CyberheistNews.knowbe4.com)

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:48:04 AM

---

***ATTENTION***

*This email was sent to the City of Sunnyvale from an external source. Please be extra vigilant when opening attachments or clicking links.*

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



## [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

### **We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.

Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and %cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.
- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible



for maintaining them.

- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.
- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

## Are You at RSA This Week? Get Your Free Book Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

### Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

**Thanks for reading CyberheistNews**

But if you want to unsubscribe, you can do that [right here](#)

**You can read CyberheistNews online at our Blog**

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

### The Dark Side of the Kremlin: Hacked Russian Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

### Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with

fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.



In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as “More\_eggs.” More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It’s previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don’t attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing

attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level

ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in

illicit profits:

<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>

7. Enterprises are blind to over half of malware sent to their employees due to SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:

<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>

9. NIST Issues Revised Guidance on Email Security:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>

10. North Korean hackers go on phishing expedition before Trump-Kim summit:

<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow'

at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.fliixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.fliixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)

- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:  
<https://gizmodo.com/video/3641115?>
- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to [wguitarte@ci.sunnyvale.ca.us](mailto:wguitarte@ci.sunnyvale.ca.us) by  
[DoNotReply@CyberheistNews.knowbe4.com](mailto:DoNotReply@CyberheistNews.knowbe4.com)

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)



**From:** [CyberheistNews](#)  
**To:** [Pamela Dunn](#)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:47:59 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.



Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint



has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to [pdunn@sunnyvale.ca.gov](mailto:pdunn@sunnyvale.ca.gov) by  
[DoNotReply@CyberheistNews.knowbe4.com](mailto:DoNotReply@CyberheistNews.knowbe4.com)

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [Leonardo Burgueno](#)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:47:14 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**



Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**



## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

## The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services



"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **lburgueno@sunnyvale.ca.gov** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [wlee@ci.sunnyvale.ca.us](mailto:wlee@ci.sunnyvale.ca.us)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:46:23 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and



%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian



## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to



SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **wlee@ci.sunnyvale.ca.us** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [ntruit@ci.sunnyvale.ca.us](mailto:ntruit@ci.sunnyvale.ca.us)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:46:20 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.



- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.



“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:



<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **ntruitt@ci.sunnyvale.ca.us** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [mpapa@ci.sunnyvale.ca.us](mailto:mpapa@ci.sunnyvale.ca.us)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:45:16 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.



- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

**Thanks for reading CyberheistNews**

But if you want to unsubscribe, you can do that [right here](#)

**You can read CyberheistNews online at our Blog**

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

**The Dark Side of the Kremlin: Hacked Russian**

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”



New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **mpapa@ci.sunnyvale.ca.us** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)



**From:** [CyberheistNews](#)  
**To:** [cnguyen@ci.sunnyvale.ca.us](mailto:cnguyen@ci.sunnyvale.ca.us)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:45:16 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.



Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint



has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **cnguyen@ci.sunnyvale.ca.us** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [Mark Witt](#)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:45:04 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**



Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**



## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services



"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to [mwitt@sunnyvale.ca.gov](mailto:mwitt@sunnyvale.ca.gov) by  
[DoNotReply@CyberheistNews.knowbe4.com](mailto:DoNotReply@CyberheistNews.knowbe4.com)

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [Kathleen Boutté Foster](#)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:44:58 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and



%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian



## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to



SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **kbfooster@sunnyvale.ca.gov** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [rgarcia@ci.sunnyvale.ca.us](mailto:rgarcia@ci.sunnyvale.ca.us)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:44:48 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.



- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.



“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:



<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to [rgarcia@ci.sunnyvale.ca.us](mailto:rgarcia@ci.sunnyvale.ca.us) by  
[DoNotReply@CyberheistNews.knowbe4.com](mailto:DoNotReply@CyberheistNews.knowbe4.com)

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)

**From:** [CyberheistNews](#)  
**To:** [kfoster@sunnyvale.ca.gov](mailto:kfoster@sunnyvale.ca.gov)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 7:44:33 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Live Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.



- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.

Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

**Are You at RSA This Week? Get Your Free Book**

## Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald, Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*  
- Dalai Lama (born 1935)

### Thanks for reading CyberheistNews

But if you want to unsubscribe, you can do that [right here](#)

### You can read CyberheistNews online at our Blog

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian

## Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

## Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker’s bank account.

These scams are the highest risk facing the legal sector, according to the UK’s Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as ‘Friday afternoon Fraud’ or ‘Monday morning Fraud,’ because attackers often strike when they know employees aren’t at the top of their game. “Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won’t be noticed until a few days later,” she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

“The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing,” he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today’s Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim’s tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won’t threaten to involve law enforcement without warning. As a general rule of thumb, if you don’t already know that you have past-due tax bills or other missed payments, the first time you find out about them won’t be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don’t click on any links and instead go directly to the IRS’ website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should “approach all emails with caution, even those from people you know.”



New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.

It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint

has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,

J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

## The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to "0000," helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker's paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to

SSL:

<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>

8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within 'Stone's Throw' of Unicorn Status with Latest KKR Investment:  
<https://www.americaninno.com/tampabay/tampa-startups/knowbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>
- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.flixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.flixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.flixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.flixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:

<https://gizmodo.com/video/3641115?>

- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.flixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.flixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.flixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.flixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

FOLLOW US ON: [Twitter](#) | [LinkedIn](#) | [YouTube](#)

Copyright © 2014-2019 KnowBe4, Inc. All rights reserved.

---

This email was sent to **kfoster@sunnyvale.ca.gov** by  
**DoNotReply@CyberheistNews.knowbe4.com**

33 N Garden Ave, Suite 1200 Clearwater, FL 33755 USA

[1-Click Unsubscribe](#)

Don't like to click? Email opt-out requests should be sent to [opt-out@knowbe4.com](mailto:opt-out@knowbe4.com)



**From:** [CyberheistNews](#)  
**To:** [kathleen.foster@sunnyvale.ca.gov](mailto:kathleen.foster@sunnyvale.ca.gov)  
**Subject:** [Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!  
**Date:** Tuesday, March 05, 2019 6:49:22 AM

---

[Heads-Up] 40 Percent of Malicious URLs Found on \*Good\* Domains... YIKES!

Email not displaying?  
[View Knowbe4 Blog](#)



CyberheistNews Vol 9 #10 | March 5th., 2019

**[Heads-Up] 40 Percent of Malicious URLs Found on  
\*Good\* Domains... YIKES!**

Webroot revealed the results of their 2019 Threat Report, showing that tried-and-true attack methods are still going strong, but new threats emerge daily, and cybercrime is highly innovative.



Hal Lonas, Webroot's CTO said: "We wax poetic about innovation in the cybersecurity field, but you only have to take one look at the stats in this year's report to know that the true innovators are the cybercriminals. They continue to find new ways to combine attack methods or compromise new and existing vectors for maximum results. My call to businesses today is to be aware, assess your risk, create a layered approach that protects multiple threat vectors and, above all, train your users to be an asset—not a weak link—in your cybersecurity program."

**We could not agree more. Here are some highlights:**

- A whopping 40 percent of malicious URLs were found on good domains. Legitimate websites are frequently compromised to host malicious content. To protect users, cybersecurity solutions need URL-level visibility or, when unavailable, domain-level metrics, that accurately represent the dangers. Very often, endpoint security does not have these, or they run hours behind, which means these links wind up in your user's inbox.
- Phishing attacks increased 36 percent, with the number of phishing sites growing 220 percent over the course of 2018. Phishing sites now use SSL certificates and HTTPS to trick internet users into believing they are secure, legitimate pages. Microsoft's latest Security Intelligence Report confirms this, they even show figures that phishing messages into Office 365 increased 250 percent over 2018.
- Seventy-seven percent of phishing attacks impersonated financial institutions, and were much more likely to use HTTPS than other types of targets. In fact, for some of the targeted financial institutions, over 80 percent of the phishing pages used HTTPS. Google was found to be the most impersonated brand in phishing overall.
- Webroot claims that after 12 months of security awareness training which combines phishing simulation campaigns with interactive, on demand training through the browser, end users are 70 percent less likely to fall for a phishing attempt. KnowBe4's numbers show closer to 90%.
- Nearly a third of malware tries to install itself in %appdata% folders. Although malware can hide almost anywhere, Webroot found several common locations, including %appdata% (29.4 percent), %temp% (24.5 percent), and

%cache% (17.5 percent), among others. These locations are prime for hiding malware because these paths are in every user directory with full user permissions to install there. These folders also are hidden by default on Windows® Vista and up.

- Devices that use Windows 10 are at least twice as secure as those running Windows 7. Webroot has seen a relatively steady decline in malware on Windows 10 machines for both consumer and business. And then there's of course Windows Defender running on those machines, which is a very capable AV engine these days.

While ransomware was less of a problem in 2018, it became more targeted, and companies will still fall victim to ransomware. Many ransomware attacks in 2018 used the Remote Desktop Protocol (RDP) as an attack vector, leveraging tools such as Shodan to scan for systems with inadequate RDP settings.

Full article with links to resources here:

<https://blog.knowbe4.com/heads-up-40-percent-of-malicious-urls-found-on-good-domains.-yikes>

## [Scam of the Week] Robocall Scams Surge to 85 Billion Globally

Robocall spam has surged to 85 billion calls globally with bank account, credit card and extortion being common scams, according to Hiya, a company that makes apps to fend off unwanted calls.

According to Hiya's first Global Robocall Radar Report, global spam calls grew 325 percent from a year ago to 85 billion. Hiya's estimate is based on an analysis of 12 billion calls per month globally.

UK, Spain, Italy, France and Argentina were the countries with the most robocalls. Like spam, robocalls have proliferated because scammers get just enough victims to rake in profits. The Federal Communications Commission and Federal Trade Commission have been looking at ways to curb robocalls, which are one of the top consumer complaints in the U.S.

The most common scams include the following:

- Bank account scams where callers pretend to be an official from a financial institution and request information to get access to accounts.

- Extortion and kidnapping. Callers call random numbers and request payment to return a kidnapped friend or family member.
- Credit card scams where callers pose as a bank official and phish for card details.
- Wangiri Scam, also known as "One Ring," is a move where there are calls to entice a victim to call back international numbers. Victims are then charged premium rates for the call.
- Neighbor scam, which refers to the use of voice over IP to mimic local numbers and trick victims to answer.

Those scams vary by country. For instance, there's a solar energy robocall scam in Italy where fake utilities ask for information. Scammers enroll victims for services that don't exist.

Here is a ready to cut-and-paste blurb I suggest you send to your users. Feel free to edit, copy/paste:

<https://blog.knowbe4.com/scam-of-the-week-robocall-scams-surge-to-85-billion-globally>

## [March Demo] See How You Can Get Audits Done in Half the Time at Half the Cost

You told us you have challenging compliance requirements, not enough time to get audits done, and keeping up with risk assessments is a continuous problem.

**We listened!** KCM now has **Risk and Policy Management** modules, transforming KCM into a full SaaS GRC platform.

Join us for a 30-minute product demonstration of the KCM GRC platform from KnowBe4. See how you can simplify the challenges of managing your compliance requirements and ease your burden when it's time for risk assessments and audits.

- **[NEW] Simplify risk management** with an intuitive interface and simple workflow based on the well-recognized NIST 800-30.
- **Quick implementation** with pre-built requirements templates for the most widely used regulations.
- You can **assign responsibility** for controls to the users who are responsible for maintaining them.
- **Secure evidence repository** and DocuLinks giving you two ways of maintaining audit evidence and documentation.

- **Dashboards with automated reminders** to quickly see what tasks have been completed, not met, and past due.

Date/Time: **TODAY, March 5, 2019 at 1:00 pm ET**

Save My Spot!

<https://event.on24.com/wcc/r/1937744/772CD30DA91C11D5B11693D84A1AFC60>

## Phishing Criminals Announce More Attacks Against Hedge Funds and Financial Firms

A new phishing campaign called "Beyond the Grave" targeted international hedge funds on January 9th, 2019. In a statement posted to BleepingComputer, the attackers have stated that they will continue to target banking and financial institutions in the future.

A member named XanderBauer has created a post in the BleepingComputer forums with a title of "Beyond The Grave Virus infecting Hedge Funds". This post states that their phishing campaign is designed to alter data confidentiality in the targeted hedge funds, but it is not clear if that is to be used for the attackers financial advantage or to cause market instability for political reasons. More: <https://www.bleepingcomputer.com/news/security/phisher-announces-more-attacks-against-hedge-funds-and-financial-firms/>

## Can You Be Spoofed? Find Out for a Chance to Win a Stormtrooper Helmet Prop Replica

Are you aware that one of the first things hackers try is to see if they can spoof the email address of someone in your own domain?

Now they can launch a "CEO fraud" spear phishing attack on your organization, and that type of attack is very hard to defend against, unless your users are highly 'security awareness' trained.

KnowBe4 can help you find out if this is the case with our **free Domain Spoof Test**. Plus, if you are in the US or Canada you'll be entered for a chance to win a First Order **Stormtrooper Helmet** Prop Replica\*.



Try to Spoof Me!

<https://info.knowbe4.com/dst-sweepstake-mar2019>

\*Terms and Conditions apply.

## Top Five IT Security Myths Your CISO Believes Are True... BUSTED!

Facts are facts... but what happens when IT security pros take myths at face value?

That got us thinking... what if we whip out our magnifying glasses, pull out the trench coats and use our research skills to differentiate fact from fiction? Join us for this interactive webinar where we'll help you decide how to **invest your time and money** wisely, how to **implement worthwhile defenses**, and what holes to plug so your organization gets the best bang for your security budget buck.

Join us on **Tuesday, March 19th @ 2:00 pm ET** when Roger Grimes, KnowBe4's Data-Driven Defense Evangelist, and Erich Kron, KnowBe4's Security Awareness Advocate, will uncover the truth behind the Top Five IT Security Myths. They'll be stating facts and slinging stats. Then YOU DECIDE whether each myth is confirmed or BUSTED!

Myths we will be investigating:

- Every organization needs antivirus and firewalls on endpoints
- Patching 99% of your environment is enough
- Biometrics are an unhackable form of authentication
- Hackers will still break in no matter what defenses you have in place
- End users can't be trained, technology is your only defense

Date/Time: **Tuesday, March 19th @ 2:00 pm (ET)**

**Save My Spot!**

[https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?](https://event.on24.com/wcc/r/1906322/8509ADFD819F129573FDB5D654BB2E89?partnerref=CHN)  
partnerref=CHN

If This Is Your First Issue of CyberheistNews...

CyberheistNews is the world's largest e-zine for IT professionals about social engineering and security awareness training, it is published by KnowBe4 Inc, arrives in your inbox once a week and looks at IT security from the human side. KnowBe4 has partnered with Kevin Mitnick to create new school Security Awareness Training combined with regular simulated phishing attacks.

In CyberheistNews we aim to help you keep your network safe with important news, hints, and tips so that you are aware of the latest social engineering scams and can do something about it.

KnowBe4 lives 100% in the cloud, we use Salesforce as our CRM and via the [www.dealsignal.com](http://www.dealsignal.com) service we licensed your address. Consider this your sample issue. You can unsubscribe at any time (a few lines below), and you will stop receiving any and all further email.

## Are You at RSA This Week? Get Your Free Book Signed by Kevin Mitnick at KnowBe4's Booth

**Get Your Free Book Signed by Kevin Mitnick:** Drop by KnowBe4's Booth #4624 North Hall, for the Kevin Mitnick Book Signing! Meet the 'World's Most Famous Hacker' and get a signed copy of his latest book. **When: Tuesday, March 5, at 4-6 PM**

Kevin and I are both be at this very "human" RSA, read the blog post, and see you there!

<https://blog.knowbe4.com/fast-changing-security-landscape-may-render-this-years-rsa-conference-the-most-human-edition-ever>

Warm Regards,  
Stu Sjouwerman  
Founder and CEO  
KnowBe4, Inc

## Quotes of the Week

*"It isn't where you came from; it's where you're going that counts."* - Ella Fitzgerald,

Singer (1917 - 1996)

*"Our prime purpose in this life is to help others. And if you can't help them, at least don't hurt them."*

- Dalai Lama (born 1935)

**Thanks for reading CyberheistNews**

But if you want to unsubscribe, you can do that [right here](#)

**You can read CyberheistNews online at our Blog**

<https://blog.knowbe4.com/cyberheistnews-vol-9-10-heads-up-40-percent-of-malicious-urls-found-on-good-domains...-yikes>

## Security News

### The Dark Side of the Kremlin: Hacked Russian Documents Explained

On Monday, a massive database totaling 170 gigabytes of confidential data relating to prominent Russian political figures, business leaders, religious leaders and the Russian military, was published online by hackers belonging to Distributed Denial of Secrets (DDoS). DDoS describes itself as a “transparency collective” made up of mostly Ukrainian and Russian “hacktivists”.

The massive data leak, dubbed “The Dark Side of the Kremlin,” includes tens of thousands of sensitive documents and emails, including personal documents of people in Putin’s inner circle. Some of the documents seem to provide insights into Russia’s activities in Ukraine in the context of its military intervention in the country. Aljazeera has the story:

<https://www.aljazeera.com/indepth/features/dark-side-kremlin-hacked-russian-documents-explained-190224223153797.html>

### Friday Afternoon, Monday Morning, and Law Firm Risk

Law firm employees appear to be getting better at avoiding conveyancing scams, says Toni Ryder-McMullin at Today’s Conveyancer. Conveyancing or real estate

scams involve a type of email fraud in which an attacker monitors and then hijacks an email conversation just before a payment is about to be made, and directs a victim to send the money to the attacker's bank account.

These scams are the highest risk facing the legal sector, according to the UK's Solicitors Regulation Authority (SRA).

Ryder-McMullin says conveyancing scams are also known as 'Friday afternoon Fraud' or 'Monday morning Fraud,' because attackers often strike when they know employees aren't at the top of their game. "Con men will target first thing Monday morning due to staff just starting their working week and perhaps not fully concentrating – or just before the weekend to avoid detection and businesses are closed for the weekend and won't be noticed until a few days later," she says.

The SRA says that conveyance firms appear to be waking up to the threat, with fewer cases observed last year. Rob Hailstone, founder of the Bold Legal Group, agrees that conveyancing firms are more aware of these scams than other types of legal firms, but these other firms are also vulnerable.

"The takeaway is that the whole legal industry needs to be aware of this, especially as the scammers are looking at different targets than just conveyancing," he said. While awareness of scams is growing within conveyancing firms, attackers are stepping up their efforts to compete with an increasingly-aware workforce.

Hailstone says the rising level of sophistication makes these scams harder and harder to spot. Employees need new-school security awareness training to help them stay ahead of these threats. Today's Conveyancer has the story: <https://www.todaysconveyancer.co.uk/main-news/law-firms-wising-up-conveyancing-scams/>

## The Season for Tax Scams

The IRS is warning taxpayers about a surge in phishing emails, links, and phone calls during tax season, according to Toni Birdsong at McAfee. The scammers pose as the IRS and threaten to seize the victim's tax refund or have them sent to jail unless the victim makes a payment.

Many of the emails also contain malicious links through which the attackers steal sensitive data, either by sending victims to a spoofed website where their information is harvested or by triggering the download of information-stealing

malware.

Scammers are also using threatening phone calls to demand immediate payment of taxes and to procure personal information from victims over the phone.

Birdsong stresses that the IRS will not demand immediate payment over a phone call or through an email, and it won't threaten to involve law enforcement without warning. As a general rule of thumb, if you don't already know that you have past-due tax bills or other missed payments, the first time you find out about them won't be in a threatening email.

These scams prey on fear and rely on victims acting impulsively. Even if you think an email might be real, don't click on any links and instead go directly to the IRS' website using a search engine. If you receive a phone call, hang up and dial in the number of your local IRS office.

In either of these cases, never reply with personal information. The best course of action is to be aware of these scams and how to avoid them. Birdsong says you should "approach all emails with caution, even those from people you know."

New-school security awareness training can educate your employees about these scams and enable them to respond calmly and rationally. McAfee has the story: <https://securingtomorrow.mcafee.com/consumer/family-safety/dont-take-the-bait-how-to-steer-clear-of-tax-time-scams/>

## Bogus Job Offers As Phishbait

A series of phishing campaigns are targeting companies in various industries with phony job offers using direct messages on LinkedIn, according to researchers at Proofpoint. The attacker initially makes contact by sending an invitation to the target on LinkedIn with a short message regarding a job opportunity.

Within a week after the target accepts the invitation, the attacker will send a follow-up email with either a link or a PDF attachment that contains embedded URLs. These links take the target to a spoofed version of a real staffing service, which forces the download of either a Word document or a JScript loader.

This document or loader will result in the installation of a JScript backdoor known as "More\_eggs." More\_eggs can be used as a downloader for additional malware, but it also has substantial information-gathering capabilities.



It's previously been used by Cobalt Group, a threat actor that primarily goes after financial organizations, although the Proofpoint researchers don't attribute this campaign to any specific group.

They do, however, believe the actor behind this campaign may be the same one responsible for another phishing campaign revealed earlier this month by Brian Krebs, which targeted Bank Secrecy Act officers at a number of financial institutions.

Despite differences in targeting and the malware used, that campaign used similar PDF attachments which, at one point, contained URLs hosted on the same domain as the one used in the phony jobs campaign.

LinkedIn is one of the most popular platforms for phishing and spearphishing attacks, because users expect to receive unsolicited messages from people they don't know. New-school security awareness training can teach your employees how to determine if a contact should be avoided and, above all, never to click on links or attachments unless they're absolutely certain of their legitimacy. Proofpoint has the story:

<https://www.proofpoint.com/us/threat-insight/post/fake-jobs-campaigns-delivering-moreeggs-backdoor-fake-job-offers>

## What KnowBe4 Customer Say

"Hi Stu – We are very pleased with the product. I am not sure how deeply all your clients customize and use the platform – but we have done quite a bit and have had extremely good response from the users and from the management team."

Thanks,  
J.C., IT Director.

"I just wanted to provide some feedback on our KnowBe4 experience so far. This product came recommended to us from several MSP's that I met at a Datto Partner conference. I spent quite a bit of time talking with them specifically and that was ultimately what led me to get in touch with KnowBe4.

We've sold this once to an Aerospace company last year and we're slow to get things going as we're a fairly large VAR and just starting to expand into the security

space this year (as evidenced by a few of our recent sales).

They set up the product entirely on their own without any input from the Managed Services side, however two other accounts are both fully managed accounts and we've been progressing through the setup and configuration with them while learning the product at the same time. I just wanted to say that this product is:

- Fairly intuitive to use
- Has the best knowledge-base I've ever seen for any product, ever.
- Deployment has gone very smoothly (thanks in large part to your excellent knowledge base)
- The ASAP feature which provide direct, relevant KB links for each step has been super helpful in having smooth deployments
- Your Support has been prompt, and helpful too

The actual Phish templates are extremely well done, with the higher difficulty level ones indistinguishable from the real thing. I hope to get much more of this product sold in 2019 and I just wanted to let you know of the positive experience I've had with it so far."

A.J., Director of Managed Services

"Thank you for reaching out! KnowBe4 has been an incredible service to use, and we've already seen benefits from it here at the county. Genells has been shepherding me through the process of getting our training and phishing simulations set up, and she's really been wonderful. I can't speak highly enough about her work.

Overall I've found the whole portal easy to use and super powerful. Way more intuitive than most of the other systems I've used or demoed.

The one feature request that I'd like to put into your ear is the option to create quizzes. That's honestly the only missing piece for me, when it comes to using KnowBe4. Thanks again for the email!"

- P.A., Cybersecurity Trainer (We are working on quizzes, stay tuned.)

The 10 Interesting News Items This Week

1. KKR Invests in Cybersecurity Firm KnowBe4 at USD 800M+ Valuation:  
<http://fortune.com/2019/03/01/kkr-invests-in-cybersecurity-firm-knowbe4-at-800m-valuation/>
2. New Evil USB Cable Shows How Attacks Can Leverage Physical Hardware:  
<https://www.theverge.com/2019/2/25/18239965/4g-5g-security-flaws-spying-hack-eavesdrop-fake-alert>
3. Deep Learning vs. Machine Learning: A Simple Explanation:  
<https://hackernoon.com/deep-learning-vs-machine-learning-a-simple-explanation-47405b3eef08>
4. New Facebook Phishing Scam is So Good It Will Fool Even You:  
<https://blog.knowbe4.com/new-facebook-phishing-scam-is-so-good-it-will-fool-even-you>
5. Comcast set mobile pins to “0000,” helping attackers steal phone numbers:  
<https://arstechnica.com/information-technology/2019/03/a-comcast-security-flub-helped-attackers-steal-mobile-phone-numbers/>
6. The hacker’s paradise: Social networks net criminals USD 3 billion a year in illicit profits:  
<https://www.zdnet.com/article/social-media-becomes-hacker-paradise-3bn-earned-a-year-in-illicit-profits/>
7. Enterprises are blind to over half of malware sent to their employees due to SSL:  
<https://www.helpnetsecurity.com/2019/03/01/2019-cloud-security-insights-threat-report/>
8. New Attacks Show Signed PDF Documents Cannot Be Trusted:  
<https://www.securityweek.com/new-attacks-show-signed-pdf-documents-cannot-be-trusted>
9. NIST Issues Revised Guidance on Email Security:  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177r1.pdf>
10. North Korean hackers go on phishing expedition before Trump-Kim summit:  
<https://www.cyberscoop.com/trump-kim-summit-vietnam-north-korea-hackers-phishing/>

Prepared in cooperation with the CyberWire research team.

## Cyberheist 'Fave' Links

### This Week's Links We Like, Tips, Hints and Fun Stuff

- KnowBe4 Within ‘Stone’s Throw’ of Unicorn Status with Latest KKR Investment:

<https://www.americaninno.com/tampabay/tampa-startups/knownbe4-within-stones-throw-of-unicorn-status-with-latest-pe-investment/>

- The guys from Dude Perfect, a Texas-based trick shot group, are back with another impressive round of trick shots involving household objects and everyday tasks:  
[https://www.fliixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm\\_source=4](https://www.fliixy.com/real-life-trick-shots-part-3-dude-perfect.htm?utm_source=4)
- People Are Awesome - Awesome people performing extraordinary feats in this week's compilation of the 'People Are Awesome' YouTube channel:  
[https://www.fliixy.com/people-are-awesome-best-of-week-7-2019.htm?utm\\_source=4](https://www.fliixy.com/people-are-awesome-best-of-week-7-2019.htm?utm_source=4)
- Magicians and Illusionists Craig Christian and Elizabeth Best perform live at the French television show The World's Greatest Cabaret:  
[https://www.fliixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm\\_source=4](https://www.fliixy.com/evolution-of-magic-the-worlds-greatest-cabaret.htm?utm_source=4)
- Lady Gaga and Bradley Cooper deliver a show stopping rendition of 'Shallow' at the Oscars. PS: She is wearing a 30-million-dollar Tiffany diamond:  
[https://www.fliixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm\\_source=4](https://www.fliixy.com/lady-gaga-and-bradley-cooper-rendition-of-shallow-at-the-oscars.htm?utm_source=4)
- World's Biggest Bee, Once Thought Extinct, Has Been Found Alive:  
[https://gizmodo.com/video/3641115?utm\\_source=4](https://gizmodo.com/video/3641115?utm_source=4)
- SPACEX Has Sent Its First Crew-Ready Capsule To The ISS:  
<https://www.wired.com/story/spacex-is-sending-its-first-crew-ready-capsule-to-the-iss/>
- Spencer Seabrooke breaks the world record for the longest free solo slackline ever, untethered:  
[https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm\\_source=4](https://www.fliixy.com/free-solo-slacklining-untethered-world-record.htm?utm_source=4)
- From The Archives. "Weird Al" Yankovics' Word Crimes. An entertaining (and educational) song in favor of proper grammar:  
[https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm\\_source=4](https://www.fliixy.com/weird-al-yankovic-word-crimes.htm?utm_source=4)
- Imagine having gecko strength. Very cool robot gripper by NASA JPL:  
<https://mobile.twitter.com/CNET/status/1101618114725400576>

1-Click Unsubscribe

Don't like to click? Email opt-out requests should be sent to opt-out@knowbe4.com



**From:** [Association of Deputy District Attorneys](#)  
**To:** [ggiquiere@ci.sunnyvale.ca.us](mailto:ggiquiere@ci.sunnyvale.ca.us)  
**Subject:** Monday Morning Memo for March 4, 2019  
**Date:** Monday, March 04, 2019 5:03:16 AM

---

Click here [Having trouble viewing this email?](#)



## Courts & Rulings

### **Value of property received from two thefts can't be combined to create felony**

A man who received stolen property from two clothing stores should

have been charged with two misdemeanor counts, rather than the value of the goods being added together, with the charge being receipt of stolen property worth in excess of \$950, a felony, the First District Court of Appeal declared yesterday.

[Metropolitan News-Enterprise](#)

### **Court rules L.A. council members wrongly blocked public testimony at 'special' meetings**

The Los Angeles City Council must allow people to testify on issues considered during their "special" meetings, which are called with just one day of notice, a three-judge panel has ruled. In a 15-page decision, the 2nd District Court of Appeal said the council improperly prevented Studio City resident Eric Preven from weighing in on a development issue taken up during a special meeting in 2015.

[MSN](#)

### **With women in combat roles, a federal court rules male-only draft unconstitutional**

A federal judge in Texas has declared that an all-male military draft is unconstitutional, ruling that "the time has passed" for a debate on whether women belong in the military. The decision deals the biggest legal blow to the Selective Service System since the Supreme Court upheld the draft registration process in 1981.

[USA Today](#)

### **Federal prosecutors' secret plea deal with politically connected sex abuser broke law, judge says**

Federal prosecutors violated the Crime Victims' Rights Act when they failed to notify a sex offender's underage victims about a secret plea deal, a federal judge in Florida has ruled. U.S. District Judge Kenneth Marra ruled Thursday on the conduct of prosecutors in the office of then-U.S. Attorney Alex Acosta of the Southern District of Florida.

[ABA Journal](#)

### **'Appointed for life, not for eternity.' Dead judge's vote shouldn't have counted, Supreme Court rule**

The U.S. Supreme Court said judges "are appointed for life, not for eternity," in setting aside a pay-discrimination ruling written by a jurist who died a week and a half before the decision was issued. The unsigned opinion said a federal appeals court was wrong to count the vote of the late Judge Stephen Reinhardt in a ruling that let a female math consultant sue a California school official.

[Bloomberg](#)

### **Los Angeles Police Union declines to appeal ruling on disciplinary records**

Leaders of the union representing Los Angeles police officers said today they have decided against appealing a judge's ruling calling for the public release of internal department records on officer-misconduct.

cases. Last week, Los Angeles Superior Court Judge Mitchell L. Beckloff rejected a bid by the Los Angeles Police Protective League to prevent the release of such records from cases that occurred prior to Jan. 1, when a new state law took effect requiring the documents to be made public.

[City News Service](#)

### **Orange County judge orders police records unsealed**

A judge in Southern California lifted a temporary seal on Orange County police misconduct records Thursday, striking another blow to police unions who've argued in courts across the state that unsealing the records violates officers' constitutional rights to privacy. The new California law opens up access to previously shielded internal records on police shootings, complaints of sexual assault by officers and internal records on police misconduct.

[Courthouse News Service](#)

### **Man who addressed council committee had right to address full body in special session**

A community activist who addressed a Los Angeles City Council committee in opposition to a project was wrongfully denied an opportunity to address the full 15-member body at a special session, the Court of Appeal for this district has held, pointing to a loophole in the Ralph M. Brown Act.

[Metropolitan News-Enterprise](#)

### **Mongols motorcycle club gets to keep prized patches, as federal judge rules against U.S. government's first-of-its-kind effort**

A federal judge has rejected the U.S. government's unprecedented effort to gain control of the prized patches that adorn the vests worn by the notorious Mongols motorcycle club, ruling seizing the outlaw organization's trademarks would be unconstitutional. The written ruling, released Thursday morning by U.S. District Judge David O. Carter, marks a setback for federal prosecutors who two months ago persuaded a Santa Ana jury to find the Southern California-based club guilty of racketeering.

[Orange County Register](#)

## **Prop 47, 57 & AB 109**

### **Man with no-bail warrant arrested after barricading himself in Goleta apartment**

A Carpinteria man was arrested Monday after leading law enforcement officers on a foot pursuit, barricading himself in a Goleta apartment and refusing to surrender, according to the Santa Barbara County Sheriff's Office. The department's AB 109 Compliance Response Team were searching for Jacob Dreyer, 28, who had a no-bail arrest warrant due to violating terms of his probation, said Kelly Hoover, a sheriff's spokeswoman.

[Noozhawk](#)

### **Auto burglars hit Menlo Park in a dozen incidents Sunday night**

Auto burglars struck several neighborhoods in Menlo Park on Sunday night (Feb. 24), according to reports from the crime log of the Menlo Park Police Department. Six of the 12 burglaries took place in the Menlo Oaks neighborhood, and three each were reported in Sharon Heights and Suburban Park - Lorelei Manor - Flood Park Triangle. Burglars broke into 10 of the vehicles by smashing windows, while one was unlocked.

[The Almanac](#)

### **California murder parolee robs Sacramento restaurant, patron shot, car-jacked**

Four-term Democratic California Governor Gov. Jerry Brown made reforming California's criminal justice sentencing guidelines a priority over his 16 total years as governor. Add to that his record number of 1,736 pardons and 284 prison commutations, and violent prison inmates have been released or made eligible for early release.

[California Globe](#)

## **Prosecutions/Prosecutors**

### **Santana: New OC DA wants to make a deal with feds ending DOJ jailhouse snitch probe**

Orange County District Attorney Todd Spitzer is calling on federal authorities to end their ongoing probe into use of jailhouse snitches in Orange County and instead make a deal to institute reforms. "I'm willing to admit everything that happened," Spitzer told me last week during a phone interview where we talked about the jail house scandal that catapulted him into office as the chief law enforcement officer in a county where that job had been seemingly phoned-in for a long time.

[Voice of OC](#)

### **Report: LAPD sends 102 allegations against former USC gynecologist to DA (Video)**

Dr. George Tyndall was fired by the school after it came to light that female patients had accused him of sexual misconduct over several decades. Jeff Michael reports.

[CBS Los Angeles](#)

### **OC judge weighing move to dismiss case Vs. 'Real Housewives' son**

A judge Tuesday put off ruling on whether to dismiss an attempted murder case against a son of a former "Real Housewives of Orange County" cast member based on allegations of outrageous governmental misconduct. Joshua Waring, the son of former "Real Housewives" cast member Lauri Peterson, is accused of shooting then-35-year-old Daniel Lopez outside a home in Costa Mesa on June 20, 2016. Two other people escaped injury in the drive-by attack.

[Costa Mesa Police Department](#)

### **District attorney declines to charge La Puente property owner of illegal marijuana sales**

A La Puente commercial landlord, who was arrested last year after authorities raided a marijuana dispensary allegedly operating without a license, will not be charged, officials confirmed Tuesday, Feb. 26. On Sept. 27, 2018, deputies with the Los Angeles County Sheriff's Department raided a marijuana dispensary that authorities said was operating illegally on a commercial property in the 15500 block of Amar Road.

[San Gabriel Valley Tribune](#)

## **Criminal Justice/Public Safety**

### **LAPD commander involved in controversial car crash is demoted**

A Los Angeles police commander has been demoted to captain after his city car was found wrecked and abandoned in Carson. Jeff Nolte, 52, who headed the LAPD's Force Investigation Group, has been on paid leave since he crashed his unmarked Dodge Charger on Jan. 24, then left the scene. With an investigation into his conduct underway, Nolte's rank was reduced one rung earlier this week, Josh Rubenstein, the department's communications director, said Friday.

[Los Angeles Times](#)

### **University professor condemned for previous comments saying cops 'need to be killed'**

UC Davis is condemning a professor's inflammatory statements where he said cops "need to be killed." English professor Joshua Clover reportedly wrote several tweets and made comments in a 2015 interview with SF Weekly where he referenced violence against law enforcement officers.

[CBS Sacramento](#)

### **Could a new California law free a teen killer convicted as an adult for a brutal double homicide?**

Six years ago, someone savagely stabbed to death Chip Northup, 87, and Claudia Maupin, 76, as they slept inside their Davis, California, home. Police found no physical evidence and investigators thought they might have some challenges finding the killer. "It was the most horrific, depraved murder I've ever seen as the district attorney in this county," Yolo County, California, D.A Jeff Reisig tells "48 Hours" correspondent Erin Moriarty.

[48 Hours](#)

### **Two inmates released after being convicted of murder**

Two men who spent years in state prison after being convicted of murder in separate cases were freed Friday following efforts spearheaded by two programs at Loyola Law School seeking their release. Michael Tirpak, now 43, had been behind bars for nearly 25



years following his 1996 conviction for first-degree murder in the 1994 killing of David Falconer in Compton.

[My News LA](#)

### **Waiting for a decision in Stephon Clark's killing, they are ready to be disappointed - and to mobilize**

An 8-foot-tall chain-link fence went up around the Sacramento County district attorney's office, weeks after police shot and killed Stephon Clark - an unarmed black man whose cellphone they mistook for a gun. Demonstrators previously had blocked the front doors, chanting "Shut it down!" as protests erupted across the capital city.

[Los Angeles Times](#)

### **Governor orders more DNA testing in 1983 California killings**

California Gov. Gavin Newsom ordered additional DNA testing Friday on evidence that a death-row inmate says will prove his innocence in a 35-year-old murder case that has drawn national attention. Former Gov. Jerry Brown previously ordered testing of four pieces of evidence that condemned inmate Kevin Cooper says will show he was framed for the 1983 hatchet and knife killings of four people, including two children, in Chino Hills.

[AP](#)

### **Herbalist sentenced to jail after death of 13-year-old diabetic boy he treated**

A Los Angeles herbalist convicted of practicing without a license was sentenced to four months in jail for child abuse in the same case in connection with the death of a 13-year-old diabetic boy, the city attorney said. Timothy Morrow, 84, was found guilty of one count of practicing without a license at a jury trial Feb. 20 and pleaded no contest Monday to a connected charge of misdemeanor child abuse likely to produce great bodily injury or death, Los Angeles City Attorney Mike Feuer said in a statement.

[NBC News](#)

### **Camfield Partners plans El Sereno warehouse for LAPD's auto theft division**

Camfield Partners wants to build a large new warehouse and office in El Sereno for storing evidence and equipment for the Los Angeles Police Department. The Laguna Hills-based firm filed plans with the city for the 80,000-square-foot warehouse earlier this month. It would be built on a vacant 6.8-acre lot at 1925 N. Marianna Avenue. Camfield, a small firm led by Ken Jackson, purchased the lot in 2015 for \$6.5 million.

[The Real Deal](#)

## **Policy & Legal Issues**

### **Bailing on bail reform**

Last September, as part of a national push for criminal-justice reform,

Robert F. Kennedy Human Rights, a charitable organization, announced a plan to pay the bail of every woman and minor held in New York City's jails. According to the group, run by Kerry Kennedy, the slain senator's daughter, "access to justice depends on whether you can afford bail. The majority of people incarcerated in the notoriously violent Rikers Island are behind bars for the crime of being too poor."

[City Journal](#)

### **California's jails and prisons becoming ground zero in the state's mental health crisis**

These days, the main path to treatment at a state psychiatric hospital is through jail. However controversial those state hospitals may be, many families conclude they are the best option for their loved ones. "That is a sad state of affairs in our society, that only when you get locked up does it become a priority to get you treatment," said Los Angeles District Attorney Jackie Lacey, who said she's heard many parents describe similar feelings of desperation.

[North Coast Journal](#)

### **California man who spent 39 years in prison gets \$21 million for wrongful conviction**

A California man who was wrongfully convicted for killing an ex-girlfriend and her son four decades ago has reached a \$21 million settlement with the city of Simi Valley, officials said. Craig Coley, 71, was sentenced to life in prison without parole for the 1978 murder of his former partner, Rhonda Wicht, and her 4-year-old son, Donald, at their apartment.

[Reuters](#)

### **As death toll keeps rising, U.S. communities start rethinking Taser use**

Warren Ragudo died after two Taser shocks by police intervening in a family altercation. Ramzi Saad died after a Taser shock by police during a dispute between Saad and his mother. Chinedu Okobi died after police used a Taser to subdue him in a confrontation they blamed on his refusal to stop walking in traffic. All three were unarmed. All three had histories of mental illness.

[Reuters](#)

### **Fire scientists say the arson case against Claude Garrett was fatally flawed. Will anyone listen?**

In a tense, crowded room inside Nashville's Riverbend Maximum Security Institution, Claude Garrett sat before a large TV monitor and stared at the screen. Behind him, a crowd of people gathered before a long conference table. Garrett wore prison-issued blue jeans, glasses, and a serious expression. Looking back at him on the screen was Richard Montgomery, chair of the Tennessee Board of Parole.

[The Intercept](#)

### **California Attorney General Xavier Becerra faces criticism from**

### **criminal justice reformers**

Another Democratic state attorney general is facing sharp criticism from activists for allegedly getting in the way of criminal justice reform and showing bad faith while doing so. Former Rep. Xavier Becerra (pictured), D-Los Angeles, was appointed in 2016 by Gov. Jerry Brown to replace state Attorney General Kamala Harris after she was elected to the U.S. Senate. He won a full term in the 2018 elections.

[CalWatchdog](#)

### **California keeps a secret list of criminal cops, but says you can't have it**

Their crimes ranged from shoplifting to embezzlement to murder. Some of them molested kids and downloaded child pornography. Others beat their wives, girlfriends or children. The one thing they had in common: a badge. Thousands of California law enforcement officers have been convicted of a crime in the past decade, according to records released by a public agency that sets standards for officers in the Golden State.

[Investigative Reporting Program, UC Berkeley](#)

### **California bill introduces new hurdle to access public records**

A San Diego lawmaker is trying to complicate the already convoluted process that reporters and Californians must take to view public records and make it harder for requesters to recoup attorney's fees when they prevail over the government in court. Introduced last Friday just ahead of a deadline for new bill proposals, Senate Bill 615 would require anyone not satisfied with a public records request to mediate with the relevant government agency before taking it to court.

[Courthouse News Service](#)

### **Woe to illegal pot shops: Water, power to be shut off**

With hundreds of illegal marijuana shops continuing to operate in Los Angeles, the City Council moved forward with a plan Tuesday aimed at cracking down on the businesses by shutting off their utilities. The idea of shutting off water and power at illegal pot shops was proposed last year by Councilwomen Nury Martinez and Monica Rodriguez, and the council voted 13-0 to have the City Attorney's Office draft an ordinance outlining the proposed policy.

[My News LA](#)

### **San Francisco dropped the Joint Terrorism Task Force two years ago. Now the FBI wants to pick things back up.**

After a two-year separation, the FBI wants to get back together with San Francisco. The bureau sent Mayor London Breed a letter on Jan. 29, touting the advantages of a currently suspended partnership between the FBI and the San Francisco Police Department - largely meant to quash terrorist threats in the region.

[Mission Local](#)

---

### **Suspect impersonates LAPD detective during Chinatown jewelry store robbery**

Authorities are searching for multiple suspects - one of whom impersonated a Los Angeles police detective - in connection with one robbery and two attempted robberies at two jewelry stores in the same Chinatown neighborhood over a four-hour period Tuesday. It's unclear if the three incidents are linked.

[CBS Los Angeles](#)

### **FBI releases preliminary semiannual crime statistics for 2018**

Statistics released today in the FBI's Preliminary Semiannual Uniform Crime Report revealed overall declines in the number of violent crimes and property crimes reported for the first six months of 2018 when compared with figures for the first six months of 2017. The report is based on information from 14,509 law enforcement agencies that submitted three to six months of comparable data to the FBI's Uniform Crime Reporting (UCR) Program.

[FBI National Press Office](#)

### **Feds: 3 men conspired with L.A. Sheriff's Deputy to steal 1,200 lbs of marijuana, \$645K cash**

Three men were arrested on Thursday morning on federal drug distribution charges alleging they conspired with a Los Angeles County sheriff's deputy and others to steal more than 1,200 pounds of marijuana and \$645,000 in cash and money orders during an armed robbery of a downtown Los Angeles warehouse that was staged to look like law enforcement was executing a search warrant, according to federal authorities.

[Fox 11 Los Angeles](#)

### **Man dressed as LADWP worker among suspects in West Hills home invasion**

Authorities say three men in ski masks - one of whom was wearing a Los Angeles Department of Water and Power vest - forced their way into a West Hills home Monday morning. The home invasion occurred at around 8 a.m. in the 7800 block of Bobbyboyar Avenue, according to L.A. police. Once they gained entry into the residence, police say the suspects tied up the homeowner, pistol-whipped him, and ransacked the home.

[CBS LA](#)

### **Meth problem puts Fresno in the national spotlight, again**

A recent documentary on "Vice News" highlighted the methamphetamine addiction problems among Fresno's homeless. A homeless woman Action News talked with named Katherine told us she has been living on the streets for four years. She acknowledged drugs are a problem in the homeless community. "You find that everywhere you go. Everywhere, it's not in just one certain spot. It's all over," she said.

[KFSN](#)

### **San Francisco man was hanged, drugged, put in suitcase and dumped in the Bay: Prosecutors**

A 47-year-old San Francisco man has been charged with torturing and murdering a 23-year-old, before putting the dead man's body into a suitcase and tossing it into the San Francisco Bay earlier this month, authorities said. Gerald William Rowe was arrested last week after the body, later identified as San Francisco resident George Randall Saldivar, was found floating in the Bay near Pier 39 on Feb. 18, according to court records.

[Los Angeles Times](#)

### **2 men indicted in \$2M kidnapping scheme in SoCal; taped and bound O.C. victim now believed dead**

Two Chinese nationals have been indicted in a \$2 million kidnapping scheme in Southern California involving a victim who was physically restrained inside a closet and is now believed dead, the U.S. Department of Justice announced Thursday. Guangyao Yang, 25, and Peicheng Shen, 33, are facing charges of conspiracy to kidnap, kidnapping, attempted extortion in violation of the Hobbs Act and threat by foreign communication, according to a DOJ news release.

[KTLA](#)

## **Los Angeles County Sheriff**

### **LA sheriff backs release of police misconduct records**

A California law requiring public disclosure of police misconduct records has been challenged by police unions in courts across the state, but received support Wednesday from Los Angeles County Sheriff Alex Villanueva. Police officer unions, including the Los Angeles Police Protective League and the Association for Los Angeles Deputy Sheriffs, have sued to bar retroactive enforcement of California Senate Bill 1421.

[Courthouse News Service](#)

### **LA's sheriff says jail reform has failed. We went inside to find out**

Los Angeles County Sheriff Alex Villanueva says reforms designed to reduce violence by deputies in the jails are a failed "social experiment." He claims attacks on guards are up, and his deputies feel the new rules keep them from fully defending themselves. Villanueva has argued his deputies need a freer hand to use force.

[LAist](#)

### **OIG report raises concerns about overcrowded jails, lack of care**

A number of concerns about the Los Angeles County Sheriff's Department - including overcrowded jails, the quality of medical and mental health care for inmates and the persistence of dangerous social cliques - have been raised by the Office of Inspector General in a report set to be formally accepted by the Board of Supervisors Tuesday.



[My News LA](#)

### **Alex Villanueva has a lot of work to do to regain L.A.'s trust**

As with other political newcomers who achieve astounding initial success, the upset victory of newly elected Los Angeles Sheriff Alex Villanueva deserves study, and props to the person who pulled it off. Almost no one saw it coming. It wasn't simply that the underfunded campaign of a retired former lieutenant didn't stand out for reasons of lack of name recognition.

[Southern California News Group](#)

## **Los Angeles County**

### **Lawsuit filed in death of Los Angeles County jail inmate who suffered from schizophrenia**

Leon Nyarecha tearfully recounts the day his younger brother died while in Los Angeles County Sheriff's custody at the Men's Central Jail last June. "Lewis was my little brother," he said. "The day he died was the worst day of my life." Leon Nyarecha is now suing the county and the sheriffs department for negligence and battery. "He suffered from schizophrenia," said attorney Jovan Blacknell.

[NBC Los Angeles](#)

### **Assaults on guards in L.A. County juvenile detention increase sharply**

Violence at times erupts with little warning inside Los Angeles County's juvenile detention halls and camps. That's what happened one February night two years ago as Edgar Arrondo - then a senior guard at a sprawling facility in Sylmar - walked a teenage detainee to a mental health evaluation. A rival gang member charged at the teen, ignoring Arrondo's verbal warnings. The youths collided. A fight ensued.

[Los Angeles Times](#)

### **Goldstein Investigation: Money flows like water at water board meetings**

David Goldstein finds the money flows like water at water board meetings. "Ms. Kwan, I'm David Goldstein with CBS2 News. Can I talk with you a second?" "No!" she replies. Carol Kwan wasn't talking. She's an elected board member for the West Basin Municipal Water District. It's a public agency which is a wholesale supplier of water to nearly one million people in 17 cities and unincorporated areas in Los Angeles County - mostly in the South Bay.

[CBS Los Angeles](#)

### **Environmentalists furious over methane capture plan in Aliso Canyon gas leak settlement**

Environmental groups are criticizing last year's \$120 million court settlement in the devastating Aliso Canyon gas leak because a large portion of the money will be used to fund a plan that would capture

methane from dairy farms in the state's farm belt - more than 100 miles from where the blowout occurred - and convert it into natural gas.

[CBS LA/AP](#)

### **Is your hospital prepared for gang violence and injuries?**

Los Angeles County has more than 1,300 gangs with over 150,000 members. In the city of Los Angeles alone, there are an estimated 450 active gangs with a combined membership of over 45,000 individuals. In the last three years, there were over 16,398 violent gang crimes in Los Angeles, according to the Los Angeles Police Department. Those crimes included 491 homicides, 7,047 felony assaults, 5,518 robberies and 98 rapes.

[Campus Safety](#)

### **Poisonous pot found in some Los Angeles-area stores**

Some of the marijuana products sold by Southern California stores and delivery services are loaded with banned toxic chemicals that could make you sick, according to an NBC4 I-Team investigation. "Why would you want to put poison in your body," said Hinaxi Patel, technical director of Brightside Scientific in Long Beach, an independent state-licensed lab that tested the pot products for NBC4.

[NBC Los Angeles](#)

### **Family files lawsuit against Democratic donor Ed Buck in overdose death**

The mother of a man who died inside the West Hollywood apartment of a prominent Democratic Party donor filed a wrongful-death lawsuit Tuesday that names him and the Los Angeles County District Attorney as defendants. LaTisha Nixon told NBC4 Tuesday she was frustrated that authorities had failed to file criminal charges for the 2017 overdose death of her 26-year-old son, Gemmel Moore, and didn't want to see any other mothers to lose their loved ones in a similar way.

[NBC Los Angeles](#)

## **Convictions/Sentences/Parole**

### **Ex-Fullerton police chief pleads guilty to attacking paramedics at Lady Antebellum concert**

A former Fullerton police chief and one of his captains plead guilty Monday to misdemeanor charges for starting a fight with paramedics at a Lady Antebellum concert last summer in Irvine while off-duty, an incident which forced the chief to resign. Former Chief David Hendricks, 47, and Capt. Thomas Oliveras, 50, pleaded guilty in Orange County Superior Court in Newport Beach to disturbing the peace by fighting.

[CBS Los Angeles](#)

### **Ex-Pasadena police officer sentenced to prison on Federal gun charges**

A former Pasadena police lieutenant was sentenced Monday to a year and a day in federal prison for selling more than 100 firearms without a license and making false statements during a gun purchase. Vasken Kenneth Gourdikian, who resigned from the Pasadena Police Department in March 2018 after a 22-year career, was also ordered by U.S. District Judge Stephen V. Wilson to pay a \$10,000 fine and serve a year of supervised release after completing his prison term.

[My News LA](#)

### **Woman sentenced to 15 years in prison for attack on 91-year-old man**

A Los Angeles woman was sentenced Thursday to 15 years in state prison for beating a 91-year-old grandfather with a brick in Willowbrook last summer. Laquisha Jones, 30, pleaded no contest Dec. 27 to a felony elder abuse charge stemming from the attack, which occurred on the Fourth of July last year. Jones attacked the man without provocation near 118th and Robin streets, according to the Los Angeles County District Attorney's Office.

[City News Service](#)

### **Parole denied for man convicted of 1982 Guerneville murder**

A man incarcerated for a 1982 murder was denied parole at a hearing Thursday, according to the Sonoma County District Attorney's Office. Vernon Bragg, 65, of Guerneville, pleaded guilty in 1985 to second-degree murder and use of a firearm in the shooting death of Ray Bragg in 1982. On Thursday, Vernon Bragg, a California Department of Corrections and Rehabilitation inmate, was given a three-year denial of parole by the State of California Board of Parole Hearings.

[Bay City News Service](#)

### **Ex-Orange County teacher sentenced to 2 years for sex with 17-year-old boy**

A man who taught at an Orange County high school was handed a two-year state prison sentence Friday for a sex act involving a 17-year-old boy who lived with him for a short time in Long Beach. Andrew Bueno-Potts - also known as Drew Bueno-Potts - was also ordered to register as a sex offender for the rest of his life and to stay away from the young man for 10 years, according to the Los Angeles County District Attorney's Office.

[City News Service](#)

### **House of horrors case: Turpin parents accused of beating, starving children plead guilty**

The California couple accused of beating, starving and holding 12 of their children captive pleaded guilty Friday to multiple charges. David and Louise Turpin pleaded guilty to 14 counts each of torture, dependent adult abuse, child endangerment and false imprisonment. Riverside County District Attorney Michael Hestrin said at a news

conference that because of the plea deal, the Turpins will not be headed to trial.

[NBC News](#)

### **Ex-NASA contractor sentenced to prison for sextortion**

A onetime NASA contractor was sentenced on Monday to nearly five years behind bars for stalking women online with threats to publish nude photos unless they provided him with additional explicit pictures.

Richard Gregory Bauer, 28, of Los Angeles, a former contractor at the NASA Armstrong Flight Research Center, must also serve three years under supervised release after completing his federal prison term.

[City News Service](#)

## **Consumer Warnings**

### **Amazon's counterfeit problem is a big one - for shareholders, brand owners and consumers alike**

On February 1, Amazon.com, Inc. filed a Form 10-K annual report with the U.S. Securities and Exchange Commission. Along with reporting its year-end earnings for the 2018 fiscal year, this particular SEC filing was notable because Amazon officially acknowledged to shareholders that the company's online sales platforms face the risk of being found liable for fraudulent or unlawful activities of sellers on those platforms.

[IP Watchdog](#)

### **Los Angeles District Attorney's Office warns against new 'tap-to-pay' credit card scam**

The District Attorney's Office (DA Office) cautions that the public should be more aware of potential "scammers trying to steal personal information as some credit card companies issue new 'tap-to-pay' cards". In this credit card fraud, the initiation takes place when scammers contact consumers who may be receiving new cards from their credit card companies.

[KHST](#)

### **Those annoying robocalls can be illegal and now some consumers are fighting back**

Robocalls can interrupt us multiple times a day. There's no sugarcoating it, they're downright annoying. But now consumers are fighting back.

According to the Federal Trade Commission, unwanted calls are "far and away the biggest consumer complaint." "Look at all of these missed calls," said Jamie Bergstein while scrolling through her phone outside of Philadelphia City Hall, "I get them all the time!"

[CBS Philly](#)

## **California/National**

### **Under new CA bill, 911 dispatchers would be trained to identify and de-escalate mental health crises**

A new California bill, AB 680, aims to reduce the criminalization of people suffering from mental health emergencies, and improve their interactions with police, by requiring all 911 dispatchers to receive mental health crisis intervention training. "Too many law enforcement interactions with people in mental health crisis end in tragedy," said the bill's author Assemblymember Kansen Chu (D-San Jose).

[Witness LA](#)

### **Law would protect crime accusers from arrest**

California lawmakers, whose antics have included attempting to designate counseling against same-sex attractions "consumer fraud" requiring school children to celebrate gay activist Harvey Milk, are at it again. A proposed law would grant immunity to residents from arrest if they are in the process of reporting a sex crime or other crime of violence.

[Seneca Standard](#)

### **The sudden death of near-legendary San Francisco public defender, Jeff Adachi, stuns Bay Area leaders & the many ordinary people whom he championed**

When the news flew around the state that San Francisco Public Defender, Jeff Adachi, 59, had died of a possible heart attack on Friday night, after having trouble breathing while having dinner with a friend, public officials, the legal community, and an unusually wide variety of ordinary people reacted with shock and genuine grief, as if for a member of the family.

[Witness LA](#)

### **For victims of hate crimes, Jussie Smollett case is a giant betrayal**

The dramatic unraveling of the story of a vicious attack on actor Jussie Smollett has spread deep concern among hate-crime victims that growing racist and anti-gay violence now may be more likely to go unreported and unpunished. Last week, Chicago police arrested Smollett, the black, openly gay star of Fox television's "Empire," and charged him with orchestrating a fake encounter on a Chicago street with two men whom he alleged had assaulted him, hung a rope around his neck, and hurled homophobic and racist slurs while shouting, "This is MAGA country."

[Los Angeles Times](#)

### **Sharon Tate's sister believes Charles Manson has more victims: 'We are just scraping the surface'**

The Manson family killings were as gruesome as they were shocking. In the early hours of Aug. 9, 1969, Charles Manson's cult followers entered the Los Angeles home of film director Roman Polanski and savagely stabbed his pregnant wife, actress Sharon Tate, and shot and stabbed four others.



## People

### **Cannabis tax revenue falls two-thirds short of \$1 billion projection in first year**

California took in \$345.2 million in cannabis tax revenue during the first year of regulated sales in 2018, just more than two-thirds below the expected \$1 billion, according to figures released by the state Tuesday. Marijuana tax revenues climbed in the first three quarters of the year, from \$60.9 million the first quarter to \$80.2 million the second quarter, to a revised \$100.8 million in the third quarter.

[KHTS](#)

### **Soda, water, guns, and tires: They could all be taxed if California Democrats have their way**

It's a standard California Republican talking point that Democrats want to raise taxes. And it's true that Golden State Democrats have introduced, or plan to introduce, legislation that would raise or create several new taxes. If there's one thing the proposals have in common, it's that they all reflect some facet of the California Democratic Party's larger environmental and social justice bent.

[Merced Sun-Star](#)

### **Legal cannabis industry continues to struggle in California**

The drumbeat of disappointment over the slow start of legal marijuana in California keeps building with many dispensary owners, growers and local and state elected officials bemoaning the robust health of the illegal cannabis black market. Last week, state officials released the official tally of tax revenue in sales, excise and cultivation taxes in 2018 - the first year recreational cannabis sales were allowed under Proposition 64.

[CalWatchdog](#)

## Guns

### **State legislators to unveil bill regulating gun shows at Del Mar Fairgrounds**

A pair of San Diego area legislators on Friday announced a bill to ban the sale of guns and ammunition at gun shows held at the Del Mar Fairgrounds. The bill introduced by Assembly members Todd Gloria, D-San Diego, and Tasha Boerner-Horvath, D-Encinitas, would bar the state's 22nd District Agricultural District, which oversees operations at the fairgrounds, from authorizing the sale of guns and ammunition on fairgrounds property.

[City News Service](#)

### **A California mayor rolls out a new ordinance that has gun store owners outraged**

The next time you purchase a gun in San Jose, you may be recorded on camera. The mayor in that city, Sam Liccardo is trying to pass a city ordinance to keep guns from getting into the wrong hands. "It's a

draconian burden to put on gun dealers, it's ridiculous." The Firing Line gun store owner Jacob Belemjian hopes to never hear about a city ordinance the San Jose mayor is trying to roll out.

[Your Central Valley](#)

## Corrections

### **California inmates accuse prison guards of orchestrating 'gladiator fights'**

It had been months since Angeleigh Garcia saw her fiancé. An inmate at California State Prison-Corcoran, Garcia's fiancé was one of 350 Facility 3C inmates who has had visitation and yard time privileges restricted for five months. On Saturday, Garcia stood alongside a dozen loved ones of inmates of 3C before going to the prison to see her fiancé. She felt lucky, she said.

[Visalia Times-Delta](#)

## Homeless

### **Orange County cities sued over lack of homeless shelters**

Homeless residents of Orange County said in a federal class action lawsuit that five South County cities violated their rights by issuing citations and confiscating their property without providing them shelter. Duane Nichols, Darren James and Bruce Stroebel said in their 50-page complaint filed Wednesday that they have no way of complying with cities' anti-camping and anti-loitering laws since cities have refused to construct shelters within their jurisdictions, even as the homeless population continues to climb across the county.

[Courthouse News Service](#)

### **LA City Council approves downtown emergency homeless shelter**

The City Council approved the finalization of a property lease Friday that clears the way for an emergency homeless shelter to be opened in the downtown Los Angeles area. Councilman Jose Huizar introduced a motion last month calling for the 115-bed shelter at 1426 Paloma St. He said it could be opened within three months, becoming the third facility to be operational under Mayor Eric Garcetti's A Bridge Home program, which aims to open a temporary shelter in every City Council district while the city works to build more permanent supportive housing through a \$1.2 billion bond measure approved by city voters in 2016.

[City News Service](#)

### **A report finds one-third of LA County's homeless are black**

Los Angeles County Supervisor Mark Ridley-Thomas said Monday a new report highlighting the elevated levels of homelessness among black Angelenos is a "critical first step" in addressing the disparities affecting the African-American community. Black people make up 9 percent of the population of Los Angeles County, but more than one-third of its population is experiencing homelessness, which is consistent

demographically across the country, according to a report by the Los Angeles Homeless Services Authority Ad Hoc Committee on Black People Experiencing Homelessness.

[City News Service](#)

## Pensions

### **LA Mayor endorses continuation of lucrative DROP program for cops, firefighters**

Los Angeles Mayor Eric Garcetti said Friday he plans to continue the city's DROP program that allows some police officers and firefighters to effectively collect double pay during the final five years of their careers. "DROP is a critical tool that helps us maintain stability and continuity at our police and fire departments," Garcetti said in a joint statement with City Council president Herb Wesson.

[NBC Los Angeles](#)

### **Texas and California pensions team up with buyout firms for more deals**

Big U.S. pensions are pushing deeper into private equity, seeking exclusive deals alongside buyout firms and at sweeter terms. Texas and California teachers are ramping up their allocations to co-investments, with more staff and new offices dedicated to buyouts. And Calpers, the largest U.S. pension, discussed this week whether to take a bolder step and do deals on its own.

[Bloomberg](#)

***For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).***

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ ggiguere@ci.sunnyvale.ca.us](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [Association of Deputy District Attorneys](#)  
**To:** [fggurina@sunnyvale.ca.gov](mailto:fggurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for March 4, 2019  
**Date:** Monday, March 04, 2019 5:03:15 AM

---

Click here [Having trouble viewing this email?](#)



## Courts & Rulings

### **Value of property received from two thefts can't be combined to create felony**

A man who received stolen property from two clothing stores should

have been charged with two misdemeanor counts, rather than the value of the goods being added together, with the charge being receipt of stolen property worth in excess of \$950, a felony, the First District Court of Appeal declared yesterday.

[Metropolitan News-Enterprise](#)

### **Court rules L.A. council members wrongly blocked public testimony at 'special' meetings**

The Los Angeles City Council must allow people to testify on issues considered during their "special" meetings, which are called with just one day of notice, a three-judge panel has ruled. In a 15-page decision, the 2nd District Court of Appeal said the council improperly prevented Studio City resident Eric Preven from weighing in on a development issue taken up during a special meeting in 2015.

[MSN](#)

### **With women in combat roles, a federal court rules male-only draft unconstitutional**

A federal judge in Texas has declared that an all-male military draft is unconstitutional, ruling that "the time has passed" for a debate on whether women belong in the military. The decision deals the biggest legal blow to the Selective Service System since the Supreme Court upheld the draft registration process in 1981.

[USA Today](#)

### **Federal prosecutors' secret plea deal with politically connected sex abuser broke law, judge says**

Federal prosecutors violated the Crime Victims' Rights Act when they failed to notify a sex offender's underage victims about a secret plea deal, a federal judge in Florida has ruled. U.S. District Judge Kenneth Marra ruled Thursday on the conduct of prosecutors in the office of then-U.S. Attorney Alex Acosta of the Southern District of Florida.

[ABA Journal](#)

### **'Appointed for life, not for eternity.' Dead judge's vote shouldn't have counted, Supreme Court rule**

The U.S. Supreme Court said judges "are appointed for life, not for eternity," in setting aside a pay-discrimination ruling written by a jurist who died a week and a half before the decision was issued. The unsigned opinion said a federal appeals court was wrong to count the vote of the late Judge Stephen Reinhardt in a ruling that let a female math consultant sue a California school official.

[Bloomberg](#)

### **Los Angeles Police Union declines to appeal ruling on disciplinary records**

Leaders of the union representing Los Angeles police officers said today they have decided against appealing a judge's ruling calling for the public release of internal department records on officer-misconduct.



cases. Last week, Los Angeles Superior Court Judge Mitchell L. Beckloff rejected a bid by the Los Angeles Police Protective League to prevent the release of such records from cases that occurred prior to Jan. 1, when a new state law took effect requiring the documents to be made public.

[City News Service](#)

### **Orange County judge orders police records unsealed**

A judge in Southern California lifted a temporary seal on Orange County police misconduct records Thursday, striking another blow to police unions who've argued in courts across the state that unsealing the records violates officers' constitutional rights to privacy. The new California law opens up access to previously shielded internal records on police shootings, complaints of sexual assault by officers and internal records on police misconduct.

[Courthouse News Service](#)

### **Man who addressed council committee had right to address full body in special session**

A community activist who addressed a Los Angeles City Council committee in opposition to a project was wrongfully denied an opportunity to address the full 15-member body at a special session, the Court of Appeal for this district has held, pointing to a loophole in the Ralph M. Brown Act.

[Metropolitan News-Enterprise](#)

### **Mongols motorcycle club gets to keep prized patches, as federal judge rules against U.S. government's first-of-its-kind effort**

A federal judge has rejected the U.S. government's unprecedented effort to gain control of the prized patches that adorn the vests worn by the notorious Mongols motorcycle club, ruling seizing the outlaw organization's trademarks would be unconstitutional. The written ruling, released Thursday morning by U.S. District Judge David O. Carter, marks a setback for federal prosecutors who two months ago persuaded a Santa Ana jury to find the Southern California-based club guilty of racketeering.

[Orange County Register](#)

## **Prop 47, 57 & AB 109**

### **Man with no-bail warrant arrested after barricading himself in Goleta apartment**

A Carpinteria man was arrested Monday after leading law enforcement officers on a foot pursuit, barricading himself in a Goleta apartment and refusing to surrender, according to the Santa Barbara County Sheriff's Office. The department's AB 109 Compliance Response Team were searching for Jacob Dreyer, 28, who had a no-bail arrest warrant due to violating terms of his probation, said Kelly Hoover, a sheriff's spokeswoman.

[Noozhawk](#)

### **Auto burglars hit Menlo Park in a dozen incidents Sunday night**

Auto burglars struck several neighborhoods in Menlo Park on Sunday night (Feb. 24), according to reports from the crime log of the Menlo Park Police Department. Six of the 12 burglaries took place in the Menlo Oaks neighborhood, and three each were reported in Sharon Heights and Suburban Park - Lorelei Manor - Flood Park Triangle. Burglars broke into 10 of the vehicles by smashing windows, while one was unlocked.

[The Almanac](#)

### **California murder parolee robs Sacramento restaurant, patron shot, car-jacked**

Four-term Democratic California Governor Gov. Jerry Brown made reforming California's criminal justice sentencing guidelines a priority over his 16 total years as governor. Add to that his record number of 1,736 pardons and 284 prison commutations, and violent prison inmates have been released or made eligible for early release.

[California Globe](#)

## **Prosecutions/Prosecutors**

### **Santana: New OC DA wants to make a deal with feds ending DOJ jailhouse snitch probe**

Orange County District Attorney Todd Spitzer is calling on federal authorities to end their ongoing probe into use of jailhouse snitches in Orange County and instead make a deal to institute reforms. "I'm willing to admit everything that happened," Spitzer told me last week during a phone interview where we talked about the jail house scandal that catapulted him into office as the chief law enforcement officer in a county where that job had been seemingly phoned-in for a long time.

[Voice of OC](#)

### **Report: LAPD sends 102 allegations against former USC gynecologist to DA (Video)**

Dr. George Tyndall was fired by the school after it came to light that female patients had accused him of sexual misconduct over several decades. Jeff Michael reports.

[CBS Los Angeles](#)

### **OC judge weighing move to dismiss case Vs. 'Real Housewives' son**

A judge Tuesday put off ruling on whether to dismiss an attempted murder case against a son of a former "Real Housewives of Orange County" cast member based on allegations of outrageous governmental misconduct. Joshua Waring, the son of former "Real Housewives" cast member Lauri Peterson, is accused of shooting then-35-year-old Daniel Lopez outside a home in Costa Mesa on June 20, 2016. Two other people escaped injury in the drive-by attack.

[Costa Mesa Police Department](#)

### **District attorney declines to charge La Puente property owner of illegal marijuana sales**

A La Puente commercial landlord, who was arrested last year after authorities raided a marijuana dispensary allegedly operating without a license, will not be charged, officials confirmed Tuesday, Feb. 26. On Sept. 27, 2018, deputies with the Los Angeles County Sheriff's Department raided a marijuana dispensary that authorities said was operating illegally on a commercial property in the 15500 block of Amar Road.

[San Gabriel Valley Tribune](#)

## **Criminal Justice/Public Safety**

### **LAPD commander involved in controversial car crash is demoted**

A Los Angeles police commander has been demoted to captain after his city car was found wrecked and abandoned in Carson. Jeff Nolte, 52, who headed the LAPD's Force Investigation Group, has been on paid leave since he crashed his unmarked Dodge Charger on Jan. 24, then left the scene. With an investigation into his conduct underway, Nolte's rank was reduced one rung earlier this week, Josh Rubenstein, the department's communications director, said Friday.

[Los Angeles Times](#)

### **University professor condemned for previous comments saying cops 'need to be killed'**

UC Davis is condemning a professor's inflammatory statements where he said cops "need to be killed." English professor Joshua Clover reportedly wrote several tweets and made comments in a 2015 interview with SF Weekly where he referenced violence against law enforcement officers.

[CBS Sacramento](#)

### **Could a new California law free a teen killer convicted as an adult for a brutal double homicide?**

Six years ago, someone savagely stabbed to death Chip Northup, 87, and Claudia Maupin, 76, as they slept inside their Davis, California, home. Police found no physical evidence and investigators thought they might have some challenges finding the killer. "It was the most horrific, depraved murder I've ever seen as the district attorney in this county," Yolo County, California, D.A Jeff Reisig tells "48 Hours" correspondent Erin Moriarty.

[48 Hours](#)

### **Two inmates released after being convicted of murder**

Two men who spent years in state prison after being convicted of murder in separate cases were freed Friday following efforts spearheaded by two programs at Loyola Law School seeking their release. Michael Tirpak, now 43, had been behind bars for nearly 25

years following his 1996 conviction for first-degree murder in the 1994 killing of David Falconer in Compton.

[My News LA](#)

### **Waiting for a decision in Stephon Clark's killing, they are ready to be disappointed - and to mobilize**

An 8-foot-tall chain-link fence went up around the Sacramento County district attorney's office, weeks after police shot and killed Stephon Clark - an unarmed black man whose cellphone they mistook for a gun. Demonstrators previously had blocked the front doors, chanting "Shut it down!" as protests erupted across the capital city.

[Los Angeles Times](#)

### **Governor orders more DNA testing in 1983 California killings**

California Gov. Gavin Newsom ordered additional DNA testing Friday on evidence that a death-row inmate says will prove his innocence in a 35-year-old murder case that has drawn national attention. Former Gov. Jerry Brown previously ordered testing of four pieces of evidence that condemned inmate Kevin Cooper says will show he was framed for the 1983 hatchet and knife killings of four people, including two children, in Chino Hills.

[AP](#)

### **Herbalist sentenced to jail after death of 13-year-old diabetic boy he treated**

A Los Angeles herbalist convicted of practicing without a license was sentenced to four months in jail for child abuse in the same case in connection with the death of a 13-year-old diabetic boy, the city attorney said. Timothy Morrow, 84, was found guilty of one count of practicing without a license at a jury trial Feb. 20 and pleaded no contest Monday to a connected charge of misdemeanor child abuse likely to produce great bodily injury or death, Los Angeles City Attorney Mike Feuer said in a statement.

[NBC News](#)

### **Camfield Partners plans El Sereno warehouse for LAPD's auto theft division**

Camfield Partners wants to build a large new warehouse and office in El Sereno for storing evidence and equipment for the Los Angeles Police Department. The Laguna Hills-based firm filed plans with the city for the 80,000-square-foot warehouse earlier this month. It would be built on a vacant 6.8-acre lot at 1925 N. Marianna Avenue. Camfield, a small firm led by Ken Jackson, purchased the lot in 2015 for \$6.5 million.

[The Real Deal](#)

## **Policy & Legal Issues**

### **Bailing on bail reform**

Last September, as part of a national push for criminal-justice reform,

Robert F. Kennedy Human Rights, a charitable organization, announced a plan to pay the bail of every woman and minor held in New York City's jails. According to the group, run by Kerry Kennedy, the slain senator's daughter, "access to justice depends on whether you can afford bail. The majority of people incarcerated in the notoriously violent Rikers Island are behind bars for the crime of being too poor."

[City Journal](#)

### **California's jails and prisons becoming ground zero in the state's mental health crisis**

These days, the main path to treatment at a state psychiatric hospital is through jail. However controversial those state hospitals may be, many families conclude they are the best option for their loved ones. "That is a sad state of affairs in our society, that only when you get locked up does it become a priority to get you treatment," said Los Angeles District Attorney Jackie Lacey, who said she's heard many parents describe similar feelings of desperation.

[North Coast Journal](#)

### **California man who spent 39 years in prison gets \$21 million for wrongful conviction**

A California man who was wrongfully convicted for killing an ex-girlfriend and her son four decades ago has reached a \$21 million settlement with the city of Simi Valley, officials said. Craig Coley, 71, was sentenced to life in prison without parole for the 1978 murder of his former partner, Rhonda Wicht, and her 4-year-old son, Donald, at their apartment.

[Reuters](#)

### **As death toll keeps rising, U.S. communities start rethinking Taser use**

Warren Ragudo died after two Taser shocks by police intervening in a family altercation. Ramzi Saad died after a Taser shock by police during a dispute between Saad and his mother. Chinedu Okobi died after police used a Taser to subdue him in a confrontation they blamed on his refusal to stop walking in traffic. All three were unarmed. All three had histories of mental illness.

[Reuters](#)

### **Fire scientists say the arson case against Claude Garrett was fatally flawed. Will anyone listen?**

In a tense, crowded room inside Nashville's Riverbend Maximum Security Institution, Claude Garrett sat before a large TV monitor and stared at the screen. Behind him, a crowd of people gathered before a long conference table. Garrett wore prison-issued blue jeans, glasses, and a serious expression. Looking back at him on the screen was Richard Montgomery, chair of the Tennessee Board of Parole.

[The Intercept](#)

### **California Attorney General Xavier Becerra faces criticism from**



### **criminal justice reformers**

Another Democratic state attorney general is facing sharp criticism from activists for allegedly getting in the way of criminal justice reform and showing bad faith while doing so. Former Rep. Xavier Becerra (pictured), D-Los Angeles, was appointed in 2016 by Gov. Jerry Brown to replace state Attorney General Kamala Harris after she was elected to the U.S. Senate. He won a full term in the 2018 elections.

[CalWatchdog](#)

### **California keeps a secret list of criminal cops, but says you can't have it**

Their crimes ranged from shoplifting to embezzlement to murder. Some of them molested kids and downloaded child pornography. Others beat their wives, girlfriends or children. The one thing they had in common: a badge. Thousands of California law enforcement officers have been convicted of a crime in the past decade, according to records released by a public agency that sets standards for officers in the Golden State.

[Investigative Reporting Program, UC Berkeley](#)

### **California bill introduces new hurdle to access public records**

A San Diego lawmaker is trying to complicate the already convoluted process that reporters and Californians must take to view public records and make it harder for requesters to recoup attorney's fees when they prevail over the government in court. Introduced last Friday just ahead of a deadline for new bill proposals, Senate Bill 615 would require anyone not satisfied with a public records request to mediate with the relevant government agency before taking it to court.

[Courthouse News Service](#)

### **Woe to illegal pot shops: Water, power to be shut off**

With hundreds of illegal marijuana shops continuing to operate in Los Angeles, the City Council moved forward with a plan Tuesday aimed at cracking down on the businesses by shutting off their utilities. The idea of shutting off water and power at illegal pot shops was proposed last year by Councilwomen Nury Martinez and Monica Rodriguez, and the council voted 13-0 to have the City Attorney's Office draft an ordinance outlining the proposed policy.

[My News LA](#)

### **San Francisco dropped the Joint Terrorism Task Force two years ago. Now the FBI wants to pick things back up.**

After a two-year separation, the FBI wants to get back together with San Francisco. The bureau sent Mayor London Breed a letter on Jan. 29, touting the advantages of a currently suspended partnership between the FBI and the San Francisco Police Department - largely meant to quash terrorist threats in the region.

[Mission Local](#)

---

### **Suspect impersonates LAPD detective during Chinatown jewelry store robbery**

Authorities are searching for multiple suspects - one of whom impersonated a Los Angeles police detective - in connection with one robbery and two attempted robberies at two jewelry stores in the same Chinatown neighborhood over a four-hour period Tuesday. It's unclear if the three incidents are linked.

[CBS Los Angeles](#)

### **FBI releases preliminary semiannual crime statistics for 2018**

Statistics released today in the FBI's Preliminary Semiannual Uniform Crime Report revealed overall declines in the number of violent crimes and property crimes reported for the first six months of 2018 when compared with figures for the first six months of 2017. The report is based on information from 14,509 law enforcement agencies that submitted three to six months of comparable data to the FBI's Uniform Crime Reporting (UCR) Program.

[FBI National Press Office](#)

### **Feds: 3 men conspired with L.A. Sheriff's Deputy to steal 1,200 lbs of marijuana, \$645K cash**

Three men were arrested on Thursday morning on federal drug distribution charges alleging they conspired with a Los Angeles County sheriff's deputy and others to steal more than 1,200 pounds of marijuana and \$645,000 in cash and money orders during an armed robbery of a downtown Los Angeles warehouse that was staged to look like law enforcement was executing a search warrant, according to federal authorities.

[Fox 11 Los Angeles](#)

### **Man dressed as LADWP worker among suspects in West Hills home invasion**

Authorities say three men in ski masks - one of whom was wearing a Los Angeles Department of Water and Power vest - forced their way into a West Hills home Monday morning. The home invasion occurred at around 8 a.m. in the 7800 block of Bobbyboyar Avenue, according to L.A. police. Once they gained entry into the residence, police say the suspects tied up the homeowner, pistol-whipped him, and ransacked the home.

[CBS LA](#)

### **Meth problem puts Fresno in the national spotlight, again**

A recent documentary on "Vice News" highlighted the methamphetamine addiction problems among Fresno's homeless. A homeless woman Action News talked with named Katherine told us she has been living on the streets for four years. She acknowledged drugs are a problem in the homeless community. "You find that everywhere you go. Everywhere, it's not in just one certain spot. It's all over," she said.

[KFSN](#)

### **San Francisco man was hanged, drugged, put in suitcase and dumped in the Bay: Prosecutors**

A 47-year-old San Francisco man has been charged with torturing and murdering a 23-year-old, before putting the dead man's body into a suitcase and tossing it into the San Francisco Bay earlier this month, authorities said. Gerald William Rowe was arrested last week after the body, later identified as San Francisco resident George Randall Saldivar, was found floating in the Bay near Pier 39 on Feb. 18, according to court records.

[Los Angeles Times](#)

### **2 men indicted in \$2M kidnapping scheme in SoCal; taped and bound O.C. victim now believed dead**

Two Chinese nationals have been indicted in a \$2 million kidnapping scheme in Southern California involving a victim who was physically restrained inside a closet and is now believed dead, the U.S. Department of Justice announced Thursday. Guangyao Yang, 25, and Peicheng Shen, 33, are facing charges of conspiracy to kidnap, kidnapping, attempted extortion in violation of the Hobbs Act and threat by foreign communication, according to a DOJ news release.

[KTLA](#)

## **Los Angeles County Sheriff**

### **LA sheriff backs release of police misconduct records**

A California law requiring public disclosure of police misconduct records has been challenged by police unions in courts across the state, but received support Wednesday from Los Angeles County Sheriff Alex Villanueva. Police officer unions, including the Los Angeles Police Protective League and the Association for Los Angeles Deputy Sheriffs, have sued to bar retroactive enforcement of California Senate Bill 1421.

[Courthouse News Service](#)

### **LA's sheriff says jail reform has failed. We went inside to find out**

Los Angeles County Sheriff Alex Villanueva says reforms designed to reduce violence by deputies in the jails are a failed "social experiment." He claims attacks on guards are up, and his deputies feel the new rules keep them from fully defending themselves. Villanueva has argued his deputies need a freer hand to use force.

[LAist](#)

### **OIG report raises concerns about overcrowded jails, lack of care**

A number of concerns about the Los Angeles County Sheriff's Department - including overcrowded jails, the quality of medical and mental health care for inmates and the persistence of dangerous social cliques - have been raised by the Office of Inspector General in a report set to be formally accepted by the Board of Supervisors Tuesday.

[My News LA](#)

### **Alex Villanueva has a lot of work to do to regain L.A.'s trust**

As with other political newcomers who achieve astounding initial success, the upset victory of newly elected Los Angeles Sheriff Alex Villanueva deserves study, and props to the person who pulled it off. Almost no one saw it coming. It wasn't simply that the underfunded campaign of a retired former lieutenant didn't stand out for reasons of lack of name recognition.

[Southern California News Group](#)

## **Los Angeles County**

### **Lawsuit filed in death of Los Angeles County jail inmate who suffered from schizophrenia**

Leon Nyarecha tearfully recounts the day his younger brother died while in Los Angeles County Sheriff's custody at the Men's Central Jail last June. "Lewis was my little brother," he said. "The day he died was the worst day of my life." Leon Nyarecha is now suing the county and the sheriffs department for negligence and battery. "He suffered from schizophrenia," said attorney Jovan Blacknell.

[NBC Los Angeles](#)

### **Assaults on guards in L.A. County juvenile detention increase sharply**

Violence at times erupts with little warning inside Los Angeles County's juvenile detention halls and camps. That's what happened one February night two years ago as Edgar Arrondo - then a senior guard at a sprawling facility in Sylmar - walked a teenage detainee to a mental health evaluation. A rival gang member charged at the teen, ignoring Arrondo's verbal warnings. The youths collided. A fight ensued.

[Los Angeles Times](#)

### **Goldstein Investigation: Money flows like water at water board meetings**

David Goldstein finds the money flows like water at water board meetings. "Ms. Kwan, I'm David Goldstein with CBS2 News. Can I talk with you a second?" "No!" she replies. Carol Kwan wasn't talking. She's an elected board member for the West Basin Municipal Water District. It's a public agency which is a wholesale supplier of water to nearly one million people in 17 cities and unincorporated areas in Los Angeles County - mostly in the South Bay.

[CBS Los Angeles](#)

### **Environmentalists furious over methane capture plan in Aliso Canyon gas leak settlement**

Environmental groups are criticizing last year's \$120 million court settlement in the devastating Aliso Canyon gas leak because a large portion of the money will be used to fund a plan that would capture

methane from dairy farms in the state's farm belt - more than 100 miles from where the blowout occurred - and convert it into natural gas.

[CBS LA/AP](#)

### **Is your hospital prepared for gang violence and injuries?**

Los Angeles County has more than 1,300 gangs with over 150,000 members. In the city of Los Angeles alone, there are an estimated 450 active gangs with a combined membership of over 45,000 individuals. In the last three years, there were over 16,398 violent gang crimes in Los Angeles, according to the Los Angeles Police Department. Those crimes included 491 homicides, 7,047 felony assaults, 5,518 robberies and 98 rapes.

[Campus Safety](#)

### **Poisonous pot found in some Los Angeles-area stores**

Some of the marijuana products sold by Southern California stores and delivery services are loaded with banned toxic chemicals that could make you sick, according to an NBC4 I-Team investigation. "Why would you want to put poison in your body," said Hinaxi Patel, technical director of Brightside Scientific in Long Beach, an independent state-licensed lab that tested the pot products for NBC4.

[NBC Los Angeles](#)

### **Family files lawsuit against Democratic donor Ed Buck in overdose death**

The mother of a man who died inside the West Hollywood apartment of a prominent Democratic Party donor filed a wrongful-death lawsuit Tuesday that names him and the Los Angeles County District Attorney as defendants. LaTisha Nixon told NBC4 Tuesday she was frustrated that authorities had failed to file criminal charges for the 2017 overdose death of her 26-year-old son, Gemmel Moore, and didn't want to see any other mothers to lose their loved ones in a similar way.

[NBC Los Angeles](#)

## **Convictions/Sentences/Parole**

### **Ex-Fullerton police chief pleads guilty to attacking paramedics at Lady Antebellum concert**

A former Fullerton police chief and one of his captains plead guilty Monday to misdemeanor charges for starting a fight with paramedics at a Lady Antebellum concert last summer in Irvine while off-duty, an incident which forced the chief to resign. Former Chief David Hendricks, 47, and Capt. Thomas Oliveras, 50, pleaded guilty in Orange County Superior Court in Newport Beach to disturbing the peace by fighting.

[CBS Los Angeles](#)

### **Ex-Pasadena police officer sentenced to prison on Federal gun charges**



A former Pasadena police lieutenant was sentenced Monday to a year and a day in federal prison for selling more than 100 firearms without a license and making false statements during a gun purchase. Vasken Kenneth Gourdikian, who resigned from the Pasadena Police Department in March 2018 after a 22-year career, was also ordered by U.S. District Judge Stephen V. Wilson to pay a \$10,000 fine and serve a year of supervised release after completing his prison term.

[My News LA](#)

### **Woman sentenced to 15 years in prison for attack on 91-year-old man**

A Los Angeles woman was sentenced Thursday to 15 years in state prison for beating a 91-year-old grandfather with a brick in Willowbrook last summer. Laquisha Jones, 30, pleaded no contest Dec. 27 to a felony elder abuse charge stemming from the attack, which occurred on the Fourth of July last year. Jones attacked the man without provocation near 118th and Robin streets, according to the Los Angeles County District Attorney's Office.

[City News Service](#)

### **Parole denied for man convicted of 1982 Guerneville murder**

A man incarcerated for a 1982 murder was denied parole at a hearing Thursday, according to the Sonoma County District Attorney's Office. Vernon Bragg, 65, of Guerneville, pleaded guilty in 1985 to second-degree murder and use of a firearm in the shooting death of Ray Bragg in 1982. On Thursday, Vernon Bragg, a California Department of Corrections and Rehabilitation inmate, was given a three-year denial of parole by the State of California Board of Parole Hearings.

[Bay City News Service](#)

### **Ex-Orange County teacher sentenced to 2 years for sex with 17-year-old boy**

A man who taught at an Orange County high school was handed a two-year state prison sentence Friday for a sex act involving a 17-year-old boy who lived with him for a short time in Long Beach. Andrew Bueno-Potts - also known as Drew Bueno-Potts - was also ordered to register as a sex offender for the rest of his life and to stay away from the young man for 10 years, according to the Los Angeles County District Attorney's Office.

[City News Service](#)

### **House of horrors case: Turpin parents accused of beating, starving children plead guilty**

The California couple accused of beating, starving and holding 12 of their children captive pleaded guilty Friday to multiple charges. David and Louise Turpin pleaded guilty to 14 counts each of torture, dependent adult abuse, child endangerment and false imprisonment. Riverside County District Attorney Michael Hestrin said at a news

conference that because of the plea deal, the Turpins will not be headed to trial.

[NBC News](#)

### **Ex-NASA contractor sentenced to prison for sextortion**

A onetime NASA contractor was sentenced on Monday to nearly five years behind bars for stalking women online with threats to publish nude photos unless they provided him with additional explicit pictures.

Richard Gregory Bauer, 28, of Los Angeles, a former contractor at the NASA Armstrong Flight Research Center, must also serve three years under supervised release after completing his federal prison term.

[City News Service](#)

## **Consumer Warnings**

### **Amazon's counterfeit problem is a big one - for shareholders, brand owners and consumers alike**

On February 1, Amazon.com, Inc. filed a Form 10-K annual report with the U.S. Securities and Exchange Commission. Along with reporting its year-end earnings for the 2018 fiscal year, this particular SEC filing was notable because Amazon officially acknowledged to shareholders that the company's online sales platforms face the risk of being found liable for fraudulent or unlawful activities of sellers on those platforms.

[IP Watchdog](#)

### **Los Angeles District Attorney's Office warns against new 'tap-to-pay' credit card scam**

The District Attorney's Office (DA Office) cautions that the public should be more aware of potential "scammers trying to steal personal information as some credit card companies issue new 'tap-to-pay' cards". In this credit card fraud, the initiation takes place when scammers contact consumers who may be receiving new cards from their credit card companies.

[KHST](#)

### **Those annoying robocalls can be illegal and now some consumers are fighting back**

Robocalls can interrupt us multiple times a day. There's no sugarcoating it, they're downright annoying. But now consumers are fighting back.

According to the Federal Trade Commission, unwanted calls are "far and away the biggest consumer complaint." "Look at all of these missed calls," said Jamie Bergstein while scrolling through her phone outside of Philadelphia City Hall, "I get them all the time!"

[CBS Philly](#)

## **California/National**

### **Under new CA bill, 911 dispatchers would be trained to identify and de-escalate mental health crises**

A new California bill, AB 680, aims to reduce the criminalization of people suffering from mental health emergencies, and improve their interactions with police, by requiring all 911 dispatchers to receive mental health crisis intervention training. "Too many law enforcement interactions with people in mental health crisis end in tragedy," said the bill's author Assemblymember Kansen Chu (D-San Jose).

[Witness LA](#)

### **Law would protect crime accusers from arrest**

California lawmakers, whose antics have included attempting to designate counseling against same-sex attractions "consumer fraud" requiring school children to celebrate gay activist Harvey Milk, are at it again. A proposed law would grant immunity to residents from arrest if they are in the process of reporting a sex crime or other crime of violence.

[Seneca Standard](#)

### **The sudden death of near-legendary San Francisco public defender, Jeff Adachi, stuns Bay Area leaders & the many ordinary people whom he championed**

When the news flew around the state that San Francisco Public Defender, Jeff Adachi, 59, had died of a possible heart attack on Friday night, after having trouble breathing while having dinner with a friend, public officials, the legal community, and an unusually wide variety of ordinary people reacted with shock and genuine grief, as if for a member of the family.

[Witness LA](#)

### **For victims of hate crimes, Jussie Smollett case is a giant betrayal**

The dramatic unraveling of the story of a vicious attack on actor Jussie Smollett has spread deep concern among hate-crime victims that growing racist and anti-gay violence now may be more likely to go unreported and unpunished. Last week, Chicago police arrested Smollett, the black, openly gay star of Fox television's "Empire," and charged him with orchestrating a fake encounter on a Chicago street with two men whom he alleged had assaulted him, hung a rope around his neck, and hurled homophobic and racist slurs while shouting, "This is MAGA country."

[Los Angeles Times](#)

### **Sharon Tate's sister believes Charles Manson has more victims: 'We are just scraping the surface'**

The Manson family killings were as gruesome as they were shocking. In the early hours of Aug. 9, 1969, Charles Manson's cult followers entered the Los Angeles home of film director Roman Polanski and savagely stabbed his pregnant wife, actress Sharon Tate, and shot and stabbed four others.

## People

### **Cannabis tax revenue falls two-thirds short of \$1 billion projection in first year**

California took in \$345.2 million in cannabis tax revenue during the first year of regulated sales in 2018, just more than two-thirds below the expected \$1 billion, according to figures released by the state Tuesday. Marijuana tax revenues climbed in the first three quarters of the year, from \$60.9 million the first quarter to \$80.2 million the second quarter, to a revised \$100.8 million in the third quarter.

[KHST](#)

### **Soda, water, guns, and tires: They could all be taxed if California Democrats have their way**

It's a standard California Republican talking point that Democrats want to raise taxes. And it's true that Golden State Democrats have introduced, or plan to introduce, legislation that would raise or create several new taxes. If there's one thing the proposals have in common, it's that they all reflect some facet of the California Democratic Party's larger environmental and social justice bent.

[Merced Sun-Star](#)

### **Legal cannabis industry continues to struggle in California**

The drumbeat of disappointment over the slow start of legal marijuana in California keeps building with many dispensary owners, growers and local and state elected officials bemoaning the robust health of the illegal cannabis black market. Last week, state officials released the official tally of tax revenue in sales, excise and cultivation taxes in 2018 - the first year recreational cannabis sales were allowed under Proposition 64.

[CalWatchdog](#)

## Guns

### **State legislators to unveil bill regulating gun shows at Del Mar Fairgrounds**

A pair of San Diego area legislators on Friday announced a bill to ban the sale of guns and ammunition at gun shows held at the Del Mar Fairgrounds. The bill introduced by Assembly members Todd Gloria, D-San Diego, and Tasha Boerner-Horvath, D-Encinitas, would bar the state's 22nd District Agricultural District, which oversees operations at the fairgrounds, from authorizing the sale of guns and ammunition on fairgrounds property.

[City News Service](#)

### **A California mayor rolls out a new ordinance that has gun store owners outraged**

The next time you purchase a gun in San Jose, you may be recorded on camera. The mayor in that city, Sam Liccardo is trying to pass a city ordinance to keep guns from getting into the wrong hands. "It's a

draconian burden to put on gun dealers, it's ridiculous." The Firing Line gun store owner Jacob Belemjian hopes to never hear about a city ordinance the San Jose mayor is trying to roll out.

[Your Central Valley](#)

## Corrections

### **California inmates accuse prison guards of orchestrating 'gladiator fights'**

It had been months since Angeleigh Garcia saw her fiancé. An inmate at California State Prison-Corcoran, Garcia's fiancé was one of 350 Facility 3C inmates who has had visitation and yard time privileges restricted for five months. On Saturday, Garcia stood alongside a dozen loved ones of inmates of 3C before going to the prison to see her fiancé. She felt lucky, she said.

[Visalia Times-Delta](#)

## Homeless

### **Orange County cities sued over lack of homeless shelters**

Homeless residents of Orange County said in a federal class action lawsuit that five South County cities violated their rights by issuing citations and confiscating their property without providing them shelter. Duane Nichols, Darren James and Bruce Stroebel said in their 50-page complaint filed Wednesday that they have no way of complying with cities' anti-camping and anti-loitering laws since cities have refused to construct shelters within their jurisdictions, even as the homeless population continues to climb across the county.

[Courthouse News Service](#)

### **LA City Council approves downtown emergency homeless shelter**

The City Council approved the finalization of a property lease Friday that clears the way for an emergency homeless shelter to be opened in the downtown Los Angeles area. Councilman Jose Huizar introduced a motion last month calling for the 115-bed shelter at 1426 Paloma St. He said it could be opened within three months, becoming the third facility to be operational under Mayor Eric Garcetti's A Bridge Home program, which aims to open a temporary shelter in every City Council district while the city works to build more permanent supportive housing through a \$1.2 billion bond measure approved by city voters in 2016.

[City News Service](#)

### **A report finds one-third of LA County's homeless are black**

Los Angeles County Supervisor Mark Ridley-Thomas said Monday a new report highlighting the elevated levels of homelessness among black Angelenos is a "critical first step" in addressing the disparities affecting the African-American community. Black people make up 9 percent of the population of Los Angeles County, but more than one-third of its population is experiencing homelessness, which is consistent



demographically across the country, according to a report by the Los Angeles Homeless Services Authority Ad Hoc Committee on Black People Experiencing Homelessness.

[City News Service](#)

## Pensions

### **LA Mayor endorses continuation of lucrative DROP program for cops, firefighters**

Los Angeles Mayor Eric Garcetti said Friday he plans to continue the city's DROP program that allows some police officers and firefighters to effectively collect double pay during the final five years of their careers. "DROP is a critical tool that helps us maintain stability and continuity at our police and fire departments," Garcetti said in a joint statement with City Council president Herb Wesson.

[NBC Los Angeles](#)

### **Texas and California pensions team up with buyout firms for more deals**

Big U.S. pensions are pushing deeper into private equity, seeking exclusive deals alongside buyout firms and at sweeter terms. Texas and California teachers are ramping up their allocations to co-investments, with more staff and new offices dedicated to buyouts. And Calpers, the largest U.S. pension, discussed this week whether to take a bolder step and do deals on its own.

[Bloomberg](#)

***For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).***

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [SANS NewsBites](#)  
**To:** [Leonardo Burgueno](#)  
**Subject:** SANS NewsBites Vol. 21 Num. 017 : US Cyber Command Blocked Russian Trolls During 2018 Elections; 2019 X-Force Threat Intelligence Report: Cybercriminals Changing Priorities  
**Date:** Friday, March 01, 2019 11:53:07 AM

---

[View this email as a web page](#)



March 1, 2019

Vol. 21, Num. 017

## Top of The News

- US Cyber Command Blocked Russian Trolls During 2018 Elections
- 2019 IBM X-Force Threat Intelligence Index

## The Rest of the Week's News

- Cisco Flaws Patched

## Cybersecurity Training Update

[SANS 2019](#) | Orlando, FL | April 1-8

[SANS San Francisco Spring 2019](#) | March 11-16

[SANS St. Louis 2019](#) | March 11-16

- [Drupal Admins Urged to Patch for Flaw That is Being Actively Exploited](#)
- [Cobalt Strike Flaw Exposes IP Addresses of Malicious Command-and-Control Servers](#)
- [Man Pleads Guilty in Booter/Stresser Case](#)
- [What Would It Take to Make a Congressional Office of Technology Assessment Work?](#)
- [DoD's Accelerated Cyber Specialist Hiring Program Needs More Staff](#)
- [Adobe Will Retire Shockwave in April](#)
- [TSA Oversees Pipeline Security](#)

## Internet Storm Center Tech Corner

[SANS Norfolk 2019](#) | March 18-23

[ICS Security Summit & Training 2019](#) | Orlando, FL | March 18-25

[Blue Team Summit & Training 2019](#) | Louisville, KY | April 11-18

[SANS Boston Spring 2019](#) | April 14-19

[SANS Seattle Spring 2019](#) | April 14-19

[SANS Northern Virginia-Alexandria 2019](#) | April 23-28

[SANS London April 2019](#) | April 8-13

[SANS Cyber Defence Canberra 2019](#) | June 24-July 13

### [SANS OnDemand and vLive Training](#)

Get a 9.7" iPad, Samsung Galaxy Tab A or Take \$250 Off with OnDemand or vLive training. Offer ends March 6.

### Single Course Training

[SANS Mentor](#) and [Community SANS](#)

View the full SANS [course catalog](#) and [skills roadmap](#)

Technical content sponsored by Atomicorp



**OSSEC Con2019, March 20-21.** "The Future of OSSEC: Security and Compliance for Cloud, On-Premise and Hybrid Environments" You will learn about the latest features, 2019 roadmap, public and private cloud deployments and the power of global threat intelligence. **FREE attendance for SANS subscribers.**

Register for **OSSEC Con2019** and enter discount code **SANS2019** at checkout: <https://www.sans.org/info/210830>

## Top of the News

### US Cyber Command Blocked Russian Trolls During 2018 Elections

(February 26, 27, & 28, 2019)

The US Cyber Command (USCYBERCOM) is responsible for having blocked the activity of a notorious Russian troll operation during the 2018 mid-term elections. The activity took place from mid-October through mid-November of 2018 and included blocking the Russian Internet Research Agency's Internet access on the day of the election. The US Department of Homeland Security provided support to USCYBERCOM in this initiative.

#### Editor's Note

[Williams]

There aren't a lot of places where military cyber action makes sense outside of assistance to kinetic operations. This is one of those places. The Russians almost certainly had a plan to disrupt the midterm elections. On the days they needed to execute that plan, they were disrupted from doing so. Any level of disruption in this particular case is a success from a CYBERCOM standpoint. That was the good part. Here's the bad part: we can't do this reliably again. Next time, they'll have a decentralized plan with multiple Internet points of presence that will be much harder to disrupt. But even if the Russians can't be fully disrupted on the days surrounding the 2020 elections, this operation has already increased the Russians' costs to mount their operations. That itself is a win. Anyone with a tested disaster recovery plan knows they aren't free.

**Read more in:**

- [www.washingtonpost.com](http://www.washingtonpost.com): U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms
- [www.eweek.com](http://www.eweek.com): U.S. Cyber-Warriors Disrupt Russian Election Attacks
- [arstechnica.com](http://arstechnica.com): Report: US Cyber Command took Russian trolls offline during midterms
- [thehill.com](http://thehill.com): US cyber operation blocked internet for Russian troll farm on Election Day 2018: report

## 2019 IBM X-Force Threat Intelligence Index

(February 26, 2019)

According to the 2019 IBM X-Force Threat Intelligence Index, cybercriminals are moving away from ransomware and instead turning to cryptojacking and business email compromise (BEC) to make money. The index also noted that attackers are increasingly using "non-malicious tools including PowerShell and PsExec to evade detection."

**Editor's Note**

[Neely]

Social Engineering will always be a challenging threat vector to mitigate and our adversaries know this. Continued diligence and user awareness, updated as the TTPs (Tactics, Techniques and Procedures) change, is the best mitigation. While file-less malware is becoming more prevalent and requires new detection and mitigation approaches, don't retire existing measures without ensuring you still have protection from prior attack vectors.

**Read more in:**

- [www.theregister.co.uk](http://www.theregister.co.uk): Who needs malware? IBM says most hackers just PowerShell through boxes now, leaving little in the way of footprints
- [www.eweek.com](http://www.eweek.com): Ransomware Attacks Decline as Cryptojacking Grows, IBM X-Force Reports
- [newsroom.ibm.com](http://newsroom.ibm.com): IBM X-Force Report: Ransomware Doesn't Pay in 2018 as Cybercriminals Turn to Cryptojacking for Profit

---

Sponsored Links

Are you involved with operational technology and ICS? SANS wants to hear from you! **Take 10 minutes to complete the State of OT/ICS Cybersecurity Survey** and enter to *win a \$400 Amazon gift card*. <https://www.sans.org/info/210835>

What does it take to establish a successful security operations program? **Take the 2019 SANS SOC Survey** and enter for a chance to *win a \$400 Amazon gift card*. <https://www.sans.org/info/210840>

Check out the **SANS Blog Page**: <https://www.sans.org/info/210850>



## Cisco Flaws Patched

(February 28, 2019)

Cisco is urging users of its wireless VPN and firewall routers to install updates to fix a critical vulnerability that could allow attackers to gain elevated privileges on unpatched systems. The security issue "is due to the improper validation of user-supplied data in the web-based management interface." Cisco also released a fix for a privilege elevation flaw affecting the Webex Meetings platform.

### Editor's Note

[Neely]

If you have Cisco RV110W, RV130W or RV215W Wireless-N VPN routers, patch them. The risk can be mitigated by disabling remote management, but this may not be practical for centralized management. Cisco also released a patch for WebEx Meetings Desktop and WebEx Productivity Tools for Windows, vulnerability CVE-2019-1674, which allows for arbitrary code execution as a privileged user. WebEx shops will want to deploy quickly to mitigate the risk.

### Read more in:

- [www.zdnet.com](http://www.zdnet.com): Cisco: Patch routers now against massive 9.8/10-severity security hole
- [www.scmagazine.com](http://www.scmagazine.com): Cisco patches two code execution vulnerabilities
- [threatpost.com](http://threatpost.com): Cisco Fixes Critical Flaw in Wireless VPN, Firewall Routers
- [threatpost.com](http://threatpost.com): Cisco Patches High-Severity Webex Vulnerability For Third Time
- [www.bleepingcomputer.com](http://www.bleepingcomputer.com): Cisco Fixes Critical RCE Vulnerability in RV110W, RV130W, and RV215W Routers

## Drupal Admins Urged to Patch for Flaw That is Being Actively Exploited

(February 27, 2019)

A critical flaw in Drupal CMS that was disclosed on February 20 is now being actively exploited. Admins are urged to apply the updates. Attackers are taking advantage of the flaw to "deliver" cryptominers and other malware. The issue can lead to arbitrary PHP code execution. Researchers from Imperva found that the immediate mitigations suggested in Drupal's February 20, 2019 advisory do not fully protect against attacks.

### Editor's Note

[Murray]

Many, not to say most, of our vulnerabilities result from the failure of input validation in the absence of more fundamental protections (e.g., finite-state operating systems, symbolic-only addressing, strongly typed objects, process to process isolation, application-only systems, and restrictive access control policies.)

### Read more in:

- [www.theregister.co.uk](http://www.theregister.co.uk): Friendly reminder to Drupal admins: Secure your sh!t before latest RCE-holes get you
- [www.scmagazine.com](http://www.scmagazine.com): Highly critical Drupal flaw being exploited in the wild
- [www.imperva.com](http://www.imperva.com): Latest Drupal RCE Flaw Used by Cryptocurrency Miners and Other Attackers
- [www.drupal.org](http://www.drupal.org): Drupal core - Highly critical - Remote Code Execution - SA-CORE-2019-003

## Cobalt Strike Flaw Exposes IP Addresses of Malicious Command-and-Control Servers



(February 28, 2019)

Cobalt Strike, a legitimate pen testing tool, has also been used by cyber criminals to host their command-and-control servers. A flaw in the tool can be exploited to determine the IP addresses of those servers. The flaw has been fixed in legitimate copies of Cobalt Strike, but as cyber criminals are often working with unregistered copies of software, the flaw could remain unpatched in those copies for some time.

#### Editor's Note

[Williams]

This flaw has been an open secret in the community for some time. There are ways to uniquely track many common penetration testing tools but the information is not widely shared, because releasing the information makes it inherently less valuable. Organizations have to decide whether keeping bad guys off their systems or attempting to help the rest of the community is the priority. On careful examination, most leadership teams decide that the community loses out.

#### Read more in:

- [www.zdnet.com](http://www.zdnet.com): Vulnerability exposes location of thousands of malware C&C servers

## Man Pleads Guilty in Booter/Stresser Case

(February 27 & 28, 2019)

A man from Illinois has pleaded guilty to conspiracy to cause damage to Internet-connected computers for his role in a scheme that offered booter and stresser services. Sergiy Usatyuk and a co-conspirator developed, controlled, and operated several of these services, which are used to launch distributed denial-of-service (DDoS) attacks.

#### Read more in:

- [krebsonsecurity.com](http://krebsonsecurity.com): Booter Boss Interviewed in 2014 Pleads Guilty

- [www.cyberscoop.com](http://www.cyberscoop.com): 20-year-old pleads guilty to DDoS-for-hire scheme that netted \$550,000

- [www.justice.gov](http://www.justice.gov): Former Operator of Illegal Booter Services Pleads Guilty to Conspiracy to Commit Computer Damage and Abuse

## What Would It Take to Make a Congressional Office of Technology Assessment Work?

(February 27, 2019)

After the Congressional Office of Technology Assessment (OTA) was shuttered in 1995 due to budget constraints, the burden of conducting research into highly technical and complex issues fell to legislative staff members. Advocates and former legislative staffers were invited by Representative Mark Takano (D-California), who sponsored a recent unsuccessful effort to revive OTA, to discuss what would be necessary to bring the office back and make it effective.

#### Editor's Note

[Pescatore, Neely]

The Congressional Research Service, under the Library of Congress, has continued to be funded and has over 600 employees. CRS has not been active enough in technology or cybersecurity; but, rather than (re)establishing yet another agency, CRS could be funded to increase staffing in their Resources, Sciences and Industry division to focus more analysis on policy-related technology issues.

#### Read more in:

- [www.nextgov.com](http://www.nextgov.com): Former Staffers: Revive Congress' Office of Technology Assessment Right or Don't Bother

## DoD's Accelerated Cyber Specialist Hiring Program Needs More Staff

(February 26, 2019)

Although the US Department of Defense (DoD) has the authority to fast track the hiring of cyber specialists through the Cyber Excepted Service program, it lacks sufficient staff to recruit the number of employees DOD needs. DOD deputy principal cyber advisor Marines Corps Brig. Gen. Dennis Crall told members of a House Armed Services subcommittee that the program needs 10 people to recruit and train the cyber specialists. Crall also noted that the security clearance process is slowing down the hiring process.

### Editor's Note

[Neely]

Obtaining a top secret clearance takes about two years, and can be expedited to one. This waiting period makes organizations face the difficult challenge of finding unclassified work for new cyber specialists and effectively integrating them into the team. A clearance is also critical for recruiters and trainers who must understand all aspects of the job.

[Northcutt]

I think that after the extended government shutdown it will be several years before the US government has any real success in attracting skilled cyber talent.

### Read more in:

- [fcw.com](#): Why the cyber fast track is stalled at DOD

## Adobe Will Retire Shockwave in April

(February 26, 2019)

Adobe is notifying enterprise customers that it plans to retire Shockwave later this year. Shockwave, which was first released in 1995, will no longer be available for download after April 8, 2019. Adobe is recommending that Shockwave users switch to HTML5, WebAssembly, or WebGL. It has been more than a year-and-a-half since Adobe announced its intent to retire Flash by 2020. Major browsers have already begun phasing out support for Flash.

### Read more in:

- [www.bleepingcomputer.com](#): Adobe Sends Emails About Retirement of Shockwave on April 9th

## TSA Oversees Pipeline Security

(February 26, 2019)

The US Transportation Security Administration (TSA) is responsible for the physical and cyber security of US pipelines. Sonya Proctor, TSA's director of the Surface Division for the Office of Security Policy and Industry Engagement told members of the House Homeland Security Committee that the five TSA employees who oversee the pipelines "have pipeline expertise, but not cybersecurity expertise," and that they work with Cybersecurity and Infrastructure Security Agency (CISA) for assessments and guidance. A December 2018 report from the Government Accountability Office (GAO) made recommendations to address weaknesses in TSA's Pipeline Security Program Management.

### Read more in:

- [fcw.com](#): TSA's pipeline security team has five employees

- [www.gao.gov](#): Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management (PDF)

## Internet Storm Center Tech Corner

Thunderbolt "Thunderclap" Vulnerabilities (PDF)  
<https://thunderclap.io>

Altering Signed PDF Documents  
<https://www.pdf-insecurity.org>

NVIDIA Patches  
<https://nvidia.custhelp.com>

Coinhive Shutting Down  
<https://coinhive.com>

Azure Blob Storage Phishing  
<https://www.edgewave.com>

Old 2014 Elasticsearch Vulnerability Exploited  
<https://blog.talosintelligence.com>

Latest Drupal Vulnerability Exploited  
<https://www.imperva.com>

F5 Big IP Patches  
<https://support.f5.com>

Emotet Backend Analysis  
<https://maxkersten.nl>

Kaspersky vs. Chromecast  
<https://www.bleepingcomputer.com>

MageCart Updates  
<https://www.riskiq.com>

---

## The Editorial Board of SANS NewsBites

[Alan Paller](#)  
[Brian Honan](#)  
[David Hoelzer](#)  
[David Turley](#)  
[Dr. Eric Cole](#)  
[Ed Skoudis](#)  
[Eric Cornelius](#)  
[Gal Shpantzer](#)  
[Jake Williams](#)  
[Dr. Johannes Ullrich](#)  
[John Pescatore](#)

[Lee Neely](#)  
[Mark Weatherford](#)  
[Mason Brown](#)  
[Michael Assante](#)  
[Rob Lee](#)  
[Sean McBride](#)  
[Shawn Henry](#)  
[Stephen Northcutt](#)  
[Suzanne Vautrinot](#)  
[Tom Liston](#)  
[William Hugh Murray](#)

### SANS Institute

11200 Rockville Pike, Suite 200, North Bethesda, MD, 20852

To create a SANS Portal Account visit [create new account](#).

To change your email address visit [update profile](#).

To change your email preferences or unsubscribe visit [manage subscriptions](#).

[Privacy Policy](#).

This mailbox is not monitored. Please email [support@sans.org](mailto:support@sans.org) or call 301-654-7267 for assistance.



**From:** [Risk Channel](#)  
**To:** [lmartinez@sunnyvale.ca.gov](mailto:lmartinez@sunnyvale.ca.gov)  
**Subject:** Risk Channel - Companies are under growing pressure about climate risks  
**Date:** Friday, March 01, 2019 5:49:20 AM

---

Risk Channel

[View this email in a browser](#)



## **Risk Channel - *North American Edition***

The latest business intelligence for Risk professionals everywhere.

To sign up to Risk Channel for free [click here](#).

**Friday, 1st March 2019**

### **THE HOT STORY**

#### **Companies are under growing pressure about climate risks**

A new study suggests companies are under increasing pressure to disclose their exposure to climate change risks. Companies are expected to face a record of 75 or more climate-related shareholder proposals in the coming round of springtime annual meetings, up from 17 in 2013, according to ISS Analytics. Meanwhile, the Financial Stability Board, an international consortium of regulators, is also tracking voluntary climate reporting and will publish its findings in June.

[Wall Street Journal](#)

### **STRATEGY**

#### **JPMorgan plans for 'no deal' Brexit fallout**

**JPMorgan** has expanded a temporary lease on office space on the outskirts of Paris to accommodate as many as 200 employees at short notice, as the U.S. investment bank weighs scenarios should the U.K. leave the EU on March 29<sup>th</sup> with no deal. Sources say the bank has also signed short-term leases on an undisclosed number of hotel rooms and apartments in Paris and several other European cities where staff may be relocated in such circumstances.

## CORPORATE

### **Kraft Heinz delays release of annual report**

**Kraft Heinz** revealed yesterday it will be late filing its annual report with the SEC, as it moves to conclude an internal investigation into its procurement department. Last week, the company revealed that regulators were investigating accounting practices in the department, and that it had conducted its own investigation with the help of outside legal and accounting advisers. The internal probe found that the company should have reported \$25m in costs in prior quarters, which it logged in the fourth quarter of last year. That compares to about \$11bn that it spends on procurement annually.

[Wall Street Journal](#) [Reuters](#)

### **HBO chief to depart after AT&T takeover**

**HBO** chief executive Richard Plepler is leaving the company in a management shake-up after telecoms company **AT&T** won an appeals court decision for its purchase of HBO parent **Time Warner**. Mr. Plepler found he had less autonomy after the merger, according to two people familiar with his thinking, reports the *New York Times*.

[New York Times](#) [Reuters](#) [Wall Street Journal](#) [Financial Times](#)

## REPUTATION

### **Amazon AI helps brands remove counterfeit listings**

**Amazon** has launched 'Project Zero,' an initiative aimed at eliminating the spread of counterfeit items on the retail site. It allows brands to remove counterfeit listings from without Amazon's help, and Amazon itself is using AI to cut down on fake listings. Machine learning algorithms will continuously scan listings to detect logos, trademarks and other 'key data' about a brand. Amazon said its algorithms scan more than 5bn product listings every day.

[CNN Business](#)

## REGULATION

### **Bankers have not learnt from the financial crash, says IMF**

IMF chief Christine Lagarde has warned that the banking industry has not learnt from the financial crisis and is still not behaving properly. Pointing to bumper bonuses, campaigns against regulation, and irresponsible investing, she said: "In too many



cases, the financial sector has strayed from its original, noble purpose. And too often, it has worked hard to serve itself rather than serve people and the economy at large. That is why the financial industry needs what I call an 'ethics upgrade'." Ms Lagarde added that cyber-attacks could cost the banking system \$350bn, while threats come from high-risk debt markets and the shadow banking sector that are less regulated than the traditional banks. She argued that instead of addressing these problems, bankers have been pushing for bigger pay packets and less regulation.

[\*The Daily Telegraph\*](#) *Reuters*

## LEGAL

### Software startup pays nearly \$800,000 in back wages

The U.S. Department of Labor has said a software startup has paid nearly \$800,000 in back wages to hundreds of members of staff after the company was found to have violated fair pay practices. The department said that Revel Systems, a San Francisco headquartered firm that makes payment systems to work with Apple's iPad, underpaid people who were eligible for overtime. The company paid them flat salaries, rather than taking into account the number of hours they worked.

"Employers must pay their employees all the wages they have legally earned," Susana Blanco, district director of the department's wage and hour division in San Jose, wrote in a statement.

[\*San Francisco Chronicle\*](#)

### EU says Facebook withholding disinformation data

The European Union's executive has accused **Facebook** of repeatedly withholding data on its alleged efforts to clamp down on disinformation ahead of the European elections. The European commission has also complained that the company only set up "fact checkers" – with the job of scrutinising information shared on the site – in eight of the EU's 28 member states. The claims will appear in a monthly update today on progress made by social media signatories – Facebook, **Google** and **Twitter** – to a new code of conduct which encourages the firms to disrupt revenue for accounts and sites misrepresenting information, clamp down on fake accounts and bots, and give prominence to more reliable sources of news while improving the transparency of funding of political advertising.

*The Guardian*

### Huawei denies U.S. trade secrets theft

Chinese tech firm **Huawei** has pleaded not guilty in a U.S. federal court to 10 separate charges alleging the company engaged or attempted to engage in theft of trade secrets. A trial date for March 2020 has been set for the case. If Huawei is found guilty, it could face a fine of up to \$5m. According to prosecutors, Huawei stole trade secrets from **T-Mobile**. A Seattle jury has previously ruled in favour of T-Mobile in a related

suit against Huawei and awarded the telecommunications company \$4.8m.

[Engadget](#)

### **Campaign will fight misconduct in health care**

Time's Up Healthcare is a new initiative to fight misconduct in U.S. health care. The campaign seeks to promote policies to make health care leadership more gender-balanced and accountable and address workplace discrimination, harassment and abuse. "We are well represented in this workforce but not in positions of power," said Dr. Esther Choo, one of the campaign's founders.

[Fortune](#) Reuters

### **Whistleblower recalls fear of tracking UBS bankers at Roland-Garros**

UBS whistleblower Stéphanie Gibaud speaks with the *FT* days after the Basel-headquartered bank was handed a €4.5bn (\$5.1bn) fine for recruiting clients in France and helping them evade taxes.

[Financial Times](#)

## **OPERATIONAL**

### **Apple to lay off self-driving staff**

Apple has announced its intention to lay off 190 employees in its self-driving car program, Project Titan. Among those to lose their jobs are at least two dozen software engineers, including a machine learning engineer, and 40 hardware engineers. Apple performed 79,745 miles of testing in California between November 31<sup>st</sup> 2017, and December 1<sup>st</sup> 2018; during that time, its autonomous system had an error or a human driver took control every 1.1 mile. By contrast, competitors Waymo and Cruise had disengagements every 11,017 and 5,024 miles respectively.

[San Francisco Chronicle](#)

## **THREATS & ATTACKS**

### **UN and IMF among organizations targeted by hackers**

A report by security firm Netscout shows that cyber attackers are increasingly targeting international bodies such as the United Nations, the U.S. state department and the International Monetary Fund. Distributed denial-of-service (Ddos) attacks against the international affairs sector increased by 200% between the second half of 2018 and the same period the year before. Netscout is monitoring 35 groups in countries including Iran, China, North Korea and Russia. The group warned: "IoT security is minimal to non-existent on many devices, making this an increasingly



dangerous and vulnerable sector, particularly as items ranging from medical devices to cars are IoT-equipped."

*City AM*

## WORKFORCE

### **Diversity executives struggle for priority treatment**

A new study suggests most diversity and inclusion executives say their employers don't make their work a priority and as such they lack the power to push for change within an organization. The analysis from executive recruiter Russell Reynolds Associates shows that most large U.S. companies still don't have a designated diversity executive, and those who are in that role say their companies doesn't prioritize their objectives. "The investment of resources into the role have left a lot of chief diversity officers with positions that are completely under-resourced in order to be able to achieve the results that they've signed up for," said study co-author Tina Shah Paikeday, head of global D&I consulting at Russell Reynolds.

[\*Bloomberg\*](#)

### **Walmart to eliminate greeters for new 'customer host' roles**

**Walmart** officials confirmed Wednesday that its store greeters, many of whom are disabled, will be replaced by "customer hosts," an expanded and more physically demanding role. To qualify, workers will need to be able to lift 25-pound packages, climb ladders and stand for long periods. The retailer initially told greeters who do not meet the requirements that they would have 60 days to find other jobs at the company, but has extended the deadline indefinitely for greeters with disabilities. The greeter issue has already prompted at least three complaints to the U.S. Equal Employment Opportunity Commission, as well as a federal lawsuit in Utah alleging discrimination under the Americans with Disabilities Act.

[\*SF Gate USA Today\*](#)

### **Survey shows politics is dividing tech firms**

A new survey of 1,924 U.S. tech workers suggests a quarter of people working in the industry identify as having very strong political views (14% left, 11% right). A third called themselves moderate, and equal shares (18% each) identified as mainstream liberal or conservative. Just 3% identified as libertarian. Some 45% of respondents believe their company promotes a political agenda. That leaning tends to be toward the left, with 48% of respondents saying their company has a clear liberal agenda, as opposed to the 38% who reported a conservative agenda.

[\*Fast Company\*](#)

### **Cohen testimony could cost employers almost \$4bn**

Michael Cohen's testimony before the House Oversight Committee could cost

employers \$3.83bn as staff spend time watching or streaming it online rather than focusing on their work, according to outplacement consulting firm Challenger, Gray & Christmas. "The nation is rapt . . . Employers will find it difficult to reign in interested workers during this proceeding, and it will impact their teams' productivity," cautioned John Challenger, the company's chief executive.

[USA Today](#)

### **How to quell an employee rebellion**

*Inc.* 's Suzanne Lucas reports on an employee rebellion at the Sonic drive-in at Circleville, Ohio. Staff walked out *en masse* after becoming increasingly unhappy with new management. The author notes that at-will employment, whereby an employee can be dismissed by an employer for any reason, also conversely means that employees can walk out. Tips for avoiding an employee rebellion are provided.

[Inc.](#)

## **ECONOMIC**

### **U.S. trade gap in goods widened 10% in 2018**

The U.S. trade deficit in goods widened 10% in December from a year earlier, the Commerce Department reported yesterday. At the end of the year, the gap reached \$79.5bn, \$7bn higher on an annual basis. Exports declined 0.3%, while imports increased 3.2%. The increase in imports last year was driven by higher purchases of foreign food products, cars, and so-called capital goods, a broad category that includes machinery and equipment. The decline in exports has been attributed to slower economic growth in Europe and Asia, leading to reduced spending on overseas goods. Additionally, the tariffs imposed by China as part of the trade dispute with the Trump administration drove up the price of U.S. exports.

[Wall Street Journal Market Watch](#)

## **TECHNOLOGY**

### **Boeing uses AR to boost productivity**

*Forbes* contributor Charlie Fink takes a look at how Upskill's Skylight software platform is helping **Boeing** manage its AR applications. "The time saved falls straight to the bottom line," says Upskill CEO Brian Ballard, noting that his company's technology has helped Boeing reduce wiring time in some aircraft by 30%.

[Forbes](#)

## **OTHER**



## **The difficulties of measuring China's jobless rate**

The *Wall Street Journal* reports on the ongoing search for credible Chinese employment data, noting that the official number for the urban population produced by China's official statistics bureau is typically too low and stable. Economists are innovating to better gauge the local job market - for example by monitoring what people are looking for on search engine giant Baidu. Searches for terms including "layoffs" and "job seeking" have surged recently, say economists at Nomura.

[Wall Street Journal](#)

---

Risk Channel delivers the latest, most relevant and useful business intelligence to key decision makers and influencers, each weekday morning.

Content is selected to an exacting brief from hundreds of influential media sources and summarised by experienced journalists into an easy-to-read digest email.

Risk Channel enhances the performance and decision-making capabilities of individuals and teams by delivering the most useful news and knowledge in a cost-effective way, while promoting a sponsor's brand to the risk and leadership communities.

If you would like to sponsor a Risk Channel special report, reaching thousands of influential professionals, companies, business leaders and decision makers through our US and/or UK & Europe editions, please get in touch on +44 (0)7495 489773

---

To Unsubscribe click [here](#)

---

© Early Morning Media Ltd.

This Service was produced by Early Morning Media.

Email: [info@earlymorningmedia.co.uk](mailto:info@earlymorningmedia.co.uk)

Registered in England No: 06719248

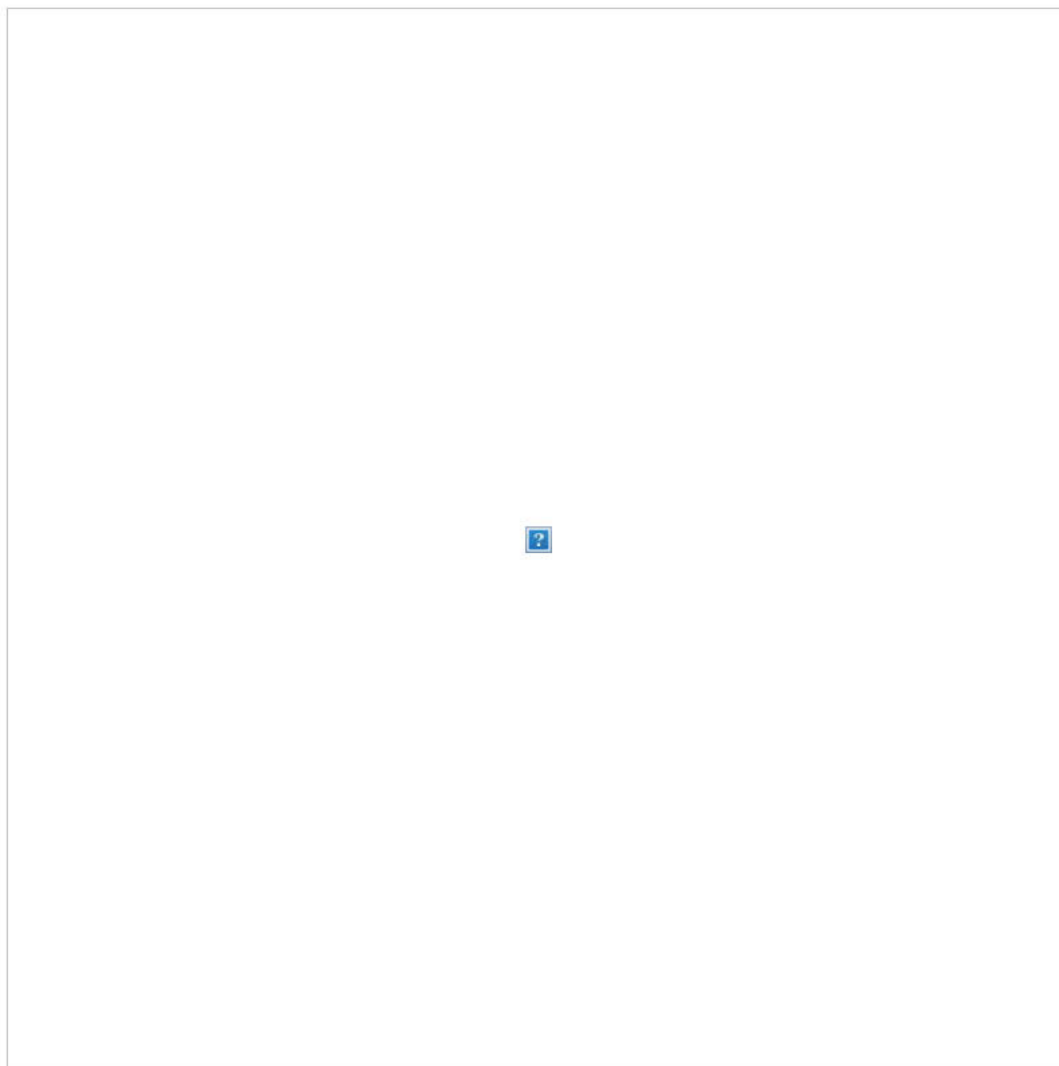
Registered Address; Global House, 1 Ashley Avenue, Epsom, KT18 5AD

Phone: 0207 186 1060

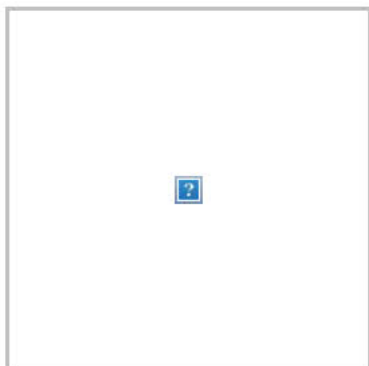


**From:** [Police K-9 Magazine](#)  
**To:** [cfontaine@ci.sunnyvale.ca.us](mailto:cfontaine@ci.sunnyvale.ca.us)  
**Subject:** Missing Man Traced by Police Dog Unit, First Responders Learn Canine First Aid, & MORE!  
**Date:** Tuesday, February 26, 2019 11:08:56 AM

---



[WEBSITE](#)   [SUBSCRIBE](#)   [ADVERTISE](#)   [IN THIS ISSUE](#)   [NEWS](#)



### 350 lbs of 'hard drugs' nabbed in Nogales, worth \$4.4 million

Nogales-area Customs and Border Protection officers seized nearly 350 pounds of "hard drugs" - including heroin, methamphetamine, cocaine and "suspected" fentanyl - worth \$4.4 million. [Read More](#)

---

## Middletown police K9 helps capture stolen car suspect

A Middletown police K9 was instrumental in identifying a Windsor stolen car suspect. Windsor officers spotted a car that had just been stolen just before 5 a.m. Friday and began following the vehicle. The car wound up veering off the road and crashing with the driver bailing out on foot. Windsor police put out an alert for any police K9s available to come track the suspect, police said. [Read More](#)

---

7 Days to Vegas\_



---

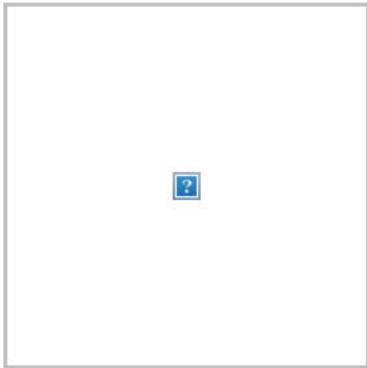
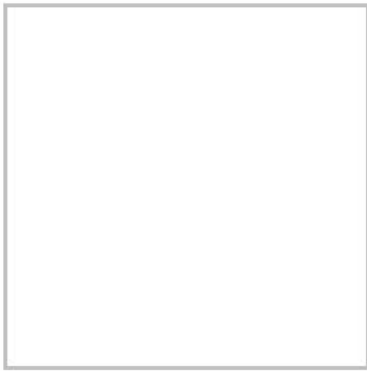
## K9 Alex Takes Down Ice Pick-Wielding Suspect in Spenard Area

A PD reports that an officer on patrol in the Spenard area spotted an armed prowler and approached to make contact and was challenged by the icepick-wielding man. Following the confrontation between the patrol officer and the suspect fled on foot as the officer attempted to taze him without effect. [Read More](#)

---

## Dog sniffs out €100,000 in fake notes during police raid on Costa Blanca

During a raid on the property belonging to the men, the officers seized 100,000 euro in counterfeit noted, 2,150 euro in legal tender, and 30 grams of cocaine, as well as various types of narcotics. [Read More](#)



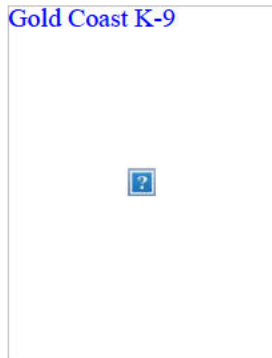
## Meet Ziggy, one of four dogs keeping guns out of CCSD schools

For most hours of the day, Ziggy is like any other dog. He enjoys belly rubs, chasing after tennis balls and making new friends. But with a simple command - "Find it!" - the 1-year-old black Labrador puts on his gun-detection dog hat. Following the direction of his guardian, Clark County School District Police Officer James Harris, Ziggy will start to sniff vigorously. [Read More](#)

### Naturich K9 Finest



### Gold Coast K-9



### Pawz Dog Boots



## Three Arrested In Ocean County Drug Probe

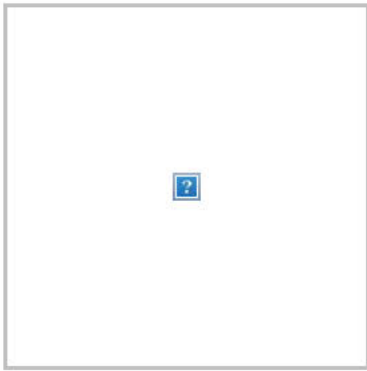
Three Ocean County residents were arrested and charged after a police found cocaine, marijuana, drug paraphernalia, and approximately \$19,000 in cash in their possession. A two-month investigation into illegal drug activity in the area was conducted by the Prosecutor's Narcotics Strike Force and the South Toms River PD. [Read More](#)

## Burglary Suspect Crashes Through Ceiling Into Sheriff's Handcuffs

The Pierce County Sheriff's Office last week thanked local residents for tips that led to the arrest of a residential burglary suspect who'd eluded capture since failing to appear for court in November 2018. Nicholas Franklin Thompson, 27, was taken to Pierce County Jail following his Feb. 21 arrest. [Read More](#)

**Welcome These NEW K-9 Officers!**

**Myrtle Beach promises newest cops will**



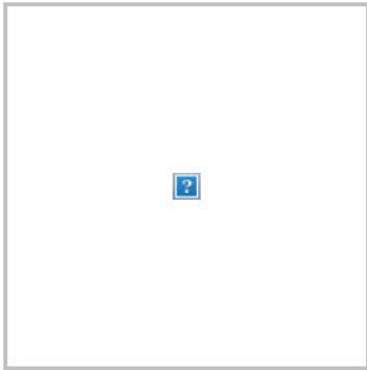
## hound criminals

Myrtle Beach police's newest hires might seem friendly, but they're going to make life ruff for criminals. It was all joy and barking at the Ted C. Collins Law Enforcement Center as police officials gathered to welcome K-9s Goggles and Bek to the department. [Read More](#)

---

## New County K-9 Program to Focus on Narcotics Detection

Two canine officers will join the FCSO this summer, thanks to support and donations from the community for the new Flathead County Sheriff K-9 fund. The campaign to raise money to purchase two narcotics detection dogs for the department reached its first goal of \$5,000 within 24 hours of posting it. [Read More](#)



## OBPD K9 unit adds two new members

Thanks to the support of the City of Orange Beach and the Orange Beach Police Benevolent Fund and the kind generosity of our citizens who supported their efforts with the Paw Ball Fundraiser, we were able to purchase two new canines for the canine program.

After 10 Weeks of training with their handlers, Canine Officers Bane and Magnum have joined the force. [Read More](#)

---

### Scent Evidence K-9



### Ready Dog Products



### Elite K-9



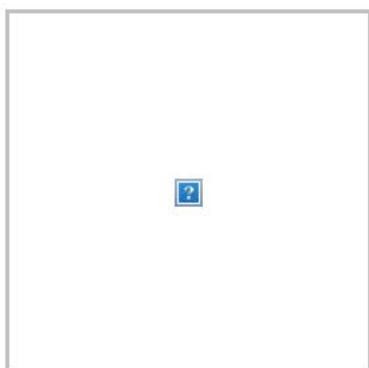
---

## Robberies, drug arrests keep Madison police active over weekend

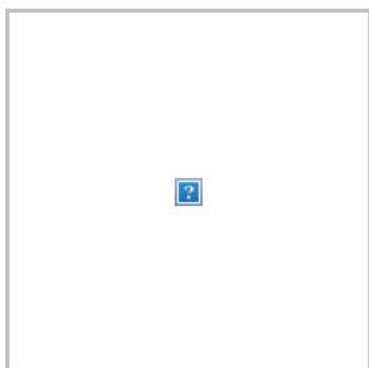
Madison police made several arrests late last week and over the weekend involving a number of robberies and a fight with a drug dealer. Saturday afternoon, officers spotted two cars participating in a drug deal and pulled one over. After a drug dog sniff picked up a scent, police conducted a search and discovered an abundance of drugs as well as a loaded gun. [Read More](#)

---

## Extra set of paws helping to snuff out influx of meth in Clyde



Two K-9 units in Clyde are helping to stop a rising influx of meth on the streets, a drug that had been curtailed locally after a meth house raid in 2015. Until May 2018, the Clyde PD had to rely on other county K-9 units to sniff out drugs on traffic stops. [Read More](#)



### Swansea Police Department sells t-shirts to raise funds for K9 officer

The Swansea Police Department is raising funds to benefit one of their K9 officers. The department posted a t-shirt design it is selling to raise money to take care of K9 Leo.

[Read More](#)

### New Concord Police state case for a drug detecting dog

Illegal drugs have wended their way into the Village of New Concord and to believe otherwise is to live not in the village, but in "Denial, Ohio," Village Police officers said during a recent meeting. To combat the problem, officers solicited support from citizens for obtaining a drug detection dog, a K-9 unit for the village. [Read More](#)

## UPCOMING K-9 EVENTS & TRAINING

<b>5th Annual International Police K-9 Conference &amp; Vendor Show</b> March 5 - 7 Las Vegas, NV <a href="#">Police K-9 Magazine</a>	<b>DLEcertification's Louisiana K9 Workshop</b> March 24 - March 29 Bastrop, LA <a href="#">Dogs for Law Enforcement</a>
<b>Electronic Dog Training Collar Class - 20 hours</b> March 27 - March 28 Ventura County, CA <a href="#">Gold Coast K9</a>	<b>2019 NNCDS Spring Seminar</b> March 31 - April 5 Huntsville, AL <a href="#">NNCDS</a>
<b>2nd Annual Murrieta PD K-9 Trials</b> April 5 - April 6 Murietta, CA <a href="#">Paws4Law</a>	<b>3-Day TacDogs Seminar</b> April 6 - April 8 Paducah, KY <a href="#">TacDogs</a>
<b>2019 APCA Spring Seminar</b> April 15 - April 17 Concord, NC <a href="#">American Police Canine Association</a>	<b>T-MACC Class 2</b> April 23 - April 24 Lake Tahoe, CA <a href="#">Canine Tactical Operations</a>

Email [info@policek9magazine.com](mailto:info@policek9magazine.com) for any upcoming K-9 events!



K2 Solutions\_ Inc.



Delta Challenge Coins



writers wanted



### Writers wanted!

Police K-9 Magazine welcomes your editorial input! Articles of varying lengths will be accepted, but please keep your article to less than 2,500 words.

**TOPICS NEEDED:** K-9 OBEDIENCE \* FEATURED AGENCY \* SWAT \* SEARCHES \* SCENT DETECTION \* K-9 BITEWORK \* LEGAL \* TRACKING/TRAILING \* K-9 ADVICE & OPINION \* K-9 HEALTHCARE \* K-9 NUTRITION \* MORE! [More Info](#)

### Police dogs create awareness about drugs in Dubai schools

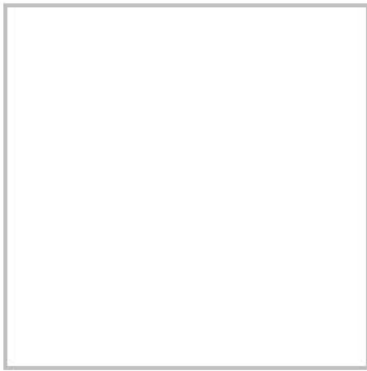
The Global Indian International School (GIIS) in Al Barsha was in for a surprise on its annual sports day on Thursday, when a fun activity got under way on its manicured greens. Just when four students sat on four chairs for an ostensible game, a man in uniform with a German Shepherd dog was seen approaching them. [Read More](#)

### Missing man Richard Finnis traced by police dog unit

A man missing from the Inverness area for more than a week has been found safe and well. Police Scotland said Richard Finnis, 30, was traced by their specialist dog unit on Sunday. [Read More](#)

### Rock County first responders learn canine first aid

Almost all the knowledge a paramedic uses to treat humans can be used to help an injured police dog. Most paramedics don't know that, said Paul McNamara, a veterinarian and owner of Odin's Fund, a nonprofit that teaches canine first aid to first responders. [Read More](#)



**Tag #policek9magazine in your pictures to be featured  
in our next Newsletter or Magazine!**

Tag [\\_policek9magazine](#) to be featured



@gabimaltosphoto

\*\*\*

PSD Bailey, one of the dogs from the Vancouver Police Department, and her handler playing around before the night shift. Vancouver, 2017

...

#documentary #vancouver #policek9magazine



### Police K-9 Magazine Issue 72

**Articles on:** Inside of a Custody K-9 Unit: Kings County (CA) Sheriff's Department by Jay Brock, SWAT and K-9 Deployments: Foundational Concepts by Kevin Hollohan, Benefits of Agitation Tracking by Nathan Kelley, E-Collar: Remote Directional Training, Part 2 - Introducing Directional Commands by Pat Nolan, Building Searches by Mike Lefave, Communication & K-9 Training, Part 2 by Dondi Hydrick, K-9 Advice & Opinion: Clarity and Continuity in Patrol Dog Training by George Daniolos, K-9 Legal: Why Can't We Do This? Federal Law vs State Law vs Agency Policy by John Peters, Attorney at Law, Nutrition: Could Bacteria be the

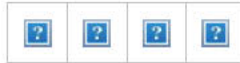
Secret to a Great Dog? by Nicci Decrisantis

**Subscribe TODAY!**

**Cover photo by: Sue Travers Photography - [www.suetraversphotography.com](http://www.suetraversphotography.com) - Officer  
Meghan Grant & K-9 Ollie - Manchester (NH) Police K-9 Unit @MAPK9603**

**[info@policek9magazine.com](mailto:info@policek9magazine.com) | [policek9magazine.com](http://policek9magazine.com) | (270) 534-0500**

STAY CONNECTED:



Police K-9 Magazine, 7660 Old US Hwy 45, Boaz, KY 42027

[SafeUnsubscribe™](#) [cfontaine@ci.sunnyvale.ca.us](mailto:cfontaine@ci.sunnyvale.ca.us)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [info@policek9magazine.com](mailto:info@policek9magazine.com) in collaboration with

[Constant Contact](#)



Try it free today

**From:** [Association of Deputy District Attorneys](#)  
**To:** [fgurina@sunnyvale.ca.gov](mailto:fgurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for February 25, 2019  
**Date:** Monday, February 25, 2019 5:04:26 AM

---

Having trouble viewing this email? [Click here](#)



## Courts & Rulings

### **Ruling affirming the rights of students accused of sexual misconduct roils California colleges**

Colleges and universities across California are scrambling to revise the

way they handle sexual misconduct cases after a state appellate court ruled that "fundamental fairness" requires that accused students have a right to a hearing and to cross-examine their accusers. The decision last month came in a USC case but applies to all California public and private colleges, and prompted many to immediately halt Title IX investigations while they reshape their procedures.

[Los Angeles Times](#)

### **Conviction to stand despite prosecutor's effort to arouse jurors' passion**

A man convicted of first degree residential burglary and second degree robbery yesterday failed in his bid for a reversal based on the prosecutor, during rebuttal argument, telling jurors to act other than as dispassionate evaluators of the evidence. The defendant, George Alfaro, in burglarizing the home of Carol Cortes for the second time in two months, punched Cortes in the face and stole her cellphone.

[Metropolitan News-Enterprise](#)

### **Judge bars immigration policing criteria for 2 grants**

A federal judge on Friday permanently blocked the Trump administration from imposing conditions that police departments cooperate with immigration authorities to receive law enforcement grants. The Department of Justice exceeded its authority and violated the constitution by requiring grant recipients to allow immigration authorities into jails and provide advance notice before releasing detainees suspected of being in the country illegally, Judge Manuel Real said.

[PBS](#)

### **Supreme Court strikes blow against states that raise revenue by hefty fines, forfeitures**

The Supreme Court ruled unanimously Wednesday that states cannot impose excessive fees, fines and forfeitures as criminal penalties. The decision, which united the court's conservatives and liberals, makes clear that the Eighth Amendment's prohibition against "excessive fines" applies to states and localities as well as the federal government.

[USA Today](#)

### **Defendant's Arbuckle right not forfeited by failing to raise it at sentencing - C.A.**

The Fifth District Court of Appeal yesterday invalidated the sentence of a woman whose drunk driving resulted in the death of her son, holding that she had a right to be sentenced by the same judge who took her no-contest pleas even though she did not invoke that right at the time of sentencing. Justice Mark W. Snauffer wrote the opinion which seeks to discern the California Supreme Court's intent in its 2017 decision in K.R. v. Superior Court.

[Metropolitan News-Enterprise](#)



### **Rocklin teen's murder sentence in sister's death upheld, as judge calls new law unconstitutional**

Rocklin teen Tanner Wood will be sentenced in April to 16 years to life in state prison for the 2016 murder of his younger sister, a Sacramento judge ordered Friday, rejecting a new juvenile justice law as unconstitutional. Sacramento Superior Court Judge James Arguelles' courtroom became the latest local testing ground for Senate Bill 1391 as the judge sparred with Wood's attorney over whether the new law barring minors younger than 16 from being tried as adults for murder and other serious crimes passed constitutional muster.

[Sacramento Bee](#)

### **Probable cause lacking for arrest based on general description**

The Ninth U.S. Circuit Court of Appeals yesterday affirmed the denial of summary judgment, sought on the ground of qualified immunity, to an El Monte police detective who arrested a light-skinned bald man for illegal sales of firearms in response to a report by an alleged confidential informant of such activity by a man of the arrestees description.

[Metropolitan News-Enterprise](#)

### **California Supreme Court ruling causes chaos for local tax measures**

Late last year, the city of Oakland put a new land parcel tax on the books, after 62 percent of voters turned out to boost funding for public education. Now a local business group is suing the city, arguing that the new tax needed two-thirds of the vote - just over 66 percent - to pass. San Francisco faces a similar problem, only twice as big.

[CALmatters](#)

### **Judge erred in declaring bail forfeited without considering medical condition of defendant**

The Fifth District Court of Appeal yesterday reversed an order denying a surety's motion to exonerate a bail bond or to toll the 180-day appearance period, declaring that the judge erred in not considering the debilitated state of the 91-year-old criminal defendant who is in hospice care and suffers from dementia.

[Metropolitan News-Enterprise](#)

### **Judge overturns \$38M verdict in lawsuit over Baltimore County police killing of Korryn Gaines**

Baltimore County judge has overturned the decision of a jury that awarded more than \$38 million to the family of Korryn Gaines, the 23-year-old Randallstown woman who was shot and killed by county police in 2016. Judge Mickey J. Norman dismissed the family's claims against the county and the officer who fatally shot Gaines.

[Baltimore Sun](#)

### **Secret records of police misconduct and shootings must be released under new law, L.A. judge rules**

A Los Angeles judge dealt a blow this week to law enforcement unions trying to limit the scope of a landmark transparency law, ruling that records from shootings, use of force and some misconduct by police officers in California are public even if they occurred before the new law took effect this year.

[Los Angeles Times](#)

### **Politifact fact-check: the Ninth Circuit is, in fact, the most reversed federal court of appeals**

Recently, cable news personality Sean Hannity commented that the Ninth Circuit is the "most overturned court in the country." Politifact rated that claim as "false." But Politifact's analysis is seriously flawed and suffers from selective analysis of the evidence, and misrepresentation of the evidence in other respects.

[Excess of Democracy](#)

### **Justice Thomas wants the Court to 'reconsider' its First Amendment jurisprudence**

Stare decisis, schmare decisis. Supreme Court Justice Clarence Thomas apparently agrees with Donald Trump when it comes to the First Amendment. The president famously vowed to "open up the libel laws" to make it easier to sue the media (even though Trump is more likely to be burned by that change in constitutional law), and in today's concurrence in *McKee v. Cosby*, Justice Thomas seems to be on board.

[Above the Law](#)

## **Prop 47, 57 & AB 109**

### **Are California's criminal justice reforms actually working?**

Prop. 47 reclassified certain theft and drug possession offenses from felonies to misdemeanors; allowed defendants serving sentences for felony offenses that would have qualified as misdemeanors under Prop. 47 to petition the courts for resentencing; allows defendants who have completed their sentences for felony convictions to apply to reclassify them as misdemeanors under the new law, according to the California Courts website.

[Bakersfield Now](#)

### **These 13 people were convicted of murder in SLO County. Some could go free under new law**

More than a dozen men and women convicted of murders they personally did not commit in San Luis Obispo County may be eligible for re-sentencing - and in some cases, release - after a change in state law late last year. In hearings scheduled over the next several months, San Luis Obispo County prosecutors and defense attorneys will argue before a judge whether people who acted as accomplices to crimes fit certain criteria and could no longer be convicted of murder under current law.

[The Tribune](#)

### **Ex-Gov. Brown, solve this**

How apropos that you run a series on homelessness. The problem was exacerbated with the passage of Proposition 47 by our liberal politicians backed by the SEIU, the ACLU and pushed as the "Safe Neighborhood and Schools" act. The passage of this liberal blunder increased the number of criminals on the street. Add to this the deluge of illegals because of "Sanctuary City" benefits and we have the mess that is the "homeless" of today.

[Opinion/Desert Sun](#)

### **Sculptures popping up around town through inmate work program**

Residents enjoying a walk through River Park may have noticed some new artwork popping up over the past few months. The metal sculptures are the work of inmates who are part of a Tehama County AB 109 program that provides training in wood and metal working as a form of alternative incarceration. "I appreciate it," said inmate Jason Horn. "I didn't want to sit in jail. Now I'm learning a few things and contributing."

[Red Bluff Daily News](#)

### **The latest in leniency for criminals**

The 2014 Proposition 47 reduced penalties for property crime and transformed some felonies into misdemeanors. The 2016 Proposition 57 barred prosecutors from directly filing juvenile cases in adult court. Senate Bill 1391, effective January 1, forbids prosecution of 14- and 15-year old criminals as adults, whatever the gravity of their crime. A new measure now takes the trend of leniency to a new level.

[California Globe](#)

## **Prosecutions/Prosecutors**

### **District Attorney successfully argues SB 1437 as unconstitutional**

On Friday, Feb. 8, 2019, during a hearing in the People v. Dejon Griffin and Aaron Jackson case, Orange County Superior Court Judge Gregg L. Prickett heard arguments on the constitutionality of Senate Bill (SB) 1437, given that it lacks the two-thirds super majority of both bodies of the California Legislature.

[Orange County Breeze](#)

### **Solano DA on record as challenging new state laws affecting violent offenders**

Solano County District Attorney Krishna Abrams said her office is on record challenging new state laws affecting violent offenders, Senate bills 1437 and 1391. Her comments came toward the end of a fast-paced, 90-minute public forum held Tuesday night in the County Events Center, next to the County Government Center, in Fairfield.

[Vacaville Reporter](#)

### **Suspect in shootout with police claims to be a 'prophet' in court**

A man facing a murder charge over a deadly shootout with police in front of a neighborhood market last summer said in court Friday that he was a "prophet" sent by Jesus and smeared a brown substance on a glass partition, but a prosecutor said it was all an act to further delay court proceedings.

[Courthouse News Service](#)

### **Riverside County man charged with killing 11-year-old Linda O'Keefe in 1973 cold-case murder**

A Colorado man has been charged with the 1973 abduction and killing of an 11-year-old Corona del Mar girl who was walking home from school, officials announced Wednesday morning, bringing a long-awaited arrest in a case that shocked the Newport Beach community. Orange County District Attorney Todd Spitzer said during a press conference that the suspect, James Alan Neal, 72, faces a special-circumstances murder charge, leaving open the possibility that prosecutors could seek the death penalty.

[Orange County Register](#)

### **Parolee charged with killing three men at Torrance bowling alley**

A parolee who allegedly shot and killed three men at a bowling alley in Torrance is scheduled to be arraigned on a charge of murder Tuesday in a case in which he could face the death penalty. Reginald Leander Wallace, 47, of Los Angeles, is scheduled to be arraigned Tuesday in a Torrance courtroom on three counts of murder for allegedly shooting Michael Radford, 20; and Robert Meekins and Astin Edwards, both 28, just before midnight Jan. 4 at Gable House Bowl at 22501 Hawthorne Blvd., along with four counts of attempted murder and one count of possession of a firearm by a felon.

[My News LA](#)

### **The Latest: Son charged with killing parents, housekeeper**

Prosecutors have charged a California man with killing his parents and their housekeeper in an upscale community. The Orange County district attorney's office charged 27-year-old Camden Nicholson on Friday with three counts of murder and an enhancement alleging multiple murders. Nicholson's arraignment was delayed to March 8. His lawyer Jessica Ann Watts didn't immediately respond to a message seeking comment.

[AP](#)

### **Man extradited from El Salvador to face murder and torture charges in estranged wife's Pacoima stabbing death**

A man extradited from El Salvador in connection with his estranged wife's stabbing death in Pacoima nearly nine years ago has been charged with murder and torture, the Los Angeles County District Attorney's Office announced Tuesday. Napoleon Eduardo Castro - also known as Juan Flores, Luis Sanchez and Trouble - is set to be arraigned March 6 at the San Fernando courthouse in connection with the torture

killing of his estranged wife, Olga Martinez, in her garage.

[City News Service](#)

### **Former Valley candidate and aide fined for violations tied to campaign funds**

A former candidate for Los Angeles City Council and his campaign treasurer have been fined more than \$38,000 for using laundered donations to get taxpayer money and mispending such dollars on personal expenses. The Los Angeles City Ethics Commission voted unanimously Tuesday to fine J. Roy Garcia, who ran unsuccessfully in 2013 for a council seat in the San Fernando Valley, and his campaign treasurer Hardy Henriquez.

[San Diego Union-Tribune](#)

## **Criminal Justice/Public Safety**

### **California's black market for pot is stifling legal sales. Now the governor wants to step up enforcement**

Before he was elected governor, Gavin Newsom was instrumental in legalizing marijuana for recreational use in California. Now, as he settles into office, he faces the challenge of fixing a system that has been slow to bloom. Newsom has urged patience with sluggish growth in the number of state-licensed cannabis businesses, saying he expected that such a complex regulatory system would take at least five years to fully develop.

[Los Angeles Times](#)

### **Female LAPD commander sues for gender discrimination**

An LAPD Commander facing termination after being accused of being drunk in public has sued the City of Los Angeles, claiming that because she is female she faced discrimination and retaliation during an internal police administrative trial. "There is compelling evidence that men were treated differently than women," Nicole Mehringer's lawsuit said.

[NBC4](#)

### **Ford's 2020 Explorer for police has hidden lifesaving design feature**

Michigan State Police 1st Lt. Mike Shaw has been nearly hit by speeding vehicles four times, twice while outside his car. "And four times is actually low. I know a trooper who has been hit more than 10 times," Shaw said. "You can probably talk to any state trooper. It's not a matter of if, but when. People just aren't paying attention out there, and sometimes they're impaired with alcohol or marijuana or even their cellphones. Maybe they're just gawking. And our troopers are getting hit."

[Detroit Free Press](#)

### **Protesters disrupt Altadena Church's Black History Celebration as Los Angeles County District Attorney attempts to speak**



Loud protesters reportedly including the mothers of several people killed during incidents involving law enforcement disrupted a Black History Celebration at Altadena Baptist Church on Sunday night. The incident occurred about 6 p.m. as keynote guest Jackie Lacey, the first African-American to serve as Los Angeles County's District Attorney, was about to speak.

[Pasadena Now](#)

## **Policy & Legal Issues**

### **Has criminal justice reform gone too far? One California lawmaker thinks so**

Overcrowded prisons. Trying teens as juveniles versus adults. The power of rehabilitation and a belief in second chances. These issues have fueled criminal justice reform in recent years in the state of California. But some say the overhaul has gone too far. People can generally agree, we all want to live in safe communities, but as Assemblymember Jim Cooper (D-Elk Grove) told ABC10, the devil is in the details.

[ABC10 Sacramento](#)

### **Felony murder law repealed? Maybe not**

Two young men drive up to a small corner grocery store in an inner city neighborhood and the driver remains at the wheel while his masked partner runs into the store, gun in hand, to commit a robbery. The armed gunman shoots and kills the clerk before grabbing cash out of the register, then jumps back into the car and the two make their getaway.

[CALmatters](#)

### **LA's illegal pot shops may have water, power shut off**

With hundreds of illegal marijuana shops continuing to operate in Los Angeles, a City Council committee today moved forward with a plan aimed at cracking down on the businesses by shutting off their utilities. The idea of shutting off water and power at illegal pot shops was proposed last year by Councilwomen Nury Martinez and Monica Rodriguez.

[City News Service](#)

### **The power of judicial review: Erwin Chemerinsky**

President Donald Trump and Attorney General Jeff Sessions have engaged in unprecedented attacks on judicial review that reflect a profound lack of understanding about the Constitution. My fear is that their rants will contribute to undermining the legitimacy of the courts and of the rule of law.

[Daily News](#)

### **Scrubbing the past to give those with a criminal record a second chance**

Latosha Poston says she made a lot of mistakes in her life. Her legal troubles began in her teens after her first child was born in

Indianapolis. Over the years, bad decisions led to some arrests, some convictions. "Sometimes we get stuck in our past and let our past guide us," she says. The 44-year-old has worked hard to straighten out her life. But her criminal records - all involving misdemeanors - continued to haunt her as she tried to find a decent job and place to live.

[NPR](#)

### **Goldstein Investigation: LAPD using electric BMWs to commute, go to lunch**

The Los Angeles Police Department's efforts to go green with electric cars is raising some red flags, including a police psychologist who was caught using one of the department's fleet of electric BMW's to commute to and from work. When CBS2/KCAL9 Investigative Reporter David Goldstein asked, "Why should taxpayers be paying for you to take this? You're basically commuting to and from your house, aren't you, sir?" the psychologist had no comment.

[CBS LA](#)

## **Crime**

### **ICE: Man who shot at Napa deputy in country illegally, deported multiple times**

The man who was shot dead by a Napa County sheriff's deputy after he fired at her point blank during a traffic stop was a Mexican national in the country illegally after being deported multiple times, according to U.S. Immigration and Customs Enforcement. Javier Hernandez-Morales shot at and missed Deputy Riley Jarecki during a traffic stop late Sunday night as she stood next to his driver-side window.

[CBS SF](#)

### **Magic Johnson's daughter home invasion suspect arrested**

Cops nabbed a guy they say pulled the home invasion that forced Magic Johnson's daughter to run for her life. Law enforcement sources tell TMZ ... LAPD identified the suspect after reviewing surveillance video from the neighborhood where Elisa Johnson's friends were renting a house back in December.

[TMZ](#)

### **Police trainer's gun stolen off baggage carousel at California airport**

A gun belonging to someone who trains police officers is on the streets after it was stolen from a baggage carousel at San Francisco International Airport, according to its owner. The gun's owner said he did everything by the book and blames United Airlines for his gun ending up in the hands of suspected thieves. The man, who didn't want to be identified, has a gun permit and trains police officers.

[NBC4](#)

### **Suspected DUI driver arrested in hit-and-run crash in South-**

### **Central L.A. caught on video**

A man suspected of driving drunk at a speed of 80 to 100 mph when he plowed into six parked vehicles in Historic South-Central L.A., ejecting and injuring one of his passengers before fleeing the scene, was arrested hours after the early Sunday morning crash, police said. Police clarified on Monday that the person sustained severe injuries but survived.

[KTLA](#)

### **Rare bulldog stolen and taken 2,000 miles, but dogged police officers track it down**

Although it was a little late, Christmas finally came for one family. All they had to do was travel 2,000 miles to get their intended gift - a rare English bulldog puppy. The dog was going to be a Christmas surprise for a suburban Chicago family in Naperville, Illinois, WWL reported. But on Dec. 18, a real-life Grinch stole the 10-week-old puppy - a blue merle English bulldog which is rare because of its coloring, according to WLS.

[Miami Herald](#)

**The Los Angeles Police issued a warning to street food vendors as an increase in assaults has been reported in the Boyle Heights area.** Officials distributed fliers written in Spanish and English to inform vendors to take care of themselves because some of their colleagues have been the target of armed attacks. "We have to worry about those who only come to get the fruit," said Alicia Cárdenas, a street vendor of fruit.

[NBC4](#)

### **Porter Ranch triple homicide victims identified**

The triple homicide that has shaken an upscale, exclusive gated community was not a random attack, and it appears the yet to be identified killer or killers were allowed into the house, the police captain overseeing the investigation said Tuesday. Called to a large house on Via Galileo in Porter Ranch's Renaissance community shortly before 4 p.m. Monday, responders found three men inside, all dead of apparent gunshot wounds.

[NBC4](#)

## **Los Angeles County Sheriff**

### **L.A. County's new sheriff announced reforms to limit ICE. Immigrant rights groups don't think they go far enough.**

A coalition of Los Angeles immigrant rights groups, many of which championed L.A. County Sheriff Alex Villanueva's long-shot campaign during the mid-term elections last year, wrote in an open letter Monday that he has "betrayed" them in just a few weeks in office by walking back pledges to limit Trump administration Immigration and Customs Enforcement agents' reach in the city.

[Pacific Standard](#)

### **Sheriff Alex Villanueva promised change. His supporters are standing by him despite controversies**

New Los Angeles County Sheriff Alex Villanueva is testing supporters with his unorthodox approach as the region's top cop. Only two months on the job, Villanueva fired his department's top brass and asked others to reapply for their positions. His reinstatement of a deputy fired amid allegations of domestic abuse and stalking prompted a rare rebuke from several Los Angeles County supervisors.

[Los Angeles Times](#)

### **LA sheriff: Fewer crimes spur transfer to immigration agents**

The new leader of the nation's largest sheriff's department on Friday further limited when inmates in Los Angeles County jails can be transferred to U.S. authorities for deportation. The department has reduced the number of misdemeanor charges that can trigger an inmate's transfer to U.S. Immigration and Customs Enforcement for deportation from 151 to 101, spokeswoman Nicole Nishida said.

[San Francisco Chronicle](#)

### **Supervisors to authorize settlement in lawsuit claiming "battery" by SCV Sheriff deputies**

County supervisors are expected to finalize a settlement reached in a lawsuit filed by a man who claimed he was beaten by local sheriff's deputies on Christmas Eve in 2016. On Tuesday, the Los Angeles County Board of Supervisors are scheduled to vote on a recommendation to authorize a \$150,000 settlement in the civil case of John Clyde Warner vs. the County of Los Angeles.

[The Signal](#)

## **Los Angeles County**

### **Probation department workplace injury payouts soar by nearly \$6 million as violence rises in juvenile lockups**

Los Angeles County supervisors are set Tuesday to discuss whether pepper spray should still be used in juvenile lockups after an alarming uptick in its use, which has led to an internal department investigation by the County Inspector General. The spike in pepper spray use comes as the population of youth offenders is dropping amid a push toward rehabilitation and as similar agencies across the country are shunning its use, saying it's ineffective, inhumane and a potential liability.

[NBC4](#)

### **Goldstein investigation: 2 men mysteriously died in his apartment, he calls our reporter 'an a-hole'**

Two men died mysteriously in the West Hollywood apartment of Democratic party fundraiser Ed Buck, but when CBS2 investigative reporter David Goldstein confronted him, Buck didn't have much to say. "Why don't you answer any questions? You have two people who died in

your house," Goldstein asks. "Because you're being an a-hole," Buck replies. Buck was blunt. Not answering any questions.

[CBS LA](#)

### **Pot entrepreneurs are running out of patience and money while waiting on L.A. permits**

For Kika Keith, a dream deferred looks like a bare, brightly illuminated room in South Los Angeles. After California legalized recreational cannabis, Los Angeles leaders had vowed that entrepreneurs such as her - with roots in communities hit hardest by the war on drugs - would get an upper hand in L.A.'s potentially lucrative marijuana market.

[Los Angeles Times](#)

### **LA County drops plan for \$2B jail in favor of mental health facility**

The Los Angeles County Board of Supervisors this week abandoned years of planning to rebuild Men's Central Jail and voted 3-2 to rebuild it as at least one mental health facility. The author and co-author of the new plan appeared on Eyewitness Newsmakers. Supervisors Janice Hahn and Mark Ridley-Thomas talked about this landmark turning point for county incarceration.

[ABC7](#)

## **Convictions/Sentences/Parole**

### **Los Angeles man found guilty of murder in pursuit crash that killed passenger**

Jurors took about four hours to find a Los Angeles man guilty of second-degree murder for leading Gardena police officers in a pursuit that ended when he crashed into a power pole, killing his passenger, officials said Thursday, Feb. 14. Candido Rivera, 29, was also found guilty in Los Angeles Superior Court of two other felony counts - assault on a peace officer and evading a peace officer causing injury or death - and misdemeanor hit-and-run causing injury, said Ricardo Santiago, a spokesman for the Los Angeles County District Attorney's office.

[Torrance Daily Breeze](#)

### **Serial groping women on Metro lines ordered to register as sex offender**

A man who has been convicted 10 times for groping women and girls on Metro buses and other public transportation lines around Los Angeles and Long Beach was ordered today to stay away from all public transportation systems, undergo a one-year residential mental health counseling program and register as a sex offender for life.

[City News Service](#)

### **Orange County daughter fighting release again of man who bludgeoned her parents to death**

More than 40 years after James and Essie Effron were bludgeoned to



death in their popular San Diego clothing store, their two children are angered that they will once again have to fight the release of their parents' killer, less than two years after he was last denied parole.

[Orange County Register](#)

### **Who stays in jail before trial? Who goes free? Sometimes, an algorithm helps decide**

On any given day in the United States, around half a million people are held in jail awaiting trial - a trend that has grown sharply since the 1980s, according to the Prison Policy Initiative, a nonprofit that researches mass criminalization. Some poor defendants can spend days, weeks or even years behind bars, just waiting for their day in court, while rich defendants remain free.

[USA Today](#)

### **South L.A. man sent to prison for robbing secret service agent**

A 23-year-old South Los Angeles man was sentenced Thursday to seven-and-a-half years in federal prison for robbing an undercover U.S. Secret Service agent at gunpoint. Richard Taron "Profit" Henderson pleaded guilty in September to conspiracy, robbery, assaulting a federal officer with a deadly weapon, using a firearm during a crime of violence and dealing counterfeit money.

[My News LA](#)

## **California/National**

### **California prison guards make nice with Gov. Gavin Newsom**

In its ongoing effort to make nice with Gov. Gavin Newsom, the California prison guards union is taking back a \$2 million contribution to a criminal justice voter initiative he opposes. The \$2 million check, in support of the Reducing Crime and Keeping California Safe Act of 2020, was cut by then-President Chuck Alexander of the California Correctional Peace Officers Association just as he headed out the door on Dec. 31.

[San Francisco Chronicle](#)

### **Vatican confirms secret Catholic Church guidelines for priests who father children**

CBS News has confirmed that the Vatican has secret guidelines for priests who father children, despite their vows of celibacy. Vincent Doyle, the founder of a support group for children of priests, told CBS News that a Vatican official showed him the confidential instructions. Doyle said he's been pushing the Church to publicly support those children, who often grow up living in shame and secrecy.

[CBS News](#)

### **New bill would grant sex workers who report violent crimes immunity from arrest and criminalization**

A new bill from Senator Scott Wiener (D-San Francisco) aims to ensure that sex workers who are victimized or who witness violent or otherwise

serious crimes are not funneled into the criminal justice system themselves when they come forward to report crimes to the police. We're all worse off when crime victims do not feel safe coming forward, for fear of arrest," said Sen. Wiener.

[Witness LA](#)

### **DMV confirms ICE has limited access to AB 60 license information**

An Escondido man said he wanted to drive legally here in California and now is facing deportation because of it. The man and his attorneys believe, AB 60, a law that was designed to help undocumented immigrants obtain California driver licenses legally is now being used against them. Playing with his children, Joel Hernandez said he has tried to shield his younger children from the fear that he faces deportation.

[NBC7 San Diego](#)

## **Consumer Warnings**

### **Counterfeit memory cards**

Consumers need to be very wary of fraudulent Remax microSD memory cards. They are common on eBay, Alibaba, Amazon and other various internet e-commerce websites, often at a fraction of a comparable brand name products price. The SD trademarks and logos ("SD Marks and Logos") are owned and licensed by SD-3C, LLC ("SD-3C"). The SD Marks and Logos are registered with the United States Patent and Trademark Office and with other trademark offices around the world.

[The Counterfeit Report](#)

### **Company warns consumers about counterfeit product on Amazon, highlighting ongoing issue**

The products were being sold by a seller who goes by the moniker of BluTiger. The seller was allegedly selling counterfeit versions of Nutramax's Avmacol dietary supplement. "We are treating these counterfeit products as a threat to your safety and well-being," the company said in a press release aimed at customers.

[NutraIngredients-USA](#)

## **Guns**

### **How California got tough on guns**

The modern American gun debate began on May 2, 1967, when 30 protesting members of the Black Panther Party marched into the California Capitol with loaded handguns, shotguns and rifles. As photos of gun-toting radicals from Oakland hit front pages across the country, many Americans were shocked to see who was embracing the Second Amendment.

[North Coast Journal](#)

### **California's gun seizure program hits hurdles**

Authorities in California are struggling to enforce a state law that permits officials to seize firearms from people with previous criminal convictions or mental health issues - running into staffing and budgetary issues that have contributed to a massive backlog of guns marked for confiscation.

[Fox News](#)

## Media

### **The L.A. Times union says hell no to management controlling creative projects**

The Los Angeles Times and the Los Angeles Times Guild are feuding over a proposal that would give management control over any non-Times related projects undertaken by its journalists. Since June, members of the Times' recently formed union have been engaged with management in negotiating the first collective bargaining agreement in the paper's history.

[Los Angeles Magazine](#)

### **How well does the US media cover criminal justice?**

Even as crime news - from mass shootings to the continued fallout from the #MeToo movement - dominate national media coverage, the continued drop in coverage of local justice issues threatens to leave millions of Americans in the dark about the practices and problems of the U.S. justice system, according to The Crime Report's annual survey of criminal justice coverage.

[The Crime Report](#)

### **Lara Logan: This interview 'is like professional suicide'**

"This is the kind of interview that is like professional suicide for me," says former CBS News Foreign Correspondent Lara Logan. The reason? In a Friday appearance on retired Navy SEAL Mike Ritland's Mike Drop podcast, she doesn't hold back when discussing the liberal media and fake news (Mediaite's headline calls it a "scorched-earth interview").

[Newser](#)

### **Why is security fortified for Gov. Newsom's press conference?**

At Friday's press conference Gov. Gavin Newsom had with California Attorney General Xavier Becerra, State Capitol police had a significantly beefed up presence, and even used a drug and/or bomb-sniffing dog checking out reporters' and media equipment. Why? Gov. Gavin Newsom very publicly criticized President Donald Trump last week as he pulled California National Guard troops from the Mexico border, claiming any border crisis was "manufactured" and all "political theater."

[California Globe](#)

## Corrections

### **California prisoners say videos show 'gladiator fights' at Soledad**

## **State Prison**

California prisoners released video recordings of two prisoner fights they say were set-up by officials at the Correctional Training Facility in Soledad, California. It is now the second facility to report so-called "gladiator fights" after prisoners spoke out about similar incidents at the state prison in Corcoran. The videos were provided after Shadowproof published reports on a hunger strike at the state prison in Corcoran over arranged prison fights at that facility.

[Shadowproof](#)

## **Nearly 50 inmates riot at Donovan State Prison, 10 injured**

A riot involving nearly 50 inmates at Richard J. Donovan Correctional Facility left 10 prisoners wounded Friday, including one so severely that he had to be life-flighted from the prison, officials confirmed. Several fights erupted simultaneously on the South Bay prison's yard for medium-custody prisoners at about 9 a.m. Friday, the California Department of Corrections and Rehabilitation (CDCR) said.

[NBC7 San Diego](#)

## **Delano prison officials investigating stabbing death of inmate**

An inmate was fatally stabbed Thursday at Delano's Kern Valley State Prison, according to prison officials. Sergio Robles, 44, was attacked by two inmates just after 10 a.m. and suffered multiple stab wounds to his head, back and upper body, according to a California Department of Corrections and Rehabilitation news release. He was taken to an outside hospital, where he was pronounced dead at 10:53 a.m., the release said.

[Bakersfield Californian](#)

## **Despite millions more in funds, quality of prison rehab programs questionable: Audit**

Although California is spending millions of dollars on rehabilitation programs for prison inmates, there's little evidence to show those programs are effective, according to a state audit. In a report released recently, the state auditor's office found that, while the budget for in-prison rehabilitation programs at the California Department of Corrections and Rehabilitation (CDCR) increased by \$64 million between 2013 and 2019, recidivism rates have remained stubbornly high, with an average of 50 percent of inmates reoffending within three years.

[East Bay Times](#)

## **California's Juvenile Justice System had 16 years to fix its abuse problems. It didn't.**

The mission statement of the California Division of Juvenile Justice - which houses about 650 of the state's most serious juvenile and young adult offenders - says that the agency's aim is to use "effective treatment, education and interventions in order to encourage positive lifestyles, reduce recidivism, strengthen families and protect our

communities."

[Huff Post](#)

## Homeless

### **A snapshot of homelessness in California**

In late January communities around the country conducted a point-in-time count of their homeless populations. Federally mandated by the US Department of Housing and Urban Development, these estimates help local, state, and federal governments allocate resources and track progress toward the goal of ending homelessness. Last year's count revealed that about 130,000 Californians were homeless - nearly a quarter of the national total.

[PPIC](#)

## Pensions

### **The California rule on public employee pensions under attack: Will we still call it the "California Rule" if it is no longer the rule in California?**

Most public employees in California are eligible to enroll in a state or county retirement system. These retirement systems are governed by state statutes, known primarily as either the Public Employees' Retirement Law ("PERL") or the County Employees' Retirement Law ("CERL"), depending on the retirement system in question.

[Business Law Today](#)

### **Public pension plan investment performance continues to lag the financial markets**

The portfolios of the organizations that manage the pension plans for Lamorinda public agencies have failed for years to deliver investment returns that match those of a mainstream domestic equity index, putting pressure on the public agencies to make up the investment shortfall out of their local operating budgets.

[Lamorinda Weekly](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)



**From:** [Association of Deputy District Attorneys](#)  
**To:** [ggiquiere@ci.sunnyvale.ca.us](mailto:ggiquiere@ci.sunnyvale.ca.us)  
**Subject:** Monday Morning Memo for February 25, 2019  
**Date:** Monday, February 25, 2019 5:04:22 AM

---

Having trouble viewing this email? [Click here](#)



## Courts & Rulings

### **Ruling affirming the rights of students accused of sexual misconduct roils California colleges**

Colleges and universities across California are scrambling to revise the

way they handle sexual misconduct cases after a state appellate court ruled that "fundamental fairness" requires that accused students have a right to a hearing and to cross-examine their accusers. The decision last month came in a USC case but applies to all California public and private colleges, and prompted many to immediately halt Title IX investigations while they reshape their procedures.

[Los Angeles Times](#)

### **Conviction to stand despite prosecutor's effort to arouse jurors' passion**

A man convicted of first degree residential burglary and second degree robbery yesterday failed in his bid for a reversal based on the prosecutor, during rebuttal argument, telling jurors to act other than as dispassionate evaluators of the evidence. The defendant, George Alfaro, in burglarizing the home of Carol Cortes for the second time in two months, punched Cortes in the face and stole her cellphone.

[Metropolitan News-Enterprise](#)

### **Judge bars immigration policing criteria for 2 grants**

A federal judge on Friday permanently blocked the Trump administration from imposing conditions that police departments cooperate with immigration authorities to receive law enforcement grants. The Department of Justice exceeded its authority and violated the constitution by requiring grant recipients to allow immigration authorities into jails and provide advance notice before releasing detainees suspected of being in the country illegally, Judge Manuel Real said.

[PBS](#)

### **Supreme Court strikes blow against states that raise revenue by hefty fines, forfeitures**

The Supreme Court ruled unanimously Wednesday that states cannot impose excessive fees, fines and forfeitures as criminal penalties. The decision, which united the court's conservatives and liberals, makes clear that the Eighth Amendment's prohibition against "excessive fines" applies to states and localities as well as the federal government.

[USA Today](#)

### **Defendant's Arbuckle right not forfeited by failing to raise it at sentencing - C.A.**

The Fifth District Court of Appeal yesterday invalidated the sentence of a woman whose drunk driving resulted in the death of her son, holding that she had a right to be sentenced by the same judge who took her no-contest pleas even though she did not invoke that right at the time of sentencing. Justice Mark W. Snauffer wrote the opinion which seeks to discern the California Supreme Court's intent in its 2017 decision in K.R. v. Superior Court.

[Metropolitan News-Enterprise](#)

### **Rocklin teen's murder sentence in sister's death upheld, as judge calls new law unconstitutional**

Rocklin teen Tanner Wood will be sentenced in April to 16 years to life in state prison for the 2016 murder of his younger sister, a Sacramento judge ordered Friday, rejecting a new juvenile justice law as unconstitutional. Sacramento Superior Court Judge James Arguelles' courtroom became the latest local testing ground for Senate Bill 1391 as the judge sparred with Wood's attorney over whether the new law barring minors younger than 16 from being tried as adults for murder and other serious crimes passed constitutional muster.

[Sacramento Bee](#)

### **Probable cause lacking for arrest based on general description**

The Ninth U.S. Circuit Court of Appeals yesterday affirmed the denial of summary judgment, sought on the ground of qualified immunity, to an El Monte police detective who arrested a light-skinned bald man for illegal sales of firearms in response to a report by an alleged confidential informant of such activity by a man of the arrestees description.

[Metropolitan News-Enterprise](#)

### **California Supreme Court ruling causes chaos for local tax measures**

Late last year, the city of Oakland put a new land parcel tax on the books, after 62 percent of voters turned out to boost funding for public education. Now a local business group is suing the city, arguing that the new tax needed two-thirds of the vote - just over 66 percent - to pass. San Francisco faces a similar problem, only twice as big.

[CALmatters](#)

### **Judge erred in declaring bail forfeited without considering medical condition of defendant**

The Fifth District Court of Appeal yesterday reversed an order denying a surety's motion to exonerate a bail bond or to toll the 180-day appearance period, declaring that the judge erred in not considering the debilitated state of the 91-year-old criminal defendant who is in hospice care and suffers from dementia.

[Metropolitan News-Enterprise](#)

### **Judge overturns \$38M verdict in lawsuit over Baltimore County police killing of Korryn Gaines**

Baltimore County judge has overturned the decision of a jury that awarded more than \$38 million to the family of Korryn Gaines, the 23-year-old Randallstown woman who was shot and killed by county police in 2016. Judge Mickey J. Norman dismissed the family's claims against the county and the officer who fatally shot Gaines.

[Baltimore Sun](#)

### **Secret records of police misconduct and shootings must be released under new law, L.A. judge rules**

A Los Angeles judge dealt a blow this week to law enforcement unions trying to limit the scope of a landmark transparency law, ruling that records from shootings, use of force and some misconduct by police officers in California are public even if they occurred before the new law took effect this year.

[Los Angeles Times](#)

### **Politifact fact-check: the Ninth Circuit is, in fact, the most reversed federal court of appeals**

Recently, cable news personality Sean Hannity commented that the Ninth Circuit is the "most overturned court in the country." Politifact rated that claim as "false." But Politifact's analysis is seriously flawed and suffers from selective analysis of the evidence, and misrepresentation of the evidence in other respects.

[Excess of Democracy](#)

### **Justice Thomas wants the Court to 'reconsider' its First Amendment jurisprudence**

Stare decisis, schmare decisis. Supreme Court Justice Clarence Thomas apparently agrees with Donald Trump when it comes to the First Amendment. The president famously vowed to "open up the libel laws" to make it easier to sue the media (even though Trump is more likely to be burned by that change in constitutional law), and in today's concurrence in *McKee v. Cosby*, Justice Thomas seems to be on board.

[Above the Law](#)

## **Prop 47, 57 & AB 109**

### **Are California's criminal justice reforms actually working?**

Prop. 47 reclassified certain theft and drug possession offenses from felonies to misdemeanors; allowed defendants serving sentences for felony offenses that would have qualified as misdemeanors under Prop. 47 to petition the courts for resentencing; allows defendants who have completed their sentences for felony convictions to apply to reclassify them as misdemeanors under the new law, according to the California Courts website.

[Bakersfield Now](#)

### **These 13 people were convicted of murder in SLO County. Some could go free under new law**

More than a dozen men and women convicted of murders they personally did not commit in San Luis Obispo County may be eligible for re-sentencing - and in some cases, release - after a change in state law late last year. In hearings scheduled over the next several months, San Luis Obispo County prosecutors and defense attorneys will argue before a judge whether people who acted as accomplices to crimes fit certain criteria and could no longer be convicted of murder under current law.

[The Tribune](#)

### **Ex-Gov. Brown, solve this**

How apropos that you run a series on homelessness. The problem was exacerbated with the passage of Proposition 47 by our liberal politicians backed by the SEIU, the ACLU and pushed as the "Safe Neighborhood and Schools" act. The passage of this liberal blunder increased the number of criminals on the street. Add to this the deluge of illegals because of "Sanctuary City" benefits and we have the mess that is the "homeless" of today.

[Opinion/Desert Sun](#)

### **Sculptures popping up around town through inmate work program**

Residents enjoying a walk through River Park may have noticed some new artwork popping up over the past few months. The metal sculptures are the work of inmates who are part of a Tehama County AB 109 program that provides training in wood and metal working as a form of alternative incarceration. "I appreciate it," said inmate Jason Horn. "I didn't want to sit in jail. Now I'm learning a few things and contributing."

[Red Bluff Daily News](#)

### **The latest in leniency for criminals**

The 2014 Proposition 47 reduced penalties for property crime and transformed some felonies into misdemeanors. The 2016 Proposition 57 barred prosecutors from directly filing juvenile cases in adult court. Senate Bill 1391, effective January 1, forbids prosecution of 14- and 15-year old criminals as adults, whatever the gravity of their crime. A new measure now takes the trend of leniency to a new level.

[California Globe](#)

## **Prosecutions/Prosecutors**

### **District Attorney successfully argues SB 1437 as unconstitutional**

On Friday, Feb. 8, 2019, during a hearing in the People v. Dejon Griffin and Aaron Jackson case, Orange County Superior Court Judge Gregg L. Prickett heard arguments on the constitutionality of Senate Bill (SB) 1437, given that it lacks the two-thirds super majority of both bodies of the California Legislature.

[Orange County Breeze](#)

### **Solano DA on record as challenging new state laws affecting violent offenders**

Solano County District Attorney Krishna Abrams said her office is on record challenging new state laws affecting violent offenders, Senate bills 1437 and 1391. Her comments came toward the end of a fast-paced, 90-minute public forum held Tuesday night in the County Events Center, next to the County Government Center, in Fairfield.

[Vacaville Reporter](#)

### **Suspect in shootout with police claims to be a 'prophet' in court**



A man facing a murder charge over a deadly shootout with police in front of a neighborhood market last summer said in court Friday that he was a "prophet" sent by Jesus and smeared a brown substance on a glass partition, but a prosecutor said it was all an act to further delay court proceedings.

[Courthouse News Service](#)

### **Riverside County man charged with killing 11-year-old Linda O'Keefe in 1973 cold-case murder**

A Colorado man has been charged with the 1973 abduction and killing of an 11-year-old Corona del Mar girl who was walking home from school, officials announced Wednesday morning, bringing a long-awaited arrest in a case that shocked the Newport Beach community. Orange County District Attorney Todd Spitzer said during a press conference that the suspect, James Alan Neal, 72, faces a special-circumstances murder charge, leaving open the possibility that prosecutors could seek the death penalty.

[Orange County Register](#)

### **Parolee charged with killing three men at Torrance bowling alley**

A parolee who allegedly shot and killed three men at a bowling alley in Torrance is scheduled to be arraigned on a charge of murder Tuesday in a case in which he could face the death penalty. Reginald Leander Wallace, 47, of Los Angeles, is scheduled to be arraigned Tuesday in a Torrance courtroom on three counts of murder for allegedly shooting Michael Radford, 20; and Robert Meekins and Astin Edwards, both 28, just before midnight Jan. 4 at Gable House Bowl at 22501 Hawthorne Blvd., along with four counts of attempted murder and one count of possession of a firearm by a felon.

[My News LA](#)

### **The Latest: Son charged with killing parents, housekeeper**

Prosecutors have charged a California man with killing his parents and their housekeeper in an upscale community. The Orange County district attorney's office charged 27-year-old Camden Nicholson on Friday with three counts of murder and an enhancement alleging multiple murders. Nicholson's arraignment was delayed to March 8. His lawyer Jessica Ann Watts didn't immediately respond to a message seeking comment.

[AP](#)

### **Man extradited from El Salvador to face murder and torture charges in estranged wife's Pacoima stabbing death**

A man extradited from El Salvador in connection with his estranged wife's stabbing death in Pacoima nearly nine years ago has been charged with murder and torture, the Los Angeles County District Attorney's Office announced Tuesday. Napoleon Eduardo Castro - also known as Juan Flores, Luis Sanchez and Trouble - is set to be arraigned March 6 at the San Fernando courthouse in connection with the torture

killing of his estranged wife, Olga Martinez, in her garage.

[City News Service](#)

### **Former Valley candidate and aide fined for violations tied to campaign funds**

A former candidate for Los Angeles City Council and his campaign treasurer have been fined more than \$38,000 for using laundered donations to get taxpayer money and misspending such dollars on personal expenses. The Los Angeles City Ethics Commission voted unanimously Tuesday to fine J. Roy Garcia, who ran unsuccessfully in 2013 for a council seat in the San Fernando Valley, and his campaign treasurer Hardy Henriquez.

[San Diego Union-Tribune](#)

## **Criminal Justice/Public Safety**

### **California's black market for pot is stifling legal sales. Now the governor wants to step up enforcement**

Before he was elected governor, Gavin Newsom was instrumental in legalizing marijuana for recreational use in California. Now, as he settles into office, he faces the challenge of fixing a system that has been slow to bloom. Newsom has urged patience with sluggish growth in the number of state-licensed cannabis businesses, saying he expected that such a complex regulatory system would take at least five years to fully develop.

[Los Angeles Times](#)

### **Female LAPD commander sues for gender discrimination**

An LAPD Commander facing termination after being accused of being drunk in public has sued the City of Los Angeles, claiming that because she is female she faced discrimination and retaliation during an internal police administrative trial. "There is compelling evidence that men were treated differently than women," Nicole Mehringer's lawsuit said.

[NBC4](#)

### **Ford's 2020 Explorer for police has hidden lifesaving design feature**

Michigan State Police 1st Lt. Mike Shaw has been nearly hit by speeding vehicles four times, twice while outside his car. "And four times is actually low. I know a trooper who has been hit more than 10 times," Shaw said. "You can probably talk to any state trooper. It's not a matter of if, but when. People just aren't paying attention out there, and sometimes they're impaired with alcohol or marijuana or even their cellphones. Maybe they're just gawking. And our troopers are getting hit."

[Detroit Free Press](#)

### **Protesters disrupt Altadena Church's Black History Celebration as Los Angeles County District Attorney attempts to speak**

Loud protesters reportedly including the mothers of several people killed during incidents involving law enforcement disrupted a Black History Celebration at Altadena Baptist Church on Sunday night. The incident occurred about 6 p.m. as keynote guest Jackie Lacey, the first African-American to serve as Los Angeles County's District Attorney, was about to speak.

[Pasadena Now](#)

## **Policy & Legal Issues**

### **Has criminal justice reform gone too far? One California lawmaker thinks so**

Overcrowded prisons. Trying teens as juveniles versus adults. The power of rehabilitation and a belief in second chances. These issues have fueled criminal justice reform in recent years in the state of California. But some say the overhaul has gone too far. People can generally agree, we all want to live in safe communities, but as Assemblymember Jim Cooper (D-Elk Grove) told ABC10, the devil is in the details.

[ABC10 Sacramento](#)

### **Felony murder law repealed? Maybe not**

Two young men drive up to a small corner grocery store in an inner city neighborhood and the driver remains at the wheel while his masked partner runs into the store, gun in hand, to commit a robbery. The armed gunman shoots and kills the clerk before grabbing cash out of the register, then jumps back into the car and the two make their getaway.

[CALmatters](#)

### **LA's illegal pot shops may have water, power shut off**

With hundreds of illegal marijuana shops continuing to operate in Los Angeles, a City Council committee today moved forward with a plan aimed at cracking down on the businesses by shutting off their utilities. The idea of shutting off water and power at illegal pot shops was proposed last year by Councilwomen Nury Martinez and Monica Rodriguez.

[City News Service](#)

### **The power of judicial review: Erwin Chemerinsky**

President Donald Trump and Attorney General Jeff Sessions have engaged in unprecedented attacks on judicial review that reflect a profound lack of understanding about the Constitution. My fear is that their rants will contribute to undermining the legitimacy of the courts and of the rule of law.

[Daily News](#)

### **Scrubbing the past to give those with a criminal record a second chance**

Latosha Poston says she made a lot of mistakes in her life. Her legal troubles began in her teens after her first child was born in

Indianapolis. Over the years, bad decisions led to some arrests, some convictions. "Sometimes we get stuck in our past and let our past guide us," she says. The 44-year-old has worked hard to straighten out her life. But her criminal records - all involving misdemeanors - continued to haunt her as she tried to find a decent job and place to live.

[NPR](#)

### **Goldstein Investigation: LAPD using electric BMWs to commute, go to lunch**

The Los Angeles Police Department's efforts to go green with electric cars is raising some red flags, including a police psychologist who was caught using one of the department's fleet of electric BMW's to commute to and from work. When CBS2/KCAL9 Investigative Reporter David Goldstein asked, "Why should taxpayers be paying for you to take this? You're basically commuting to and from your house, aren't you, sir?" the psychologist had no comment.

[CBS LA](#)

## **Crime**

### **ICE: Man who shot at Napa deputy in country illegally, deported multiple times**

The man who was shot dead by a Napa County sheriff's deputy after he fired at her point blank during a traffic stop was a Mexican national in the country illegally after being deported multiple times, according to U.S. Immigration and Customs Enforcement. Javier Hernandez-Morales shot at and missed Deputy Riley Jarecki during a traffic stop late Sunday night as she stood next to his driver-side window.

[CBS SF](#)

### **Magic Johnson's daughter home invasion suspect arrested**

Cops nabbed a guy they say pulled the home invasion that forced Magic Johnson's daughter to run for her life. Law enforcement sources tell TMZ ... LAPD identified the suspect after reviewing surveillance video from the neighborhood where Elisa Johnson's friends were renting a house back in December.

[TMZ](#)

### **Police trainer's gun stolen off baggage carousel at California airport**

A gun belonging to someone who trains police officers is on the streets after it was stolen from a baggage carousel at San Francisco International Airport, according to its owner. The gun's owner said he did everything by the book and blames United Airlines for his gun ending up in the hands of suspected thieves. The man, who didn't want to be identified, has a gun permit and trains police officers.

[NBC4](#)

### **Suspected DUI driver arrested in hit-and-run crash in South-**

### **Central L.A. caught on video**

A man suspected of driving drunk at a speed of 80 to 100 mph when he plowed into six parked vehicles in Historic South-Central L.A., ejecting and injuring one of his passengers before fleeing the scene, was arrested hours after the early Sunday morning crash, police said. Police clarified on Monday that the person sustained severe injuries but survived.

[KTLA](#)

### **Rare bulldog stolen and taken 2,000 miles, but dogged police officers track it down**

Although it was a little late, Christmas finally came for one family. All they had to do was travel 2,000 miles to get their intended gift - a rare English bulldog puppy. The dog was going to be a Christmas surprise for a suburban Chicago family in Naperville, Illinois, WWL reported. But on Dec. 18, a real-life Grinch stole the 10-week-old puppy - a blue merle English bulldog which is rare because of its coloring, according to WLS.

[Miami Herald](#)

**The Los Angeles Police issued a warning to street food vendors as an increase in assaults has been reported in the Boyle Heights area.** Officials distributed fliers written in Spanish and English to inform vendors to take care of themselves because some of their colleagues have been the target of armed attacks. "We have to worry about those who only come to get the fruit," said Alicia Cárdenas, a street vendor of fruit.

[NBC4](#)

### **Porter Ranch triple homicide victims identified**

The triple homicide that has shaken an upscale, exclusive gated community was not a random attack, and it appears the yet to be identified killer or killers were allowed into the house, the police captain overseeing the investigation said Tuesday. Called to a large house on Via Galileo in Porter Ranch's Renaissance community shortly before 4 p.m. Monday, responders found three men inside, all dead of apparent gunshot wounds.

[NBC4](#)

## **Los Angeles County Sheriff**

### **L.A. County's new sheriff announced reforms to limit ICE. Immigrant rights groups don't think they go far enough.**

A coalition of Los Angeles immigrant rights groups, many of which championed L.A. County Sheriff Alex Villanueva's long-shot campaign during the mid-term elections last year, wrote in an open letter Monday that he has "betrayed" them in just a few weeks in office by walking back pledges to limit Trump administration Immigration and Customs Enforcement agents' reach in the city.

[Pacific Standard](#)



### **Sheriff Alex Villanueva promised change. His supporters are standing by him despite controversies**

New Los Angeles County Sheriff Alex Villanueva is testing supporters with his unorthodox approach as the region's top cop. Only two months on the job, Villanueva fired his department's top brass and asked others to reapply for their positions. His reinstatement of a deputy fired amid allegations of domestic abuse and stalking prompted a rare rebuke from several Los Angeles County supervisors.

[Los Angeles Times](#)

### **LA sheriff: Fewer crimes spur transfer to immigration agents**

The new leader of the nation's largest sheriff's department on Friday further limited when inmates in Los Angeles County jails can be transferred to U.S. authorities for deportation. The department has reduced the number of misdemeanor charges that can trigger an inmate's transfer to U.S. Immigration and Customs Enforcement for deportation from 151 to 101, spokeswoman Nicole Nishida said.

[San Francisco Chronicle](#)

### **Supervisors to authorize settlement in lawsuit claiming "battery" by SCV Sheriff deputies**

County supervisors are expected to finalize a settlement reached in a lawsuit filed by a man who claimed he was beaten by local sheriff's deputies on Christmas Eve in 2016. On Tuesday, the Los Angeles County Board of Supervisors are scheduled to vote on a recommendation to authorize a \$150,000 settlement in the civil case of John Clyde Warner vs. the County of Los Angeles.

[The Signal](#)

## **Los Angeles County**

### **Probation department workplace injury payouts soar by nearly \$6 million as violence rises in juvenile lockups**

Los Angeles County supervisors are set Tuesday to discuss whether pepper spray should still be used in juvenile lockups after an alarming uptick in its use, which has led to an internal department investigation by the County Inspector General. The spike in pepper spray use comes as the population of youth offenders is dropping amid a push toward rehabilitation and as similar agencies across the country are shunning its use, saying it's ineffective, inhumane and a potential liability.

[NBC4](#)

### **Goldstein investigation: 2 men mysteriously died in his apartment, he calls our reporter 'an a-hole'**

Two men died mysteriously in the West Hollywood apartment of Democratic party fundraiser Ed Buck, but when CBS2 investigative reporter David Goldstein confronted him, Buck didn't have much to say. "Why don't you answer any questions? You have two people who died in

your house," Goldstein asks. "Because you're being an a-hole," Buck replies. Buck was blunt. Not answering any questions.

[CBS LA](#)

### **Pot entrepreneurs are running out of patience and money while waiting on L.A. permits**

For Kika Keith, a dream deferred looks like a bare, brightly illuminated room in South Los Angeles. After California legalized recreational cannabis, Los Angeles leaders had vowed that entrepreneurs such as her - with roots in communities hit hardest by the war on drugs - would get an upper hand in L.A.'s potentially lucrative marijuana market.

[Los Angeles Times](#)

### **LA County drops plan for \$2B jail in favor of mental health facility**

The Los Angeles County Board of Supervisors this week abandoned years of planning to rebuild Men's Central Jail and voted 3-2 to rebuild it as at least one mental health facility. The author and co-author of the new plan appeared on Eyewitness Newsmakers. Supervisors Janice Hahn and Mark Ridley-Thomas talked about this landmark turning point for county incarceration.

[ABC7](#)

## **Convictions/Sentences/Parole**

### **Los Angeles man found guilty of murder in pursuit crash that killed passenger**

Jurors took about four hours to find a Los Angeles man guilty of second-degree murder for leading Gardena police officers in a pursuit that ended when he crashed into a power pole, killing his passenger, officials said Thursday, Feb. 14. Candido Rivera, 29, was also found guilty in Los Angeles Superior Court of two other felony counts - assault on a peace officer and evading a peace officer causing injury or death - and misdemeanor hit-and-run causing injury, said Ricardo Santiago, a spokesman for the Los Angeles County District Attorney's office.

[Torrance Daily Breeze](#)

### **Serial groping women on Metro lines ordered to register as sex offender**

A man who has been convicted 10 times for groping women and girls on Metro buses and other public transportation lines around Los Angeles and Long Beach was ordered today to stay away from all public transportation systems, undergo a one-year residential mental health counseling program and register as a sex offender for life.

[City News Service](#)

### **Orange County daughter fighting release again of man who bludgeoned her parents to death**

More than 40 years after James and Essie Effron were bludgeoned to

death in their popular San Diego clothing store, their two children are angered that they will once again have to fight the release of their parents' killer, less than two years after he was last denied parole.

[Orange County Register](#)

### **Who stays in jail before trial? Who goes free? Sometimes, an algorithm helps decide**

On any given day in the United States, around half a million people are held in jail awaiting trial - a trend that has grown sharply since the 1980s, according to the Prison Policy Initiative, a nonprofit that researches mass criminalization. Some poor defendants can spend days, weeks or even years behind bars, just waiting for their day in court, while rich defendants remain free.

[USA Today](#)

### **South L.A. man sent to prison for robbing secret service agent**

A 23-year-old South Los Angeles man was sentenced Thursday to seven-and-a-half years in federal prison for robbing an undercover U.S. Secret Service agent at gunpoint. Richard Taron "Profit" Henderson pleaded guilty in September to conspiracy, robbery, assaulting a federal officer with a deadly weapon, using a firearm during a crime of violence and dealing counterfeit money.

[My News LA](#)

## **California/National**

### **California prison guards make nice with Gov. Gavin Newsom**

In its ongoing effort to make nice with Gov. Gavin Newsom, the California prison guards union is taking back a \$2 million contribution to a criminal justice voter initiative he opposes. The \$2 million check, in support of the Reducing Crime and Keeping California Safe Act of 2020, was cut by then-President Chuck Alexander of the California Correctional Peace Officers Association just as he headed out the door on Dec. 31.

[San Francisco Chronicle](#)

### **Vatican confirms secret Catholic Church guidelines for priests who father children**

CBS News has confirmed that the Vatican has secret guidelines for priests who father children, despite their vows of celibacy. Vincent Doyle, the founder of a support group for children of priests, told CBS News that a Vatican official showed him the confidential instructions. Doyle said he's been pushing the Church to publicly support those children, who often grow up living in shame and secrecy.

[CBS News](#)

### **New bill would grant sex workers who report violent crimes immunity from arrest and criminalization**

A new bill from Senator Scott Wiener (D-San Francisco) aims to ensure that sex workers who are victimized or who witness violent or otherwise

serious crimes are not funneled into the criminal justice system themselves when they come forward to report crimes to the police. We're all worse off when crime victims do not feel safe coming forward, for fear of arrest," said Sen. Wiener.

[Witness LA](#)

### **DMV confirms ICE has limited access to AB 60 license information**

An Escondido man said he wanted to drive legally here in California and now is facing deportation because of it. The man and his attorneys believe, AB 60, a law that was designed to help undocumented immigrants obtain California driver licenses legally is now being used against them. Playing with his children, Joel Hernandez said he has tried to shield his younger children from the fear that he faces deportation.

[NBC7 San Diego](#)

## **Consumer Warnings**

### **Counterfeit memory cards**

Consumers need to be very wary of fraudulent Remax microSD memory cards. They are common on eBay, Alibaba, Amazon and other various internet e-commerce websites, often at a fraction of a comparable brand name products price. The SD trademarks and logos ("SD Marks and Logos") are owned and licensed by SD-3C, LLC ("SD-3C"). The SD Marks and Logos are registered with the United States Patent and Trademark Office and with other trademark offices around the world.

[The Counterfeit Report](#)

### **Company warns consumers about counterfeit product on Amazon, highlighting ongoing issue**

The products were being sold by a seller who goes by the moniker of BluTiger. The seller was allegedly selling counterfeit versions of Nutramax's Avmacol dietary supplement. "We are treating these counterfeit products as a threat to your safety and well-being," the company said in a press release aimed at customers.

[NutraIngredients-USA](#)

## **Guns**

### **How California got tough on guns**

The modern American gun debate began on May 2, 1967, when 30 protesting members of the Black Panther Party marched into the California Capitol with loaded handguns, shotguns and rifles. As photos of gun-toting radicals from Oakland hit front pages across the country, many Americans were shocked to see who was embracing the Second Amendment.

[North Coast Journal](#)

### **California's gun seizure program hits hurdles**

Authorities in California are struggling to enforce a state law that permits officials to seize firearms from people with previous criminal convictions or mental health issues - running into staffing and budgetary issues that have contributed to a massive backlog of guns marked for confiscation.

[Fox News](#)

## Media

### **The L.A. Times union says hell no to management controlling creative projects**

The Los Angeles Times and the Los Angeles Times Guild are feuding over a proposal that would give management control over any non-Times related projects undertaken by its journalists. Since June, members of the Times' recently formed union have been engaged with management in negotiating the first collective bargaining agreement in the paper's history.

[Los Angeles Magazine](#)

### **How well does the US media cover criminal justice?**

Even as crime news - from mass shootings to the continued fallout from the #MeToo movement - dominate national media coverage, the continued drop in coverage of local justice issues threatens to leave millions of Americans in the dark about the practices and problems of the U.S. justice system, according to The Crime Report's annual survey of criminal justice coverage.

[The Crime Report](#)

### **Lara Logan: This interview 'is like professional suicide'**

"This is the kind of interview that is like professional suicide for me," says former CBS News Foreign Correspondent Lara Logan. The reason? In a Friday appearance on retired Navy SEAL Mike Ritland's Mike Drop podcast, she doesn't hold back when discussing the liberal media and fake news (Mediaite's headline calls it a "scorched-earth interview").

[Newser](#)

### **Why is security fortified for Gov. Newsom's press conference?**

At Friday's press conference Gov. Gavin Newsom had with California Attorney General Xavier Becerra, State Capitol police had a significantly beefed up presence, and even used a drug and/or bomb-sniffing dog checking out reporters' and media equipment. Why? Gov. Gavin Newsom very publicly criticized President Donald Trump last week as he pulled California National Guard troops from the Mexico border, claiming any border crisis was "manufactured" and all "political theater."

[California Globe](#)

## Corrections

### **California prisoners say videos show 'gladiator fights' at Soledad**



## **State Prison**

California prisoners released video recordings of two prisoner fights they say were set-up by officials at the Correctional Training Facility in Soledad, California. It is now the second facility to report so-called "gladiator fights" after prisoners spoke out about similar incidents at the state prison in Corcoran. The videos were provided after Shadowproof published reports on a hunger strike at the state prison in Corcoran over arranged prison fights at that facility.

[Shadowproof](#)

## **Nearly 50 inmates riot at Donovan State Prison, 10 injured**

A riot involving nearly 50 inmates at Richard J. Donovan Correctional Facility left 10 prisoners wounded Friday, including one so severely that he had to be life-flighted from the prison, officials confirmed. Several fights erupted simultaneously on the South Bay prison's yard for medium-custody prisoners at about 9 a.m. Friday, the California Department of Corrections and Rehabilitation (CDCR) said.

[NBC7 San Diego](#)

## **Delano prison officials investigating stabbing death of inmate**

An inmate was fatally stabbed Thursday at Delano's Kern Valley State Prison, according to prison officials. Sergio Robles, 44, was attacked by two inmates just after 10 a.m. and suffered multiple stab wounds to his head, back and upper body, according to a California Department of Corrections and Rehabilitation news release. He was taken to an outside hospital, where he was pronounced dead at 10:53 a.m., the release said.

[Bakersfield Californian](#)

## **Despite millions more in funds, quality of prison rehab programs questionable: Audit**

Although California is spending millions of dollars on rehabilitation programs for prison inmates, there's little evidence to show those programs are effective, according to a state audit. In a report released recently, the state auditor's office found that, while the budget for in-prison rehabilitation programs at the California Department of Corrections and Rehabilitation (CDCR) increased by \$64 million between 2013 and 2019, recidivism rates have remained stubbornly high, with an average of 50 percent of inmates reoffending within three years.

[East Bay Times](#)

## **California's Juvenile Justice System had 16 years to fix its abuse problems. It didn't.**

The mission statement of the California Division of Juvenile Justice - which houses about 650 of the state's most serious juvenile and young adult offenders - says that the agency's aim is to use "effective treatment, education and interventions in order to encourage positive lifestyles, reduce recidivism, strengthen families and protect our

communities."

[Huff Post](#)

## Homeless

### **A snapshot of homelessness in California**

In late January communities around the country conducted a point-in-time count of their homeless populations. Federally mandated by the US Department of Housing and Urban Development, these estimates help local, state, and federal governments allocate resources and track progress toward the goal of ending homelessness. Last year's count revealed that about 130,000 Californians were homeless - nearly a quarter of the national total.

[PPIC](#)

## Pensions

### **The California rule on public employee pensions under attack: Will we still call it the "California Rule" if it is no longer the rule in California?**

Most public employees in California are eligible to enroll in a state or county retirement system. These retirement systems are governed by state statutes, known primarily as either the Public Employees' Retirement Law ("PERL") or the County Employees' Retirement Law ("CERL"), depending on the retirement system in question.

[Business Law Today](#)

### **Public pension plan investment performance continues to lag the financial markets**

The portfolios of the organizations that manage the pension plans for Lamorinda public agencies have failed for years to deliver investment returns that match those of a mainstream domestic equity index, putting pressure on the public agencies to make up the investment shortfall out of their local operating budgets.

[Lamorinda Weekly](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ ggiguere@ci.sunnyvale.ca.us](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [emc-isac](#)  
**To:** [vmata@sunnyvale.ca.gov](mailto:vmata@sunnyvale.ca.gov)  
**Subject:** HSIN Emergency Services Update February 1-15, 2019: denial of service hits non-emergency police lines; 5G wireless communications primer  
**Date:** Friday, February 22, 2019 12:21:02 PM

---



**WARNING:** This document contains FOR OFFICIAL USE ONLY (FOUO) information. It is subject to release restrictions as detailed in the Homeland Security Act of 2002 (6 U.S.C. 482) and the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy for FOUO information and is not to be released to the public, media, or other personnel who do not have an authorized "need-to-know" without appropriate prior approval of an authorized DHS official.

---

Below is a list of some of the many information products posted to the Emergency Services community on the Homeland Security Information Network (HSIN) between February 1-15, 2019. These include a bulletin on extremists adopting foreign terrorist organization's behaviors; denial of service attacks against non-emergency police lines; and a public safety primer for 5G wireless communications.

---

#### **HSIN Emergency Services Update February 1-15, 2019**

<b>CONTROLLED DANGEROUS SUBSTANCES/DRUGS (State &amp; Local)</b>	
<a href="#">Benzyl Fentanyl</a>	NCR - Threat Intelligence Consortium
<a href="#">Narcotics Report - February 4-10, 2019</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">2018 Overview - Drug Environment Report</a>	New Hampshire Information and Analysis Center (NHIAC)
<a href="#">Counterfeit Adderall Pills Containing Methamphetamine Seized During 3 Separate Investigations in SE Michigan</a>	Michigan Intelligence Operations Center (MIOC)
<a href="#">Narcotics Bulletin - January 28-February 3, 2019</a>	Greater Cincinnati Fusion Center (GCFC)
<b>CYBER SECURITY (State &amp; Local)</b>	
<a href="#">Cyber Security Snapshot - Social Engineering</a>	Michigan Cyber Command Center/Michigan State Police
<a href="#">Cutting Through the Cybersecurity Noise - February 8, 2019</a>	Phoenix UASI
<a href="#">Psycho Social Network - Tor-based Social Network Draws Hackers to Share Exploits and Tools</a>	Central Florida Intelligence Exchange (CFIX)
<a href="#">Vulnerabilities in Underlying Infrastructure of Click2Gov Software May Expose Organizations to Cyberattacks</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">Business Email Compromise Scams Potentially Result in Data Breaches and Financial Losses</a>	NCRIC/MS-ISAC
<a href="#">NDSLIC Bi-Weekly Cybersecurity Rollup - February 1, 2019</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<b>BORDER SECURITY (State &amp; Local)</b>	
<a href="#">Border Security Alert - February 3-9 2019</a>	Patrick Henry College Strategic Intelligence Program
<a href="#">Border Security Alert - January 27 - February 02, 2019</a>	Patrick Henry College Strategic Intelligence Program
<b>OTHER (State &amp; Local)</b>	
<a href="#">5G Wireless Communications - Public Safety Primer</a>	NVRIC/VFC
<a href="#">Tactics and Threats for Violence By Pipeline Opposition Actors</a>	VFC
<a href="#">Human Trafficking Awareness</a>	Oregon Titan Fusion Center (TITAN)
	Southern Nevada Counter Terrorism

<a href="#">Disease Outbreak and Investigation Report - February 12, 2019</a>	Center (SNCTC)
<a href="#">Ku Klux Klan Recruitment Activity in Philadelphia Regional Area</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">First Anniversary of Mass Shooting at Marjory Stoneman Douglas High School in Parkland, Florida</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Increase of Hepatitis A Virus (HAV) Infections in Clark County, NV</a>	Southern Nevada Health District
<b>SPECIAL EVENTS - LISTS AND THREAT ASSESSMENTS (State &amp; Local)</b>	
<a href="#">Key Information Regarding the February 14, 2019 National Rifle Association Events</a>	VFC/NVRIC
<a href="#">2019 Coors Light NHL Stadium Series - Flyers vs. Penguins</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Stoneman Douglas Shooting Anniversary</a>	Delaware Valley Intelligence Center (DVIC)
<b>TERRORISM (State &amp; Local)</b>	
<a href="#">ISIS Threats to Energy Sector</a>	Colorado Information Analysis Center (CIAC)
<a href="#">Extremist Adoption of Foreign Terrorist Organization Behaviors Increases Threat of Violence</a>	NCR - Threat Intelligence Consortium
<b>STATE &amp; LOCAL FUSION CENTER PERIODICALS</b>	
<a href="#">ARIC Quarterly SAR Report</a>	Austin Regional Intelligence Center (ARIC)
<a href="#">Critical Infrastructure Monthly Open Source Review</a>	Massachusetts Commonwealth Fusion Center (CFC)
<a href="#">CIAC Weekly Summary</a>	Colorado Information Analysis Center (CIAC)
<a href="#">DVIC Biweekly Open Source Bulletin</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">The Watchline</a>	FDNY Center for Counter Terrorism & Domestic Preparedness (CTDP)
<a href="#">Fire, HazMat, and EMS Intelligence Bulletin</a>	Georgia Information Sharing and Analysis Center (GISAC)
<a href="#">Weekly Intelligence Bulletin</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">KCTEW Bulletin</a>	Kansas City (MO) Regional TEW (KCTEW)
<a href="#">KIFC Open Source Weekly</a>	Kentucky Intelligence Fusion Center (KIFC)
<a href="#">Monthly Threat Awareness Bulletin</a>	Indiana Intelligence Fusion Center (IIFC)
<a href="#">MCAC Critical Infrastructure Bi-Weekly Summary</a>	Maryland Coordination & Analysis Center (MCAC)
<a href="#">MN Fusion Center Weekly Partner Brief</a>	Minnesota Fusion Center
<a href="#">NCRIC Partner Update Brief</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">ND Anti-Terrorism Weekly Summary</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<a href="#">NHIAC All Hazards Digest</a>	New Hampshire Information & Analysis Center (NHIAC)
<a href="#">NIAC Weekly Infrastructure Awareness Brief</a>	Nebraska Information Analysis Center (NIAC)
<a href="#">NNRIC Bi-Weekly Briefing</a>	Northern Nevada Regional Intelligence Center (NNRIC)
	Northern Virginia Regional Intelligence

<a href="#">Weekly Intelligence Feed</a>	Center (NVRIC)
<a href="#">CBRN Weekly</a>	New York Police Department (NYPD)
<a href="#">OCIAC Partner Bi-Weekly Brief</a>	Orange County Intelligence Assessment Center (OCIAC)
<a href="#">OTFC Weekly Bulletin</a>	Oregon TITAN Fusion Center
<a href="#">CI - KR Monthly Report</a>	Pennsylvania Criminal Intelligence Center (PaCIC)
<a href="#">Pittsburgh Regional Intelligence Brief</a>	Region 13 Fusion Center (Pittsburgh, PA)
<a href="#">SD-LECC Extremism Open Source Bulletin</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">SC Fusion Center Information Bulletin</a>	South Carolina Fusion Center (SCFC)
<a href="#">Emergency Services Chronicle</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">STAC Bi-Weekly Review</a>	California State Threat Assessment Center (STAC)
<a href="#">WA State Fusion Center Insider</a>	Washington State Fusion Center (WSFC)
<a href="#">WSIC Weekly Bulletin</a>	Wisconsin Statewide Information Center (WSIC)
<a href="#">WRTAC DC FEMS Intelligence Size-Up</a>	Washington Regional Threat and Analysis Center (WRTAC)
<b>JCAT</b>	
<a href="#">Counterterrorism Weekly - 13 February 2019</a>	National Counterterrorism Center
<a href="#">Counterterrorism Weekly - 6 February 2019</a>	National Counterterrorism Center
<a href="#">JCAT Production Snapshot February 2019 FINAL</a>	JCAT
<a href="#">Foreign Terrorist Inspired Enabled and Directed Attacks in the US Since 9-11 as of January 2019</a>	National Counterterrorism Center
<b>FEDERAL DOCUMENTS</b>	
<a href="#">The Cyber Shield - February 15, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">This Week in Transportation Cyber Security February 15, 2019</a>	Transportation Security Administration (TSA)
<a href="#">The Cyber Shield - February 14, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 13, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 12, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 11, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">This Week in Transportation Cyber Security - February 8, 2019</a>	Transportation Security Administration
<a href="#">Partial Identification and Tradecraft Used by Members of a Group Involved in ATM Skimming Between 2016 and 2018</a>	FBI Albuquerque Division
<a href="#">Cyber Criminals Conducting Successful Spearphishing Campaigns Against Students at Multiple Universities</a>	FBI Cyber Division
<a href="#">RE-ISAC Cyber Security Report - 07 February 2019 - Preparing for CEEW</a>	RE-ISAC
<a href="#">The Cyber Shield - February 6, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 5, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">Telephony Denial of Service Disrupts Non-Emergency Police Lines</a>	



<a href="#">in Maryland and California</a>	FBI Baltimore Division
<a href="#">Secret Service Issues Tax Season Phishing Alert</a>	U.S. Secret Service
<a href="#">This Week in Transportation Cyber Security - February 1, 2019</a>	Transportation Security Administration
<a href="#">2019 Haiti Departure Status</a>	OSAC
<a href="#">Individual Responsible for Food Tampering at Retail Establishments in Multiple States Arrested</a>	FBI
<a href="#">International - China Expanding Interests by Buying Foreign Ports</a>	CBP
<a href="#">Almaty Earthquake Preparedness</a>	OSAC
<a href="#">FBI Arrests Texas-Based Individual for Conspiracy To Provide Material Support to Lashkar-e-Tayyiba</a>	DHS/FBI
<a href="#">FBI Arrests New York-Based Individual for Attempting To Provide Material Support to Lashkar-e-Tayyiba</a>	DHS/FBI
<a href="#">Weekly Physical Security Report - 05 February 2019 - Terrorism Interview</a>	RE-ISAC
<b>OTHER DOCUMENTS</b>	
<a href="#">Current Situation Reports</a>	<a href="#">Daily Reports</a>
<a href="#">BATS</a>	<a href="#">PT/ST-ISAC Cyber Report</a>
<a href="#">Counterterrorism Daily - NCTC</a>	<a href="#">Joint Counterterrorism Assessment Team (JCAT)</a>
<a href="#">IT-ISAC Open Source News</a>	<a href="#">IED News</a>
<a href="#">Emerging Diseases</a>	<a href="#">FEMA Disaster Emergency Communications Division Newsletter</a>
<a href="#">NH-ISAC Daily Security Intelligence Report</a>	<a href="#">Training &amp; Conference Calendar</a>

For HSIN password resets, [click here](#). For further assistance with your HSIN account, contact the HSIN 24/7 Help Desk at 866-430-0162. For other difficulties opening FOUO documents (e.g., not nominated and validated), contact the EMR-ISAC at [emr-isac@fema.dhs.gov](mailto:emr-isac@fema.dhs.gov) or at 301-447-1325.

You are subscribed to Bulletin - FOUO Template for EMR-ISAC. This information has recently been updated, and is now available.

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your [Subscriber Preferences Page](#). You will need to use your email address to log in. If you have questions or problems with the subscription service, please visit [subscriberhelp.govdelivery.com](https://subscriberhelp.govdelivery.com).

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.

This email was sent to [vmata@sunnyvale.ca.gov](mailto:vmata@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: U.S. Fire Administration · U.S. Department of Homeland Security · Emmitsburg, MD 21727 · (301) 447-1325



**From:** [emr-isac](#)  
**To:** [Jeffrey Hunter](#)  
**Subject:** HSIN Emergency Services Update February 1-15, 2019: denial of service hits non-emergency police lines; 5G wireless communications primer  
**Date:** Friday, February 22, 2019 12:20:30 PM

---



**WARNING:** This document contains FOR OFFICIAL USE ONLY (FOUO) information. It is subject to release restrictions as detailed in the Homeland Security Act of 2002 (6 U.S.C. 482) and the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy for FOUO information and is not to be released to the public, media, or other personnel who do not have an authorized "need-to-know" without appropriate prior approval of an authorized DHS official.

---

Below is a list of some of the many information products posted to the Emergency Services community on the Homeland Security Information Network (HSIN) between February 1-15, 2019. These include a bulletin on extremists adopting foreign terrorist organization's behaviors; denial of service attacks against non-emergency police lines; and a public safety primer for 5G wireless communications.

---

#### **HSIN Emergency Services Update February 1-15, 2019**

<b>CONTROLLED DANGEROUS SUBSTANCES/DRUGS (State &amp; Local)</b>	
<a href="#">Benzyl Fentanyl</a>	NCR - Threat Intelligence Consortium
<a href="#">Narcotics Report - February 4-10, 2019</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">2018 Overview - Drug Environment Report</a>	New Hampshire Information and Analysis Center (NHIAC)
<a href="#">Counterfeit Adderall Pills Containing Methamphetamine Seized During 3 Separate Investigations in SE Michigan</a>	Michigan Intelligence Operations Center (MIOC)
<a href="#">Narcotics Bulletin - January 28-February 3, 2019</a>	Greater Cincinnati Fusion Center (GCFC)
<b>CYBER SECURITY (State &amp; Local)</b>	
<a href="#">Cyber Security Snapshot - Social Engineering</a>	Michigan Cyber Command Center/Michigan State Police
<a href="#">Cutting Through the Cybersecurity Noise - February 8, 2019</a>	Phoenix UASI
<a href="#">Psycho Social Network - Tor-based Social Network Draws Hackers to Share Exploits and Tools</a>	Central Florida Intelligence Exchange (CFIX)
<a href="#">Vulnerabilities in Underlying Infrastructure of Click2Gov Software May Expose Organizations to Cyberattacks</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">Business Email Compromise Scams Potentially Result in Data Breaches and Financial Losses</a>	NCRIC/MS-ISAC
<a href="#">NDSLIC Bi-Weekly Cybersecurity Rollup - February 1, 2019</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<b>BORDER SECURITY (State &amp; Local)</b>	
<a href="#">Border Security Alert - February 3-9 2019</a>	Patrick Henry College Strategic Intelligence Program
<a href="#">Border Security Alert - January 27 - February 02, 2019</a>	Patrick Henry College Strategic Intelligence Program
<b>OTHER (State &amp; Local)</b>	
<a href="#">5G Wireless Communications - Public Safety Primer</a>	NVRIC/VFC
<a href="#">Tactics and Threats for Violence By Pipeline Opposition Actors</a>	VFC
<a href="#">Human Trafficking Awareness</a>	Oregon Titan Fusion Center (TITAN)
	Southern Nevada Counter Terrorism

<a href="#">Disease Outbreak and Investigation Report - February 12, 2019</a>	Center (SNCTC)
<a href="#">Ku Klux Klan Recruitment Activity in Philadelphia Regional Area</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">First Anniversary of Mass Shooting at Marjory Stoneman Douglas High School in Parkland, Florida</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Increase of Hepatitis A Virus (HAV) Infections in Clark County, NV</a>	Southern Nevada Health District
<b>SPECIAL EVENTS - LISTS AND THREAT ASSESSMENTS (State &amp; Local)</b>	
<a href="#">Key Information Regarding the February 14, 2019 National Rifle Association Events</a>	VFC/NVRIC
<a href="#">2019 Coors Light NHL Stadium Series - Flyers vs. Penguins</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Stoneman Douglas Shooting Anniversary</a>	Delaware Valley Intelligence Center (DVIC)
<b>TERRORISM (State &amp; Local)</b>	
<a href="#">ISIS Threats to Energy Sector</a>	Colorado Information Analysis Center (CIAC)
<a href="#">Extremist Adoption of Foreign Terrorist Organization Behaviors Increases Threat of Violence</a>	NCR - Threat Intelligence Consortium
<b>STATE &amp; LOCAL FUSION CENTER PERIODICALS</b>	
<a href="#">ARIC Quarterly SAR Report</a>	Austin Regional Intelligence Center (ARIC)
<a href="#">Critical Infrastructure Monthly Open Source Review</a>	Massachusetts Commonwealth Fusion Center (CFC)
<a href="#">CIAC Weekly Summary</a>	Colorado Information Analysis Center (CIAC)
<a href="#">DVIC Biweekly Open Source Bulletin</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">The Watchline</a>	FDNY Center for Counter Terrorism & Domestic Preparedness (CTDP)
<a href="#">Fire, HazMat, and EMS Intelligence Bulletin</a>	Georgia Information Sharing and Analysis Center (GISAC)
<a href="#">Weekly Intelligence Bulletin</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">KCTEW Bulletin</a>	Kansas City (MO) Regional TEW (KCTEW)
<a href="#">KIFC Open Source Weekly</a>	Kentucky Intelligence Fusion Center (KIFC)
<a href="#">Monthly Threat Awareness Bulletin</a>	Indiana Intelligence Fusion Center (IIFC)
<a href="#">MCAC Critical Infrastructure Bi-Weekly Summary</a>	Maryland Coordination & Analysis Center (MCAC)
<a href="#">MN Fusion Center Weekly Partner Brief</a>	Minnesota Fusion Center
<a href="#">NCRIC Partner Update Brief</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">ND Anti-Terrorism Weekly Summary</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<a href="#">NHIAC All Hazards Digest</a>	New Hampshire Information & Analysis Center (NHIAC)
<a href="#">NIAC Weekly Infrastructure Awareness Brief</a>	Nebraska Information Analysis Center (NIAC)
<a href="#">NNRIC Bi-Weekly Briefing</a>	Northern Nevada Regional Intelligence Center (NNRIC)
	Northern Virginia Regional Intelligence

<a href="#">Weekly Intelligence Feed</a>	Center (NVRIC)
<a href="#">CBRN Weekly</a>	New York Police Department (NYPD)
<a href="#">OCIAC Partner Bi-Weekly Brief</a>	Orange County Intelligence Assessment Center (OCIAC)
<a href="#">OTFC Weekly Bulletin</a>	Oregon TITAN Fusion Center
<a href="#">CI - KR Monthly Report</a>	Pennsylvania Criminal Intelligence Center (PaCIC)
<a href="#">Pittsburgh Regional Intelligence Brief</a>	Region 13 Fusion Center (Pittsburgh, PA)
<a href="#">SD-LECC Extremism Open Source Bulletin</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">SC Fusion Center Information Bulletin</a>	South Carolina Fusion Center (SCFC)
<a href="#">Emergency Services Chronicle</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">STAC Bi-Weekly Review</a>	California State Threat Assessment Center (STAC)
<a href="#">WA State Fusion Center Insider</a>	Washington State Fusion Center (WSFC)
<a href="#">WSIC Weekly Bulletin</a>	Wisconsin Statewide Information Center (WSIC)
<a href="#">WRTAC DC FEMS Intelligence Size-Up</a>	Washington Regional Threat and Analysis Center (WRTAC)
<b>JCAT</b>	
<a href="#">Counterterrorism Weekly - 13 February 2019</a>	National Counterterrorism Center
<a href="#">Counterterrorism Weekly - 6 February 2019</a>	National Counterterrorism Center
<a href="#">JCAT Production Snapshot February 2019 FINAL</a>	JCAT
<a href="#">Foreign Terrorist Inspired Enabled and Directed Attacks in the US Since 9-11 as of January 2019</a>	National Counterterrorism Center
<b>FEDERAL DOCUMENTS</b>	
<a href="#">The Cyber Shield - February 15, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">This Week in Transportation Cyber Security February 15, 2019</a>	Transportation Security Administration (TSA)
<a href="#">The Cyber Shield - February 14, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 13, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 12, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 11, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">This Week in Transportation Cyber Security - February 8, 2019</a>	Transportation Security Administration
<a href="#">Partial Identification and Tradecraft Used by Members of a Group Involved in ATM Skimming Between 2016 and 2018</a>	FBI Albuquerque Division
<a href="#">Cyber Criminals Conducting Successful Spearphishing Campaigns Against Students at Multiple Universities</a>	FBI Cyber Division
<a href="#">RE-ISAC Cyber Security Report - 07 February 2019 - Preparing for CEEW</a>	RE-ISAC
<a href="#">The Cyber Shield - February 6, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">The Cyber Shield - February 5, 2019</a>	New Mexico Counterintelligence Working Group (NMCIWG)
<a href="#">Telephony Denial of Service Disrupts Non-Emergency Police Lines</a>	

<a href="#">in Maryland and California</a>	FBI Baltimore Division
<a href="#">Secret Service Issues Tax Season Phishing Alert</a>	U.S. Secret Service
<a href="#">This Week in Transportation Cyber Security - February 1, 2019</a>	Transportation Security Administration
<a href="#">2019 Haiti Departure Status</a>	OSAC
<a href="#">Individual Responsible for Food Tampering at Retail Establishments in Multiple States Arrested</a>	FBI
<a href="#">International - China Expanding Interests by Buying Foreign Ports</a>	CBP
<a href="#">Almaty Earthquake Preparedness</a>	OSAC
<a href="#">FBI Arrests Texas-Based Individual for Conspiracy To Provide Material Support to Lashkar-e-Tayyiba</a>	DHS/FBI
<a href="#">FBI Arrests New York-Based Individual for Attempting To Provide Material Support to Lashkar-e-Tayyiba</a>	DHS/FBI
<a href="#">Weekly Physical Security Report - 05 February 2019 - Terrorism Interview</a>	RE-ISAC
<b>OTHER DOCUMENTS</b>	
<a href="#">Current Situation Reports</a>	<a href="#">Daily Reports</a>
<a href="#">BATS</a>	<a href="#">PT/ST-ISAC Cyber Report</a>
<a href="#">Counterterrorism Daily - NCTC</a>	<a href="#">Joint Counterterrorism Assessment Team (JCAT)</a>
<a href="#">IT-ISAC Open Source News</a>	<a href="#">IED News</a>
<a href="#">Emerging Diseases</a>	<a href="#">FEMA Disaster Emergency Communications Division Newsletter</a>
<a href="#">NH-ISAC Daily Security Intelligence Report</a>	<a href="#">Training &amp; Conference Calendar</a>

For HSIN password resets, [click here](#). For further assistance with your HSIN account, contact the HSIN 24/7 Help Desk at 866-430-0162. For other difficulties opening FOUO documents (e.g., not nominated and validated), contact the EMR-ISAC at [emr-isac@fema.dhs.gov](mailto:emr-isac@fema.dhs.gov) or at 301-447-1325.

You are subscribed to Bulletin - FOUO Template for EMR-ISAC. This information has recently been updated, and is now available.

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your [Subscriber Preferences Page](#). You will need to use your email address to log in. If you have questions or problems with the subscription service, please visit [subscriberhelp.govdelivery.com](https://subscriberhelp.govdelivery.com).

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.

This email was sent to [jhunter@sunnyvale.ca.gov](mailto:jhunter@sunnyvale.ca.gov) using GovDelivery Communications Cloud on behalf of: U.S. Fire Administration · U.S. Department of Homeland Security · Emmitsburg, MD 21727 · (301) 447-1325





**From:** [Spanish Publishers](#)  
**To:** [Karina Huerta](#)  
**Subject:** (6) Top new releases | Lanzamientos importantes  
**Date:** Thursday, January 31, 2019 12:03:11 PM

Having trouble viewing this email? [www.spanishpublishers.net](http://www.spanishpublishers.net)

URANO-OBELISCO-SIRIO-ROCA-ANAGRAMA-EDAF-ALMUZARA  
SALAMANDRA-SAN PABLO-SELECTOR-ALMADIA-DIAMANTE



[www.spanishpublishers.net](http://www.spanishpublishers.net)

5000+ Spanish titles | 100+ new releases per month | trending U.S. bestsellers

## CONFESIONES | Admissions

**By: Henry Marsh**

9788498388725 | PB | 304 Pages | \$23.95 | Ediciones Salamandra |  
Biography & Memoirs



**Amazon Best Sellers Rank: #49 in Books > Medical Books > Medicine > Surgery > Thoracic & Vascular**

Marsh has retired, which means he's taking a thorough inventory of his life. His reflections and recollections make *Admissions* an even more introspective memoir than his first, if such a thing is possible.

*New York Times*

It feels like a privilege to spend time with Marsh, an exemplary person with lambent emotions whose fearsome skills and hidden fears are a reminder of how exultant, sad, ardent, and swift life really is.

*The New Yorker*

His descriptions of his work demonstrate again his gift with both scalpel and pen. In vivid prose, he captures the terrifying risks he faces with each cut, each decision.

### *The Washington Post*

Sus frases se nos antojan obra de la más delicada ejecución, realizadas con el mismo amor que Marsh destina a la carpintería y la cirugía.

*The Daily Telegraph*

Sensacional. Nos encontramos con un Marsh cascarrabias, atrevido, inalterable, e invariablemente guiado por la curiosidad.

*The Sunday Times*

Un libro muy entretenido. Abunda en él la honestidad, una cualidad tan rara y admirable entre los cirujanos de elite como, supongo, entre los escritores de libros de memorias.

*The Guardian*

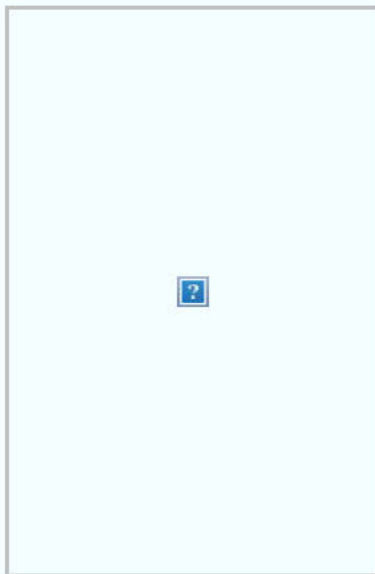
**SINOPSIS:** [Click on book cover](#) (pulse en la cubierta)

(Our shopping cart is now active | El carrito de compras ya está activo)

## **UN DUETO OSCURO | Our Dark Duet**

**By: Victoria Schwab**

9788496886964 | PB | 480 Pages | \$16.95 | Ediciones Urano |  
Young Adult



**A New York Times Bestseller.**

**The bestselling sequel-and conclusion-to Victoria Schwab's instant #1 *New York Times* bestseller *This Savage Song*.**

**Amazon Best Sellers Rank:**

**#53 in Books > Teens > Science Fiction & Fantasy**

**#82 in Books > Teens > Mysteries & Thrillers > Law & Crime**

**Masterly writing, a fast-moving plot, and just the right amount of bittersweet romance make this book hard to put down. A necessary first purchase for all teen collections. *School Library Journal***

**Explosive... Be prepared for a breakneck pace, new monsters, darkness, and all the feels.**

**If *This Savage Song* was a tense exploration of human nature, this sequel is a reckoning... Schwab folds questions of identity, morality, and judgment into her stunningly crafted narrative. ...readers will be hard-pressed to put this action-driven finale down.**

***Booklist***

La secuela del best seller #1 de *The New York Times* *Una canción salvaje*.

Una historia vertiginosa que se resuelve con un final conmovedor. Afortunadamente, los muchos fanáticos que esperan con pasión este volumen, se deleitarán con todas estas emociones.

*Kirkus Reviews*

La escritura es magistral, una trama de movimiento rápido y la cantidad justa de romance agrisulce hacen que este libro sea difícil de dejar. Una primera compra necesaria para todas las colecciones de adolescentes.

*School Library Journal*

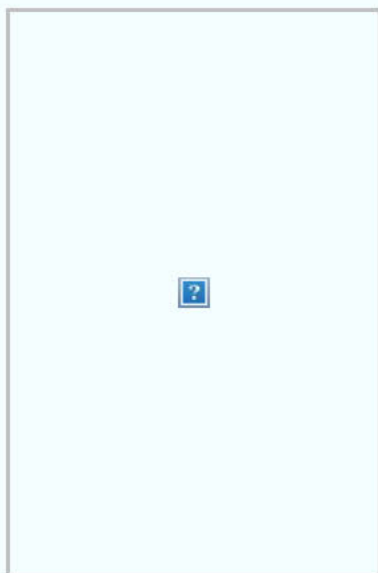
**SINOPSIS:** [Click on book cover](#) (pulse en la cubierta)

(Our shopping cart is now active | El carrito de compras ya está activo)

## **EL INTERCAMBIO | The Exchange**

**By: Fernando Aleu**

9788417541194 | HC | 418 Pages | \$21.95 | Roca Editorial | Historic Fiction



**Love, duty, friendship, espionage, diplomacy, war and denial: revives a historical moment of great intensity. A truly captivating novel.**

**The story recreates with vibrant pulse, an event that Aleu was an occasional witness, which in addition, involves a bunch of characters.**

***La Vanguardia***

Amor, deber, amistad, espionaje, diplomacia, guerra, renuncia: revive un momento histórico de gran intensidad. Una novela realmente cautivadora.

*El intercambio* es, más que una novela histórica, una novela nostálgica, romántica incluso, que describe un mundo que se fue y no volverá. Una Barcelona de comienzos de los años cuarenta del pasado siglo a la que uno de sus hijos cosmopolitas rinde homenaje y dice adiós.

*ABC Cultural*

Recrea con vibrante pulso un suceso del que Aleu fue testigo ocasional, y que implica a una gavilla de personajes.

*La Vanguardia*

**SINOPSIS:** [Click on book cover](#) (pulse en la cubierta)



(Our shopping cart is now active | El carrito de compras ya está activo)

## **AYUDA A TU HIJO A CONCENTRARSE CON EL METODO MONTESSORI | Help Your Child to**

### **Concentrate with the Montessori Method**

**By: Sylvie & Noémie D'Esclaibes**

9788441438859 | PB | 192 Pages | \$18.95 | Editorial Edaf | Parenting & Family



**The first way the child needs to find is the path of concentration and the key is to recognize the valuable moments of concentration to apply them in learning.**

**This book includes more than 40 activities, colorful photos, facts to understand challenges, explanations for the adult in the preparation of the environment and the enthusiasm of connection between you and your child.**

El primer camino que tiene que encontrar el niño es el camino de la concentración y la clave es reconocer los valiosos instantes de la concentración para aplicarlos en el aprendizaje.

Este libro incluye más de 40 actividades, fotos a todo color, datos para entender los retos y explicaciones para el adulto en la preparación del entorno y de un ambiente de conexión entre tú y tu hijo.

**SINOPSIS:** **Click on book cover** (pulse en la cubierta)

(Our shopping cart is now active | El carrito de compras ya está activo)

## **LOS ESENIOS | The Essenes: Children of the Light**

**By: Stuart Wilson & Joanna Prentis**

9788491113911 | PB | 336 Pages | \$20.95 | Ediciones Obelisco | Metaphysical - Esoteric

**Take a trip through time to uncover the mysterious knowledge of the Essenes and the secret teachings of Jesus Christ. Discover the mysterious discernment and secrets of the Essenes in this exhaustive and profound book.**

Thanks to the regression technique to past lives, this story can be told for the first



**time, opening a window to a fascinating, unique and crucial time.**

Un viaje a través de la regresión que revela el misterioso conocimiento de los esenios y las enseñanzas secretas de Jesucristo. Descubre el misterioso discernimiento y los secretos de los Esenios en este exhaustivo y profundo libro.

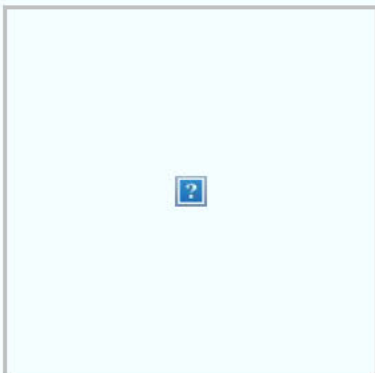
Gracias a la técnica de la regresión a vidas pasadas, esta historia puede ser contada por primera vez, abriendo una ventana a una época fascinante, única y crucial.

**SINOPSIS:** [Click on book cover](#) (pulse en la cubierta)  
(Our shopping cart is now active | El carrito de compras ya está activo)

## **IZQUIERDA DERECHA | Left Right**

**By: Siirsel Tas & Gokce Akgül**

9788491452058 | PB | 38 Pages | \$14.95 | Editorial Picarona | Children



***Left Right, ¡Distinguish them!* is going to help all those children who find it difficult to distinguish the left/right concepts. And all in an entertaining and playful way.**

**Includes colorful cut out bracelets to carry on the right hand and on the left and thus facilitate the right and left way. A useful and fun book for children.**

*Izquierda derecha ¡Distínguelas!* va a ayudar a todos esos niños/as a los que les cuesta distinguir los conceptos izquierda/derecha. Y todo de manera entretenida y lúdica.

Incluye pulseras recortables de colores para llevar en la mano derecha y en la izquierda y así facilitar el camino derecho y el izquierdo. Un libro muy divertido.

**SINOPSIS:** [Click on book cover](#) (pulse en la cubierta)  
(Our shopping cart is now active | El carrito de compras ya está activo)



**For more information or to request a printed catalog,  
please contact us:**

**[www.spanishpublishers.net](http://www.spanishpublishers.net)**

**[sales@spanishpublishers.net](mailto:sales@spanishpublishers.net)**

**1-866-448-7266 x 17 (toll free) | 305-251-1310 (fax)**

**8871 SW 129 Terrace | Miami, FL 33176 | USA**



Spanish Publishers, 8871 SW 129 Terrace, Miami, FL 33176

[SafeUnsubscribe™](#) [khuerta@sunnyvale.ca.gov](mailto:khuerta@sunnyvale.ca.gov)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [sales@spanishpublishers.net](mailto:sales@spanishpublishers.net) in collaboration with

[Constant Contact](#)



Try it free today

**From:** [Center on National Security at Fordham Law School](#)  
**To:** [egolembiewski@sunnyvale.ca.gov](mailto:egolembiewski@sunnyvale.ca.gov)  
**Subject:** Cyber Brief: Pressures Mount on Huawei's European Business  
**Date:** Monday, January 28, 2019 6:53:09 AM



## FEATURED STORY

MONDAY, JANUARY 28, 2019

### PRESSURES MOUNT ON HUAWEI'S EUROPEAN BUSINESS

The Chinese telecom giant faced more setbacks in Europe last week with Vodafone, the world's largest mobile carrier outside China, announcing plans to pause purchases of Huawei gear used in the core of new 5G networks. The UK-based carrier said it was concerned that some European governments may restrict Huawei sales because of national-security fears.

In another blow, the Polish government said it will cut Huawei from its 5G network in favour of European companies—potentially Finland's Nokia and Sweden's Ericsson—following the recent arrest of a Huawei employee on espionage charges.

In related news, Canadian Prime Minister Justin Trudeau fired his government's ambassador to China, John McCallum, on Saturday. Earlier in the week, McCallum had publicly argued that the U.S. extradition request for Huawei's chief financial officer, Meng Wanzhou, was seriously flawed. Meng is wanted in the U.S. on charges of fraud and violating sanctions against Iran. ([WSJ](#), [Reuters](#), [Guardian](#))

## HACKERS

**Russia Docs:** An online group known as DDoSecrets released a trove of hacked documents that are reportedly from inside Russia, including messages and files from politicians, journalists, oligarchs, religious figures, and Russian operatives in Ukraine. Analysts say the leak is intended as a counterstrike against Russia's dissemination of hacked emails intended to interfere in the 2016 U.S. presidential election. ([NYT](#))

**Nest Camera:** A northern California family received quite a scare when an unidentified hacker gained access to their Nest security camera and blasted a fake warning of an imminent North Korean nuclear missile attack. Nest, which is owned by Google, said the company was not breached but that the family was likely using a compromised password. ([Mercury News](#))

## COURTS

**Biometric Data:** In a case with broad implications for many companies, the Illinois Supreme Court upheld a consumer's right to sue businesses—in this case, Six Flags—that collect biometric data, like fingerprints, without informing them how it will be used. The state has one of the strictest biometric privacy laws in the nation and has become a hotbed of lawsuits over alleged misuses of this data. ([CT](#))

**Initial Coin Offerings:** Social-media startup Kik Interactive plans to fight an enforcement by the SEC, which said the Canadian company issued an unregistered security when it sold \$100 million in digital tokens. Analysts say the case could help define the scope of the SEC's authority to regulate the ICO market. ([WSJ](#))

## ON THE HILL

**Mueller Probe:** The special counsel's office indicted longtime Trump associate Roger

## MUST READS

[U.S. and China Battle in 5G Race:](#) “In interviews with current and former senior American government officials, intelligence officers and top telecommunications executives, it is clear that the potential of 5G has created a zero-sum calculus in the Trump White House — a conviction that there must be a single winner in this arms race, and the loser must be banished,” write authors for the *New York Times*.

[The Dark Age of Surveillance Capitalism:](#) “While both the Russian government and the plutocrat Robert Mercer, part owner of the now defunct Cambridge Analytica and donor to Donald Trump's presidential campaign, learnt how to massage the complex secretive machine that Facebook built, these operations and the digital

Stone on multiple counts, including obstruction, making false statements, and witness tampering. Most notably, Mueller's team alleges that a senior Trump campaign official directed Stone to get information from WikiLeaks about hacked Democratic emails. ([NYT](#))

#### PRIVATE SECTOR

**Facebook:** CEO Mark Zuckerberg plans to merge the social network's messaging services— WhatsApp, Instagram, and Facebook Messenger—onto a single technical infrastructure, although they will continue to function as standalone apps. The move raises antitrust, privacy, and security concerns. He also reportedly wants all the apps to have end-to-end encryption. ([NYT](#))

**WhatsApp:** The Facebook-owned company is limiting the number of times a user can forward a message, to five, in an attempt to stem the viral spread of false information. Over the past two years, at least two dozen people in India have been killed by mobs incited by online rumors. ([WaPo](#))

**Google:** The search giant has an in-house counterespionage group, known as the Threat Analysis Group, of about two dozen people that tracks more than 200 hacker groups. The team was first to link North Korea to the devastating WannaCry computer-worm outbreak in 2017. ([WSJ](#))

**YouTube:** Responding to criticism that it has helped fuel conspiracy theories, the online platform said it will attempt to recommend fewer videos that “could misinform users in harmful ways.” For example, the company said it would target “videos promoting a phony miracle cure for a serious illness, claiming the Earth is flat, or making blatantly false claims about historic events like 9/11.” ([Guardian](#))

**Amazon:** A study by researchers at MIT found that the company's facial recognition software, which it has marketed to U.S. law enforcement agencies, struggles to make basic assessments about target individuals, like their gender, particularly when the individual is darker-skinned. ([WaPo](#))

apparatus through which they function do not begin or end with Facebook. Instead, they are key elements in a new economic logic that I call “surveillance capitalism”. Such practices were invented at Google, travelled to Facebook, engulfed Silicon Valley and have since spread through every economic sector,” writes Shoshana Zuboff in the **Financial Times**.

#### [Your TV Is Now a Computer, But Not in a Good Way:](#)

“Analysts estimate that smart TVs now make up about 70 percent of all new TV sales. The television is no longer a mere display, but a full-fledged computer, for good and for ill. And what is a computer now? On the one hand, it's something companies sell to consumers for money. But after you've purchased an internet-connected device of any kind, it begins to generate information that the company can use itself or sell to third parties. Earlier this month, Vizio's chief technology officer, Bill Baxter, told The Verge that the reason his company can sell TVs so cheaply now is that it makes up the money by selling bits of data and access to your TV after you purchase it. Baxter called this “post-purchase monetization,” writes Alexis Madrigal in the **Atlantic**.



Center on National Security  
Fordham University School of Law  
150 W. 62nd St. 7th Floor  
New York, NY 10023 US

Copyright © 2016 Center on National Security, All rights reserved.

[unsubscribe from this list](#) | [update subscription preferences](#) | [view email in browser](#)



From: US-CERT  
To: Tanner McGinnis  
Subject: SB19-021: Vulnerability Summary for the Week of January 14, 2019  
Date: Tuesday, January 22, 2019 9:19:14 AM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## SB19-021: Vulnerability Summary for the Week of January 14, 2019

01/21/2019 09:22 PM EST

Original release date: January 21, 2019 | Last revised: January 22, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- apple_tv	In iOS before 11.2.5, macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, watchOS before 4.2.2, and tvOS before 11.2.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	10.0	<a href="#">CVE-2018-4189</a> CONFIRM MISC MISC MISC
apple -- apple_tv	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a permissions issue existed in Remote Management. This issue was addressed through improved permission validation.	2019-01-11	10.0	<a href="#">CVE-2018-4298</a> CONFIRM MISC
apple -- iphone_os	In iOS before 9.3.3, a memory corruption issue existed in the kernel. This issue was addressed through improved memory handling.	2019-01-11	9.3	<a href="#">CVE-2016-7576</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a logic error existed in the validation of credentials. This was addressed with improved credential validation.	2019-01-11	7.5	<a href="#">CVE-2017-13889</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, an out-of-bounds read was addressed with improved input validation.	2019-01-11	10.0	<a href="#">CVE-2018-4169</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions on CUPS.	2019-01-11	7.2	<a href="#">CVE-2018-4182</a> MISC CONFIRM DEBIAN
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions.	2019-01-11	7.2	<a href="#">CVE-2018-4183</a> MISC CONFIRM DEBIAN
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an input validation issue existed in the kernel. This issue was addressed with improved input validation.	2019-01-11	10.0	<a href="#">CVE-2018-4254</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved size validation.	2019-01-11	10.0	<a href="#">CVE-2018-4257</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved bounds checking.	2019-01-11	10.0	<a href="#">CVE-2018-4258</a> CONFIRM
icmsdev -- icms	An issue was discovered in idreamsoft iCMS V7 0.13. There is SQL Injection via the app/article/article admincp.php_data_id parameter.	2019-01-14	7.5	<a href="#">CVE-2019-6259</a> MISC
mailenable -- mailenable	MailEnable before 8.60 allows Directory Traversal for reading the messages of other users, uploading files, and deleting files because "/" and "/" are mishandled.	2019-01-16	7.5	<a href="#">CVE-2015-9277</a> MISC MISC MISC
	Vulnerability in the Oracle Retail Xstore Payment component of Oracle Retail Applications (subcomponent: Security). The supported version that is affected is 3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Xstore Payment. Successful			



oracle -- retail_xstore_payment	attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Xstore Payment accessible data as well as unauthorized update, insert or delete access to some of Oracle Retail Xstore Payment accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Xstore Payment. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I L/A L).	2019-01-16	7.5	<a href="#">CVE-2018-3311</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I N/A H).	2019-01-16	7.8	<a href="#">CVE-2019-2437</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I N/A H).	2019-01-16	7.8	<a href="#">CVE-2019-2511</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
skymoonlabs -- cleanto	Cleanto 5.0 has SQL Injection via the assets/lib/service_method_ajax.php service_id parameter.	2019-01-15	7.5	<a href="#">CVE-2019-6295</a> <a href="#">MISC</a>
skymoonlabs -- cleanto	Cleanto 5.0 has SQL Injection via the assets/lib/export_ajax.php id parameter.	2019-01-15	7.5	<a href="#">CVE-2019-6296</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- apple_tv	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, proxy authentication incorrectly reported HTTP proxies received credentials securely. This issue was addressed through improved warnings.	2019-01-11	4.3	<a href="#">CVE-2016-4642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
apple -- apple_tv	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a validation issue existed in the parsing of 407 responses. This issue was addressed through improved response validation.	2019-01-11	4.0	<a href="#">CVE-2016-4643</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
apple -- apple_tv	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a downgrade issue existed with HTTP authentication credentials saved in Keychain. This issue was addressed by storing the authentication types with the credentials.	2019-01-11	4.0	<a href="#">CVE-2016-4644</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
apple -- apple_tv	In iOS before 11.3, Safari before 11.1, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, an array indexing issue existed in the handling of a function in javascript core. This issue was addressed with improved checks.	2019-01-11	6.8	<a href="#">CVE-2018-4210</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">UBUNTU</a>
apple -- apple_tv	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	6.8	<a href="#">CVE-2018-4212</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
apple -- apple_tv	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	6.8	<a href="#">CVE-2018-4213</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
apple -- apple_tv	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, multiple memory corruption issues were addressed with improved memory handling.	2019-01-11	6.8	<a href="#">CVE-2018-4262</a> <a href="#">SECTRAK</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
	In iOS before 11.4.1, watchOS before 4.3.2, tvOS before 11.4.1, Safari			<a href="#">CVE-2018-4277</a> <a href="#">SECTRAK</a>

apple -- apple_tv	before 11.1.1, macOS High Sierra before 10.13.6, a spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation.	2019-01-11	5.0	MISC MISC MISC CONF RM MISC
apple -- apple_tv	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, sound fetched through audio elements may be exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.	2019-01-11	4.3	CVE-2018-4278 SECTRAK MISC GENTOO CONF RM MISC MISC MISC UBUNTU
apple -- icloud	In iCloud for Windows before 7.3, Safari before 11.0.3, iTunes before 12.7.3 for Windows, and iOS before 11.2.5, multiple memory corruption issues exist and were addressed with improved memory handling.	2019-01-11	6.8	CVE-2018-4147 CONF RM MISC MISC MISC
apple -- iphone_os	In iOS before 11.2, a type confusion issue was addressed with improved memory handling.	2019-01-11	5.0	CVE-2017-13888 CONF RM
apple -- iphone_os	In iOS before 11.2, an inconsistent user interface issue was addressed through improved state management.	2019-01-11	4.3	CVE-2017-13891 CONF RM
apple -- iphone_os	In iOS before 11.2, exchange rates were retrieved from HTTP rather than HTTPS. This was addressed by enabling HTTPS for exchange rates.	2019-01-11	4.3	CVE-2017-2411 CONF RM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	4.9	CVE-2018-4181 MLIST CONF RM UBUNTU DEBIAN
apple -- mac_os_x	In macOS High Sierra before 10.13.5, a privacy issue in the handling of Open Directory records was addressed with improved indexing.	2019-01-11	5.0	CVE-2018-4217 CONF RM
cairographics -- cairo	An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_arc_in_direction in the file cairo-arc.c.	2019-01-16	4.3	CVE-2019-6461 MISC MISC
cairographics -- cairo	An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_normalized in the file cairo-arc.c, related to _arc_max_angle_for_tolerance_normalized.	2019-01-16	4.3	CVE-2019-6462 MISC MISC
castlamp -- zenbership	Zenbership v107 has CSRF via admin/cp-functions/event-add.php.	2019-01-15	6.8	CVE-2016-10738 EXPLOIT-DB
cisco -- identity_services_engine_software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of an affected system. The vulnerability is due to insufficient sanitization of user-supplied data that is written to log files and displayed in certain web pages of the web-based management interface of an affected device. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link or view an affected log file. The injected script code may be executed in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	2019-01-15	4.3	CVE-2018-15440 MISC CISCO
cisco -- identity_services_engine_software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient input validation of some parameters passed to the web-based management interface of an affected device. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	2019-01-15	4.3	CVE-2018-15463 MISC CISCO
citysearch / _hotfrog / _gelbeseiten_clone_script_project -- citysearch / _hotfrog / _gelbeseiten_clone_script	PHP Scripts Mall Citysearch / Hotfrog / Gelbeseiten Clone Script 2.0.1 has Reflected XSS via the srch parameter, as demonstrated by restaurants-details.php.	2019-01-12	4.3	CVE-2019-6248 MISC
easycms -- easycms	An issue was discovered in EasyCMS 1.5. There is CSRF via the index.php?s=/admin/article/insert/navTabId/listarticle/callbackType/closeCurrentURI.	2019-01-15	6.8	CVE-2019-6294 MISC
frog_cms_project -- frog_cms	Frog CMS 0.9.5 allows XSS via the forgot password page (aka the /admin/?/login/forgot URI).	2019-01-11	4.3	CVE-2019-6243 MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a double-free problem in the function rec_mset_elem_destroy() in the file rec-mset.c.	2019-01-16	4.3	CVE-2019-6455 MISC

gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a NULL pointer dereference in the function rec_fex_size() in the file rec-fex.c of librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6456</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a memory leak in rec_aggregate_reg_new in rec-aggregate.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6457</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a memory leak in rec_buf_new in rec-buf.c when called from rec_parse_rset in rec-parser.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6458</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a memory leak in rec_extract_type in rec-utils.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6459</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a NULL pointer dereference in the function rec_field_set_name() in the file rec-field.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6460</a> MISC
hucart -- hucart	An issue was discovered in HuCart v5.7.4. There is a CSRF vulnerability that can add an admin account via /adminsys/index.php?load=admins&act=edit_info&act_type=add.	2019-01-13	6.8	<a href="#">CVE-2019-6249</a> MISC EXPLOIT-DB
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 153628.	2019-01-14	5.0	<a href="#">CVE-2018-1956</a> X-Force CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153748.	2019-01-14	4.3	<a href="#">CVE-2018-1967</a> X-Force CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 153750.	2019-01-14	6.5	<a href="#">CVE-2018-1969</a> X-Force CONFIRM
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate escaping in com_contact leads to a stored XSS vulnerability.	2019-01-16	4.3	<a href="#">CVE-2019-6261</a> X-Force CONFIRM
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate escaping in mod_banners leads to a stored XSS vulnerability.	2019-01-16	4.3	<a href="#">CVE-2019-6264</a> X-Force CONFIRM
libpng -- libpng	png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp.	2019-01-11	6.8	<a href="#">CVE-2019-6129</a> MISC
libtiff -- libtiff	The TIFFFdOpen function in tif_unix.c in LibTIFF 4.0.10 has a memory leak, as demonstrated by pal2rgb.	2019-01-11	6.8	<a href="#">CVE-2019-6128</a> MISC
mailenable -- mailenable	MailEnable before 8.60 allows Stored XSS via malformed use of "<img/src" with no ">" character in the body of an e-mail message.	2019-01-16	4.3	<a href="#">CVE-2015-9279</a> MISC MISC MISC
mailenable -- mailenable	MailEnable before 8.60 allows XXE via an XML document in the request aspx Options parameter.	2019-01-16	5.0	<a href="#">CVE-2015-9280</a> MISC MISC MISC
microsoft -- team_foundation_server	An information disclosure vulnerability exists when Team Foundation Server does not properly handle variables marked as secret, aka "Team Foundation Server Information Disclosure Vulnerability." This affects Team.	2019-01-17	4.0	<a href="#">CVE-2019-0647</a> X-Force CONFIRM
oracle -- application_testing_suite	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). Supported versions that are affected are 12.5.0.3, 13.1.0.1, 13.2.0.1 and 13.3.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2019-01-16	6.4	<a href="#">CVE-2018-3304</a> X-Force CONFIRM CONFIRM
oracle -- application_testing_suite	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). Supported versions that are affected are 12.5.0.3, 13.1.0.1, 13.2.0.1 and 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	2019-01-16	6.5	<a href="#">CVE-2018-3305</a> X-Force CONFIRM CONFIRM

	(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).			
oracle -- argus_safety	Vulnerability in the Oracle Argus Safety component of Oracle Health Sciences Applications (subcomponent: Console). Supported versions that are affected are 8.1 and 8.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Argus Safety. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Argus Safety accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2430</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- argus_safety	Vulnerability in the Oracle Argus Safety component of Oracle Health Sciences Applications (subcomponent: Console). Supported versions that are affected are 8.1 and 8.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Argus Safety. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Argus Safety accessible data. CVSS 3.0 Base Score 6.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2431</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- argus_safety	Vulnerability in the Oracle Argus Safety component of Oracle Health Sciences Applications (subcomponent: Login). Supported versions that are affected are 8.1 and 8.2. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Argus Safety. While the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Argus Safety accessible data as well as unauthorized read access to a subset of Oracle Argus Safety accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N).	2019-01-16	4.9	<a href="#">CVE-2019-2432</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- content_manager	Vulnerability in the Oracle Content Manager component of Oracle E-Business Suite (subcomponent: Cover Letter). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Content Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Content Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Content Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Content Manager accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2445</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- database	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2406</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- database	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2444</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2396</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Session Management). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base	2019-01-16	5.0	<a href="#">CVE-2019-2488</a> <a href="#">CONF RM</a> <a href="#">BID</a>

	Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
oracle -- e-business_suite	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2491</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2492</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2496</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2497</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: SQL Extensions). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2546</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- enterprise_manager_base_platform	Vulnerability in the Enterprise Manager Base Platform component of Oracle Enterprise Manager Products Suite (subcomponent: EM Console). Supported versions that are affected are 13.2 and 13.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2018-3303</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_cruise_shipboard_property_management_system	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: SPMS Suite). The supported version that is affected is 8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise Shipboard Property Management System, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Cruise Shipboard Property Management System as well as unauthorized update, insert or delete	2019-01-16	4.9	<a href="#">CVE-2019-2411</a> <a href="#">CONF RM</a> <a href="#">BID</a>



	access to some of Oracle Hospitality Cruise Shipboard Property Management System accessible data. CVSS 3.0 Base Score 7.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:H).			
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Admin privilege with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-01-16	5.5	<a href="#">CVE-2019-2401</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2019-2425</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_symphony	Vulnerability in the Oracle Hospitality Symphony component of Oracle Food and Beverage Applications. The supported version that is affected is 2.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Symphony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Symphony accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Symphony accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Symphony. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L).	2019-01-16	6.8	<a href="#">CVE-2019-2402</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_symphony	Vulnerability in the Oracle Hospitality Symphony component of Oracle Food and Beverage Applications. The supported version that is affected is 2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Symphony. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Symphony accessible data as well as unauthorized read access to a subset of Oracle Hospitality Symphony accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2019-2403</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- http_server	Vulnerability in the Oracle HTTP Server component of Oracle Fusion Middleware (subcomponent: Web Listener). The supported version that is affected is 12.2.1.3. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle HTTP Server executes to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in takeover of Oracle HTTP Server. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2414</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hyperion_bi+	Vulnerability in the Hyperion BI+ component of Oracle Hyperion (subcomponent: Foundation UI & Servlets). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion BI+ accessible data as well as unauthorized read access to a subset of Hyperion BI+ accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion BI+. CVSS 3.0 Base Score 4.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L).	2019-01-16	6.0	<a href="#">CVE-2019-2415</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u201, 8u192 and 11 0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2422</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are			

oracle -- jdk	Java SE: 7u201, 8u192 and 11 0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2426</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2420</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2434</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2019-01-16	5.5	<a href="#">CVE-2019-2436</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2455</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2481</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2482</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2486</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2494</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high			<a href="#">CVE-2019-</a>

oracle -- mysql	privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">2495</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2502</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2507</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2510</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2528</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2529</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2530</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2531</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2532</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2533</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior.			

oracle -- mysql	Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2019-01-16	5.5	<a href="#">CVE-2019-2534</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2537</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2539</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H).	2019-01-16	5.8	<a href="#">CVE-2019-2429</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-01-16	6.4	<a href="#">CVE-2019-2456</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2457</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2458</a> <a href="#">CONF RM</a> <a href="#">BID</a>
	Vulnerability in the Oracle Outside In Technology component of Oracle			

oracle -- outside_in_technology	Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2459 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2460 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2461 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. While the vulnerability is in Oracle Outside In Technology, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L).	2019-01-16	6.4	<a href="#">CVE-2019-2462 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2019-01-16	6.4	<a href="#">CVE-2019-2463 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Confidentiality	2019-01-16	5.0	<a href="#">CVE-2019-2464 CONF RM BID</a>



	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2465</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2466</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2467</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2468</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC H/PR:N/UI:N/S:U/C:L/I:N/A:H).	2019-01-16	5.8	<a href="#">CVE-2019-2469</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the	2019-01-16	5.0	<a href="#">CVE-2019-2472</a> <a href="#">CONF RM</a> <a href="#">BID</a>

	CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:L).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2473</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2474</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2475</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2476</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2477</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability	2019-01-16	5.0	<a href="#">CVE-2019-2478</a> <a href="#">CONF RM</a> <a href="#">BID</a>

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2479 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2480 CONF RM BID</a>
oracle -- peoplesoft_enterprise	Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM eProcurement, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2519 CONF RM BID</a>
oracle -- peoplesoft_enterprise_cost_center_common_application_objects	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects component of Oracle PeopleSoft Products (subcomponent: Form and Approval Builder). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CC Common Application Objects. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise CC Common Application Objects, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CC Common Application Objects accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CC Common Application Objects accessible data. Note: This Enterprise Common Component is used by all PeopleSoft Application products. Please refer to the <a target=" _blank" href="https://support.oracle.com/rs?type=doc&id=2487756.1">MOS Note Doc ID 2493366.1 for patch information. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	4.9	<a href="#">CVE-2019-2419 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2404 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Security). Supported versions that are affected are 8.55, 8.56 and 8.57. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.0	<a href="#">CVE-2019-2405 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Feeds). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the	2019-01-	4.3	<a href="#">CVE-2019-2408</a>

	attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	16		<a href="#">CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2416 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Performance Monitor). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2019-2417 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Search). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2423 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: XML Publisher). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2433 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2439 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Core). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2442 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: XML Publisher). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2443 CONF RM BID</a>
	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful			

oracle -- peoplesoft_enterprise_peopletools	attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2471</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Panel Processor). Supported versions that are affected are 8.55, 8 56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2490</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Search Functionality). Supported versions that are affected are 8.55, 8 56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2499</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- primavera_p6_enterprise_project_portfolio_management	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.1, 15 2, 16.1, 16.2, 17.7-17.12 and 18.8. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2512</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- reports_developer	Vulnerability in the Oracle Reports Developer component of Oracle Fusion Middleware (subcomponent: Valid Session). The supported version that is affected is 12.2.1 3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data as well as unauthorized read access to a subset of Oracle Reports Developer accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2413</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">EXPLOIT-DB</a>
oracle -- retail_merchandising_system	Vulnerability in the Oracle Retail Merchandising System component of Oracle Retail Applications (subcomponent: Security (SQL Logger)). The supported version that is affected is 14.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Merchandising System. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Merchandising System accessible data as well as unauthorized read access to a subset of Oracle Retail Merchandising System accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2018-3125</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- sun_zfs_storage_appliance_kit	Vulnerability in the Sun ZFS Storage Appliance Kit (AK) component of Oracle Sun Systems Products Suite (subcomponent: Object Store). The supported version that is affected is prior to 8.8 2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Sun ZFS Storage Appliance Kit (AK) executes to compromise Sun ZFS Storage Appliance Kit (AK). Successful attacks of this vulnerability can result in takeover of Sun ZFS Storage Appliance Kit (AK). CVSS 3.0 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/H:A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2412</a> <a href="#">CONF RM</a> <a href="#">BID</a>
	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: UI Infrastructure). Supported versions that are affected are 6.3.7, 6.4.1, 6.4 2 and 6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle	2019-01-		<a href="#">CVE-2019-2487</a>



oracle -- transportation_management	Transportation Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Transportation Management accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	16	4.0	<a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is prior to 5.2.22. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2018-3309</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2500</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	2019-01-16	4.9	<a href="#">CVE-2019-2508</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	2019-01-16	4.9	<a href="#">CVE-2019-2509</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2520</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2521</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2522</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2523</a> <a href="#">CONF RM</a>

	Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).			BID
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2524</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2526</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2548</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2552</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- web_cache	Vulnerability in the Oracle Web Cache component of Oracle Fusion Middleware (subcomponent: ESI/Partial Page Caching). The supported version that is affected is 11.1.1.9.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Cache. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Cache, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Web Cache accessible data as well as unauthorized update, insert or delete access to some of Oracle Web Cache accessible data. CVSS 3.0 Base Score 6.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2438</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- webcenter_portal	Vulnerability in the Oracle WebCenter Portal component of Oracle Fusion Middleware (subcomponent: WebCenter Spaces Application). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Portal accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2427</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). The supported version that is affected is 10.3.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L).	2019-01-16	5.5	<a href="#">CVE-2019-2395</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Deployment). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2398</a> <a href="#">CONF RM</a> <a href="#">BID</a>
	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components).			

oracle -- weblogic_server	Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/L:I/A:L).	2019-01-16	6.8	<a href="#">CVE-2019-2418</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Application Container - JavaEE). The supported version that is affected is 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2441</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2452</a> <a href="#">CONF RM</a> <a href="#">BID</a>
premiumwpsuite -- easy_redirect_manager	The Premium WP Suite Easy Redirect Manager plugin 28.07-17 for WordPress has XSS via a crafted GET request that is mishandled during log viewing at the templates/admin/redirect-log.php URI.	2019-01-14	4.3	<a href="#">CVE-2019-6267</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
shopware -- shopware	Shopware before 5.4.3 allows SQL Injection by remote authenticated users, aka SW-21404.	2019-01-15	6.5	<a href="#">CVE-2018-20713</a> <a href="#">MISC</a>
tiki -- tikiwiki_cms/groupware	In Tiki before 17.2, the user task component is vulnerable to a SQL Injection via the tiki-user_tasks.php show_history parameter.	2019-01-15	6.5	<a href="#">CVE-2018-20719</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	2.1	<a href="#">CVE-2018-4255</a> <a href="#">CONFIRM</a>
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	2.1	<a href="#">CVE-2018-4256</a> <a href="#">CONFIRM</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in color_templates.php in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Name field for a Color.	2019-01-16	3.5	<a href="#">CVE-2018-20723</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in pollers.php in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Website Hostname for Data Collectors.	2019-01-16	3.5	<a href="#">CVE-2018-20724</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in graph_templates.php in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Graph Vertical Label.	2019-01-16	3.5	<a href="#">CVE-2018-20725</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in host.php (via tree.php) in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Website Hostname field for Devices.	2019-01-16	3.5	<a href="#">CVE-2018-20726</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cubecart -- cubecart	CubeCart 6.2.2 has Reflected XSS via a {/ADMIN-FILE}/ query string.	2019-01-13	3.5	<a href="#">CVE-2018-20703</a> <a href="#">MISC</a>
ibm -- spss_analytic_server	IBM SPSS Analytic Server 3.1.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 148689.	2019-01-15	3.5	<a href="#">CVE-2018-1772</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2019-</a>

joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate checks of the Global Configuration helpurl settings allowed stored XSS.	2019-01-16	<a href="#">3.5</a>	<a href="#">6262 BID CONFIRM</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate checks of the Global Configuration Text Filter settings allowed stored XSS.	2019-01-16	<a href="#">3.5</a>	<a href="#">CVE-2019-6263 BID CONFIRM EXPLOIT-DB</a>
jpress -- jpress	XSS exists in JPress v1.0.4 via Markdown input, or Markdown input with the code input option.	2019-01-14	<a href="#">3.5</a>	<a href="#">CVE-2019-6278 MISC</a>
oracle -- database_server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java VM. CVSS 3.0 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L).	2019-01-16	<a href="#">3.5</a>	<a href="#">CVE-2019-2547 CONFIRM BID</a>
oracle -- hospitality_cruise_shipboard_property_management_system	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: SPMS Suite). The supported version that is affected is 8.0.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Cruise Shipboard Property Management System executes to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise Shipboard Property Management System, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Cruise Shipboard Property Management System as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Shipboard Property Management System accessible data and unauthorized read access to a subset of Oracle Hospitality Cruise Shipboard Property Management System accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/L/I:L/A:H).	2019-01-16	<a href="#">3.3</a>	<a href="#">CVE-2019-2409 CONFIRM BID</a>
oracle -- hospitality_cruise_shipboard_property_management_system	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: DGS RES Online, FMS Sender, FMS Receiver, OHC WPF Security). The supported version that is affected is 8.0.8. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hospitality Cruise Shipboard Property Management System executes to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Shipboard Property Management System accessible data as well as unauthorized read access to a subset of Oracle Hospitality Cruise Shipboard Property Management System accessible data. CVSS 3.0 Base Score 5.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	<a href="#">3.6</a>	<a href="#">CVE-2019-2410 CONFIRM BID</a>
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Report privilege with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 4.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	<a href="#">3.6</a>	<a href="#">CVE-2019-2397 CONFIRM BID</a>
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Report privilege with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2019-01-16	<a href="#">3.6</a>	<a href="#">CVE-2019-2407 CONFIRM BID</a>
	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). The supported version that is affected is Java SE: 8u192. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a			<a href="#">CVE-2019-</a>

oracle -- jdk	partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).	2019-01-16	2.6	<a href="#">2449</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).	2019-01-16	3.8	<a href="#">CVE-2019-2503</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.5 (Confidentiality impacts). CVSS Vector: (CVSS 3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N).	2019-01-16	1.2	<a href="#">CVE-2019-2513</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	1.9	<a href="#">CVE-2019-2535</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:N/A:H).	2019-01-16	1.2	<a href="#">CVE-2019-2536</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- peoplesoft_enterprise_campus_software_campus_community	Vulnerability in the PeopleSoft Enterprise CS Campus Community component of Oracle PeopleSoft Products (subcomponent: Frameworks). Supported versions that are affected are 9.0 and 9.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2019-01-16	2.6	<a href="#">CVE-2019-2493</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2446</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2448</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise			<a href="#">CVE-2019-</a>



oracle -- vm_virtualbox	Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">2450 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2451 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2501 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2504 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2505 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2506 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 5.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	1.9	<a href="#">CVE-2019-2525 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	2019-01-16	2.1	<a href="#">CVE-2019-2527 CONFIRM BID</a>
	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable			

oracle -- vm_virtualbox	vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3 8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2553</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2554</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2555</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2556</a> <a href="#">CONFIRM</a> <a href="#">BID</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- relion_630_devices	ABB Relion 630 devices 1.1 before 1.1.0.C0, 1.2 before 1.2.0.B3, and 1.3 before 1.3.0.A6 allow remote attackers to cause a denial of service (reboot) via a reboot command in an SPA message.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20720</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19711</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19719</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19717</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19716</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19715</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19714</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19713</a> <a href="#">BID</a>

[illegible]

[illegible]

[illegible]



[illegible]

adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16039</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16027</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16029</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16030</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16031</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16032</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16033</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16034</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16035</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16036</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16028</a> BID CONFIRM
adobe -- connect	Adobe Connect versions 9.8.1 and earlier have a session token exposure vulnerability. Successful exploitation could lead to exposure of the privileges granted to a session.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19718</a> BID CONFIRM
adobe -- digital_editions	Adobe Digital Editions versions 4.5.9 and below have an out of bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-12817</a> BID CONFIRM
adobe -- flash_player	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-15982</a> BID REDHAT CONFIRM EXPLOIT-DB
adobe -- flash_player	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation.	2019-01-18	not yet calculated	<a href="#">CVE-2018-15983</a> BID CONFIRM
apple -- multiple_products	In iOS before 11.4, iCloud for Windows before 7.5, watchOS before 4.3.1, iTunes before 12.7.5 for Windows, and macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4194</a> MISC CONFIRM
apple -- multiple_products	In iOS before 11.3, tvOS before 11.3, watchOS before 4.3, and macOS before High Sierra 10.13.4, an information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4185</a> MISC MISC CONFIRM MISC
atlassian -- universal_plugin_manager	The Upload add-on resource in Atlassian Universal Plugin Manager before version 2.22.14 allows remote attackers who have system administrator privileges to read files, make network requests and perform a denial of service attack via an XML External Entity vulnerability in the parsing of atlassian plugin xml files in an uploaded JAR.	2019-01-18	not yet calculated	<a href="#">CVE-2018-20233</a> CONFIRM
ceph -- ceph	It was found Ceph versions before 13.2.4 that authenticated ceph users with read only permissions could steal dm-crypt encryption keys used in ceph disk encryption.	2019-01-15	not yet calculated	<a href="#">CVE-2018-14662</a> CONFIRM MISC
ceph -- ceph	It was found in Ceph versions before 13.2.4 that authenticated ceph RGW	2019-01-15	not yet	<a href="#">CVE-2018-16846</a> CONFIRM

	users can cause a denial of service against OMAPs holding bucket indices.		calculated	MISC
cisco -- 900_series_aggregation_services_router	A vulnerability in Cisco 900 Series Aggregation Services Router (ASR) software could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient handling of certain broadcast packets ingress to the device. An attacker could exploit this vulnerability by sending large streams of broadcast packets to an affected device. If successful, an exploit could allow an attacker to impact services running on the device, resulting in a partial DoS condition.	2019-01-11	not yet calculated	<a href="#">CVE-2018-15464</a> BID <a href="#">CISCO</a>
cubecart -- cubecart	CubeCart before 6.1.13 has SQL Injection via the validate[] parameter of the "I forgot my Password!" feature.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20716</a> MISC
dell -- networking_os10	Dell Networking OS10 versions prior to 10.4.3.0 contain a vulnerability in the Phone Home feature which does not properly validate the server's certificate authority during TLS handshake. Use of an invalid or malicious certificate could potentially allow an attacker to spoof a trusted entity by using a man-in-the-middle (MITM) attack.	2019-01-18	not yet calculated	<a href="#">CVE-2018-15784</a> MISC
drupal -- drupal	In Drupal 8 prior to 8.3.7; When using the REST API, users without the correct permission can post comments via REST that are approved even if the user does not have permission to post approved comments. This issue only affects sites that have the RESTful Web Services (rest) module enabled, the comment entity REST resource enabled, and where an attacker can access a user account on the site with permissions to post comments, or where anonymous users can post comments.	2019-01-15	not yet calculated	<a href="#">CVE-2017-6924</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a>
drupal -- drupal	In versions of Drupal 8 core prior to 8.3.7; There is a vulnerability in the entity access system that could allow unwanted access to view, create, update, or delete entities. This only affects entities that do not use or do not have UUIDs, and entities that have different access restrictions on different revisions of the same entity.	2019-01-15	not yet calculated	<a href="#">CVE-2017-6925</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a>
drupal -- drupal	In Drupal 8 prior to 8.3.4; The file REST resource does not properly validate some fields when manipulating files. A site is only affected by this if the site has the RESTful Web Services (rest) module enabled, the file REST resource is enabled and allows PATCH requests, and an attacker can get or register a user account on the site with permissions to upload files and to modify the file resource.	2019-01-15	not yet calculated	<a href="#">CVE-2017-6921</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a>
etcd -- etcd	etcd versions 3.2.x before 3.2.26 and 3.3.x before 3.3.11 are vulnerable to an improper authentication issue when role-based access control (RBAC) is used and client-cert-auth is enabled. If an etcd client server TLS certificate contains a Common Name (CN) which matches a valid RBAC username, a remote attacker may authenticate as that user with any valid (trusted) client certificate in a REST API request to the gRPC-gateway.	2019-01-14	not yet calculated	<a href="#">CVE-2018-16886</a> BID <a href="#">CONFIRM</a> MISC MISC
gnu -- binutils	A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	2019-01-14	not yet calculated	<a href="#">CVE-2018-20712</a> BID MISC MISC
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 Virtual Appliance is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 155265.	2019-01-18	not yet calculated	<a href="#">CVE-2018-2019</a> BID XF <a href="#">CONFIRM</a>
isc -- bind	Mistaken assumptions about the ordering of records in the answer section of a response containing CNAME or DNAME resource records could lead to a situation in which named would exit with an assertion failure when processing a response in which records occurred in an unusual order. Affects BIND 9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0-P3, 9.11.1b1->9.11.1rc1, and 9.9.9-S8.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3137</a> BID <a href="#">SECTrack</a> <a href="#">SECTrack</a> REDHAT REDHAT REDHAT <a href="#">CONFIRM</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> DEBIAN
isc -- bind	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name for the zone and service being targeted may be able to manipulate BIND into accepting an unauthorized dynamic update. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.10-S2, 9.10.5-S1->9.10.5-S2.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3143</a> BID <a href="#">SECTrack</a> REDHAT REDHAT <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> DEBIAN
isc -- bind	The BIND installer on Windows uses an unquoted service path which can enable a local user to achieve privilege escalation if the host file system permissions allow this. Affects BIND 9.2.6-P2->9.2.9, 9.3.2-P1->9.3.6, 9.4.0->9.8.8, 9.9.0->9.10, 9.10.0->9.10.5, 9.11.0->9.11.1, 9.9.3-S1->9.10-S1, 9.10.5-S1.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3141</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> EXPLOIT-DB
isc -- bind	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name may be able to circumvent TSIG authentication of AXFR requests via a carefully constructed request packet. A server that relies solely on TSIG keys for protection with no other ACL protection could be manipulated into: providing an AXFR of a zone to an unauthorized recipient or accepting bogus NOTIFY packets. Affects BIND 9.4.0->9.8.8, 9.9.0->9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.10-S2, 9.10.5-S1->9.10.5-S2.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3142</a> BID <a href="#">SECTrack</a> REDHAT REDHAT <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> DEBIAN
isc -- bind	Under some conditions when using both DNS64 and RPZ to rewrite query responses, query processing can resume in an inconsistent state leading to either an INSIST assertion failure or an attempt to read through a NULL pointer. Affects BIND 9.8.8, 9.9.3-S1->9.9.9-S7, 9.9.3->9.9.9-P5, 9.9.10b1,	2019-01-16	not yet calculated	<a href="#">CVE-2017-3135</a> REDHAT BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

	9.10.0 -> 9.10.4-P5, 9.10.5b1, 9.11.0 -> 9.11.0-P2, 9.11.1b1.			<a href="#">GENTOO CONFIRM</a> <a href="#">DEBIAN</a>
isc -- bind	If named is configured to use Response Policy Zones (RPZ) an error processing some rule types can lead to a condition where BIND will endlessly loop while handling a query. Affects BIND 9.9.10, 9.10.5, 9.11.0->9.11.1, 9.9.10-S1, 9.10.5-S1.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3140 BID</a> <a href="#">SECTrack CONFIRM</a> <a href="#">GENTOO CONFIRM</a>
isc -- bind	named contains a feature which allows operators to issue commands to a running server by communicating with the server process over a control channel, using a utility program such as rndc. A regression introduced in a recent feature change has created a situation under which some versions of named can be caused to exit with a REQUIRE assertion failure if they are sent a null command string. Affects BIND 9.9.9-P7, 9.9.10b1->9.9.10rc2, 9.10.4->9.10.4-P7, 9.10.5b1->9.10.5rc2, 9.11.0->9.11.0-P4, 9.11.1b1->9.11.1rc2, 9.9.9-S1->9.9.9-S9.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3138 BID</a> <a href="#">SECTrack CONFIRM</a> <a href="#">GENTOO CONFIRM</a> <a href="#">DEBIAN</a>
isc -- bind	A query with a specific set of characteristics could cause a server using DNS64 to encounter an assertion failure and terminate. An attacker could deliberately construct a query, enabling denial-of-service against a server if it was configured to use the DNS64 feature and other preconditions were met. Affects BIND 9.8.0 -> 9.8.8-P1, 9.9.0 -> 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.0 -> 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0 -> 9.11.0-P3, 9.11.1b1->9.11.1rc1, 9.9.3-S1 -> 9.9.9-S8.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3136 BID</a> <a href="#">SECTrack REDHAT</a> <a href="#">REDHAT CONFIRM</a> <a href="#">GENTOO CONFIRM</a> <a href="#">DEBIAN</a>
isc -- bind	An error in handling certain queries can cause an assertion failure when a server is using the nxdomain-redirect feature to cover a zone for which it is also providing authoritative service. A vulnerable server could be intentionally stopped by an attacker if it was using a configuration that met the criteria for the vulnerability and if the attacker could cause it to accept a query that possessed the required attributes. Please note: This vulnerability affects the "nxdomain-redirect" feature, which is one of two methods of handling NXDOMAIN redirection, and is only available in certain versions of BIND. Redirection using zones of type "redirect" is not affected by this vulnerability. Affects BIND 9.9.8-S1 -> 9.9.8-S3, 9.9.9-S1 -> 9.9.9-S6, 9.11.0-9.11.0-P1.	2019-01-16	not yet calculated	<a href="#">CVE-2016-9778 BID</a> <a href="#">SECTrack CONFIRM</a> <a href="#">GENTOO CONFIRM</a>
isc -- bind	BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named. Affects BIND 9.0.0 to 9.8.x, 9.9.0 to 9.9.11, 9.10.0 to 9.10.6, 9.11.0 to 9.11.2, 9.9.3-S1 to 9.9.11-S1, 9.10.5-S1 to 9.10.6-S1, 9.12.0a1 to 9.12.0rc1.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3145 BID</a> <a href="#">SECTrack REDHAT</a> <a href="#">REDHAT CONFIRM</a> <a href="#">MLIST CONFIRM</a> <a href="#">DEBIAN</a>
isc -- dhcp	A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of socket descriptors available to the DHCP server. Affects ISC DHCP 4.1.0 to 4.1-ESV-R15, 4.2.0 to 4.2.8, 4.3.0 to 4.3.6. Older versions may also be affected but are well beyond their end-of-life (EOL). Releases prior to 4.1.0 have not been tested.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3144 BID</a> <a href="#">SECTrack REDHAT</a> <a href="#">CONFIRM UBUNTU</a> <a href="#">DEBIAN</a>
limesurvey -- limesurvey	LimeSurvey before 2.72.4 has Stored XSS by using the Continue Later (aka Resume later) feature to enter an email address, which is mishandled in the admin panel.	2019-01-15	not yet calculated	<a href="#">CVE-2017-18358 MISC</a> <a href="#">MISC</a>
mailenable -- mailenable	MailEnable before 8.60 allows Privilege Escalation because admin accounts could be created as a consequence of %0A mishandling in AUTH.TAB after a password-change request.	2019-01-16	not yet calculated	<a href="#">CVE-2015-9278 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- nedi	A stored cross site scripting (XSS) vulnerability in NeDi before 1.7Cp3 allows remote attackers to inject arbitrary web script or HTML via User-Chat.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20731 MISC</a> <a href="#">MISC</a>
nedi_consulting -- nedi	A SQL injection vulnerability in NeDi before 1.7Cp3 allows any user to execute arbitrary SQL read commands via the query.php component.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20730 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- nedi	A reflected cross site scripting (XSS) vulnerability in NeDi before 1.7Cp3 allows remote attackers to inject arbitrary web script or HTML via the reg parameter in mh.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20729 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- nedi	A cross site request forgery (CSRF) vulnerability in NeDi before 1.7Cp3 allows remote attackers to escalate privileges via User-Management.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20728 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- nedi	Multiple command injection vulnerabilities in NeDi before 1.7Cp3 allow authenticated users to execute code on the server side via the fit parameter to Nodes-Traffic.php, the dv parameter to Devices-Graph.php, or the tit parameter to drawmap.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20727 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
oxid -- esales	The DB abstraction layer of OX D eSales 4.10.6 is vulnerable to SQL injection via the oxid or synchoxid parameter to the oxConfig::getRequestParameter() method in core/oxconfig.php.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20715 MISC</a> <a href="#">MISC</a>
prestashop -- prestashop	In the orders section of PrestaShop before 1.7.2.5, an attack is possible after gaining access to a target store with a user role with the rights of at least a Salesman or higher privileges. The attacker can then inject arbitrary PHP objects into the process and abuse an object chain in order to gain Remote Code Execution. This occurs because protection against serialized objects looks for a 0: followed by an integer, but does not consider 0:+ followed by an	2019-01-15	not yet calculated	<a href="#">CVE-2018-20717 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	integer.			
pydio -- pydio	In Pydio before 8.2.2, an attack is possible via PHP Object Injection because a user is allowed to use the \$phpserial\$a:0:{} syntax to store a preference. An attacker either needs a "public link" of a file, or access to any unprivileged user account for creation of such a link.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20718</a> MISC
qualcomm -- snapdragon	While processing a packet decode request in MQTT, Race condition can occur leading to an out-of-bounds access in snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, SD 210/SD 212/SD 205, SD 427, SD 435, SD 450, SD 625, SD 636, SD 835, SDA660, SDM630, SDM660, Snapdragon_High_Med_2016	2019-01-18	not yet calculated	<a href="#">CVE-2018-11998</a> CONFIRM
qualcomm -- snapdragon	Spoofed SMS can be used to send a large number of messages to the device which will in turn initiate a flood of registration updates with the server in snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 625, SD 636, SDA660, SDM630, SDM660, SDX20	2019-01-18	not yet calculated	<a href="#">CVE-2018-11284</a> CONFIRM
qualcomm -- snapdragon	Security keys are logged when any WCDMA call is configured or reconfigured in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDX20, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2017-18332</a> BID CONFIRM
qualcomm -- snapdragon	Improper access control on secure display buffers in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, MSM8996AU, SD 210/SD 212/SD 205, SD 820, SD 820A, SD 835, SDA660	2019-01-18	not yet calculated	<a href="#">CVE-2017-18331</a> BID CONFIRM
qualcomm -- snapdragon	AGPS session failure in GNSS module due to cyphersuites are hardcoded and needed manual update everytime in snapdragon mobile and snapdragon wear in versions MDM9635M, MDM9645, MDM9650, MDM9655, MSM8909W, SD 835, SD 845, SD 850	2019-01-18	not yet calculated	<a href="#">CVE-2017-18160</a> BID CONFIRM
qualcomm -- snapdragon	Improper authorization involving a fuse in TrustZone in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 810, SD 820, SD 820A, SD 835, SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016.	2019-01-18	not yet calculated	<a href="#">CVE-2017-8276</a> BID CONFIRM
qualcomm -- snapdragon	Improper check while accessing the local memory stack on MQTT connection request can lead to buffer overflow in snapdragon wear in versions MDM9206, MDM9607	2019-01-18	not yet calculated	<a href="#">CVE-2018-11993</a> CONFIRM
qualcomm -- snapdragon	Lack of check of input size can make device memory get corrupted because of buffer overflow in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 810, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2018-11279</a> BID CONFIRM
qualcomm -- snapdragon	Improper input validation in trustzone can lead to denial of service in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9635M, MDM9650, MDM9655, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM630, SDM660, SDX24	2019-01-18	not yet calculated	<a href="#">CVE-2018-11999</a> BID CONFIRM
qualcomm -- snapdragon	Anti-rollback can be bypassed in replay scenario during app loading due to improper error handling of RPMB writes in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDX24, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2018-3595</a> BID CONFIRM
qualcomm -- snapdragon	Possible undefined behavior due to lack of size check in function for parameter segment_idx can lead to a read outside of the intended region in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDX24, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2018-11288</a> CONFIRM
rsa -- authentication_manager	The Quick Setup component of RSA Authentication Manager versions prior to 8.4 is vulnerable to a relative path traversal vulnerability. A local attacker could potentially provide an administrator with a crafted license that if used during the quick setup deployment of the initial RSA Authentication Manager system, could allow the attacker unauthorized access to that system.	2019-01-16	not yet calculated	<a href="#">CVE-2018-15782</a> FULLDISC
sas -- web_infrastructure_platform	SAS Web Infrastructure Platform before 9.4M6 allows remote attackers to execute arbitrary code via a Java deserialization variant.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20732</a> BID MISC
sas -- web_infrastructure_platform	BI Web Services in SAS Web Infrastructure Platform before 9.4M6 allows XXE.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20733</a> MISC
sas -- web_infrastructure_platform	Logon Manager in SAS Web Infrastructure Platform before 9.4M3 allows reflected XSS on the Timeout page.	2019-01-16	not yet calculated	<a href="#">CVE-2015-9281</a> MISC
serendipity -- serendipity	Serendipity 2.0.4 has XSS via the serendipity_admin.php serendipity[body] parameter.	2019-01-15	not yet calculated	<a href="#">CVE-2016-10737</a> EXPLOIT-DB
shopware -- shopware	Shopware before 5.3.4 has a PHP Object Instantiation issue via the sort parameter to the loadPreviewAction() method of the Shopware_Controller_Backend_ProductStream controller, with resultant XXE via instantiation of a SimpleXMLElement object.	2019-01-15	not yet calculated	<a href="#">CVE-2017-18357</a> MISC MISC
smartertools -- smartermail	SmarterTools SmarterMail before 13.3.5535 was vulnerable to stored XSS by bypassing the anti-XSS mechanisms. It was possible to run JavaScript code when a victim user opens or replies to the attacker's email, which contained a malicious payload. Therefore, users' passwords could be reset by using an XSS attack, as the password reset page did not need the current password.	2019-01-16	not yet calculated	<a href="#">CVE-2015-9276</a> MISC MISC MISC



systemd -- systemd-journald	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16866</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
systemd -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16864</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
systemd -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16865</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
systemd -- systemd	It was discovered systemd does not correctly check the content of P DFile files before using it to kill processes. When a service is run from an unprivileged user (e.g. User field set in the service file), a local attacker who is able to write to the PIDFile of the mentioned service may use this flaw to trick systemd into killing other services and/or privileged processes. Versions before v237 are vulnerable.	2019-01-14	not yet calculated	<a href="#">CVE-2018-16888</a> <a href="#">CONFIRM</a>
tibco -- spotfire	The Spotfire Library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace, and T BCO Spotfire Server contains a vulnerability that might theoretically fail to restrict users with read-only access from modifying files stored in the Spotfire Library, only when the Spotfire Library is configured to use external storage. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace versions up to and including 10.0.0, and T BCO Spotfire Server versions up to and including 7.10.1; 7.11.0; 7.11.1; 7.12.0; 7.13 0; 7.14.0; 10 0 0.	2019-01-16	not yet calculated	<a href="#">CVE-2018-18812</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- spotfire	The Spotfire web server component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace, and T BCO Spotfire Server contains multiple vulnerabilities that may allow persistent and reflected cross-site scripting attacks. Affected releases are T BCO Software Inc. TIBCO Spotfire Analytics Platform for AWS Marketplace: versions up to and including 10.0.0, and TIBCO Spotfire Server: versions up to and including 7.10.1; 7.11.0; 7.11.1; 7.12.0; 7.13.0; 7.14.0; 10.0.0.	2019-01-16	not yet calculated	<a href="#">CVE-2018-18813</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- spotfire	The TIBCO Spotfire authentication component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace, and TIBCO Spotfire Server contains a vulnerability in the handling of the authentication that theoretically may allow an attacker to gain full access to a target account, independent of configured authentication mechanisms. Affected releases are TIBCO Software Inc. TIBCO Spotfire Analytics Platform for AWS Marketplace: versions up to and including 10.0.0, and T BCO Spotfire Server: versions up to and including 7.10.1; 7.11.0; 7.11.1; 7.12.0; 7.13 0; 7.14.0.	2019-01-16	not yet calculated	<a href="#">CVE-2018-18814</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
uriparser -- uriparser	URI_FUNC() in UriParse c in uriparser before 0.9.1 has an out-of-bounds read (in uriParse*Ex* functions) for an incomplete URI with an Pv6 address containing an embedded IPv4 address, such as a "://[:44.1" address.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20721</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The logging system of the Automattic WooCommerce plugin before 3.4.6 for WordPress is vulnerable to a File Deletion vulnerability. This allows deletion of woocommerce.php, which leads to certain privilege checks not being in place, and therefore a shop manager can escalate privileges to admin.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20714</a> <a href="#">MISC</a>
wordpress -- wordpress	In the Automattic WooCommerce plugin before 3 2.4 for WordPress, an attack is possible after gaining access to the target site with a user account that has at least Shop manager privileges. The attacker then constructs a specifically crafted string that will turn into a PHP object injection involving the includes/shortcodes/class-wc-shortcode-products.php WC_Shortcode_Products: get_products() use of cached queries within shortcodes.	2019-01-15	not yet calculated	<a href="#">CVE-2017-18356</a> <a href="#">MISC</a> <a href="#">MISC</a>

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@nrcas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

From: US-CERT  
To: [usultarte@ci.sunnvale.ca.us](mailto:usultarte@ci.sunnvale.ca.us)  
Subject: SB19-021: Vulnerability Summary for the Week of January 14, 2019  
Date: Tuesday, January 22, 2019 7:40:44 AM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## SB19-021: Vulnerability Summary for the Week of January 14, 2019

01/21/2019 09:22 PM EST

Original release date: January 21, 2019 | Last revised: January 22, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- apple_tv	In iOS before 11.2.5, macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, watchOS before 4.2.2, and tvOS before 11.2.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	<a href="#">10.0</a>	<a href="#">CVE-2018-4189</a> CONFIRM MISC MISC MISC
apple -- apple_tv	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a permissions issue existed in Remote Management. This issue was addressed through improved permission validation.	2019-01-11	<a href="#">10.0</a>	<a href="#">CVE-2018-4298</a> CONFIRM MISC
apple -- iphone_os	In iOS before 9.3.3, a memory corruption issue existed in the kernel. This issue was addressed through improved memory handling.	2019-01-11	<a href="#">9.3</a>	<a href="#">CVE-2016-7576</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a logic error existed in the validation of credentials. This was addressed with improved credential validation.	2019-01-11	<a href="#">7.5</a>	<a href="#">CVE-2017-13889</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, an out-of-bounds read was addressed with improved input validation.	2019-01-11	<a href="#">10.0</a>	<a href="#">CVE-2018-4169</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions on CUPS.	2019-01-11	<a href="#">7.2</a>	<a href="#">CVE-2018-4182</a> MISC CONFIRM DEBIAN
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions.	2019-01-11	<a href="#">7.2</a>	<a href="#">CVE-2018-4183</a> MISC CONFIRM DEBIAN
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an input validation issue existed in the kernel. This issue was addressed with improved input validation.	2019-01-11	<a href="#">10.0</a>	<a href="#">CVE-2018-4254</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved size validation.	2019-01-11	<a href="#">10.0</a>	<a href="#">CVE-2018-4257</a> CONFIRM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved bounds checking.	2019-01-11	<a href="#">10.0</a>	<a href="#">CVE-2018-4258</a> CONFIRM
icmsdev -- icms	An issue was discovered in idreamsoft iCMS V7 0.13. There is SQL Injection via the app/article/article admincp.php_data_id parameter.	2019-01-14	<a href="#">7.5</a>	<a href="#">CVE-2019-6259</a> MISC
mailenable -- mailenable	MailEnable before 8.60 allows Directory Traversal for reading the messages of other users, uploading files, and deleting files because "/" and "/" are mishandled.	2019-01-16	<a href="#">7.5</a>	<a href="#">CVE-2015-9277</a> MISC MISC MISC
	Vulnerability in the Oracle Retail Xstore Payment component of Oracle Retail Applications (subcomponent: Security). The supported version that is affected is 3.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Xstore Payment. Successful			

oracle -- retail_xstore_payment	attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Retail Xstore Payment accessible data as well as unauthorized update, insert or delete access to some of Oracle Retail Xstore Payment accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Retail Xstore Payment. CVSS 3.0 Base Score 8.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I L/A L).	2019-01-16	7.5	<a href="#">CVE-2018-3311</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- solaris	Vulnerability in the Oracle Solaris component of Oracle Sun Systems Products Suite (subcomponent: Kernel). The supported version that is affected is 11. Easily exploitable vulnerability allows unauthenticated attacker with network access via TCP to compromise Oracle Solaris. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Solaris. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I N/A H).	2019-01-16	7.8	<a href="#">CVE-2019-2437</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via SOAP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I N/A H).	2019-01-16	7.8	<a href="#">CVE-2019-2511</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
skymoonlabs -- cleanto	Cleanto 5.0 has SQL Injection via the assets/lib/service_method_ajax.php service_id parameter.	2019-01-15	7.5	<a href="#">CVE-2019-6295</a> <a href="#">MISC</a>
skymoonlabs -- cleanto	Cleanto 5.0 has SQL Injection via the assets/lib/export_ajax.php id parameter.	2019-01-15	7.5	<a href="#">CVE-2019-6296</a> <a href="#">MISC</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- apple_tv	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, proxy authentication incorrectly reported HTTP proxies received credentials securely. This issue was addressed through improved warnings.	2019-01-11	4.3	<a href="#">CVE-2016-4642</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
apple -- apple_tv	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a validation issue existed in the parsing of 407 responses. This issue was addressed through improved response validation.	2019-01-11	4.0	<a href="#">CVE-2016-4643</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
apple -- apple_tv	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a downgrade issue existed with HTTP authentication credentials saved in Keychain. This issue was addressed by storing the authentication types with the credentials.	2019-01-11	4.0	<a href="#">CVE-2016-4644</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a>
apple -- apple_tv	In iOS before 11.3, Safari before 11.1, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, an array indexing issue existed in the handling of a function in javascript core. This issue was addressed with improved checks.	2019-01-11	6.8	<a href="#">CVE-2018-4210</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">UBUNTU</a>
apple -- apple_tv	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	6.8	<a href="#">CVE-2018-4212</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
apple -- apple_tv	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	6.8	<a href="#">CVE-2018-4213</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
apple -- apple_tv	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, multiple memory corruption issues were addressed with improved memory handling.	2019-01-11	6.8	<a href="#">CVE-2018-4262</a> <a href="#">SECTRAK</a> <a href="#">GENTOO</a> <a href="#">MISC</a> <a href="#">CONF RM</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
	In iOS before 11.4.1, watchOS before 4.3.2, tvOS before 11.4.1, Safari			<a href="#">CVE-2018-4277</a> <a href="#">SECTRAK</a>

apple -- apple_tv	before 11.1.1, macOS High Sierra before 10.13.6, a spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation.	2019-01-11	5.0	MISC MISC MISC CONF RM MISC
apple -- apple_tv	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, sound fetched through audio elements may be exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.	2019-01-11	4.3	CVE-2018-4278 SECTRAK MISC GENTOO CONF RM MISC MISC MISC UBUNTU
apple -- icloud	In iCloud for Windows before 7.3, Safari before 11.0.3, iTunes before 12.7.3 for Windows, and iOS before 11.2.5, multiple memory corruption issues exist and were addressed with improved memory handling.	2019-01-11	6.8	CVE-2018-4147 CONF RM MISC MISC MISC
apple -- iphone_os	In iOS before 11.2, a type confusion issue was addressed with improved memory handling.	2019-01-11	5.0	CVE-2017-13888 CONF RM
apple -- iphone_os	In iOS before 11.2, an inconsistent user interface issue was addressed through improved state management.	2019-01-11	4.3	CVE-2017-13891 CONF RM
apple -- iphone_os	In iOS before 11.2, exchange rates were retrieved from HTTP rather than HTTPS. This was addressed by enabling HTTPS for exchange rates.	2019-01-11	4.3	CVE-2017-2411 CONF RM
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	4.9	CVE-2018-4181 MLIST CONF RM UBUNTU DEBIAN
apple -- mac_os_x	In macOS High Sierra before 10.13.5, a privacy issue in the handling of Open Directory records was addressed with improved indexing.	2019-01-11	5.0	CVE-2018-4217 CONF RM
cairographics -- cairo	An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_arc_in_direction in the file cairo-arc.c.	2019-01-16	4.3	CVE-2019-6461 MISC MISC
cairographics -- cairo	An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_normalized in the file cairo-arc.c, related to _arc_max_angle_for_tolerance_normalized.	2019-01-16	4.3	CVE-2019-6462 MISC MISC
castlamp -- zenbership	Zenbership v107 has CSRF via admin/cp-functions/event-add.php.	2019-01-15	6.8	CVE-2016-10738 EXPLOIT-DB
cisco -- identity_services_engine_software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of an affected system. The vulnerability is due to insufficient sanitization of user-supplied data that is written to log files and displayed in certain web pages of the web-based management interface of an affected device. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link or view an affected log file. The injected script code may be executed in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	2019-01-15	4.3	CVE-2018-15440 MISC CISCO
cisco -- identity_services_engine_software	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based interface. The vulnerability is due to insufficient input validation of some parameters passed to the web-based management interface of an affected device. An attacker could exploit this vulnerability by convincing a user of the interface to click a specific link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	2019-01-15	4.3	CVE-2018-15463 MISC CISCO
citysearch / _hotfrog / _gelbeseiten_clone_script_project -- citysearch / _hotfrog / _gelbeseiten_clone_script	PHP Scripts Mall Citysearch / Hotfrog / Gelbeseiten Clone Script 2.0.1 has Reflected XSS via the srch parameter, as demonstrated by restaurants-details.php.	2019-01-12	4.3	CVE-2019-6248 MISC
easycms -- easycms	An issue was discovered in EasyCMS 1.5. There is CSRF via the index.php?s=/admin/article/insert/navTabId/listarticle/callbackType/closeCurrentURI.	2019-01-15	6.8	CVE-2019-6294 MISC
frog_cms_project -- frog_cms	Frog CMS 0.9.5 allows XSS via the forgot password page (aka the /admin/?/login/forgot URI).	2019-01-11	4.3	CVE-2019-6243 MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a double-free problem in the function rec_mset_elem_destroy() in the file rec-mset.c.	2019-01-16	4.3	CVE-2019-6455 MISC

gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a NULL pointer dereference in the function rec_fex_size() in the file rec-fex.c of librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6456</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a memory leak in rec_aggregate_reg_new in rec-aggregate.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6457</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a memory leak in rec_buf_new in rec-buf.c when called from rec_parse_rset in rec-parser.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6458</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a memory leak in rec_extract_type in rec-utils.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6459</a> MISC
gnu -- recutils	An issue was discovered in GNU Recutils 1.8. There is a NULL pointer dereference in the function rec_field_set_name() in the file rec-field.c in librec.a.	2019-01-16	4.3	<a href="#">CVE-2019-6460</a> MISC
hucart -- hucart	An issue was discovered in HuCart v5.7.4. There is a CSRF vulnerability that can add an admin account via /admins/index.php?load=admins&act=edit_info&act_type=add.	2019-01-13	6.8	<a href="#">CVE-2019-6249</a> MISC EXPLOIT-DB
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 153628.	2019-01-14	5.0	<a href="#">CVE-2018-1956</a> X-Force CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153748.	2019-01-14	4.3	<a href="#">CVE-2018-1967</a> X-Force CONFIRM
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 153750.	2019-01-14	6.5	<a href="#">CVE-2018-1969</a> X-Force CONFIRM
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate escaping in com_contact leads to a stored XSS vulnerability.	2019-01-16	4.3	<a href="#">CVE-2019-6261</a> X-Force CONFIRM
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate escaping in mod_banners leads to a stored XSS vulnerability.	2019-01-16	4.3	<a href="#">CVE-2019-6264</a> X-Force CONFIRM
libpng -- libpng	png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp.	2019-01-11	6.8	<a href="#">CVE-2019-6129</a> MISC
libtiff -- libtiff	The TIFFFdOpen function in tif_unix.c in LibTIFF 4.0.10 has a memory leak, as demonstrated by pal2rgb.	2019-01-11	6.8	<a href="#">CVE-2019-6128</a> MISC
mailenable -- mailenable	MailEnable before 8.60 allows Stored XSS via malformed use of "<img/src" with no ">" character in the body of an e-mail message.	2019-01-16	4.3	<a href="#">CVE-2015-9279</a> MISC MISC MISC
mailenable -- mailenable	MailEnable before 8.60 allows XXE via an XML document in the request aspx Options parameter.	2019-01-16	5.0	<a href="#">CVE-2015-9280</a> MISC MISC MISC
microsoft -- team_foundation_server	An information disclosure vulnerability exists when Team Foundation Server does not properly handle variables marked as secret, aka "Team Foundation Server Information Disclosure Vulnerability." This affects Team.	2019-01-17	4.0	<a href="#">CVE-2019-0647</a> X-Force CONFIRM
oracle -- application_testing_suite	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). Supported versions that are affected are 12.5.0.3, 13.1.0.1, 13.2.0.1 and 13.3.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2019-01-16	6.4	<a href="#">CVE-2018-3304</a> X-Force CONFIRM CONFIRM
oracle -- application_testing_suite	Vulnerability in the Oracle Application Testing Suite component of Oracle Enterprise Manager Products Suite (subcomponent: Load Testing for Web Apps). Supported versions that are affected are 12.5.0.3, 13.1.0.1, 13.2.0.1 and 13.3.0.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Testing Suite. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Testing Suite accessible data as well as unauthorized read access to a subset of Oracle Application Testing Suite accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Application Testing Suite. CVSS 3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector:	2019-01-16	6.5	<a href="#">CVE-2018-3305</a> X-Force CONFIRM CONFIRM



	(CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).			
oracle -- argus_safety	Vulnerability in the Oracle Argus Safety component of Oracle Health Sciences Applications (subcomponent: Console). Supported versions that are affected are 8.1 and 8.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Argus Safety. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Argus Safety accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2430</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- argus_safety	Vulnerability in the Oracle Argus Safety component of Oracle Health Sciences Applications (subcomponent: Console). Supported versions that are affected are 8.1 and 8.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Argus Safety. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Argus Safety accessible data. CVSS 3.0 Base Score 6.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2431</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- argus_safety	Vulnerability in the Oracle Argus Safety component of Oracle Health Sciences Applications (subcomponent: Login). Supported versions that are affected are 8.1 and 8.2. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Argus Safety. While the vulnerability is in Oracle Argus Safety, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Argus Safety accessible data as well as unauthorized read access to a subset of Oracle Argus Safety accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N).	2019-01-16	4.9	<a href="#">CVE-2019-2432</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- content_manager	Vulnerability in the Oracle Content Manager component of Oracle E-Business Suite (subcomponent: Cover Letter). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Content Manager. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Content Manager, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Content Manager accessible data as well as unauthorized update, insert or delete access to some of Oracle Content Manager accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2445</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- database	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2406</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- database	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2444</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2396</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Session Management). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base	2019-01-16	5.0	<a href="#">CVE-2019-2488</a> <a href="#">CONF RM</a> <a href="#">BID</a>

	Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
oracle -- e-business_suite	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2491</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle Email Center component of Oracle E-Business Suite (subcomponent: Message Display). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Email Center. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Email Center, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Email Center accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2492</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2496</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle CRM Technical Foundation component of Oracle E-Business Suite (subcomponent: Messages). Supported versions that are affected are 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle CRM Technical Foundation, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle CRM Technical Foundation accessible data as well as unauthorized update, insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/H:I/L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2497</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- e-business_suite	Vulnerability in the Oracle Applications Manager component of Oracle E-Business Suite (subcomponent: SQL Extensions). Supported versions that are affected are 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 and 12.2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications Manager accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2546</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- enterprise_manager_base_platform	Vulnerability in the Enterprise Manager Base Platform component of Oracle Enterprise Manager Products Suite (subcomponent: EM Console). Supported versions that are affected are 13.2 and 13.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Enterprise Manager Base Platform. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Enterprise Manager Base Platform accessible data as well as unauthorized read access to a subset of Enterprise Manager Base Platform accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2018-3303</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_cruise_shipboard_property_management_system	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: SPMS Suite). The supported version that is affected is 8.0.8. Easily exploitable vulnerability allows low privileged attacker with network access via TCP to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise Shipboard Property Management System, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Cruise Shipboard Property Management System as well as unauthorized update, insert or delete	2019-01-16	4.9	<a href="#">CVE-2019-2411</a> <a href="#">CONF RM</a> <a href="#">BID</a>

	access to some of Oracle Hospitality Cruise Shipboard Property Management System accessible data. CVSS 3.0 Base Score 7.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:H).			
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Admin privilege with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	2019-01-16	5.5	<a href="#">CVE-2019-2401</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2019-2425</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_symphony	Vulnerability in the Oracle Hospitality Symphony component of Oracle Food and Beverage Applications. The supported version that is affected is 2.10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Symphony. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Hospitality Symphony accessible data as well as unauthorized access to critical data or complete access to all Oracle Hospitality Symphony accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Hospitality Symphony. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L).	2019-01-16	6.8	<a href="#">CVE-2019-2402</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hospitality_symphony	Vulnerability in the Oracle Hospitality Symphony component of Oracle Food and Beverage Applications. The supported version that is affected is 2.10. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Symphony. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Symphony accessible data as well as unauthorized read access to a subset of Oracle Hospitality Symphony accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2019-2403</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- http_server	Vulnerability in the Oracle HTTP Server component of Oracle Fusion Middleware (subcomponent: Web Listener). The supported version that is affected is 12.2.1.3. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle HTTP Server executes to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in takeover of Oracle HTTP Server. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2414</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- hyperion_bi+	Vulnerability in the Hyperion BI+ component of Oracle Hyperion (subcomponent: Foundation UI & Servlets). The supported version that is affected is 11.1.2.4. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Hyperion BI+ accessible data as well as unauthorized read access to a subset of Hyperion BI+ accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Hyperion BI+. CVSS 3.0 Base Score 4.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:L).	2019-01-16	6.0	<a href="#">CVE-2019-2415</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- jdk	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u201, 8u192 and 11 0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2422</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are			

oracle -- jdk	Java SE: 7u201, 8u192 and 11 0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2426</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2420</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2434</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).	2019-01-16	5.5	<a href="#">CVE-2019-2436</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2455</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2481</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2482</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2486</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2494</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high			<a href="#">CVE-2019-</a>

oracle -- mysql	privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">2495</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2502</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2507</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2510</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2528</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2529</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2530</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2531</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2532</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2533</a> <a href="#">CONF RM</a> <a href="#">CONF RM</a>
	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior.			



oracle -- mysql	Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2019-01-16	5.5	<a href="#">CVE-2019-2534</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2537</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 8.0.13 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	4.0	<a href="#">CVE-2019-2539</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">CONF RM</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H).	2019-01-16	5.8	<a href="#">CVE-2019-2429</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).	2019-01-16	6.4	<a href="#">CVE-2019-2456</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2457</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2458</a> <a href="#">CONF RM</a> <a href="#">BID</a>
	Vulnerability in the Oracle Outside In Technology component of Oracle			

oracle -- outside_in_technology	Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2459 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2460 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2461 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. While the vulnerability is in Oracle Outside In Technology, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.2 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:L).	2019-01-16	6.4	<a href="#">CVE-2019-2462 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	2019-01-16	6.4	<a href="#">CVE-2019-2463 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Confidentiality	2019-01-16	5.0	<a href="#">CVE-2019-2464 CONF RM BID</a>

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2465</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2466</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2467</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2468</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology and unauthorized read access to a subset of Oracle Outside In Technology accessible data. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H).	2019-01-16	5.8	<a href="#">CVE-2019-2469</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the	2019-01-16	5.0	<a href="#">CVE-2019-2472</a> <a href="#">CONF RM</a> <a href="#">BID</a>

	CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:L).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2473</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2474</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2475</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2476</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2477</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability	2019-01-16	5.0	<a href="#">CVE-2019-2478</a> <a href="#">CONF RM</a> <a href="#">BID</a>

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).			
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	5.0	<a href="#">CVE-2019-2479 CONF RM BID</a>
oracle -- outside_in_technology	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). Supported versions that are affected are 8.5.3 and 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).	2019-01-16	5.0	<a href="#">CVE-2019-2480 CONF RM BID</a>
oracle -- peoplesoft_enterprise	Vulnerability in the PeopleSoft Enterprise SCM eProcurement component of Oracle PeopleSoft Products (subcomponent: Manage Requisition Status). The supported version that is affected is 9.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise SCM eProcurement. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise SCM eProcurement, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise SCM eProcurement accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise SCM eProcurement accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2519 CONF RM BID</a>
oracle -- peoplesoft_enterprise_cost_center_common_application_objects	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects component of Oracle PeopleSoft Products (subcomponent: Form and Approval Builder). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CC Common Application Objects. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise CC Common Application Objects, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CC Common Application Objects accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CC Common Application Objects accessible data. Note: This Enterprise Common Component is used by all PeopleSoft Application products. Please refer to the <a target=" _blank" href="https://support.oracle.com/rs?type=doc&id=2487756.1">MOS Note Doc ID 2493366.1 for patch information. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	4.9	<a href="#">CVE-2019-2419 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2404 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Security). Supported versions that are affected are 8.55, 8.56 and 8.57. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.0	<a href="#">CVE-2019-2405 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Feeds). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the	2019-01-	4.3	<a href="#">CVE-2019-2408</a>



	attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N).	16		<a href="#">CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Application Server). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2416 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Performance Monitor). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2019-2417 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Search). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2423 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: XML Publisher). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2433 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2439 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Fluid Core). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2442 CONF RM BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: XML Publisher). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2443 CONF RM BID</a>
	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Portal). Supported versions that are affected are 8.55, 8.56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful			

oracle -- peoplesoft_enterprise_peopletools	attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2471</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: Panel Processor). Supported versions that are affected are 8.55, 8 56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).	2019-01-16	4.3	<a href="#">CVE-2019-2490</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- peoplesoft_enterprise_peopletools	Vulnerability in the PeopleSoft Enterprise PeopleTools component of Oracle PeopleSoft Products (subcomponent: PIA Search Functionality). Supported versions that are affected are 8.55, 8 56 and 8.57. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2499</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- primavera_p6_enterprise_project_portfolio_management	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management component of Oracle Construction and Engineering Suite (subcomponent: Web Access). Supported versions that are affected are 8.4, 15.1, 15 2, 16.1, 16.2, 17.7-17.12 and 18.8. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primavera P6 Enterprise Project Portfolio Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Primavera P6 Enterprise Project Portfolio Management, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Primavera P6 Enterprise Project Portfolio Management accessible data as well as unauthorized read access to a subset of Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2512</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- reports_developer	Vulnerability in the Oracle Reports Developer component of Oracle Fusion Middleware (subcomponent: Valid Session). The supported version that is affected is 12.2.1 3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Reports Developer. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Reports Developer, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Reports Developer accessible data as well as unauthorized read access to a subset of Oracle Reports Developer accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	2019-01-16	5.8	<a href="#">CVE-2019-2413</a> <a href="#">CONF RM</a> <a href="#">BID</a> <a href="#">EXPLOIT-DB</a>
oracle -- retail_merchandising_system	Vulnerability in the Oracle Retail Merchandising System component of Oracle Retail Applications (subcomponent: Security (SQL Logger)). The supported version that is affected is 14.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Retail Merchandising System. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Retail Merchandising System accessible data as well as unauthorized read access to a subset of Oracle Retail Merchandising System accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	6.4	<a href="#">CVE-2018-3125</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- sun_zfs_storage_appliance_kit	Vulnerability in the Sun ZFS Storage Appliance Kit (AK) component of Oracle Sun Systems Products Suite (subcomponent: Object Store). The supported version that is affected is prior to 8.8 2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Sun ZFS Storage Appliance Kit (AK) executes to compromise Sun ZFS Storage Appliance Kit (AK). Successful attacks of this vulnerability can result in takeover of Sun ZFS Storage Appliance Kit (AK). CVSS 3.0 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:L/H:A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2412</a> <a href="#">CONF RM</a> <a href="#">BID</a>
	Vulnerability in the Oracle Transportation Management component of Oracle Supply Chain Products Suite (subcomponent: UI Infrastructure). Supported versions that are affected are 6.3.7, 6.4.1, 6.4 2 and 6.4.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle	2019-01-		<a href="#">CVE-2019-2487</a>

oracle -- transportation_management	Transportation Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Transportation Management accessible data. CVSS 3.0 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).	16	4.0	<a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). The supported version that is affected is prior to 5.2.22. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2018-3309</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2500</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	2019-01-16	4.9	<a href="#">CVE-2019-2508</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	2019-01-16	4.9	<a href="#">CVE-2019-2509</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2520</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2521</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2522</a> <a href="#">CONF RM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2523</a> <a href="#">CONF RM</a>

	Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).			BID
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2524</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	2019-01-16	4.4	<a href="#">CVE-2019-2526</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2548</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.0 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/H/I:H/A:H).	2019-01-16	4.6	<a href="#">CVE-2019-2552</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- web_cache	Vulnerability in the Oracle Web Cache component of Oracle Fusion Middleware (subcomponent: ESI/Partial Page Caching). The supported version that is affected is 11.1.1.9.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Web Cache. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Web Cache, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Web Cache accessible data as well as unauthorized update, insert or delete access to some of Oracle Web Cache accessible data. CVSS 3.0 Base Score 6.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:L/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2438</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- webcenter_portal	Vulnerability in the Oracle WebCenter Portal component of Oracle Fusion Middleware (subcomponent: WebCenter Spaces Application). Supported versions that are affected are 11.1.1.9.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCenter Portal accessible data. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2427</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). The supported version that is affected is 10.3.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L).	2019-01-16	5.5	<a href="#">CVE-2019-2395</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Deployment). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	2019-01-16	4.0	<a href="#">CVE-2019-2398</a> <a href="#">CONF RM</a> <a href="#">BID</a>
	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components).			

oracle -- weblogic_server	Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/L:I/A:L).	2019-01-16	6.8	<a href="#">CVE-2019-2418</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Application Container - JavaEE). The supported version that is affected is 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	2019-01-16	5.0	<a href="#">CVE-2019-2441</a> <a href="#">CONF RM</a> <a href="#">BID</a>
oracle -- weblogic_server	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H).	2019-01-16	6.5	<a href="#">CVE-2019-2452</a> <a href="#">CONF RM</a> <a href="#">BID</a>
premiumwpsuite -- easy_redirect_manager	The Premium WP Suite Easy Redirect Manager plugin 28.07-17 for WordPress has XSS via a crafted GET request that is mishandled during log viewing at the templates/admin/redirect-log.php URI.	2019-01-14	4.3	<a href="#">CVE-2019-6267</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
shopware -- shopware	Shopware before 5.4.3 allows SQL Injection by remote authenticated users, aka SW-21404.	2019-01-15	6.5	<a href="#">CVE-2018-20713</a> <a href="#">MISC</a>
tiki -- tikiwiki_cms/groupware	In Tiki before 17.2, the user task component is vulnerable to a SQL Injection via the tiki-user_tasks.php show_history parameter.	2019-01-15	6.5	<a href="#">CVE-2018-20719</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	2.1	<a href="#">CVE-2018-4255</a> <a href="#">CONFIRM</a>
apple -- mac_os_x	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	2.1	<a href="#">CVE-2018-4256</a> <a href="#">CONFIRM</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in color_templates.php in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Name field for a Color.	2019-01-16	3.5	<a href="#">CVE-2018-20723</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in pollers.php in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Website Hostname for Data Collectors.	2019-01-16	3.5	<a href="#">CVE-2018-20724</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in graph_templates.php in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Graph Vertical Label.	2019-01-16	3.5	<a href="#">CVE-2018-20725</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cacti -- cacti	A cross-site scripting (XSS) vulnerability exists in host.php (via tree.php) in Cacti before 1.2.0 due to lack of escaping of unintended characters in the Website Hostname field for Devices.	2019-01-16	3.5	<a href="#">CVE-2018-20726</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cubecart -- cubecart	CubeCart 6.2.2 has Reflected XSS via a /{ADMIN-FILE}/ query string.	2019-01-13	3.5	<a href="#">CVE-2018-20703</a> <a href="#">MISC</a>
ibm -- spss_analytic_server	IBM SPSS Analytic Server 3.1.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 148689.	2019-01-15	3.5	<a href="#">CVE-2018-1772</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2019-</a>



joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate checks of the Global Configuration helpurl settings allowed stored XSS.	2019-01-16	<a href="#">3.5</a>	<a href="#">6262 BID CONFIRM</a>
joomla -- joomla!	An issue was discovered in Joomla! before 3.9.2. Inadequate checks of the Global Configuration Text Filter settings allowed stored XSS.	2019-01-16	<a href="#">3.5</a>	<a href="#">CVE-2019-6263 BID CONFIRM EXPLOIT-DB</a>
jpress -- jpress	XSS exists in JPress v1.0.4 via Markdown input, or Markdown input with the code input option.	2019-01-14	<a href="#">3.5</a>	<a href="#">CVE-2019-6278 MISC</a>
oracle -- database_server	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java VM. CVSS 3.0 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L).	2019-01-16	<a href="#">3.5</a>	<a href="#">CVE-2019-2547 CONFIRM BID</a>
oracle -- hospitality_cruise_shipboard_property_management_system	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: SPMS Suite). The supported version that is affected is 8.0.8. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle Hospitality Cruise Shipboard Property Management System executes to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Hospitality Cruise Shipboard Property Management System, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Cruise Shipboard Property Management System as well as unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Shipboard Property Management System accessible data and unauthorized read access to a subset of Oracle Hospitality Cruise Shipboard Property Management System accessible data. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:C/L/I:L/A:H).	2019-01-16	<a href="#">3.3</a>	<a href="#">CVE-2019-2409 CONFIRM BID</a>
oracle -- hospitality_cruise_shipboard_property_management_system	Vulnerability in the Oracle Hospitality Cruise Shipboard Property Management System component of Oracle Hospitality Applications (subcomponent: DGS RES Online, FMS Sender, FMS Receiver, OHC WPF Security). The supported version that is affected is 8.0.8. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Hospitality Cruise Shipboard Property Management System executes to compromise Oracle Hospitality Cruise Shipboard Property Management System. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Cruise Shipboard Property Management System accessible data as well as unauthorized read access to a subset of Oracle Hospitality Cruise Shipboard Property Management System accessible data. CVSS 3.0 Base Score 5.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	<a href="#">3.6</a>	<a href="#">CVE-2019-2410 CONFIRM BID</a>
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Report privilege with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized read access to a subset of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 4.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	2019-01-16	<a href="#">3.6</a>	<a href="#">CVE-2019-2397 CONFIRM BID</a>
oracle -- hospitality_reporting_and_analytics	Vulnerability in the Oracle Hospitality Reporting and Analytics component of Oracle Food and Beverage Applications. The supported version that is affected is 9.1.0. Easily exploitable vulnerability allows low privileged attacker having Report privilege with logon to the infrastructure where Oracle Hospitality Reporting and Analytics executes to compromise Oracle Hospitality Reporting and Analytics. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Reporting and Analytics accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Reporting and Analytics accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).	2019-01-16	<a href="#">3.6</a>	<a href="#">CVE-2019-2407 CONFIRM BID</a>
	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). The supported version that is affected is Java SE: 8u192. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a			<a href="#">CVE-2019-</a>

oracle -- jdk	partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).	2019-01-16	2.6	<a href="#">2449</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).	2019-01-16	3.8	<a href="#">CVE-2019-2503</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Shell). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 2.5 (Confidentiality impacts). CVSS Vector: (CVSS 3.0/AV:L/AC:H/PR:L/UI:R/S:C/C:L/I:N/A:N).	2019-01-16	1.2	<a href="#">CVE-2019-2513</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS 3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	2019-01-16	1.9	<a href="#">CVE-2019-2535</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- mysql	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 8.0.13 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.0 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:N/A:H).	2019-01-16	1.2	<a href="#">CVE-2019-2536</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
oracle -- peoplesoft_enterprise_campus_software_campus_community	Vulnerability in the PeopleSoft Enterprise CS Campus Community component of Oracle PeopleSoft Products (subcomponent: Frameworks). Supported versions that are affected are 9.0 and 9.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise CS Campus Community. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CS Campus Community accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS 3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).	2019-01-16	2.6	<a href="#">CVE-2019-2493</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2446</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2448</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise			<a href="#">CVE-2019-</a>

oracle -- vm_virtualbox	Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">2450 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2451 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2501 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2504 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2505 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2506 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 5.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	1.9	<a href="#">CVE-2019-2525 CONFIRM BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).	2019-01-16	2.1	<a href="#">CVE-2019-2527 CONFIRM BID</a>
	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable			

oracle -- vm_virtualbox	vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 3 8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2553</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2554</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2555</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
oracle -- vm_virtualbox	Vulnerability in the Oracle VM VirtualBox component of Oracle Virtualization (subcomponent: Core). Supported versions that are affected are prior to 5.2.24 and prior to 6.0.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).	2019-01-16	2.1	<a href="#">CVE-2019-2556</a> <a href="#">CONFIRM</a> <a href="#">BID</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- relion_630_devices	ABB Relion 630 devices 1.1 before 1.1.0.C0, 1.2 before 1.2.0.B3, and 1.3 before 1.3.0.A6 allow remote attackers to cause a denial of service (reboot) via a reboot command in an SPA message.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20720</a> <a href="#">CONFIRM</a> <a href="#">BID</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19711</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19719</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19717</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19716</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19715</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19714</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19713</a> <a href="#">BID</a>

[illegible]



[illegible]

[illegible]

[illegible]

adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16039</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16027</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16029</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16030</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16031</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16032</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16033</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16034</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16035</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16036</a> BID CONFIRM
adobe -- acrobat_and_reader	Adobe Acrobat and Reader versions 2019.008.20081 and earlier, 2019.008.20080 and earlier, 2019.008.20081 and earlier, 2017.011.30106 and earlier version, 2017.011.30105 and earlier version, 2015.006.30457 and earlier, and 2015.006.30456 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-16028</a> BID CONFIRM
adobe -- connect	Adobe Connect versions 9.8.1 and earlier have a session token exposure vulnerability. Successful exploitation could lead to exposure of the privileges granted to a session.	2019-01-18	not yet calculated	<a href="#">CVE-2018-19718</a> BID CONFIRM
adobe -- digital_editions	Adobe Digital Editions versions 4.5.9 and below have an out of bounds read vulnerability. Successful exploitation could lead to information disclosure.	2019-01-18	not yet calculated	<a href="#">CVE-2018-12817</a> BID CONFIRM
adobe -- flash_player	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.	2019-01-18	not yet calculated	<a href="#">CVE-2018-15982</a> BID REDHAT CONFIRM EXPLOIT-DB
adobe -- flash_player	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation.	2019-01-18	not yet calculated	<a href="#">CVE-2018-15983</a> BID CONFIRM
apple -- multiple_products	In iOS before 11.4, iCloud for Windows before 7.5, watchOS before 4.3.1, iTunes before 12.7.5 for Windows, and macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4194</a> MISC CONFIRM
apple -- multiple_products	In iOS before 11.3, tvOS before 11.3, watchOS before 4.3, and macOS before High Sierra 10.13.4, an information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4185</a> MISC MISC CONFIRM MISC
atlassian -- universal_plugin_manager	The Upload add-on resource in Atlassian Universal Plugin Manager before version 2.22.14 allows remote attackers who have system administrator privileges to read files, make network requests and perform a denial of service attack via an XML External Entity vulnerability in the parsing of atlassian plugin xml files in an uploaded JAR.	2019-01-18	not yet calculated	<a href="#">CVE-2018-20233</a> CONFIRM
ceph -- ceph	It was found Ceph versions before 13.2.4 that authenticated ceph users with read only permissions could steal dm-crypt encryption keys used in ceph disk encryption.	2019-01-15	not yet calculated	<a href="#">CVE-2018-14662</a> CONFIRM MISC
ceph -- ceph	It was found in Ceph versions before 13.2.4 that authenticated ceph RGW	2019-01-15	not yet	<a href="#">CVE-2018-16846</a> CONFIRM

	users can cause a denial of service against OMAPs holding bucket indices.		calculated	MISC
cisco -- 900_series_aggregation_services_router	A vulnerability in Cisco 900 Series Aggregation Services Router (ASR) software could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient handling of certain broadcast packets ingress to the device. An attacker could exploit this vulnerability by sending large streams of broadcast packets to an affected device. If successful, an exploit could allow an attacker to impact services running on the device, resulting in a partial DoS condition.	2019-01-11	not yet calculated	<a href="#">CVE-2018-15464</a> BID <a href="#">CISCO</a>
cubecart -- cubecart	CubeCart before 6.1.13 has SQL Injection via the validate[] parameter of the "I forgot my Password!" feature.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20716</a> MISC
dell -- networking_os10	Dell Networking OS10 versions prior to 10.4.3.0 contain a vulnerability in the Phone Home feature which does not properly validate the server's certificate authority during TLS handshake. Use of an invalid or malicious certificate could potentially allow an attacker to spoof a trusted entity by using a man-in-the-middle (MITM) attack.	2019-01-18	not yet calculated	<a href="#">CVE-2018-15784</a> MISC
drupal -- drupal	In Drupal 8 prior to 8.3.7; When using the REST API, users without the correct permission can post comments via REST that are approved even if the user does not have permission to post approved comments. This issue only affects sites that have the RESTful Web Services (rest) module enabled, the comment entity REST resource enabled, and where an attacker can access a user account on the site with permissions to post comments, or where anonymous users can post comments.	2019-01-15	not yet calculated	<a href="#">CVE-2017-6924</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a>
drupal -- drupal	In versions of Drupal 8 core prior to 8.3.7; There is a vulnerability in the entity access system that could allow unwanted access to view, create, update, or delete entities. This only affects entities that do not use or do not have UUIDs, and entities that have different access restrictions on different revisions of the same entity.	2019-01-15	not yet calculated	<a href="#">CVE-2017-6925</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a>
drupal -- drupal	In Drupal 8 prior to 8.3.4; The file REST resource does not properly validate some fields when manipulating files. A site is only affected by this if the site has the RESTful Web Services (rest) module enabled, the file REST resource is enabled and allows PATCH requests, and an attacker can get or register a user account on the site with permissions to upload files and to modify the file resource.	2019-01-15	not yet calculated	<a href="#">CVE-2017-6921</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a>
etcd -- etcd	etcd versions 3.2.x before 3.2.26 and 3.3.x before 3.3.11 are vulnerable to an improper authentication issue when role-based access control (RBAC) is used and client-cert-auth is enabled. If an etcd client server TLS certificate contains a Common Name (CN) which matches a valid RBAC username, a remote attacker may authenticate as that user with any valid (trusted) client certificate in a REST API request to the gRPC-gateway.	2019-01-14	not yet calculated	<a href="#">CVE-2018-16886</a> BID <a href="#">CONFIRM</a> MISC MISC
gnu -- binutils	A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU libiberty, as distributed in GNU Binutils 2.31.1. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by c++filt.	2019-01-14	not yet calculated	<a href="#">CVE-2018-20712</a> BID MISC MISC
ibm -- security_identity_manager	IBM Security Identity Manager 6.0.0 Virtual Appliance is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 155265.	2019-01-18	not yet calculated	<a href="#">CVE-2018-2019</a> BID XF <a href="#">CONFIRM</a>
isc -- bind	Mistaken assumptions about the ordering of records in the answer section of a response containing CNAME or DNAME resource records could lead to a situation in which named would exit with an assertion failure when processing a response in which records occurred in an unusual order. Affects BIND 9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0-P3, 9.11.1b1->9.11.1rc1, and 9.9.9-S8.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3137</a> BID <a href="#">SECTrack</a> <a href="#">SECTrack</a> REDHAT REDHAT REDHAT <a href="#">CONFIRM</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> DEBIAN
isc -- bind	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name for the zone and service being targeted may be able to manipulate BIND into accepting an unauthorized dynamic update. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.10-S2, 9.10.5-S1->9.10.5-S2.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3143</a> BID <a href="#">SECTrack</a> REDHAT REDHAT <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> DEBIAN
isc -- bind	The BIND installer on Windows uses an unquoted service path which can enable a local user to achieve privilege escalation if the host file system permissions allow this. Affects BIND 9.2.6-P2->9.2.9, 9.3.2-P1->9.3.6, 9.4.0->9.8.8, 9.9.0->9.10, 9.10.0->9.10.5, 9.11.0->9.11.1, 9.9.3-S1->9.10-S1, 9.10.5-S1.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3141</a> BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> EXPLOIT-DB
isc -- bind	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name may be able to circumvent TSIG authentication of AXFR requests via a carefully constructed request packet. A server that relies solely on TSIG keys for protection with no other ACL protection could be manipulated into: providing an AXFR of a zone to an unauthorized recipient or accepting bogus NOTIFY packets. Affects BIND 9.4.0->9.8.8, 9.9.0->9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.10-S2, 9.10.5-S1->9.10.5-S2.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3142</a> BID <a href="#">SECTrack</a> REDHAT REDHAT <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> DEBIAN
isc -- bind	Under some conditions when using both DNS64 and RPZ to rewrite query responses, query processing can resume in an inconsistent state leading to either an INSIST assertion failure or an attempt to read through a NULL pointer. Affects BIND 9.8.8, 9.9.3-S1->9.9.9-S7, 9.9.3->9.9.9-P5, 9.9.10b1,	2019-01-16	not yet calculated	<a href="#">CVE-2017-3135</a> REDHAT BID <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>



	9.10.0 -> 9.10.4-P5, 9.10.5b1, 9.11.0 -> 9.11.0-P2, 9.11.1b1.			<a href="#">GENTOO CONFIRM</a> <a href="#">DEBIAN</a>
isc -- bind	If named is configured to use Response Policy Zones (RPZ) an error processing some rule types can lead to a condition where BIND will endlessly loop while handling a query. Affects BIND 9.9.10, 9.10.5, 9.11.0->9.11.1, 9.10-S1, 9.10.5-S1.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3140 BID</a> <a href="#">SECTrack CONFIRM</a> <a href="#">GENTOO CONFIRM</a>
isc -- bind	named contains a feature which allows operators to issue commands to a running server by communicating with the server process over a control channel, using a utility program such as rndc. A regression introduced in a recent feature change has created a situation under which some versions of named can be caused to exit with a REQUIRE assertion failure if they are sent a null command string. Affects BIND 9.9.9-P7, 9.10b1->9.10rc2, 9.10.4->9.10.4-P7, 9.10.5b1->9.10.5rc2, 9.11.0->9.11.0-P4, 9.11.1b1->9.11.1rc2, 9.9.9-S1->9.9.9-S9.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3138 BID</a> <a href="#">SECTrack CONFIRM</a> <a href="#">GENTOO CONFIRM</a> <a href="#">DEBIAN</a>
isc -- bind	A query with a specific set of characteristics could cause a server using DNS64 to encounter an assertion failure and terminate. An attacker could deliberately construct a query, enabling denial-of-service against a server if it was configured to use the DNS64 feature and other preconditions were met. Affects BIND 9.8.0 -> 9.8.8-P1, 9.9.0 -> 9.9.9-P6, 9.10b1->9.10rc1, 9.10.0 -> 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0 -> 9.11.0-P3, 9.11.1b1->9.11.1rc1, 9.9.3-S1 -> 9.9.9-S8.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3136 BID</a> <a href="#">SECTrack REDHAT</a> <a href="#">REDHAT CONFIRM</a> <a href="#">GENTOO CONFIRM</a> <a href="#">DEBIAN</a>
isc -- bind	An error in handling certain queries can cause an assertion failure when a server is using the nxdomain-redirect feature to cover a zone for which it is also providing authoritative service. A vulnerable server could be intentionally stopped by an attacker if it was using a configuration that met the criteria for the vulnerability and if the attacker could cause it to accept a query that possessed the required attributes. Please note: This vulnerability affects the "nxdomain-redirect" feature, which is one of two methods of handling NXDOMAIN redirection, and is only available in certain versions of BIND. Redirection using zones of type "redirect" is not affected by this vulnerability. Affects BIND 9.9.8-S1 -> 9.9.8-S3, 9.9.9-S1 -> 9.9.9-S6, 9.11.0-9.11.0-P1.	2019-01-16	not yet calculated	<a href="#">CVE-2016-9778 BID</a> <a href="#">SECTrack CONFIRM</a> <a href="#">GENTOO CONFIRM</a>
isc -- bind	BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named. Affects BIND 9.0.0 to 9.8.x, 9.9.0 to 9.11.1, 9.10.0 to 9.10.6, 9.11.0 to 9.11.2, 9.9.3-S1 to 9.11-S1, 9.10.5-S1 to 9.10.6-S1, 9.12.0a1 to 9.12.0rc1.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3145 BID</a> <a href="#">SECTrack REDHAT</a> <a href="#">REDHAT CONFIRM</a> <a href="#">MLIST CONFIRM</a> <a href="#">DEBIAN</a>
isc -- dhcp	A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of socket descriptors available to the DHCP server. Affects ISC DHCP 4.1.0 to 4.1-ESV-R15, 4.2.0 to 4.2.8, 4.3.0 to 4.3.6. Older versions may also be affected but are well beyond their end-of-life (EOL). Releases prior to 4.1.0 have not been tested.	2019-01-16	not yet calculated	<a href="#">CVE-2017-3144 BID</a> <a href="#">SECTrack REDHAT</a> <a href="#">CONFIRM UBUNTU</a> <a href="#">DEBIAN</a>
limesurvey -- limesurvey	LimeSurvey before 2.72.4 has Stored XSS by using the Continue Later (aka Resume later) feature to enter an email address, which is mishandled in the admin panel.	2019-01-15	not yet calculated	<a href="#">CVE-2017-18358 MISC</a> <a href="#">MISC</a>
mailenable -- mailenable	MailEnable before 8.60 allows Privilege Escalation because admin accounts could be created as a consequence of %0A mishandling in AUTH.TAB after a password-change request.	2019-01-16	not yet calculated	<a href="#">CVE-2015-9278 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- ned	A stored cross site scripting (XSS) vulnerability in NeDi before 1.7Cp3 allows remote attackers to inject arbitrary web script or HTML via User-Chat.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20731 MISC</a> <a href="#">MISC</a>
nedi_consulting -- ned	A SQL injection vulnerability in NeDi before 1.7Cp3 allows any user to execute arbitrary SQL read commands via the query.php component.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20730 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- ned	A reflected cross site scripting (XSS) vulnerability in NeDi before 1.7Cp3 allows remote attackers to inject arbitrary web script or HTML via the reg parameter in mh.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20729 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- ned	A cross site request forgery (CSRF) vulnerability in NeDi before 1.7Cp3 allows remote attackers to escalate privileges via User-Management.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20728 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
nedi_consulting -- ned	Multiple command injection vulnerabilities in NeDi before 1.7Cp3 allow authenticated users to execute code on the server side via the fit parameter to Nodes-Traffic.php, the dv parameter to Devices-Graph.php, or the tit parameter to drawmap.php.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20727 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
oxid -- esales	The DB abstraction layer of OX D eSales 4.10.6 is vulnerable to SQL injection via the oxid or synchoxid parameter to the oxConfig::getRequestParameter() method in core/oxconfig.php.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20715 MISC</a> <a href="#">MISC</a>
prestashop -- prestashop	In the orders section of PrestaShop before 1.7.2.5, an attack is possible after gaining access to a target store with a user role with the rights of at least a Salesman or higher privileges. The attacker can then inject arbitrary PHP objects into the process and abuse an object chain in order to gain Remote Code Execution. This occurs because protection against serialized objects looks for a 0: followed by an integer, but does not consider 0:+ followed by an	2019-01-15	not yet calculated	<a href="#">CVE-2018-20717 MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>

	integer.			
pydio -- pydio	In Pydio before 8.2.2, an attack is possible via PHP Object Injection because a user is allowed to use the \$phpserial\$a:0:{} syntax to store a preference. An attacker either needs a "public link" of a file, or access to any unprivileged user account for creation of such a link.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20718</a> MISC
qualcomm -- snapdragon	While processing a packet decode request in MQTT, Race condition can occur leading to an out-of-bounds access in snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, SD 210/SD 212/SD 205, SD 427, SD 435, SD 450, SD 625, SD 636, SD 835, SDA660, SDM630, SDM660, Snapdragon_High_Med_2016	2019-01-18	not yet calculated	<a href="#">CVE-2018-11998</a> CONFIRM
qualcomm -- snapdragon	Spoofed SMS can be used to send a large number of messages to the device which will in turn initiate a flood of registration updates with the server in snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 625, SD 636, SDA660, SDM630, SDM660, SDX20	2019-01-18	not yet calculated	<a href="#">CVE-2018-11284</a> CONFIRM
qualcomm -- snapdragon	Security keys are logged when any WCDMA call is configured or reconfigured in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9607, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDX20, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2017-18332</a> BID CONFIRM
qualcomm -- snapdragon	Improper access control on secure display buffers in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, MSM8996AU, SD 210/SD 212/SD 205, SD 820, SD 820A, SD 835, SDA660	2019-01-18	not yet calculated	<a href="#">CVE-2017-18331</a> BID CONFIRM
qualcomm -- snapdragon	AGPS session failure in GNSS module due to cyphersuites are hardcoded and needed manual update everytime in snapdragon mobile and snapdragon wear in versions MDM9635M, MDM9645, MDM9650, MDM9655, MSM8909W, SD 835, SD 845, SD 850	2019-01-18	not yet calculated	<a href="#">CVE-2017-18160</a> BID CONFIRM
qualcomm -- snapdragon	Improper authorization involving a fuse in TrustZone in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 632, SD 636, SD 650/52, SD 810, SD 820, SD 820A, SD 835, SDA660, SDM439, SDM630, SDM660, SDX24, Snapdragon_High_Med_2016.	2019-01-18	not yet calculated	<a href="#">CVE-2017-8276</a> BID CONFIRM
qualcomm -- snapdragon	Improper check while accessing the local memory stack on MQTT connection request can lead to buffer overflow in snapdragon wear in versions MDM9206, MDM9607	2019-01-18	not yet calculated	<a href="#">CVE-2018-11993</a> CONFIRM
qualcomm -- snapdragon	Lack of check of input size can make device memory get corrupted because of buffer overflow in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9615, MDM9625, MDM9635M, MDM9640, MDM9645, MDM9650, MDM9655, MSM8909W, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 425, SD 427, SD 430, SD 435, SD 439 / SD 429, SD 450, SD 615/16/SD 415, SD 625, SD 636, SD 650/52, SD 712 / SD 710 / SD 670, SD 810, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM439, SDM630, SDM660, SDX20, Snapdragon_High_Med_2016, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2018-11279</a> BID CONFIRM
qualcomm -- snapdragon	Improper input validation in trustzone can lead to denial of service in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9635M, MDM9650, MDM9655, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 636, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDM630, SDM660, SDX24	2019-01-18	not yet calculated	<a href="#">CVE-2018-11999</a> BID CONFIRM
qualcomm -- snapdragon	Anti-rollback can be bypassed in replay scenario during app loading due to improper error handling of RPMB writes in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, MSM8996AU, SD 210/SD 212/SD 205, SD 425, SD 430, SD 450, SD 625, SD 650/52, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDA660, SDX24, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2018-3595</a> BID CONFIRM
qualcomm -- snapdragon	Possible undefined behavior due to lack of size check in function for parameter segment_idx can lead to a read outside of the intended region in snapdragon automobile, snapdragon mobile and snapdragon wear in versions MDM9206, MDM9607, MDM9650, MDM9655, MSM8996AU, SD 210/SD 212/SD 205, SD 410/12, SD 712 / SD 710 / SD 670, SD 820, SD 820A, SD 835, SD 845 / SD 850, SDX24, SXR1130	2019-01-18	not yet calculated	<a href="#">CVE-2018-11288</a> CONFIRM
rsa -- authentication_manager	The Quick Setup component of RSA Authentication Manager versions prior to 8.4 is vulnerable to a relative path traversal vulnerability. A local attacker could potentially provide an administrator with a crafted license that if used during the quick setup deployment of the initial RSA Authentication Manager system, could allow the attacker unauthorized access to that system.	2019-01-16	not yet calculated	<a href="#">CVE-2018-15782</a> FULLDISC
sas -- web_infrastructure_platform	SAS Web Infrastructure Platform before 9.4M6 allows remote attackers to execute arbitrary code via a Java deserialization variant.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20732</a> BID MISC
sas -- web_infrastructure_platform	BI Web Services in SAS Web Infrastructure Platform before 9.4M6 allows XXE.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20733</a> MISC
sas -- web_infrastructure_platform	Logon Manager in SAS Web Infrastructure Platform before 9.4M3 allows reflected XSS on the Timeout page.	2019-01-16	not yet calculated	<a href="#">CVE-2015-9281</a> MISC
serendipity -- serendipity	Serendipity 2.0.4 has XSS via the serendipity_admin.php serendipity[body] parameter.	2019-01-15	not yet calculated	<a href="#">CVE-2016-10737</a> EXPLOIT-DB
shopware -- shopware	Shopware before 5.3.4 has a PHP Object Instantiation issue via the sort parameter to the loadPreviewAction() method of the Shopware_Controllers_Backend_ProductStream controller, with resultant XXE via instantiation of a SimpleXMLElement object.	2019-01-15	not yet calculated	<a href="#">CVE-2017-18357</a> MISC MISC
smartertools -- smartermail	SmarterTools SmarterMail before 13.3.5535 was vulnerable to stored XSS by bypassing the anti-XSS mechanisms. It was possible to run JavaScript code when a victim user opens or replies to the attacker's email, which contained a malicious payload. Therefore, users' passwords could be reset by using an XSS attack, as the password reset page did not need the current password.	2019-01-16	not yet calculated	<a href="#">CVE-2015-9276</a> MISC MISC MISC

systemd -- systemd-journald	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16866</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
systemd -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16864</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
systemd -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16865</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a> <a href="#">MISC</a>
systemd -- systemd	It was discovered systemd does not correctly check the content of P DFile files before using it to kill processes. When a service is run from an unprivileged user (e.g. User field set in the service file), a local attacker who is able to write to the PIDFile of the mentioned service may use this flaw to trick systemd into killing other services and/or privileged processes. Versions before v237 are vulnerable.	2019-01-14	not yet calculated	<a href="#">CVE-2018-16888</a> <a href="#">CONFIRM</a>
tibco -- spotfire	The Spotfire Library component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace, and T BCO Spotfire Server contains a vulnerability that might theoretically fail to restrict users with read-only access from modifying files stored in the Spotfire Library, only when the Spotfire Library is configured to use external storage. Affected releases are TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace versions up to and including 10.0.0, and T BCO Spotfire Server versions up to and including 7.10.1; 7.11.0; 7.11.1; 7.12.0; 7.13 0; 7.14.0; 10 0 0.	2019-01-16	not yet calculated	<a href="#">CVE-2018-18812</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- spotfire	The Spotfire web server component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace, and T BCO Spotfire Server contains multiple vulnerabilities that may allow persistent and reflected cross-site scripting attacks. Affected releases are T BCO Software Inc. TIBCO Spotfire Analytics Platform for AWS Marketplace: versions up to and including 10.0.0, and TIBCO Spotfire Server: versions up to and including 7.10.1; 7.11.0; 7.11.1; 7.12.0; 7.13.0; 7.14.0; 10.0.0.	2019-01-16	not yet calculated	<a href="#">CVE-2018-18813</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- spotfire	The TIBCO Spotfire authentication component of TIBCO Software Inc.'s TIBCO Spotfire Analytics Platform for AWS Marketplace, and TIBCO Spotfire Server contains a vulnerability in the handling of the authentication that theoretically may allow an attacker to gain full access to a target account, independent of configured authentication mechanisms. Affected releases are TIBCO Software Inc. TIBCO Spotfire Analytics Platform for AWS Marketplace: versions up to and including 10.0.0, and T BCO Spotfire Server: versions up to and including 7.10.1; 7.11.0; 7.11.1; 7.12.0; 7.13 0; 7.14.0.	2019-01-16	not yet calculated	<a href="#">CVE-2018-18814</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
uriparser -- uriparser	URI_FUNC() in UriParse c in uriparser before 0.9.1 has an out-of-bounds read (in uriParse*Ex* functions) for an incomplete URI with an Pv6 address containing an embedded IPv4 address, such as a "://[:44.1" address.	2019-01-16	not yet calculated	<a href="#">CVE-2018-20721</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
wordpress -- wordpress	The logging system of the Automattic WooCommerce plugin before 3.4.6 for WordPress is vulnerable to a File Deletion vulnerability. This allows deletion of woocommerce.php, which leads to certain privilege checks not being in place, and therefore a shop manager can escalate privileges to admin.	2019-01-15	not yet calculated	<a href="#">CVE-2018-20714</a> <a href="#">MISC</a>
wordpress -- wordpress	In the Automattic WooCommerce plugin before 3 2.4 for WordPress, an attack is possible after gaining access to the target site with a user account that has at least Shop manager privileges. The attacker then constructs a specifically crafted string that will turn into a PHP object injection involving the includes/shortcodes/class-wc-shortcode-products.php WC_Shortcode_Products: get_products() use of cached queries within shortcodes.	2019-01-15	not yet calculated	<a href="#">CVE-2017-18356</a> <a href="#">MISC</a> <a href="#">MISC</a>

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

**From:** [US-CERT](#)  
**To:** [Tanner McGinnis](#)  
**Subject:** SB19-014: Vulnerability Summary for the Week of January 7, 2019  
**Date:** Monday, January 14, 2019 1:58:49 PM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## SB19-014: Vulnerability Summary for the Week of January 7, 2019

01/14/2019 06:27 AM EST

Original release date: January 14, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge.	2019-01-08	7.6	<a href="#">CVE-2019-0565</a> B.D <a href="#">CONFIRM</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arc_project -- arc	ARC 5.21q allows directory traversal via a full pathname in an archive file.	2019-01-07	5.0	<a href="#">CVE-2015-9275</a> MISC MISC
getbootstrap -- bootstrap	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	2019-01-09	4.3	<a href="#">CVE-2016-10735</a> MISC MISC MISC MISC MISC
ibm -- api_connect	BM API Connect 5.0.0.0 through 5.0.8.4 could allow a user authenticated as an administrator with limited rights to escalate their privileges. IBM X-Force ID: 151258.	2019-01-04	6.5	<a href="#">CVE-2018-1859</a> B.D X.E <a href="#">CONFIRM</a>
microsoft -- asp_net_core	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka "ASP.NET Core Denial of Service Vulnerability." This affects ASP.NET Core 2.1. This CVE ID is unique from CVE-2019-0548.	2019-01-08	5.0	<a href="#">CVE-2019-0564</a> B.D REDHAT <a href="#">CONFIRM</a>
microsoft -- office	An information disclosure vulnerability exists when Microsoft Outlook improperly handles certain types of messages, aka "Microsoft Outlook Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Outlook.	2019-01-08	4.3	<a href="#">CVE-2019-0559</a> B.D <a href="#">CONFIRM</a>
microsoft -- office	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka "Microsoft Office Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office.	2019-01-08	4.3	<a href="#">CVE-2019-0560</a> B.D <a href="#">CONFIRM</a>
yunucms -- yunucms	YUNUCMS 1.1.8 has XSS in app/admin/controller/System.php because crafted data can be written to the sys.php file, as demonstrated by site_title in an admin/system/basic POST request.	2019-01-04	4.3	<a href="#">CVE-2019-5310</a> MISC
yunucms -- yunucms	An issue was discovered in YUNUCMS V1.1.8. app/index/controller/Show.php has an XSS vulnerability via the index.php/index/show/index_cw parameter.	2019-01-04	4.3	<a href="#">CVE-2019-5311</a> MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frog cms_project -- frog cms	Frog CMS 0.9.5 has XSS in the admin/?/page/edit/1 body field.	2019-01-09	3.5	<a href="#">CVE-2018-20680</a>

				MISC
ibm -- rational_publishing_engine	BM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-force ID: 144883.	2019-01-04	3.5	<a href="#">CVE-2018-1657</a> <a href="#">B.D</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>
ibm -- rational_publishing_engine	BM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153494.	2019-01-04	3.5	<a href="#">CVE-2018-1951</a> <a href="#">B.D</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- karaf	Apache Karaf provides a features deployer, which allows users to "hot deploy" a features XML by dropping the file directly in the deploy folder. The features XML is parsed by XMLInputFactory class. Apache Karaf XMLInputFactory class doesn't contain any mitigation codes against XXE. This is a potential security risk as an user can inject external XML entities in Apache Karaf version prior to 4.1.7 or 4.2.2. It has been fixed in Apache Karaf 4.1.7 and 4.2.2 releases.	2019-01-07	not yet calculated	<a href="#">CVE-2018-11788</a> <a href="#">MISC</a> <a href="#">B.D</a>
apache -- thrift	Apache Thrift Java client library versions 0.5.0 through 0.11.0 can bypass SASL negotiation isComplete validation in the org.apache.thrift.transport.TSaslTransport class. An assert used to determine if the SASL handshake had successfully completed could be disabled in production settings making the validation incomplete.	2019-01-07	not yet calculated	<a href="#">CVE-2018-1320</a> <a href="#">MISC</a>
apache -- thrift	The Apache Thrift Node.js static web server in versions 0.9.2 through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webservers docroot path.	2019-01-07	not yet calculated	<a href="#">CVE-2018-11798</a> <a href="#">B.D</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the Clean My Mac X, version 4.04, helper service due to improper input validation. A user with local access can use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4043</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4047</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the way the CleanMyMac X software improperly validates inputs. An attacker with local access could use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4032</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4033</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4034</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4045</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the running kernel extensions on the system.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4036</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access can use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4037</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4035</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable denial-of-service vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. A user with local access can use this vulnerability to terminate a privileged helper application. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4046</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4041</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4042</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4044</a> <a href="#">MISC</a>
apple -- ios	In iOS before 11.2, exchange rates were retrieved from HTTP rather than HTTPS. This was addressed by enabling HTTPS for exchange rates.	2019-01-11	not yet calculated	<a href="#">CVE-2017-2411</a> <a href="#">CONFIRM</a>
	In iOS before 11.4 and macOS High Sierra before 10.13.5, a memory	2019-01-	not yet	<a href="#">CVE-2018-4404</a> <a href="#">MISC</a>



apple -- ios	corruption issue exists and was addressed with improved memory handling.	11	calculated	<a href="#">CONFIRM</a> <a href="#">EXPLOIT-DB</a>
apple -- ios	In iOS before 11.2, an inconsistent user interface issue was addressed through improved state management.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13891</a> <a href="#">CONFIRM</a>
apple -- ios	In iOS before 11.2, a type confusion issue was addressed with improved memory handling.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13888</a> <a href="#">CONFIRM</a>
apple -- ios	In iOS before 11.4, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4330</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">CONFIRM</a>
apple -- ios	In iOS before 9.3.3, a memory corruption issue existed in the kernel. This issue was addressed through improved memory handling.	2019-01-11	not yet calculated	<a href="#">CVE-2016-7576</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4257</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4255</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an input validation issue existed in the kernel. This issue was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4254</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a privacy issue in the handling of Open Directory records was addressed with improved indexing.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4217</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4183</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions on CUPS.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4182</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4181</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4180</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved bounds checking.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4258</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4256</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.4, there was an issue with the handling of smartcard PNs. This issue was addressed with additional logic.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4179</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, an access issue existed with privileged WiFi system configuration. This issue was addressed with additional restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13886</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, a logic issue existed in APFS when deleting keys during hibernation. This was addressed with improved state management.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13887</a> <a href="#">CONFIRM</a>
apple -- multiple_products	In iOS before 11.4, iCloud for Windows before 7.5, watchOS before 4.3.1, iTunes before 12.7.5 for Windows, and macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4194</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a logic error existed in the validation of credentials. This was addressed with improved credential validation.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13889</a> <a href="#">CONFIRM</a>
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4169</a> <a href="#">CONFIRM</a>
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, sound fetched through audio elements may be exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4278</a> <a href="#">SECTRAK</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
apple -- multiple_products	In iOS before 11.4.1, watchOS before 4.3.2, tvOS before 11.4.1, Safari before 11.1.1, macOS High Sierra before 10.13.6, a spoofing issue existed in the handling of URLs. This issue was addressed with	2019-01-11	not yet calculated	<a href="#">CVE-2018-4277</a> <a href="#">SECTRAK</a> <a href="#">MISC</a> <a href="#">MISC</a>

	improved input validation.			MISC CONFIRM MISC
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, multiple memory corruption issues were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4262 SECTRACK GENTOO MISC CONFIRM MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4213 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a permissions issue existed in Remote Management. This issue was addressed through improved permission validation.	2019-01-11	not yet calculated	CVE-2018-4298 CONFIRM MISC
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4212 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, an array indexing issue existed in the handling of a function in javascript core. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4210 GENTOO MISC MISC CONFIRM UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4209 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4208 GENTOO MISC MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4207 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.2.5, macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, watchOS before 4.2.2, and tvOS before 11.2.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4189 CONFIRM MISC MISC
apple -- multiple_products	In iCloud for Windows before 7.3, Safari before 11.0.3, iTunes before 12.7.3 for Windows, and iOS before 11.2.5, multiple memory corruption issues exist and were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4147 CONFIRM MISC MISC MISC
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a downgrade issue existed with HTTP authentication credentials saved in Keychain. This issue was addressed by storing the authentication types with the credentials.	2019-01-11	not yet calculated	CVE-2016-4644 MISC MISC CONFIRM
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a validation issue existed in the parsing of 407 responses. This issue was addressed through improved response validation.	2019-01-11	not yet calculated	CVE-2016-4643 MISC MISC CONFIRM
	In iOS before 11.3, tvOS before 11.3, watchOS before 4.3, and			CVE-2018-4185

apple -- multiple_products	macOS before High Sierra 10.13.4, an information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling.	2019-01-11	not yet calculated	MISC <a href="#">MISC CONFIRM MISC</a>
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, proxy authentication incorrectly reported HTTP proxies received credentials securely. This issue was addressed through improved warnings.	2019-01-11	not yet calculated	<a href="#">CVE-2016-4642</a> MISC <a href="#">MISC CONFIRM</a>
apple -- safari	In Safari before 11.1, an information leakage issue existed in the handling of downloads in Safari Private Browsing. This issue was addressed with additional validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4186</a> <a href="#">CONFIRM</a>
apple -- swiftnio	In SwiftNIO before 1.8.0, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4281</a> <a href="#">CONFIRM</a>
artifex -- mupdf	Artifex MuPDF 1.14.0 has a SEGV in the function fz_load_page of the fitz/document.c file, as demonstrated by mutool. This is related to page-number mishandling in cbz/mucbz.c, cbz/mulimg.c, and svg/svg-doc.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6130</a> <a href="#">MISC</a>
artifex -- mupdf	svg-run.c in Artifex MuPDF 1.14.0 has infinite recursion with stack consumption in svg_run_use_symbol, svg_run_element, and svg_run_use, as demonstrated by mutool.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6131</a> <a href="#">MISC</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter or bootmode parameter of a certain URL.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0634</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via filename parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0635</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter of a certain URL, different URL from CVE-2018-0634.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0636</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via import cgi encKey parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0638</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via tools_firmware cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0639</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary code via netWizard.cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0640</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary code via tools_system cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0641</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via export cgi encKey parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0637</a> MISC <a href="#">JVN</a>
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via submit-url parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0633</a> MISC <a href="#">JVN</a>
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via HTTP request and response.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0632</a> MISC <a href="#">JVN</a>
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via targetAPSSid parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0631</a> MISC <a href="#">JVN</a>
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0629</a> MISC <a href="#">JVN</a>
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via sysCmd parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0630</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0628</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via targetAPSSid parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0627</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via sysCmd in formVsc parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0626</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via formSysCmd parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0625</a> MISC <a href="#">JVN</a>
bento4 -- bento4	An issue was discovered in Bento4 v1.5.1-627. There is a memory leak in AP4_DescriptorFactory::CreateDescriptorFromStream in Core/AP4DescriptorFactory.cpp when called from the AP4_EsdsAtom class in Core/AP4EsdsAtom.cpp, as demonstrated by mp42aac.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6132</a> <a href="#">MISC</a>

bodhi -- bodhi	Bodhi 2.9 0 and lower is vulnerable to cross-site scripting resulting in code injection caused by incorrect validation of bug titles.	2019-01-10	not yet calculated	<a href="#">CVE-2017-1002152</a> <a href="#">CONFIRM</a>
bootstrap -- bootstrap	In Bootstrap before 3.4 0, XSS is possible in the affix configuration target property.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20677</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bootstrap -- bootstrap	In Bootstrap before 3.4 0, XSS is possible in the tooltip data-viewport attribute.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20676</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
busybox -- busybox	An issue was discovered in BusyBox through 1 30 0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and/or relay) might allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to assurance of a 4-byte length when decoding DHCP_SUBNET. NOTE: this issue exists because of an incomplete fix for CVE-2018-20679.	2019-01-09	not yet calculated	<a href="#">CVE-2019-5747</a> <a href="#">MISC</a> <a href="#">MISC</a>
busybox -- busybox	An issue was discovered in BusyBox before 1 30 0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and relay) allows a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to verification in udhcp_get_option() in networking/udhcp/common.c that 4-byte options are indeed 4 bytes.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20679</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cimtechniques -- cimsan	In CIMTechniques C MScan 6 x through 6 2, the SOAP WSDL parser allows attackers to execute SQL code.	2019-01-10	not yet calculated	<a href="#">CVE-2018-16803</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- 900_series_aggregation_services_router	A vulnerability in Cisco 900 Series Aggregation Services Router (ASR) software could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient handling of certain broadcast packets ingress to the device. An attacker could exploit this vulnerability by sending large streams of broadcast packets to an affected device. If successful, an exploit could allow an attacker to impact services running on the device, resulting in a partial DoS condition.	2019-01-11	not yet calculated	<a href="#">CVE-2018-15464</a> <a href="#">CISCO</a>
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the Secure/Multipurpose Internet Mail Extensions (S/M ME) Decryption and Verification or S/M ME Public Key Harvesting features of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause an affected device to corrupt system memory. A successful exploit could cause the filtering process to unexpectedly reload, resulting in a denial of service (DoS) condition on the device. The vulnerability is due to improper input validation of S/M ME-signed emails. An attacker could exploit this vulnerability by sending a malicious S/MIME-signed email through a targeted device. If Decryption and Verification or Public Key Harvesting is configured, the filtering process could crash due to memory corruption and restart, resulting in a DoS condition. The software could then resume processing the same S/M ME-signed email, causing the filtering process to crash and restart again. A successful exploit could allow the attacker to cause a permanent DoS condition. This vulnerability may require manual intervention to recover the ESA.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15453</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) could allow an unauthenticated, remote attacker to cause the CPU utilization to increase to 100 percent, causing a denial of service (DoS) condition on an affected device. The vulnerability is due to improper filtering of email messages that contain references to whitelisted URLs. An attacker could exploit this vulnerability by sending a malicious email message that contains a large number of whitelisted URLs. A successful exploit could allow the attacker to cause a sustained DoS condition that could force the affected device to stop scanning and forwarding email messages.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15460</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	A vulnerability in the Shell Access Filter feature of Cisco Firepower Management Center (FMC), when used in conjunction with remote authentication, could allow an unauthenticated, remote attacker to cause high disk utilization, resulting in a denial of service (DoS) condition. The vulnerability occurs because the configuration of the Shell Access Filter, when used with a specific type of remote authentication, can cause a system file to have unbounded writes. An attacker could exploit this vulnerability by sending a steady stream of remote authentication requests to the appliance when the specific configuration is applied. Successful exploitation could allow the attacker to increase the size of a system log file so that it consumes most of the disk space. The lack of available disk space could lead to a DoS condition in which the device functions could operate abnormally, making the device unstable.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15458</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the Admin Portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to view saved passwords in plain text. The vulnerability is due to the incorrect inclusion of saved passwords when loading configuration pages in the Admin Portal. An attacker with read or write access to the Admin Portal could exploit this vulnerability by browsing to a page that contains sensitive data. An exploit could allow the attacker to recover passwords for unauthorized use and expose those accounts to further attack.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15456</a> <a href="#">B D</a> <a href="#">CISCO</a>
	A vulnerability in the TCP socket code of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to a state			

cisco -- ios_and_ios_xe_software	condition between the socket state and the transmission control block (TCB) state. While this vulnerability potentially affects all TCP applications, the only affected application observed so far is the HTTP server. An attacker could exploit this vulnerability by sending specific HTTP requests at a sustained rate to a reachable IP address of the affected software. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition on an affected device.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0282</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the access control logic of the Secure Shell (SSH) server of Cisco IOS and IOS XE Software may allow connections sourced from a virtual routing and forwarding (VRF) instance despite the absence of the vrf-also keyword in the access-class configuration. The vulnerability is due to a missing check in the SSH server. An attacker could use this vulnerability to open an SSH connection to an affected Cisco IOS or IOS XE device with a source address belonging to a VRF instance. Once connected, the attacker would still need to provide valid credentials to access the device.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0484</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- ip_phone_8800_series_software	A vulnerability in the Cisco IP Phone 8800 Series Software could allow an unauthenticated, remote attacker to conduct an arbitrary script injection attack on an affected device. The vulnerability exists because the software running on an affected device insufficiently validates user-supplied data. An attacker could exploit this vulnerability by persuading a user to click a malicious link provided to the user or through the interface of an affected device. A successful exploit could allow an attacker to execute arbitrary script code in the context of the user interface or access sensitive system-based information, which under normal circumstances should be prohibited.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0461</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- jabber_client_framework	A vulnerability in the Cisco Jabber Client Framework (JCF) software, installed as part of the Cisco Jabber for Mac client, could allow an authenticated, local attacker to corrupt arbitrary files on an affected device that has elevated privileges. The vulnerability exists due to insecure directory permissions set on a JCF created directory. An authenticated attacker with the ability to access an affected directory could create a hard link to an arbitrary location on the affected system. An attacker could convince another user that has administrative privileges to perform an install or update the Cisco Jabber for Mac client to perform such actions, allowing files to be created in an arbitrary location on the disk or an arbitrary file to be corrupted when it is appended to or overwritten.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0449</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- jabber_client_framework	A vulnerability in Cisco Jabber Client Framework (JCF) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of an affected system. The vulnerability is due to insufficient validation of user-supplied input of an affected client. An attacker could exploit this vulnerability by executing arbitrary JavaScript in the Jabber client of the recipient. A successful exploit could allow the attacker to execute arbitrary script code in the context of the targeted client or allow the attacker to access sensitive client-based information.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0483</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- policy_suite_for_mobile_and_policy_suite_diameter_routing_agent_software	A vulnerability in the Redis implementation used by the Cisco Policy Suite for Mobile and Cisco Policy Suite Diameter Routing Agent software could allow an unauthenticated, remote attacker to modify key-value pairs for short-lived events stored by the Redis server. The vulnerability is due to improper authentication when accessing the Redis server. An unauthenticated attacker could exploit this vulnerability by modifying key-value pairs stored within the Redis server database. An exploit could allow the attacker to reduce the efficiency of the Cisco Policy Suite for Mobile and Cisco Policy Suite Diameter Routing Agent software.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0181</a> <a href="#">CISCO</a>
cisco -- policy_suite	A vulnerability in the Graphite web interface of the Policy and Charging Rules Function (PCRF) of Cisco Policy Suite (CPS) could allow an unauthenticated, remote attacker to access the Graphite web interface. The attacker would need to have access to the internal VLAN where CPS is deployed. The vulnerability is due to lack of authentication. An attacker could exploit this vulnerability by directly connecting to the Graphite web interface. An exploit could allow the attacker to access various statistics and Key Performance Indicators (KPIs) regarding the Cisco Policy Suite environment.	2019-01-11	not yet calculated	<a href="#">CVE-2018-15466</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15457</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- prime_network_control_system	A vulnerability in the web-based management interface of Cisco Prime Network Control System could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of the affected system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0482</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- telepresence_management_suite	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive	2019-01-11	not yet calculated	<a href="#">CVE-2018-15467</a> <a href="#">B.D</a> <a href="#">CISCO</a>



	browser-based information.			
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to view digest credentials in clear text. The vulnerability is due to the incorrect inclusion of saved passwords in configuration pages. An attacker could exploit this vulnerability by logging in to the Cisco Unified Communications Manager web-based management interface and viewing the source code for the configuration page. A successful exploit could allow the attacker to recover passwords and expose those accounts to further attack.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0474</a> CISCO
cisco -- webex_business_suite	A vulnerability in the MyWebex component of Cisco Webex Business Suite could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by convincing a user to click a crafted URL. To exploit this vulnerability, the attacker may provide a link that directs a user to a malicious site and use misleading language or instructions to persuade the user to follow the provided link.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15461</a> B.D CISCO
cybozu -- dezie	Directory traversal vulnerability in Cybozu Dezie 8.0.2 to 8.1.2 allows remote attackers to read arbitrary files via HTTP requests.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0705</a> JVN MISC
cybozu -- garoon	Cybozu Garoon 3.0.0 to 4.10.0 allows remote attackers to bypass access restriction to view information available only for a sign-on user via Single sign-on function.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16178</a> JVN MISC
cybozu -- mailwise	Directory traversal vulnerability in Cybozu Mailwise 5.0.0 to 5.4.5 allows remote attackers to delete arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0702</a> JVN MISC
cybozu -- office	Directory traversal vulnerability in Cybozu Office 10.0.0 to 10.8.1 allows remote attackers to delete arbitrary files via HTTP requests.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0703</a> JVN MISC
cybozu -- office	Directory traversal vulnerability in Cybozu Office 10.0.0 to 10.8.1 allows remote attackers to delete arbitrary files via Keitai Screen.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0704</a> JVN MISC
cybozu -- remote_service	Cybozu Remote Service 3.0.0 to 3.1.0 allows remote authenticated attackers to upload and execute Java code file on the server via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16169</a> JVN MISC
cybozu -- remote_service	Improper countermeasure against clickjacking attack in client certificates management screen was discovered in Cybozu Remote Service 3.0.0 to 3.1.8, that allows remote attackers to trick a user to delete the registered client certificate.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16172</a> JVN MISC
cybozu -- remote_service	Directory traversal vulnerability in Cybozu Remote Service 3.0.0 to 3.1.8 allows remote attackers to execute Java code file on the server via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16171</a> JVN MISC
cybozu -- remote_service	Directory traversal vulnerability in Cybozu Remote Service 3.0.0 to 3.1.8 for Windows allows remote authenticated attackers to read arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16170</a> JVN MISC
d-link -- multiple_devices	D-Link D R-822 C1 before v3.11B01Beta, DIR-822-US C1 before v3.11B01Beta, D R-850L A* before v1 21B08Beta, D R-850L B* before v2.22B03Beta, and DIR-880L A* before v1 20B02Beta devices allow authentication bypass.	2019-01-08	not yet calculated	<a href="#">CVE-2018-20675</a> MISC
d-link -- multiple_devices	D-Link D R-822 C1 before v3.11B01Beta, DIR-822-US C1 before v3.11B01Beta, D R-850L A* before v1 21B08Beta, D R-850L B* before v2.22B03Beta, and DIR-880L A* before v1 20B02Beta devices allow authenticated remote command execution.	2019-01-08	not yet calculated	<a href="#">CVE-2018-20674</a> MISC
digital_arts -- i-filter	HTTP header injection vulnerability in i-FILTER Ver 9.50R05 and earlier may allow remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks that may result in an arbitrary script injection or setting an arbitrary cookie values via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16181</a> MISC JVN
digital_arts -- i-filter	Cross-site scripting vulnerability in i-FILTER Ver.9.50R05 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16180</a> MISC JVN
django -- django	In Django 1.11.x before 1.11.18, 2.0.x before 2.0.10, and 2.1.x before 2.1.5, an Improper Neutralization of Special Elements in Output Used by a Downstream Component issue exists in django.views.defaults.page_not_found(), leading to content spoofing (in a 404 error page) if a user fails to recognize that a crafted URL has malicious content.	2019-01-09	not yet calculated	<a href="#">CVE-2019-3498</a> B.D MISC MLIST UBUNTU DEBIAN MISC
docker_engine -- docker_engine	Docker Engine before 18.09 allows attackers to cause a denial of service (dockerd memory consumption) via a large integer in a --cpuset-mems or --cpuset-cpus value, related to daemon/daemon_unix.go, pkg/parsers/parsers.go, and pkg/sysinfo/sysinfo.go.	2019-01-11	not yet calculated	<a href="#">CVE-2018-20699</a> MISC MISC
dokan -- dokan	Dokan, versions between 1.0.0.5000 and 1.2.0.1000, are vulnerable to a stack-based buffer overflow in the dokan1.sys driver. An attacker can create a device handle to the system driver and send arbitrary input that will trigger the vulnerability. This vulnerability was introduced in the 1.0.0.5000 version update.	2019-01-07	not yet calculated	<a href="#">CVE-2018-5410</a> B.D MISC CONFIRM CERT-VN
elfinder -- elfinder	php/elfinder.class.php in elfinder before 2.1.45 leaks information if PHP's curl extension is enabled and safe_mode or open_basedir is not set.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5884</a> MISC MISC

fork -- fork_cms	Fork CMS 5.0.6 allows stored XSS via the private/en/settings facebook_admin_ids parameter (aka "Admin ids" input in the Facebook section).	2019-01-09	not yet calculated	<a href="#">CVE-2018-20682</a> <a href="#">MISC</a>
frog_cms -- frog_cms	Frog CMS 0.9.5 allows XSS via the forgot password page (aka the /admin/?/login/forgot URI).	2019-01-11	not yet calculated	<a href="#">CVE-2019-6243</a> <a href="#">MISC</a>
frontaccounting -- frontaccounting	includes/db/class.reflines_db.inc in FrontAccounting 2.4.6 contains a SQL Injection vulnerability in the reference field that can allow the attacker to grab the entire database of the application via the void_transaction.php filterType parameter.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5720</a> <a href="#">MISC</a>
frouting -- frouting	bgpd in FRRouting FRR (aka Free Range Routing) 2.x and 3.x before 3.0.4, 4.x before 4.0.1, 5.x before 5.0.2, and 6.x before 6.0.2 (not affecting Cumulus Linux or VyOS), when ENABLE_BGP_VNC is used for Virtual Network Control, allows remote attackers to cause a denial of service (peering session flap) via attribute 255 in a BGP UPDATE packet. This occurred during Disco in January 2019 because FRR does not implement RFC 7606, and therefore the packets with 255 were considered invalid VNC data and the BGP session was closed.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5892</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitolite -- gitolite	commands/rsync in Gitolite before 3.6.11, if gitolite rc enables rsync, mishandles the rsync command line, which allows attackers to have a "bad" impact by triggering use of an option other than -v, -n, -q, or -P.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20683</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- binutils	load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20671</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20673</a> <a href="#">B.D</a> <a href="#">MISC</a>
google -- chrome	The default selected dialog button in CustomHandlers in Google Chrome prior to 69.0.3497.81 allowed a remote attacker who convinced the user to perform certain operations to open external programs via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16084</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Failure to prevent navigation to top frame to data URLs in Navigation in Google Chrome on iOS prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20069</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of 304 status codes in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20068</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	A renderer initiated back navigation was incorrectly allowed to cancel a browser initiated one in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20067</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect object lifecycle in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20066</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Handling of URI action in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to initiate potentially unsafe navigations without a user gesture via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20065</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6166</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6163</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of reloads in Navigation in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6165</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient origin checks for CSS content in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6164</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
				<a href="#">CVE-2018-</a>

google -- chrome	Improper deserialization in WebGL in Google Chrome on Mac prior to 68.0 3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">6162</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A heap buffer overflow in GPU in Google Chrome prior to 70.0 3538.67 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17470</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An out of bounds read in PDFium in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17461</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of clicks in the omnibox in Navigation in Google Chrome prior to 69.0 3497.92 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17459</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	An improper update of the WebAssembly dispatch table in WebAssembly in Google Chrome prior to 69.0 3497.92 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17458</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	An object lifecycle issue in Blink could lead to a use after free in WebAudio in Google Chrome prior to 69.0 3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17457</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	JavaScript alert handling in Prompts in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6160</a> <a href="#">B.D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0 3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20070</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6167</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficiently strict origin checks during JIT payment app installation in Payments in Google Chrome prior to 70.0 3538.67 allowed a remote attacker to install a service worker for a domain that can host attacker controlled files via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20071</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Insufficient data validation in V8 builtins string generator could lead to out of bounds read and write access in V8 in Google Chrome prior to 62.0 3202.94 and allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15428</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	A missing check for whether a property of a JS object is private in V8 in Google Chrome prior to 55.0 2883.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2016-9651</a> <a href="#">REDHAT</a> <a href="#">B.D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	A memory corruption bug in WebAssembly could lead to out of bounds read and write through V8 in WebAssembly in Google Chrome prior to 62.0 3202.62 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15401</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Using an ID that can be controlled by a compromised renderer which allows any frame to overwrite the page_state of any other frame in the same process in Navigation in Google Chrome on Chrome OS prior to 62.0.3202.74 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15402</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Insufficient data validation in crosh could lead to a command injection under chronos privileges in Networking in Google Chrome on Chrome OS prior to 61.0 3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15403</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	An ability to process crash dumps under root privileges and inappropriate symlinks handling could lead to a local privilege escalation in Crash Reporting in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to perform privilege escalation via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15404</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Inappropriate symlink handling and a race condition in the stateful recovery feature implementation could lead to a persistence established by a malicious code running with root privileges in cryptohomed in Google Chrome on Chrome OS prior to 61.0 3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15405</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
				<a href="#">CVE-2018-6179</a>

google -- chrome	Insufficient enforcement of file access permission in the activeTab case in Extensions in Google Chrome prior to 68.0 3440.75 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.	2019-01-09	not yet calculated	B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A precision error in Skia in Google Chrome prior to 68.0 3440.75 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6153</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Eliding from the wrong side in an infobar in DevTools in Google Chrome prior to 68.0 3440.75 allowed an attacker who convinced a user to install a malicious extension to Hide Chrome Security UI via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6178</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6175</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Integer overflows in Swiftshader in Google Chrome prior to 68.0 3440.75 potentially allowed a remote attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6174</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6173</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6172</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A bad cast in PDFium in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6170</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Lack of timeout on extension install prompt in Extensions in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to trigger installation of an unwanted extension via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6169</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A race condition in Oilpan in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6158</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Bad cast in DevTools in Google Chrome on Win, Linux, Mac, Chrome OS prior to 66.0 3359.117 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6151</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A use after free in ResourceCoordinator in Google Chrome prior to 69.0 3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16085</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO</a>
google -- chrome	A missing check for popup window handling in Fullscreen in Google Chrome on macOS prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML	2019-01-09	not yet calculated	<a href="#">CVE-2018-16080</a> B D <a href="#">REDHAT</a>

	page.			<a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Unsafe handling of credit card details in Autofill in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16078</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Incorrect handling of asynchronous methods in Fullscreen in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to enter full screen without showing a warning via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6097</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A race condition between permission prompts and navigations in Prompts in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16079</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6100</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An asynchronous generator may return an incorrect state in V8 in Google Chrome prior to 66.0.3359.117 allowing a remote attacker to potentially exploit object corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6106</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	readAsText() can indefinitely read the file picked by the user, rather than only once at the time the file is picked in File API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to access data on the user file system without explicit consent via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6109</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Parsing documents as HTML in Downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to cause Chrome to execute scripts via a local non-HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6110</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An object lifetime issue in the developer tools network handler in Google Chrome prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6111</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Allowing the chrome debugger API to run on file:/// URLs in DevTools in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system without file access permission via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16081</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	A JavaScript focused window could overlap the fullscreen notification in Fullscreen in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6096</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An out of bounds read in Swiftshader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16082</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	An out of bounds read in forward error correction code in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16083</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">EXPLOIT-DB</a>
				<a href="#">CVE-2018-</a>



google -- chrome	Making URLs clickable and allowing them to be styled in DevTools in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6112</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Improper handling of pending navigation entries in Navigation in Google Chrome on iOS prior to 66.0 3359.117 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6113</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect enforcement of CSP for <object> tags in Blink in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6114</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Confusing settings in Autofill in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6117</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6120</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A missing check for JS-simulated input events in Blink in Google Chrome prior to 69.0 3497.81 allowed a remote attacker to download arbitrary files with no user input via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16088</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Lack of proper state tracking in Permissions in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16087</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Missing bounds check in PDFium in Google Chrome prior to 69.0 3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16076</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Insufficient origin checks in Blink in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6093</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Lack of secure text entry mode in Browser UI in Google Chrome on Mac prior to 67.0.3396.62 allowed a local attacker to obtain potentially sensitive information from process memory via a local process.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6147</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Early free of object in use in IndexedDB in Google Chrome prior to 67.0 3396.62 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6127</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Off-by-one error in PDFium in Google Chrome prior to 67.0 3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6144</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient validation in V8 in Google Chrome prior to 67.0 3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6143</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

				<a href="#">DEBIAN</a>
google -- chrome	Insufficient validation of an image filter in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6141</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Allowing the chrome debugger API to attach to Web UI pages in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6140</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient target checks on the chrome.debugger API in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6139</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	CSS Paint API in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6137</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Lack of clearing the previous site before loading alerts from a new one in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6135</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6133</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6126</a> <a href="#">B.D</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	Service Workers can intercept any request made by an <embed> or <object> tag in Fetch API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6091</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Type confusion in ReadableStreams in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6124</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6123</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	A Javascript reentrancy issues that caused a use-after-free in V8 in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16065</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>

google -- chrome	A use after free in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16066</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Missing validation in Mojo in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16068</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A use after free in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16071</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	A missing origin check related to HLS manifests in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16072</a> <a href="#">B.D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Type confusion could lead to a heap out-of-bounds write in V8 in Google Chrome prior to 64.0.3282.168 allowing a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6056</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficiently sanitized distributed objects in Updater in Google Chrome on macOS prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via an executable file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6084</a> <a href="#">B.D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	A use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16067</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient data validation on image data in PDFium in Google Chrome prior to 51.0.2704.63 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2016-10403</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- api_connect	BM API Connect 5.0 0 0 through 5 0 8.4 is affected by a vulnerability in the role-based access control in the management server that could allow an authenticated user to obtain highly sensitive information. BM X-Force ID: 153175.	2019-01-08	not yet calculated	<a href="#">CVE-2018-1932</a> <a href="#">CONFIRM</a> <a href="#">B.D</a> <a href="#">XF</a>
ibm -- i_access_for_windows	An untrusted search path vulnerability in IBM i Access for Windows versions 7.1 and earlier on Windows can allow arbitrary code execution via a Trojan horse DLL in the current working directory, related to use of the LoadLibrary function. IBM X-Force ID: 152079.	2019-01-04	not yet calculated	<a href="#">CVE-2018-1888</a> <a href="#">B.D</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- jazz_reporting_service	BM Jazz Reporting Service (JRS) 6 0.3, 6 0.4, 6 0.5, and 6 0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152785.	2019-01-08	not yet calculated	<a href="#">CVE-2018-1918</a> <a href="#">CONFIRM</a> <a href="#">B.D</a> <a href="#">XF</a>
ibm -- spectrum_scale	BM Spectrum Scale (GPFS) 4.1.1, 4.2 0, 4 2.1, 4 2.2, 4.2.3, and 5 0 0 where the use of Local Read Only Cache (LROC) is enabled may caused read operation on a file to return data from a different file. IBM X-Force ID: 154440.	2019-01-08	not yet calculated	<a href="#">CVE-2018-1993</a> <a href="#">B.D</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
imperva -- securesphere	Imperva SecureSphere running v12.0.0.50 is vulnerable to local arbitrary code execution, escaping sealed-mode.	2019-01-10	not yet calculated	<a href="#">CVE-2018-5412</a> <a href="#">EXPLOIT-DB</a>
imperva -- securesphere	Imperva SecureSphere running v13.0, v12 0, or v11.5 allows low privileged users to add SSH login keys to the admin user, resulting in privilege escalation.	2019-01-10	not yet calculated	<a href="#">CVE-2018-5413</a> <a href="#">EXPLOIT-DB</a>
imperva -- securesphere_gateway	Imperva SecureSphere gateway (GW) running v13, for both pre-First Time Login or post-First Time Login (FTL), if the attacker knows the basic authentication passwords, the GW may be vulnerable to RCE through specially crafted requests, from the web access management interface.	2019-01-10	not yet calculated	<a href="#">CVE-2018-5403</a> <a href="#">EXPLOIT-DB</a>
intel -- nuc_firmware	Improper setting of device configuration in system firmware for Intel(R) NUC kits may allow a privileged user to potentially enable escalation of privilege via physical access.	2019-01-10	not yet calculated	<a href="#">CVE-2017-3718</a> <a href="#">CONFIRM</a>
intel -- optane_ssd_dc_p4800x	Firmware update routine in bootloader for Intel(R) Optane(TM) SSD DC P4800X before version E2010435 may allow a privileged user to	2019-01-	not yet	<a href="#">CVE-2018-12167</a>

	potentially enable a denial of service via local access.	10	calculated	<a href="#">CONFIRM</a>
intel -- optane_ssd_dc_p4800x	Insufficient write protection in firmware for Intel(R) Optane(TM) SSD DC P4800X before version E2010435 may allow a privileged user to potentially enable a denial of service via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-12166</a> <a href="#">CONFIRM</a>
intel -- proset/wireless_wifi_software	Improper directory permissions in the ZeroConfig service in Intel(R) PROSet/Wireless WiFi Software before version 20.90.0.7 may allow an authorized user to potentially enable escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-12177</a> <a href="#">CONFIRM</a>
intel -- sgx_sdk_and_platform_software_for_window	Improper file verification in install routine for Intel(R) SGX SDK and Platform Software for Windows before 2.2.100 may allow an escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-18098</a> <a href="#">CONFIRM</a>
intel -- ssd_data_center_tool_for_windows	Improper directory permissions in the installer for the Intel(R) SSD Data Center Tool for Windows before v3.0.17 may allow authenticated users to potentially enable an escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-3703</a> <a href="#">CONFIRM</a>
intel -- system_support_utility_for_windows	Insufficient path checking in Intel(R) System Support Utility for Windows before 2.5.0.15 may allow an authenticated user to potentially enable an escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2019-0088</a> <a href="#">CONFIRM</a>
irssi -- irssi	Irssi 1.1 x before 1.1.2 has a use after free when hidden lines are expired from the scroll buffer.	2019-01-09	not yet calculated	<a href="#">CVE-2019-5882</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
japan_atomic_energy_agency -- mapping_tool	Untrusted search path vulnerability in Installer of Mapping Tool 2 0.1.6 and 2 0.1.7 allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16176</a> <a href="#">MISC</a> <a href="#">JVN</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Jira Plugin 3 0.1 and earlier in JiraSite.java that allows attackers with Overall/Read access to have Jenkins connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000412</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Crowd 2 Integration Plugin 2 0.0 and earlier in CrowdSecurityRealm.java that allows attackers to have Jenkins perform a connection test, connecting to an attacker-specified server with attacker-specified credentials and connection settings.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000422</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/model/Api.java that allows attackers to specify URLs to Jenkins that result in rendering arbitrary attacker-controlled HTML by Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000407</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A denial of service vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/security/HudsonPrivateSecurityRealm.java that allows attackers without Overall/Read permission to access a specific URL on instances using the built-in Jenkins user database security realm that results in the creation of an ephemeral user record in memory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000408</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A session fixation vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/security/HudsonPrivateSecurityRealm.java that prevented Jenkins from invalidating the existing session and creating a new one when a user signed up for a new user account.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000409</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Git Changelog Plugin 2.6 and earlier in GitChangelogSummaryDecorator/summary.jelly, GitChangelogLeftsideBuildDecorator/badge.jelly, GitLogJiraFilterPostPublisher/config.jelly, GitLogBasicChangelogPostPublisher/config.jelly that allows attackers able to control the Git history parsed by the plugin to have Jenkins render arbitrary HTML on some pages.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000426</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins SonarQube Scanner Plugin 2 8 and earlier in SonarInstallation.java that allows attackers with local file system access to obtain the credentials used to connect to SonarQube.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000425</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Crowd 2 Integration Plugin 2 0.0 and earlier in CrowdSecurityRealm.java, CrowdConfigurationService.java that allows attackers with local file system access to obtain the credentials used to connect to Crowd 2.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000423</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Mesos Plugin 0.17.1 and earlier in MesosCloud.java that allows attackers with Overall/Read access to initiate a test connection to an attacker-specified Mesos server with attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000421</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability exists in Jenkins JUnit Plugin 1.25 and earlier in TestObject.java that allows setting the description of a test result.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000411</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Mesos Plugin 0.17.1 and earlier in MesosCloud.java that allows attackers with Overall/Read access to obtain credentials IDs for credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000420</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins HipChat Plugin 2.2.0 and earlier in HipChatNotifier.java that allows attackers with Overall/Read access to obtain credentials IDs for credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000419</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins HipChat Plugin 2.2.0 and earlier in HipChatNotifier.java that allows attackers with Overall/Read access to send test notifications to an attacker-specified HipChat server with attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000418</a> <a href="#">CONFIRM</a>
	A cross-site request forgery vulnerability exists in Jenkins Email			

jenkins -- jenkins	Extension Template Plugin 1.0 and earlier in ExtEmailTemplateManagement.java that allows creating or removing templates.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000417 CONFIRM</a>
jenkins -- jenkins	A reflected cross-site scripting vulnerability exists in Jenkins Job Config History Plugin 2.18 and earlier in all Jelly files that shows arbitrary attacker-specified HTML in Jenkins to users with Job/Configure access.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000416 CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier, and the Stapler framework used by these releases, in core/src/main/java/org/kohsuke/stapler/RequestImpl.java, core/src/main/java/hudson/model/Descriptor.java that allows attackers with Overall/Administer permission or access to the local file system to obtain credentials entered by users if the form submission could not be successfully processed.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000410 CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability exists in Jenkins Config File Provider Plugin 3.1 and earlier in ConfigFilesManagement.java, FolderConfigFileAction.java that allows creating and editing configuration file definitions.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000414 CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Config File Provider Plugin 3.1 and earlier in configfiles.jelly, providerlist.jelly that allows users with the ability to configure configuration files to insert arbitrary HTML into some pages in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000413 CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Rebuilder Plugin 1.28 and earlier in RebuildAction/BooleanParameterValue.jelly, RebuildAction/ExtendedChoiceParameterValue.jelly, RebuildAction/FileParameterValue.jelly, RebuildAction/LabelParameterValue.jelly, RebuildAction/ListSubversionTagsParameterValue.jelly, RebuildAction/MavenMetadataParameterValue.jelly, RebuildAction/NodeParameterValue.jelly, RebuildAction/PasswordParameterValue.jelly, RebuildAction/RandomStringParameterValue.jelly, RebuildAction/RunParameterValue.jelly, RebuildAction/StringParameterValue.jelly, RebuildAction/TextParameterValue.jelly, RebuildAction/ValidatingStringParameterValue.jelly that allows users with Job/Configuration permission to insert arbitrary HTML into rebuild forms.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000415 CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Artifactory Plugin 2.16.1 and earlier in ArtifactoryBuilder.java, CredentialsConfig.java that allows attackers with local file system access to obtain old credentials configured for the plugin before it integrated with Credentials Plugin.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000424 CONFIRM</a>
jenkins -- jenkins	A path traversal vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/model/FileParameterValue.java that allows attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000406 CONFIRM</a>
jpccert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to conduct Python code injection attacks via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16168 MISC</a>
jpccert_coordination_center -- logontracer	Cross-site scripting vulnerability in LogonTracer 1.2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16165 MISC</a>
jpccert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to conduct XML External Entity (XXE) attacks via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16166 MISC</a>
jpccert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16167 MISC</a>
lib60870 -- lib60870	An issue was discovered in lib60870 2.1.1. LinkLayer_setAddress in link_layer/link_layer.c has a NULL pointer dereference.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6137 MISC</a>
libiec61850 -- libiec61850	An issue has been found in lib EC61850 v1.3.1. Ethernet_setProtocolFilter in hal/ethernet/linux/ethernet_linux.c has a SEGV, as demonstrated by sv_subscriber_example.c and sv_subscriber.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6136 MISC</a>
libiec61850 -- libiec61850	An issue has been found in lib EC61850 v1.3.1. Memory_malloc and Memory_calloc in hal/memory/lib_memory.c have memory leaks when called from mms/iso_mms/common/mms_value.c, server/mms_mapping/mms_mapping.c, and server/mms_mapping/mms_sv.c (via common/string_utilities.c), as demonstrated by iec61850_9_2_LE_example.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6138 MISC</a>
libiec61850 -- libiec61850	An issue has been found in lib EC61850 v1.3.1. Memory_malloc in hal/memory/lib_memory.c has a memory leak when called from Asn1PrimitiveValue_create in mms/asn1/asn1_ber_primitive_value.c, as demonstrated by goose_publisher_example.c and iec61850_9_2_LE_example.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6135 MISC</a>
libpng -- libpng	png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6129 MISC</a>
libtiff -- libtiff	The T_FFFdOpen function in tif_unix.c in LibTiff 4.0.10 has a memory leak, as demonstrated by pal2rgb.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6128 MISC</a>
linux -- linux_kernel	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of	2019-01-07	not yet calculated	<a href="#">CVE-2019-5489 MISC</a>



	the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.			MISC MISC MISC
linux -- linux_kernel	EARCLNK ESPCMS-P8 has SQL injection in the install_pack/index.php?ac=Member&at=verifyAccount verify_key parameter. install_pack/espcms_public/espcms_db.php may allow retrieving sensitive information from the ESPCMS database.	2019-01-07	not yet calculated	CVE-2019-5488 MISC
lockon -- ec-cube	Open redirect vulnerability in EC-CUBE (EC-CUBE 3.0.0, EC-CUBE 3.0.1, EC-CUBE 3.0.2, EC-CUBE 3.0.3, EC-CUBE 3.0.4, EC-CUBE 3.0.5, EC-CUBE 3.0.6, EC-CUBE 3.0.7, EC-CUBE 3.0.8, EC-CUBE 3.0.9, EC-CUBE 3.0.10, EC-CUBE 3.0.11, EC-CUBE 3.0.12, EC-CUBE 3.0.12-p1, EC-CUBE 3.0.13, EC-CUBE 3.0.14, EC-CUBE 3.0.15, EC-CUBE 3.0.16) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16191 JVN MISC
mate_desktop_environment -- mate-screensaver	mate-screensaver before 1.20.2 in MATE Desktop Environment allows physically proximate attackers to view screen content and possibly control applications. By unplugging and re-plugging or power-cycling external output devices (such as additionally attached graphical outputs via HDMI, VGA, DVI, etc.) the content of a screensaver-locked session can be revealed. In some scenarios, the attacker can execute applications, such as by clicking with a mouse.	2019-01-09	not yet calculated	CVE-2018-20681 MISC MISC MISC MISC
mcafee -- web_gateway	Improper input validation in the proxy component of McAfee Web Gateway 7.8.2.0 and later allows remote attackers to cause a denial of service via a crafted HTTP request parameter.	2019-01-09	not yet calculated	CVE-2019-3581 CONFIRM
micronet -- inplc	Nplc-RT 3.08 and earlier allows remote attackers to bypass authentication to execute an arbitrary command through the protocol-compliant traffic. This is a different vulnerability than CVE-2018-0670.	2019-01-09	not yet calculated	CVE-2018-0669 MISC JVN
micronet -- inplc	Buffer overflow in INplc-RT 3.08 and earlier allows remote attackers to cause denial-of-service (DoS) condition that may result in executing arbitrary code via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0668 MISC JVN
micronet -- inplc	Privilege escalation vulnerability in Nplc-RT 3.08 and earlier allows an attacker with administrator rights to execute arbitrary code on the Windows system via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0671 MISC JVN
micronet -- inplc	Nplc-RT 3.08 and earlier allows remote attackers to bypass authentication to execute an arbitrary command through the protocol-compliant traffic. This is a different vulnerability than CVE-2018-0669.	2019-01-09	not yet calculated	CVE-2018-0670 MISC JVN
micronet -- inplc	Untrusted search path vulnerability in Installer of Nplc SDK Express 3.08 and earlier and Installer of Nplc SDK Pro+ 3.08 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	CVE-2018-0667 MISC JVN
microsoft -- net_framework	An information disclosure vulnerability exists in .NET Framework and .NET Core which allows bypassing Cross-origin Resource Sharing (CORS) configurations, aka ".NET Framework Information Disclosure Vulnerability." This affects Microsoft .NET Framework 2.0, Microsoft .NET Framework 3.0, Microsoft .NET Framework 4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET Framework 4.6, Microsoft .NET Framework 4.6.4/4.6.1/4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.7.1/4.7.2, .NET Core 2.1, Microsoft .NET Framework 4.7.1/4.7.2, Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4.6.4/4.6.1/4.6.2, .NET Core 2.2, Microsoft .NET Framework 4.7.2.	2019-01-08	not yet calculated	CVE-2019-0545 B.D REDHAT CONFIRM
microsoft -- asp_net_core	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka "ASP.NET Core Denial of Service Vulnerability." This affects ASP.NET Core 2.2, ASP.NET Core 2.1. This CVE ID is unique from CVE-2019-0564.	2019-01-08	not yet calculated	CVE-2019-0548 B.D REDHAT CONFIRM
microsoft -- edge	An elevation of privilege vulnerability exists in Microsoft Edge Browser Broker COM object, aka "Microsoft Edge Elevation of Privilege Vulnerability." This affects Microsoft Edge.	2019-01-08	not yet calculated	CVE-2019-0566 B.D CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0567.	2019-01-08	not yet calculated	CVE-2019-0568 B.D CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0568.	2019-01-08	not yet calculated	CVE-2019-0539 B.D CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0568.	2019-01-08	not yet calculated	CVE-2019-0567 B.D CONFIRM
microsoft -- exchange_server	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka "Microsoft Exchange Memory Corruption Vulnerability." This affects Microsoft Exchange Server.	2019-01-08	not yet calculated	CVE-2019-0586 B.D CONFIRM
microsoft -- exchange_server	An information disclosure vulnerability exists when the Microsoft Exchange PowerShell API grants calendar contributors more view permissions than intended, aka "Microsoft Exchange Information Disclosure Vulnerability." This affects Microsoft Exchange Server.	2019-01-08	not yet calculated	CVE-2019-0588 B.D CONFIRM
microsoft -- multiple_products	An information disclosure vulnerability exists when Microsoft Word macro buttons are used improperly, aka "Microsoft Word Information Disclosure Vulnerability." This affects Microsoft Word, Office 365 ProPlus, Microsoft Office, Word.	2019-01-08	not yet calculated	CVE-2019-0561 B.D CONFIRM
	A remote code execution vulnerability exists in the way that the			CVE-2019-

microsoft -- multiple_products	MSHTML engine improperly validates input, aka "MSHTML Engine Remote Code Execution Vulnerability." This affects Microsoft Office, Microsoft Office Word Viewer, Internet Explorer 9, Internet Explorer 11, Microsoft Excel Viewer, Internet Explorer 10, Office 365 ProPlus.	2019-01-08	not yet calculated	<a href="#">0541</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka "Microsoft Word Remote Code Execution Vulnerability." This affects Word, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft SharePoint, Microsoft Office Online Server, Microsoft Word, Microsoft SharePoint Server.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0585</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- multiple_products	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint Server, Microsoft SharePoint, Microsoft Business Productivity Servers. This CVE ID is unique from CVE-2019-0556, CVE-2019-0557.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0558</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint. This CVE ID is unique from CVE-2019-0557, CVE-2019-0558.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0556</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft SharePoint Elevation of Privilege Vulnerability." This affects Microsoft SharePoint Server, Microsoft SharePoint.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0562</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint. This CVE ID is unique from CVE-2019-0556, CVE-2019-0558.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0557</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- skype_for_android	An elevation of privilege vulnerability exists when Skype for Android fails to properly handle specific authentication requests, aka "Skype for Android Elevation of Privilege Vulnerability." This affects Skype 8.35.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0622</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- visual_studio	A remote code execution vulnerability exists in Visual Studio when the C++ compiler improperly handles specific combinations of C++ constructs, aka "Visual Studio Remote Code Execution Vulnerability." This affects Microsoft Visual Studio.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0546</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- visual_studio	An information disclosure vulnerability exists when Visual Studio improperly discloses arbitrary file contents if the victim opens a malicious .vscontent file, aka "Microsoft Visual Studio Information Disclosure Vulnerability." This affects Microsoft Visual Studio.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0537</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0572, CVE-2019-0573, CVE-2019-0574.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0571</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka "Windows Runtime Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0570</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0536, CVE-2019-0549, CVE-2019-0554.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0569</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0538</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka "Windows Hyper-V Remote Code Execution Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019. This CVE ID is unique from CVE-2019-0551.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0550</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0536, CVE-2019-0554, CVE-2019-0569.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0549</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka "Microsoft Windows Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0543</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
	An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the			

microsoft -- windows	AppContainer sandbox in the browser, aka "Microsoft XmlDocument Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0555</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0536, CVE-2019-0549, CVE-2019-0569.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0554</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka "Windows Subsystem for Linux Information Disclosure Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0553</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0572, CVE-2019-0574.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0573</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege exists in Windows COM Desktop Broker, aka "Windows COM Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0552</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka "Windows Hyper-V Remote Code Execution Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE D is unique from CVE-2019-0550.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0551</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0573, CVE-2019-0574.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0572</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0576</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0572, CVE-2019-0573.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0574</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0577</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0581</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0582</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0578</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>

microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0579</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0580</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0583</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0584</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0575</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0549, CVE-2019-0554, CVE-2019-0569.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0536</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
mizuho_bank -- mizuho_direct_app_for_android	The Mizuho Direct App for Android version 3.13.0 and earlier does not verify server certificates, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16179</a> <a href="#">MISC</a> <a href="#">MISC</a>
modulemd -- modulemd	modulemd 1.3.1 and earlier uses an unsafe function for processing externally provided data, leading to remote code execution.	2019-01-10	not yet calculated	<a href="#">CVE-2017-1002157</a> <a href="#">CONFIRM</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands via SOAP interface of UPnP.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16195</a> <a href="#">MISC</a> <a href="#">JVN</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allow an attacker on the same network segment to obtain information registered on the device via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16192</a> <a href="#">MISC</a> <a href="#">JVN</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Cross-site scripting vulnerability in Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16193</a> <a href="#">MISC</a> <a href="#">JVN</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows authenticated attackers to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16194</a> <a href="#">MISC</a> <a href="#">JVN</a>
nelson -- open_source_erp	Nelson Open Source ERP v6.3.1 allows SQL Injection via the db/utills/query/data.xml query parameter.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5893</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
netapp -- oncommand_unified_manager_for_7-mode	OnCommand Unified Manager for 7-Mode (core package) prior to 5.2.4 uses cookies that lack the secure attribute in certain circumstances making it vulnerable to impersonation via man-in-the-middle (MITM) attacks.	2019-01-07	not yet calculated	<a href="#">CVE-2018-5481</a> <a href="#">CONFIRM</a>
nippon_telegraph_and_telephone_west_corporation -- security_measures_tool	Untrusted search path vulnerability in The installer of Windows10 Fall Creators Update Modify module for Security Measures tool allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16177</a> <a href="#">MISC</a> <a href="#">JVN</a>
				<a href="#">CVE-2018-</a>

npm -- cordova-plugin-ionic-webview	Directory traversal vulnerability in cordova-plugin-ionic-webview versions prior to 2.2.0 (not including 2.0.0-beta.0, 2.0.0-beta.1, 2.0.0-beta.2, and 2.1.0-0) allows remote attackers to access arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">16202</a> <a href="#">MISC</a> <a href="#">JVN</a> <a href="#">MISC</a>
openssh -- openssh	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename.	2019-01-10	not yet calculated	<a href="#">CVE-2018-20685</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
panasonic -- bn-sdwb3_firmware	Buffer overflow in BN-SDWB3 firmware version 1.0.9 and earlier allows an attacker on the same network segment to execute arbitrary code via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0678</a> <a href="#">JVN</a> <a href="#">MISC</a>
panasonic -- bn-sdwb3_firmware	BN-SDWB3 firmware version 1.0.9 and earlier allows attacker with administrator rights on the same network segment to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0677</a> <a href="#">JVN</a> <a href="#">MISC</a>
panasonic -- bn-sdwb3_firmware	BN-SDWB3 firmware version 1.0.9 and earlier allows an attacker on the same network segment to bypass authentication to access to the management screen and execute an arbitrary command via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0676</a> <a href="#">JVN</a> <a href="#">MISC</a>
panasonic -- multiple_pcs	An unquoted search path vulnerability in some pre-installed applications on Panasonic PC run on Windows 7 (32bit), Windows 7 (64bit), Windows 8 (64bit), Windows 8.1 (64bit), Windows 10 (64bit) delivered in or later than October 2009 allow local users to gain privileges via a Trojan horse executable file and execute arbitrary code with elevated privileges.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16183</a> <a href="#">JVN</a> <a href="#">MISC</a>
pgpool -- global_development_group_pgpooladmin	PgpoolAdmin 4.0 and earlier allows remote attackers to bypass the login authentication and obtain the administrative privilege of the PostgreSQL database via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16203</a> <a href="#">JVN</a> <a href="#">MISC</a>
phpscriptsmall.com -- advance_peer_to_peer_mlm_script	The Admin Panel of PHP Scripts Mall Advance Peer to Peer MLM Script v1.7.0 allows remote attackers to bypass intended access restrictions by directly navigating to admin/dashboard.php or admin/user.php, as demonstrated by disclosure of information about users and staff.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6126</a> <a href="#">MISC</a>
phpscriptsmall.com -- citysearch_/hotfrog/_gelbeseiten_clone_script	PHP Scripts Mall Citysearch / Hotfrog / Gelbeseiten Clone Script 2.0.1 has Reflected XSS via the srch parameter, as demonstrated by restaurants-details.php.	2019-01-12	not yet calculated	<a href="#">CVE-2019-6248</a> <a href="#">MISC</a>
pivotal -- concourse	Pivotal Concourse, all versions prior to 4.2.2, puts the user access token in a url during the login flow. A remote attacker who gains access to a user's browser history could obtain the access token and use it to authenticate as the user.	2019-01-11	not yet calculated	<a href="#">CVE-2019-3803</a> <a href="#">CONFIRM</a>
policykit -- policykit	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6133</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qibosoft -- qibosoft	qibosoft through V7 allows remote attackers to read arbitrary files via the member/index.php main parameter, as demonstrated by SSRF to a URL on the same web site to read a .sql file.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5725</a> <a href="#">MISC</a>
rakuten_securities -- market_speed	Untrusted search path vulnerability in the installer of MARKET SPEED Ver.16.4 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16182</a> <a href="#">JVN</a> <a href="#">MISC</a>
red_hat -- satellite	A cross-site scripting (XSS) flaw was found in the katello component of Satellite. An attacker with privilege to create/edit organizations and locations is able to execute a XSS attacks against other users through the Subscriptions or the Red Hat Repositories wizards. This can possibly lead to malicious code execution and extraction of the anti-CSRF token of higher privileged users. Versions before 3.9.0 are vulnerable.	2019-01-12	not yet calculated	<a href="#">CVE-2018-16887</a> <a href="#">CONFIRM</a>
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.6 to V2.2, D5500 V1.6 to V2.2, D5510 V1.6 to V2.2, and the display versions with RICOH Interactive Whiteboard Controller Type1 V1.6 to V2.2 attached (D5520, D6500, D6510, D7500, D8400) allows remote attackers to execute arbitrary commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16184</a> <a href="#">JVN</a> <a href="#">MISC</a>
ricoh -- interactive_whiteboard	The RICOH Interactive Whiteboard D2200 V1.3 to V2.2, D5500 V1.3 to V2.2, D5510 V1.3 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.3 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) does not verify its server certificates, which allows man-in-the-middle attackers to eversdrop on encrypted communication.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16187</a> <a href="#">JVN</a> <a href="#">MISC</a>
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.1 to V2.2, D5500 V1.1 to V2.2, D5510 V1.1 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.1 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) uses hard-coded credentials, which may allow an attacker on the same network segments to login to the administrators settings screen and change the configuration.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16186</a> <a href="#">JVN</a> <a href="#">MISC</a>
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.1 to V2.2, D5500 V1.1 to V2.2, D5510 V1.1 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.1 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) allows remote attackers to execute a malicious program.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16185</a> <a href="#">JVN</a> <a href="#">MISC</a>
	SQL injection vulnerability in the RICOH Interactive Whiteboard D2200 V1.3 to V2.2, D5500 V1.3 to V2.2, D5510 V1.3 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1			<a href="#">CVE-2018-</a>



ricoh -- interactive_whiteboard	V1 3 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137 0 attached (D5520, D6510, D7500, D8400) allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">16188</a> <a href="#">JVN</a> <a href="#">MISC</a>
sap -- business_objects_mobile_for_android	SAP Business Objects Mobile for Android (before 6.3.5) application allows an attacker to provide malicious input in the form of a SAP BI link, preventing legitimate users from accessing the application by crashing it.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0240</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- bw/4hana	Under some circumstances, masterdata maintenance in SAP BW/4HANA (fixed in DW4CORE version 1.0 (SP08)) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0243</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- cloud_connector	SAP Cloud Connector, before version 2.11.3, allows an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0247</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- cloud_connector	SAP Cloud Connector, before version 2.11.3, does not perform any authentication checks for functionalities that require user identity.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0246</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- commerce	SAP Commerce (previously known as SAP Hybris Commerce), before version 6.7, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0238</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- crm_webclient_ui	SAP CRM WebClient UI (fixed in SAPSCORE 1.12; S4FND 1 02; WEBCU F 7 31, 7.46, 7.47, 7.48, 8 0, 8 01) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0244</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- crm_webclient_ui	SAP CRM WebClient UI (fixed in SAPSCORE 1.12; S4FND 1 02; WEBCU F 7 31, 7.46, 7.47, 7.48, 8 0, 8 01) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0245</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- enterprise_financial_services	SAP Enterprise Financial Services (fixed in SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1 03; EA-F NSERV 1.10, 2 0, 5 0, 6 0, 6 03, 6.04, 6.05, 6 06, 6.16, 6.17, 6.18, 8.0; Bank/CFM 4.63_20) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-01-08	not yet calculated	<a href="#">CVE-2018-2484</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- financial_consolidation_cube_designer	A security weakness in SAP Financial Consolidation Cube Designer (BOBJ_EADES fixed in versions 8.0, 10.1) may allow an attacker to discover the password hash of an admin user.	2019-01-08	not yet calculated	<a href="#">CVE-2018-2499</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- gateway_of_abap_application_server	Under certain conditions SAP Gateway of ABAP Application Server (fixed in SAP_GWFND 7.5, 7.51, 7.52, 7.53; SAP_BASIS 7 5) allows an attacker to access information which would otherwise be restricted.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0248</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- landscape_management	Under certain conditions SAP Landscape Management (VCM 3.0) allows an attacker to access information which would otherwise be restricted.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0249</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- work_and_inventory_manager	SAP Work and Inventory Manager (Agentry_SDK , before 7.0, 7.1) allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0241</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
seiko_epson -- printers_and_scanners	HTTP header injection vulnerability in SEIKO EPSON printers and scanners (DS-570W firmware versions released prior to 2018 March 13, DS-780N firmware versions released prior to 2018 March 13, EP-10VA firmware versions released prior to 2017 September 4, EP-30VA firmware versions released prior to 2017 June 19, EP-707A firmware versions released prior to 2017 August 1, EP-708A firmware versions released prior to 2017 August 7, EP-709A firmware versions released prior to 2017 June 12, EP-777A firmware versions released prior to 2017 August 1, EP-807AB/AW/AR firmware versions released prior to 2017 August 1, EP-808AB/AW/AR firmware versions released prior to 2017 August 7, EP-879AB/AW/AR firmware versions released prior to 2017 June 12, EP-907F firmware versions released prior to 2017 August 1, EP-977A3 firmware versions released prior to 2017 August 1, EP-978A3 firmware versions released prior to 2017 August 7, EP-979A3 firmware versions released prior to 2017 June 12, EP-M570T firmware versions released prior to 2017 September 6, EW-M5071FT firmware versions released prior to 2017 November 2, EW-M660FT firmware versions released prior to 2018 April 19, EW-M770T firmware versions released prior to 2017 September 6, PF-70 firmware versions released prior to 2018 April 20, PF-71 firmware versions released prior to 2017 July 18, PF-81 firmware versions released prior to 2017 September 14, PX-048A firmware versions released prior to 2017 July 4, PX-049A firmware versions released prior to 2017 September 11, PX-437A firmware versions released prior to 2017 July 24, PX-M350F firmware versions released prior to 2018 February 23, PX-M5040F firmware versions released prior to 2017 November 20, PX-M5041F firmware versions released prior to 2017 November 20, PX-M650A firmware versions released prior to 2017 October 17, PX-M650F firmware versions released prior to 2017 October 17, PX-M680F firmware versions released prior to 2017 June 29, PX-M7050F firmware versions released prior to 2017 October 13, PX-M7050FP firmware versions released prior to 2017 October 13, PX-M7050FX firmware versions released prior to 2017	2019-01-09	not yet calculated	<a href="#">CVE-2018-0689</a> <a href="#">JVN</a> <a href="#">MISC</a>

	November 7, PX-M7070FX firmware versions released prior to 2017 April 27, PX-M740F firmware versions released prior to 2017 December 4, PX-M741F firmware versions released prior to 2017 December 4, PX-M780F firmware versions released prior to 2017 June 29, PX-M781F firmware versions released prior to 2017 June 27, PX-M840F firmware versions released prior to 2017 November 16, PX-M840FX firmware versions released prior to 2017 December 8, PX-M860F firmware versions released prior to 2017 October 25, PX-S05B/W firmware versions released prior to 2018 March 9, PX-S350 firmware versions released prior to 2018 February 23, PX-S5040 firmware versions released prior to 2017 November 20, PX-S7050 firmware versions released prior to 2018 February 21, PX-S7050PS firmware versions released prior to 2018 February 21, PX-S7050X firmware versions released prior to 2017 November 7, PX-S7070X firmware versions released prior to 2017 April 27, PX-S740 firmware versions released prior to 2017 December 3, PX-S840 firmware versions released prior to 2017 November 16, PX-S840X firmware versions released prior to 2017 December 8, PX-S860 firmware versions released prior to 2017 December 7) may allow a remote attackers to lead a user to a phishing site or execute an arbitrary script on the user's web browser.			
seiko_epson -- printers_and_scanners	Open redirect vulnerability in SE KO EPSON printers and scanners (DS-570W firmware versions released prior to 2018 March 13, DS-780N firmware versions released prior to 2018 March 13, EP-10VA firmware versions released prior to 2017 September 4, EP-30VA firmware versions released prior to 2017 June 19, EP-707A firmware versions released prior to 2017 August 1, EP-708A firmware versions released prior to 2017 August 7, EP-709A firmware versions released prior to 2017 June 12, EP-777A firmware versions released prior to 2017 August 1, EP-807AB/AW/AR firmware versions released prior to 2017 August 1, EP-808AB/AW/AR firmware versions released prior to 2017 August 7, EP-879AB/AW/AR firmware versions released prior to 2017 June 12, EP-907F firmware versions released prior to 2017 August 1, EP-977A3 firmware versions released prior to 2017 August 1, EP-978A3 firmware versions released prior to 2017 August 7, EP-979A3 firmware versions released prior to 2017 June 12, EP-M570T firmware versions released prior to 2017 September 6, EW-M5071FT firmware versions released prior to 2017 November 2, EW-M660FT firmware versions released prior to 2018 April 19, EW-M770T firmware versions released prior to 2017 September 6, PF-70 firmware versions released prior to 2018 April 20, PF-71 firmware versions released prior to 2017 July 18, PF-81 firmware versions released prior to 2017 September 14, PX-048A firmware versions released prior to 2017 July 4, PX-049A firmware versions released prior to 2017 September 11, PX-437A firmware versions released prior to 2017 July 24, PX-M350F firmware versions released prior to 2018 February 23, PX-M5040F firmware versions released prior to 2017 November 20, PX-M5041F firmware versions released prior to 2017 November 20, PX-M650A firmware versions released prior to 2017 October 17, PX-M650F firmware versions released prior to 2017 October 17, PX-M680F firmware versions released prior to 2017 June 29, PX-M7050F firmware versions released prior to 2017 October 13, PX-M7050FP firmware versions released prior to 2017 October 13, PX-M7050FX firmware versions released prior to 2017 November 7, PX-M7070FX firmware versions released prior to 2017 April 27, PX-M740F firmware versions released prior to 2017 December 4, PX-M741F firmware versions released prior to 2017 December 4, PX-M780F firmware versions released prior to 2017 June 29, PX-M781F firmware versions released prior to 2017 June 27, PX-M840F firmware versions released prior to 2017 November 16, PX-M840FX firmware versions released prior to 2017 December 8, PX-M860F firmware versions released prior to 2017 October 25, PX-S05B/W firmware versions released prior to 2018 March 9, PX-S350 firmware versions released prior to 2018 February 23, PX-S5040 firmware versions released prior to 2017 November 20, PX-S7050 firmware versions released prior to 2018 February 21, PX-S7050PS firmware versions released prior to 2018 February 21, PX-S7050X firmware versions released prior to 2017 November 7, PX-S7070X firmware versions released prior to 2017 April 27, PX-S740 firmware versions released prior to 2017 December 3, PX-S840 firmware versions released prior to 2017 November 16, PX-S840X firmware versions released prior to 2017 December 8, PX-S860 firmware versions released prior to 2017 December 7) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the web interface of the affected product.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0688</a> <a href="#">JVN</a> <a href="#">MISC</a>
shopxo -- shopxo	An issue was discovered in ShopXO 1.2.0. In the UnlinkDir method of the FileUtil.php file, the input parameters are not checked, resulting in input mishandling by the rmdir method. Attackers can delete arbitrary files by using "." directory traversal.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5887</a> <a href="#">MISC</a>
shopxo -- shopxo	An issue was discovered in ShopXO 1.2.0. In the application/install/controller/index.php file, there is no validation lock file in the Add method, which allows an attacker to reinstall the database. The attacker can write arbitrary code to database.php during system reinstallation.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5886</a> <a href="#">MISC</a>
svgpp -- svgpp	An issue was discovered in Anti-Grain Geometry (AGG) 2.4 as used in SVG++ (aka svgpp) 1.2.3. A heap-based buffer overflow bug in svgpp_agg_render may lead to code execution. In the render_scanlines_aa_solid function, the blend_hline function is called repeatedly multiple times. blend_hline is equivalent to a loop containing write operations. Each call writes a piece of heap data, and multiple calls overwrite the data in the heap.	2019-01-12	not yet calculated	<a href="#">CVE-2019-6247</a> <a href="#">MISC</a>
svgpp -- svgpp	An issue was discovered in SVG++ (aka svgpp) 1.2.3. After calling the gil::get_color function in Generic Image Library in Boost, the return code is used as an address, leading to an Access Violation because of an out-of-bounds read.	2019-01-12	not yet calculated	<a href="#">CVE-2019-6246</a> <a href="#">MISC</a>
svgpp -- svgpp	An issue was discovered in Anti-Grain Geometry (AGG) 2.4 as used in SVG++ (aka svgpp) 1.2.3. In the function agg::cell_aa::not_equal, dx is assigned to (x2 - x1). If dx >= dx_limit, which is (16384 << poly_subpixel_shift), this function will call itself recursively. There can	2019-01-12	not yet calculated	<a href="#">CVE-2019-6245</a>

	be a situation where $(x2 - x1)$ is always bigger than $dx\_limit$ during the recursion, leading to continual stack consumption.			MISC
systemd-journald -- systemd-journald	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16866</a> B.D <a href="#">CONFIRM</a> UBUNTU MISC
systemd-journald -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16865</a> B.D <a href="#">CONFIRM</a> UBUNTU MISC
systemd-journald -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16864</a> B.D <a href="#">CONFIRM</a> UBUNTU MISC
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an attacker on the same network segment to bypass access restriction to access the information and files stored on the affected device.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16197</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier may allow an attacker on the same network segment to access a non-documented developer screen to perform operations on the affected device.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16198</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Cross-site scripting vulnerability in Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an remote attacker to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16199</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an attacker on the same network segment to execute arbitrary OS commands.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16200</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier uses hard-coded credentials, which may allow an attacker on the same network segment to login to the administrators settings screen and change the configuration or execute arbitrary OS commands.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16201</a> MISC JVN
traccar -- traccar_server	In Traccar Server version 4.2, protocol/SpotProtocolDecoder.java might allow XXE attacks.	2019-01-09	not yet calculated	<a href="#">CVE-2019-5748</a> MISC MISC
usualtoolcms -- usualtoolcms	An issue was discovered in UsualToolCMS 8.0. cmsadmin/a_sqlbackx.php?t=sql allows CSRF attacks that can execute SQL statements, and consequently execute arbitrary PHP code by writing that code into a php file.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6244</a> MISC
weseek -- growi	Cross-site scripting vulnerability in GROWI v3.2.3 and earlier allows remote attackers to inject arbitrary web script or HTML via New Page modal.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16205</a> JVN MISC
weseek -- growi	Cross-site scripting vulnerability in GROWI v3.2.3 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0698</a> JVN MISC
windows -- dhcp_client	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka "Windows DHCP Client Remote Code Execution Vulnerability." This affects Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0547</a> B.D <a href="#">CONFIRM</a>
winscp -- winscp	In WinSCP before 5.14 beta, due to missing validation, the scp implementation would accept arbitrary files sent by the server, potentially overwriting unrelated files. This affects TSCPFileSystem::SCPSink in core/ScpFileSystem.cpp.	2019-01-10	not yet calculated	<a href="#">CVE-2018-20684</a> B.D MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the RTSE dissector and other ASN.1 dissectors could crash. This was addressed in epan/charsets.c by adding a get_t61_string length check.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5718</a> B.D MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the ISAKMP dissector could crash. This was addressed in epan/dissectors/packet-isakmp.c by properly handling the case of a missing decryption data block.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5719</a> MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the P_MUL dissector could crash. This was addressed in epan/dissectors/packet-p_mul.c by rejecting the invalid sequence number of zero.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5717</a> B.D MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.4.0 to 2.4.11, the ENIP dissector could crash. This was addressed in epan/dissectors/packet-enip.c by changing the memory-management approach so that a use-after-free is avoided.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5721</a> MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5, the 6LoWPAN dissector could crash. This was addressed in epan/dissectors/packet-6lowpan.c by avoiding use of a TVB before its creation.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5716</a> B.D MISC MISC

				MISC
wordpress -- wordpress	Cross-site scripting vulnerability in WordPress plugin spam-byebye 2.2.1 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-12	not yet calculated	<a href="#">CVE-2018-16206</a> JVN MISC
wordpress -- wordpress	SQL injection vulnerability in the LearnPress prior to version 3.1.0 allows attacker with administrator rights to execute arbitrary SQL commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16175</a> JVN MISC
wordpress -- wordpress	Open redirect vulnerability in LearnPress prior to version 3.1.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16174</a> JVN MISC
wordpress -- wordpress	Cross-site scripting vulnerability in LearnPress prior to version 3.1.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16173</a> JVN MISC
wordpress -- wordpress	The "Social Pug - Easy Social Share Buttons" plugin before 1.2.6 for WordPress allows XSS via the wp-admin/admin.php?page=dpsp-toolkit&dpsp_message_class parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2016-10736</a> MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Event Calendar WD version 1.1.21 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16164</a> JVN MISC MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Google XML Sitemaps Version 4.0.9 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16204</a> JVN MISC
xiaocms -- xiaocms	An issue was discovered in XiaoCms 20141229. It allows admin/index.php?c=database table[] SQL injection. This can be used for PHP code execution via " NTO UTF LE" with a .php filename.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6127</a> MISC
xterm.js -- xterm.js	A remote code execution vulnerability exists in Xterm.js when the component mishandles special characters, aka "Xterm Remote Code Execution Vulnerability." This affects xterm.js.	2019-01-09	not yet calculated	<a href="#">CVE-2019-0542</a> B.D MISC
yamaha -- multiple_routers	Yamaha routers RT57i Rev 8.00.95 and earlier, RT58i Rev 9.01.51 and earlier, NVR500 Rev.11.00.36 and earlier, RTX810 Rev.11.01.31 and earlier, allow an administrative user to embed arbitrary scripts to the configuration data through a certain form field of the configuration page, which may be executed on another administrative user's web browser. This is a different vulnerability from CVE-2018-0666.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0665</a> MISC MISC JVN MISC
yamaha -- multiple_routers	Yamaha routers RT57i Rev 8.00.95 and earlier, RT58i Rev 9.01.51 and earlier, NVR500 Rev.11.00.36 and earlier, RTX810 Rev.11.01.31 and earlier, allow an administrative user to embed arbitrary scripts to the configuration data through a certain form field of the configuration page, which may be executed on another administrative user's web browser. This is a different vulnerability from CVE-2018-0665.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0666</a> MISC MISC JVN MISC
yokogawa -- multiple_products	Buffer overflow in the license management function of YOKOGAWA products (iDefine for ProSafe-RS R1.16.3 and earlier, STARDOM VDS R7.50 and earlier, STARDOM FCN/FCJ Simulator R4.20 and earlier, ASTPLANNER R15.01 and earlier, TriFellows V5.04 and earlier) allows remote attackers to stop the license management function or execute an arbitrary program via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0651</a> B.D MISC MISC
yokogawa -- multiple_products	Multiple Yokogawa products that contain Vnet/ P Open Communication Driver (CENTUM CS 3000(R3.05.00 - R3.09.50), CENTUM CS 3000 Entry Class(R3.05.00 - R3.09.50), CENTUM VP(R4.01.00 - R6.03.10), CENTUM VP Entry Class(R4.01.00 - R6.03.10), Exaopc(R3.10.00 - R3.75.00), PRM(R2.06.00 - R3.31.00), ProSafe-RS(R1.02.00 - R4.02.00), FAST/TOOLS(R9.02.00 - R10.02.00), B/M9000 VP(R6.03.01 - R8.01.90)) allows remote attackers to cause a denial of service attack that may result in stopping Vnet/IP Open Communication Driver's communication via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16196</a> B.D MISC MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

From: [US-CERT](#)  
To: [wpulfate@cs.sunnyvale.ca.us](mailto:wpulfate@cs.sunnyvale.ca.us)  
Subject: SB19-014: Vulnerability Summary for the Week of January 7, 2019  
Date: Monday, January 14, 2019 1:08:48 PM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## SB19-014: Vulnerability Summary for the Week of January 7, 2019

01/14/2019 06:27 AM EST

Original release date: January 14, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- edge	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka "Microsoft Edge Memory Corruption Vulnerability." This affects Microsoft Edge.	2019-01-08	7.6	<a href="#">CVE-2019-0565</a> B D <a href="#">CONFIRM</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
arc_project -- arc	ARC 5.21q allows directory traversal via a full pathname in an archive file.	2019-01-07	5.0	<a href="#">CVE-2015-9275</a> MISC MISC
getbootstrap -- bootstrap	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.	2019-01-09	4.3	<a href="#">CVE-2016-10735</a> MISC MISC MISC MISC MISC
ibm -- api_connect	BM API Connect 5.0.0.0 through 5.0.8.4 could allow a user authenticated as an administrator with limited rights to escalate their privileges. IBM X-Force ID: 151258.	2019-01-04	6.5	<a href="#">CVE-2018-1859</a> B D X E <a href="#">CONFIRM</a>
microsoft -- asp_net_core	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka "ASP.NET Core Denial of Service Vulnerability." This affects ASP.NET Core 2.1. This CVE ID is unique from CVE-2019-0548.	2019-01-08	5.0	<a href="#">CVE-2019-0564</a> B D REDHAT <a href="#">CONFIRM</a>
microsoft -- office	An information disclosure vulnerability exists when Microsoft Outlook improperly handles certain types of messages, aka "Microsoft Outlook Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Outlook.	2019-01-08	4.3	<a href="#">CVE-2019-0559</a> B D <a href="#">CONFIRM</a>
microsoft -- office	An information disclosure vulnerability exists when Microsoft Office improperly discloses the contents of its memory, aka "Microsoft Office Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office.	2019-01-08	4.3	<a href="#">CVE-2019-0560</a> B D <a href="#">CONFIRM</a>
yunucms -- yunucms	YUNUCMS 1.1.8 has XSS in app/admin/controller/System.php because crafted data can be written to the sys.php file, as demonstrated by site_title in an admin/system/basic POST request.	2019-01-04	4.3	<a href="#">CVE-2019-5310</a> MISC
yunucms -- yunucms	An issue was discovered in YUNUCMS V1.1.8. app/index/controller/Show.php has an XSS vulnerability via the index.php/index/show/index_cw parameter.	2019-01-04	4.3	<a href="#">CVE-2019-5311</a> MISC

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
frog cms_project -- frog cms	Frog CMS 0.9.5 has XSS in the admin/?/page/edit/1 body field.	2019-01-09	3.5	<a href="#">CVE-2018-20680</a>



				MISC
ibm -- rational_publishing_engine	BM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-force ID: 144883.	2019-01-04	3.5	<a href="#">CVE-2018-1657</a> <a href="#">B.D</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>
ibm -- rational_publishing_engine	BM Publishing Engine 2.1.2, 6.0.5, and 6.0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 153494.	2019-01-04	3.5	<a href="#">CVE-2018-1951</a> <a href="#">B.D</a> <a href="#">X.F</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- karaf	Apache Karaf provides a features deployer, which allows users to "hot deploy" a features XML by dropping the file directly in the deploy folder. The features XML is parsed by XMLInputFactory class. Apache Karaf XMLInputFactory class doesn't contain any mitigation codes against XXE. This is a potential security risk as an user can inject external XML entities in Apache Karaf version prior to 4.1.7 or 4.2.2. It has been fixed in Apache Karaf 4.1.7 and 4.2.2 releases.	2019-01-07	not yet calculated	<a href="#">CVE-2018-11788</a> <a href="#">MISC</a> <a href="#">B.D</a>
apache -- thrift	Apache Thrift Java client library versions 0.5.0 through 0.11.0 can bypass SASL negotiation isComplete validation in the org.apache.thrift.transport.TSaslTransport class. An assert used to determine if the SASL handshake had successfully completed could be disabled in production settings making the validation incomplete.	2019-01-07	not yet calculated	<a href="#">CVE-2018-1320</a> <a href="#">MISC</a>
apache -- thrift	The Apache Thrift Node.js static web server in versions 0.9.2 through 0.11.0 have been determined to contain a security vulnerability in which a remote user has the ability to access files outside the set webservers docroot path.	2019-01-07	not yet calculated	<a href="#">CVE-2018-11798</a> <a href="#">B.D</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the Clean My Mac X, version 4.04, helper service due to improper input validation. A user with local access can use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4043</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4047</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the way the CleanMyMac X software improperly validates inputs. An attacker with local access could use this vulnerability to modify the file system as root. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4032</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4033</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4034</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4045</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access could use this vulnerability to modify the running kernel extensions on the system.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4036</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability due to improper input validation. An attacker with local access can use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4037</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	The CleanMyMac X software contains an exploitable privilege escalation vulnerability that exists due to improper input validation. An attacker with local access could use this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4035</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable denial-of-service vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. A user with local access can use this vulnerability to terminate a privileged helper application. An attacker would need local access to the machine for a successful exploit.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4046</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4041</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4042</a> <a href="#">MISC</a>
apple -- cleanmy_mac_x	An exploitable privilege escalation vulnerability exists in the helper service of Clean My Mac X, version 4.04, due to improper input validation. An attacker with local access could exploit this vulnerability to modify the file system as root.	2019-01-10	not yet calculated	<a href="#">CVE-2018-4044</a> <a href="#">MISC</a>
apple -- ios	In iOS before 11.2, exchange rates were retrieved from HTTP rather than HTTPS. This was addressed by enabling HTTPS for exchange rates.	2019-01-11	not yet calculated	<a href="#">CVE-2017-2411</a> <a href="#">CONFIRM</a>
	In iOS before 11.4 and macOS High Sierra before 10.13.5, a memory	2019-01-	not yet	<a href="#">CVE-2018-4404</a> <a href="#">MISC</a>

apple -- ios	corruption issue exists and was addressed with improved memory handling.	11	calculated	<a href="#">CONFIRM</a> <a href="#">EXPLOIT-DB</a>
apple -- ios	In iOS before 11.2, an inconsistent user interface issue was addressed through improved state management.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13891</a> <a href="#">CONFIRM</a>
apple -- ios	In iOS before 11.2, a type confusion issue was addressed with improved memory handling.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13888</a> <a href="#">CONFIRM</a>
apple -- ios	In iOS before 11.4, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4330</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">CONFIRM</a>
apple -- ios	In iOS before 9.3.3, a memory corruption issue existed in the kernel. This issue was addressed through improved memory handling.	2019-01-11	not yet calculated	<a href="#">CVE-2016-7576</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4257</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4255</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an input validation issue existed in the kernel. This issue was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4254</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a privacy issue in the handling of Open Directory records was addressed with improved indexing.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4217</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4183</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an access issue was addressed with additional sandbox restrictions on CUPS.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4182</a> <a href="#">CONFIRM</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4181</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4180</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved bounds checking.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4258</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4256</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.4, there was an issue with the handling of smartcard PNs. This issue was addressed with additional logic.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4179</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, an access issue existed with privileged WiFi system configuration. This issue was addressed with additional restrictions.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13886</a> <a href="#">CONFIRM</a>
apple -- macos_high_sierra	In macOS High Sierra before 10.13.2, a logic issue existed in APFS when deleting keys during hibernation. This was addressed with improved state management.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13887</a> <a href="#">CONFIRM</a>
apple -- multiple_products	In iOS before 11.4, iCloud for Windows before 7.5, watchOS before 4.3.1, iTunes before 12.7.5 for Windows, and macOS High Sierra before 10.13.5, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4194</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a logic error existed in the validation of credentials. This was addressed with improved credential validation.	2019-01-11	not yet calculated	<a href="#">CVE-2017-13889</a> <a href="#">CONFIRM</a>
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, an out-of-bounds read was addressed with improved input validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4169</a> <a href="#">CONFIRM</a>
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, sound fetched through audio elements may be exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4278</a> <a href="#">SECTRAK</a> <a href="#">GENTOO</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">UBUNTU</a>
apple -- multiple_products	In iOS before 11.4.1, watchOS before 4.3.2, tvOS before 11.4.1, Safari before 11.1.1, macOS High Sierra before 10.13.6, a spoofing issue existed in the handling of URLs. This issue was addressed with	2019-01-11	not yet calculated	<a href="#">CVE-2018-4277</a> <a href="#">SECTRAK</a> <a href="#">MISC</a> <a href="#">MISC</a>

	improved input validation.			MISC CONFIRM MISC
apple -- multiple_products	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, multiple memory corruption issues were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4262 SECTRACK GENTOO MISC CONFIRM MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4213 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, a permissions issue existed in Remote Management. This issue was addressed through improved permission validation.	2019-01-11	not yet calculated	CVE-2018-4298 CONFIRM MISC
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4212 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, an array indexing issue existed in the handling of a function in javascript core. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4210 GENTOO MISC MISC CONFIRM UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4209 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4208 GENTOO MISC MISC CONFIRM MISC UBUNTU
apple -- multiple_products	In iOS before 11.3, Safari before 11.1, iCloud for Windows before 7.4, tvOS before 11.3, watchOS before 4.3, iTunes before 12.7.4 for Windows, unexpected interaction causes an ASSERT failure. This issue was addressed with improved checks.	2019-01-11	not yet calculated	CVE-2018-4207 GENTOO MISC CONFIRM MISC MISC UBUNTU
apple -- multiple_products	In iOS before 11.2.5, macOS High Sierra before 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan, watchOS before 4.2.2, and tvOS before 11.2.5, a memory corruption issue exists and was addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4189 CONFIRM MISC MISC
apple -- multiple_products	In iCloud for Windows before 7.3, Safari before 11.0.3, iTunes before 12.7.3 for Windows, and iOS before 11.2.5, multiple memory corruption issues exist and were addressed with improved memory handling.	2019-01-11	not yet calculated	CVE-2018-4147 CONFIRM MISC MISC MISC
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a downgrade issue existed with HTTP authentication credentials saved in Keychain. This issue was addressed by storing the authentication types with the credentials.	2019-01-11	not yet calculated	CVE-2016-4644 MISC MISC CONFIRM
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, a validation issue existed in the parsing of 407 responses. This issue was addressed through improved response validation.	2019-01-11	not yet calculated	CVE-2016-4643 MISC MISC CONFIRM
	In iOS before 11.3, tvOS before 11.3, watchOS before 4.3, and			CVE-2018-4185

apple -- multiple_products	macOS before High Sierra 10.13.4, an information disclosure issue existed in the transition of program state. This issue was addressed with improved state handling.	2019-01-11	not yet calculated	MISC <a href="#">MISC CONFIRM MISC</a>
apple -- multiple_products	In iOS before 9.3.3, tvOS before 9.2.2, and OS X El Capitan before v10.11.6 and Security Update 2016-004, proxy authentication incorrectly reported HTTP proxies received credentials securely. This issue was addressed through improved warnings.	2019-01-11	not yet calculated	<a href="#">CVE-2016-4642</a> MISC <a href="#">MISC CONFIRM</a>
apple -- safari	In Safari before 11.1, an information leakage issue existed in the handling of downloads in Safari Private Browsing. This issue was addressed with additional validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4186</a> <a href="#">CONFIRM</a>
apple -- swiftnio	In SwiftNIO before 1.8.0, a buffer overflow was addressed with improved size validation.	2019-01-11	not yet calculated	<a href="#">CVE-2018-4281</a> <a href="#">CONFIRM</a>
artifex -- mupdf	Artifex MuPDF 1.14.0 has a SEGV in the function fz_load_page of the fitz/document.c file, as demonstrated by mutool. This is related to page-number mishandling in cbz/mucbz.c, cbz/mulimg.c, and svg/svg-doc.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6130</a> MISC
artifex -- mupdf	svg-run.c in Artifex MuPDF 1.14.0 has infinite recursion with stack consumption in svg_run_use_symbol, svg_run_element, and svg_run_use, as demonstrated by mutool.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6131</a> MISC
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter or bootmode parameter of a certain URL.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0634</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via filename parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0635</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via FactoryPassword parameter of a certain URL, different URL from CVE-2018-0634.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0636</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via import cgi encKey parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0638</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via tools_firmware cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0639</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary code via netWizard.cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0640</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Buffer overflow in Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary code via tools_system cgi date parameter, time parameter, and offset parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0641</a> MISC <a href="#">JVN</a>
aterm -- hc100rc	Aterm HC100RC Ver1.0.1 and earlier allows attacker with administrator rights to execute arbitrary OS commands via export cgi encKey parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0637</a> MISC <a href="#">JVN</a>
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via submit-url parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0633</a> MISC <a href="#">JVN</a>
aterm -- w300p	Buffer overflow in Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary code via HTTP request and response.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0632</a> MISC <a href="#">JVN</a>
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via targetAPSSid parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0631</a> MISC <a href="#">JVN</a>
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0629</a> MISC <a href="#">JVN</a>
aterm -- w300p	Aterm W300P Ver1.0.13 and earlier allows attacker with administrator rights to execute arbitrary OS commands via sysCmd parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0630</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via HTTP request and response.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0628</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via targetAPSSid parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0627</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via sysCmd in formVsc parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0626</a> MISC <a href="#">JVN</a>
aterm -- wg1200hp_firmware	Aterm WG1200HP firmware Ver1.0.31 and earlier allows attacker with administrator rights to execute arbitrary OS commands via formSysCmd parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0625</a> MISC <a href="#">JVN</a>
bento4 -- bento4	An issue was discovered in Bento4 v1.5.1-627. There is a memory leak in AP4_DescriptorFactory::CreateDescriptorFromStream in Core/AP4DescriptorFactory.cpp when called from the AP4_EsdsAtom class in Core/AP4EsdsAtom.cpp, as demonstrated by mp42aac.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6132</a> MISC

bodhi -- bodhi	Bodhi 2.9 0 and lower is vulnerable to cross-site scripting resulting in code injection caused by incorrect validation of bug titles.	2019-01-10	not yet calculated	<a href="#">CVE-2017-1002152</a> <a href="#">CONFIRM</a>
bootstrap -- bootstrap	In Bootstrap before 3.4 0, XSS is possible in the affix configuration target property.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20677</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
bootstrap -- bootstrap	In Bootstrap before 3.4 0, XSS is possible in the tooltip data-viewport attribute.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20676</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
busybox -- busybox	An issue was discovered in BusyBox through 1 30 0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and/or relay) might allow a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to assurance of a 4-byte length when decoding DHCP_SUBNET. NOTE: this issue exists because of an incomplete fix for CVE-2018-20679.	2019-01-09	not yet calculated	<a href="#">CVE-2019-5747</a> <a href="#">MISC</a> <a href="#">MISC</a>
busybox -- busybox	An issue was discovered in BusyBox before 1 30 0. An out of bounds read in udhcp components (consumed by the DHCP server, client, and relay) allows a remote attacker to leak sensitive information from the stack by sending a crafted DHCP message. This is related to verification in udhcp_get_option() in networking/udhcp/common.c that 4-byte options are indeed 4 bytes.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20679</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cimtechniques -- cimsan	In CIMTechniques C MScan 6 x through 6 2, the SOAP WSDL parser allows attackers to execute SQL code.	2019-01-10	not yet calculated	<a href="#">CVE-2018-16803</a> <a href="#">MISC</a> <a href="#">MISC</a>
cisco -- 900_series_aggregation_services_router	A vulnerability in Cisco 900 Series Aggregation Services Router (ASR) software could allow an unauthenticated, remote attacker to cause a partial denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient handling of certain broadcast packets ingress to the device. An attacker could exploit this vulnerability by sending large streams of broadcast packets to an affected device. If successful, an exploit could allow an attacker to impact services running on the device, resulting in a partial DoS condition.	2019-01-11	not yet calculated	<a href="#">CVE-2018-15464</a> <a href="#">CISCO</a>
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the Secure/Multipurpose Internet Mail Extensions (S/M ME) Decryption and Verification or S/M ME Public Key Harvesting features of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause an affected device to corrupt system memory. A successful exploit could cause the filtering process to unexpectedly reload, resulting in a denial of service (DoS) condition on the device. The vulnerability is due to improper input validation of S/M ME-signed emails. An attacker could exploit this vulnerability by sending a malicious S/MIME-signed email through a targeted device. If Decryption and Verification or Public Key Harvesting is configured, the filtering process could crash due to memory corruption and restart, resulting in a DoS condition. The software could then resume processing the same S/M ME-signed email, causing the filtering process to crash and restart again. A successful exploit could allow the attacker to cause a permanent DoS condition. This vulnerability may require manual intervention to recover the ESA.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15453</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- cisco_asyncos_software_for_cisco_email_security_appliance	A vulnerability in the email message filtering feature of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) could allow an unauthenticated, remote attacker to cause the CPU utilization to increase to 100 percent, causing a denial of service (DoS) condition on an affected device. The vulnerability is due to improper filtering of email messages that contain references to whitelisted URLs. An attacker could exploit this vulnerability by sending a malicious email message that contains a large number of whitelisted URLs. A successful exploit could allow the attacker to cause a sustained DoS condition that could force the affected device to stop scanning and forwarding email messages.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15460</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- firepower_management_center	A vulnerability in the Shell Access Filter feature of Cisco Firepower Management Center (FMC), when used in conjunction with remote authentication, could allow an unauthenticated, remote attacker to cause high disk utilization, resulting in a denial of service (DoS) condition. The vulnerability occurs because the configuration of the Shell Access Filter, when used with a specific type of remote authentication, can cause a system file to have unbounded writes. An attacker could exploit this vulnerability by sending a steady stream of remote authentication requests to the appliance when the specific configuration is applied. Successful exploitation could allow the attacker to increase the size of a system log file so that it consumes most of the disk space. The lack of available disk space could lead to a DoS condition in which the device functions could operate abnormally, making the device unstable.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15458</a> <a href="#">B D</a> <a href="#">CISCO</a>
cisco -- identity_services_engine	A vulnerability in the Admin Portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to view saved passwords in plain text. The vulnerability is due to the incorrect inclusion of saved passwords when loading configuration pages in the Admin Portal. An attacker with read or write access to the Admin Portal could exploit this vulnerability by browsing to a page that contains sensitive data. An exploit could allow the attacker to recover passwords for unauthorized use and expose those accounts to further attack.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15456</a> <a href="#">B D</a> <a href="#">CISCO</a>
	A vulnerability in the TCP socket code of Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload. The vulnerability is due to a state			



cisco -- ios_and_ios_xe_software	condition between the socket state and the transmission control block (TCB) state. While this vulnerability potentially affects all TCP applications, the only affected application observed so far is the HTTP server. An attacker could exploit this vulnerability by sending specific HTTP requests at a sustained rate to a reachable IP address of the affected software. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition on an affected device.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0282</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- ios_and_ios_xe_software	A vulnerability in the access control logic of the Secure Shell (SSH) server of Cisco IOS and IOS XE Software may allow connections sourced from a virtual routing and forwarding (VRF) instance despite the absence of the vrf-also keyword in the access-class configuration. The vulnerability is due to a missing check in the SSH server. An attacker could use this vulnerability to open an SSH connection to an affected Cisco IOS or IOS XE device with a source address belonging to a VRF instance. Once connected, the attacker would still need to provide valid credentials to access the device.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0484</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- ip_phone_8800_series_software	A vulnerability in the Cisco IP Phone 8800 Series Software could allow an unauthenticated, remote attacker to conduct an arbitrary script injection attack on an affected device. The vulnerability exists because the software running on an affected device insufficiently validates user-supplied data. An attacker could exploit this vulnerability by persuading a user to click a malicious link provided to the user or through the interface of an affected device. A successful exploit could allow an attacker to execute arbitrary script code in the context of the user interface or access sensitive system-based information, which under normal circumstances should be prohibited.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0461</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- jabber_client_framework	A vulnerability in the Cisco Jabber Client Framework (JCF) software, installed as part of the Cisco Jabber for Mac client, could allow an authenticated, local attacker to corrupt arbitrary files on an affected device that has elevated privileges. The vulnerability exists due to insecure directory permissions set on a JCF created directory. An authenticated attacker with the ability to access an affected directory could create a hard link to an arbitrary location on the affected system. An attacker could convince another user that has administrative privileges to perform an install or update the Cisco Jabber for Mac client to perform such actions, allowing files to be created in an arbitrary location on the disk or an arbitrary file to be corrupted when it is appended to or overwritten.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0449</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- jabber_client_framework	A vulnerability in Cisco Jabber Client Framework (JCF) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of an affected system. The vulnerability is due to insufficient validation of user-supplied input of an affected client. An attacker could exploit this vulnerability by executing arbitrary JavaScript in the Jabber client of the recipient. A successful exploit could allow the attacker to execute arbitrary script code in the context of the targeted client or allow the attacker to access sensitive client-based information.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0483</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- policy_suite_for_mobile_and_policy_suite_diameter_routing_agent_software	A vulnerability in the Redis implementation used by the Cisco Policy Suite for Mobile and Cisco Policy Suite Diameter Routing Agent software could allow an unauthenticated, remote attacker to modify key-value pairs for short-lived events stored by the Redis server. The vulnerability is due to improper authentication when accessing the Redis server. An unauthenticated attacker could exploit this vulnerability by modifying key-value pairs stored within the Redis server database. An exploit could allow the attacker to reduce the efficiency of the Cisco Policy Suite for Mobile and Cisco Policy Suite Diameter Routing Agent software.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0181</a> <a href="#">CISCO</a>
cisco -- policy_suite	A vulnerability in the Graphite web interface of the Policy and Charging Rules Function (PCRF) of Cisco Policy Suite (CPS) could allow an unauthenticated, remote attacker to access the Graphite web interface. The attacker would need to have access to the internal VLAN where CPS is deployed. The vulnerability is due to lack of authentication. An attacker could exploit this vulnerability by directly connecting to the Graphite web interface. An exploit could allow the attacker to access various statistics and Key Performance Indicators (KPIs) regarding the Cisco Policy Suite environment.	2019-01-11	not yet calculated	<a href="#">CVE-2018-15466</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15457</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- prime_network_control_system	A vulnerability in the web-based management interface of Cisco Prime Network Control System could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the web interface of the affected system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web-based management interface or allow the attacker to access sensitive browser-based information.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0482</a> <a href="#">B.D</a> <a href="#">CISCO</a>
cisco -- telepresence_management_suite	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive	2019-01-11	not yet calculated	<a href="#">CVE-2018-15467</a> <a href="#">B.D</a> <a href="#">CISCO</a>

	browser-based information.			
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to view digest credentials in clear text. The vulnerability is due to the incorrect inclusion of saved passwords in configuration pages. An attacker could exploit this vulnerability by logging in to the Cisco Unified Communications Manager web-based management interface and viewing the source code for the configuration page. A successful exploit could allow the attacker to recover passwords and expose those accounts to further attack.	2019-01-10	not yet calculated	<a href="#">CVE-2018-0474</a> CISCO
cisco -- webex_business_suite	A vulnerability in the MyWebex component of Cisco Webex Business Suite could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by convincing a user to click a crafted URL. To exploit this vulnerability, the attacker may provide a link that directs a user to a malicious site and use misleading language or instructions to persuade the user to follow the provided link.	2019-01-10	not yet calculated	<a href="#">CVE-2018-15461</a> B.D CISCO
cybozu -- dezie	Directory traversal vulnerability in Cybozu Dezie 8.0.2 to 8.1.2 allows remote attackers to read arbitrary files via HTTP requests.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0705</a> JVN MISC
cybozu -- garoon	Cybozu Garoon 3.0.0 to 4.10.0 allows remote attackers to bypass access restriction to view information available only for a sign-on user via Single sign-on function.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16178</a> JVN MISC
cybozu -- mailwise	Directory traversal vulnerability in Cybozu Mailwise 5.0.0 to 5.4.5 allows remote attackers to delete arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0702</a> JVN MISC
cybozu -- office	Directory traversal vulnerability in Cybozu Office 10.0.0 to 10.8.1 allows remote attackers to delete arbitrary files via HTTP requests.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0703</a> JVN MISC
cybozu -- office	Directory traversal vulnerability in Cybozu Office 10.0.0 to 10.8.1 allows remote attackers to delete arbitrary files via Keitai Screen.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0704</a> JVN MISC
cybozu -- remote_service	Cybozu Remote Service 3.0.0 to 3.1.0 allows remote authenticated attackers to upload and execute Java code file on the server via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16169</a> JVN MISC
cybozu -- remote_service	Improper countermeasure against clickjacking attack in client certificates management screen was discovered in Cybozu Remote Service 3.0.0 to 3.1.8, that allows remote attackers to trick a user to delete the registered client certificate.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16172</a> JVN MISC
cybozu -- remote_service	Directory traversal vulnerability in Cybozu Remote Service 3.0.0 to 3.1.8 allows remote attackers to execute Java code file on the server via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16171</a> JVN MISC
cybozu -- remote_service	Directory traversal vulnerability in Cybozu Remote Service 3.0.0 to 3.1.8 for Windows allows remote authenticated attackers to read arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16170</a> JVN MISC
d-link -- multiple_devices	D-Link D R-822 C1 before v3.11B01Beta, DIR-822-US C1 before v3.11B01Beta, D R-850L A* before v1 21B08Beta, D R-850L B* before v2.22B03Beta, and DIR-880L A* before v1 20B02Beta devices allow authentication bypass.	2019-01-08	not yet calculated	<a href="#">CVE-2018-20675</a> MISC
d-link -- multiple_devices	D-Link D R-822 C1 before v3.11B01Beta, DIR-822-US C1 before v3.11B01Beta, D R-850L A* before v1 21B08Beta, D R-850L B* before v2.22B03Beta, and DIR-880L A* before v1 20B02Beta devices allow authenticated remote command execution.	2019-01-08	not yet calculated	<a href="#">CVE-2018-20674</a> MISC
digital_arts -- i-filter	HTTP header injection vulnerability in i-FILTER Ver 9.50R05 and earlier may allow remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks that may result in an arbitrary script injection or setting an arbitrary cookie values via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16181</a> MISC JVN
digital_arts -- i-filter	Cross-site scripting vulnerability in i-FILTER Ver.9.50R05 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16180</a> MISC JVN
django -- django	In Django 1.11.x before 1.11.18, 2.0.x before 2.0.10, and 2.1.x before 2.1.5, an Improper Neutralization of Special Elements in Output Used by a Downstream Component issue exists in django.views.defaults.page_not_found(), leading to content spoofing (in a 404 error page) if a user fails to recognize that a crafted URL has malicious content.	2019-01-09	not yet calculated	<a href="#">CVE-2019-3498</a> B.D MISC MLIST UBUNTU DEBIAN MISC
docker_engine -- docker_engine	Docker Engine before 18.09 allows attackers to cause a denial of service (dockerd memory consumption) via a large integer in a --cpuset-mems or --cpuset-cpus value, related to daemon/daemon_unix.go, pkg/parsers/parsers.go, and pkg/sysinfo/sysinfo.go.	2019-01-11	not yet calculated	<a href="#">CVE-2018-20699</a> MISC MISC
dokan -- dokan	Dokan, versions between 1.0.0.5000 and 1.2.0.1000, are vulnerable to a stack-based buffer overflow in the dokan1.sys driver. An attacker can create a device handle to the system driver and send arbitrary input that will trigger the vulnerability. This vulnerability was introduced in the 1.0.0.5000 version update.	2019-01-07	not yet calculated	<a href="#">CVE-2018-5410</a> B.D MISC CONFIRM CERT-VN
elfinder -- elfinder	php/elfinder.class.php in elfinder before 2.1.45 leaks information if PHP's curl extension is enabled and safe_mode or open_basedir is not set.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5884</a> MISC MISC

fork -- fork_cms	Fork CMS 5.0.6 allows stored XSS via the private/en/settings facebook_admin_ids parameter (aka "Admin ids" input in the Facebook section).	2019-01-09	not yet calculated	<a href="#">CVE-2018-20682</a> <a href="#">MISC</a>
frog_cms -- frog_cms	Frog CMS 0.9.5 allows XSS via the forgot password page (aka the /admin/?/login/forgot URI).	2019-01-11	not yet calculated	<a href="#">CVE-2019-6243</a> <a href="#">MISC</a>
frontaccounting -- frontaccounting	includes/db/class.reflines_db.inc in FrontAccounting 2.4.6 contains a SQL Injection vulnerability in the reference field that can allow the attacker to grab the entire database of the application via the void_transaction.php filterType parameter.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5720</a> <a href="#">MISC</a>
frouting -- frouting	bgpd in FRRouting FRR (aka Free Range Routing) 2.x and 3.x before 3.0.4, 4.x before 4.0.1, 5.x before 5.0.2, and 6.x before 6.0.2 (not affecting Cumulus Linux or VyOS), when ENABLE_BGP_VNC is used for Virtual Network Control, allows remote attackers to cause a denial of service (peering session flap) via attribute 255 in a BGP UPDATE packet. This occurred during Disco in January 2019 because FRR does not implement RFC 7606, and therefore the packets with 255 were considered invalid VNC data and the BGP session was closed.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5892</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gitolite -- gitolite	commands/rsync in Gitolite before 3.6.11, if gitolite rc enables rsync, mishandles the rsync command line, which allows attackers to have a "bad" impact by triggering use of an option other than -v, -n, -q, or -P.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20683</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- binutils	load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20671</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20673</a> <a href="#">B.D</a> <a href="#">MISC</a>
google -- chrome	The default selected dialog button in CustomHandlers in Google Chrome prior to 69.0.3497.81 allowed a remote attacker who convinced the user to perform certain operations to open external programs via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16084</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Failure to prevent navigation to top frame to data URLs in Navigation in Google Chrome on iOS prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20069</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of 304 status codes in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20068</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	A renderer initiated back navigation was incorrectly allowed to cancel a browser initiated one in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of the current page via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20067</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect object lifecycle in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20066</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Handling of URI action in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to initiate potentially unsafe navigations without a user gesture via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20065</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6166</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6163</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of reloads in Navigation in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6165</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient origin checks for CSS content in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6164</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
				<a href="#">CVE-2018-</a>

google -- chrome	Improper deserialization in WebGL in Google Chrome on Mac prior to 68.0 3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">6162</a> <a href="#">B D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A heap buffer overflow in GPU in Google Chrome prior to 70.0 3538.67 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17470</a> <a href="#">B D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An out of bounds read in PDFium in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17461</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of clicks in the omnibox in Navigation in Google Chrome prior to 69.0 3497.92 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17459</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	An improper update of the WebAssembly dispatch table in WebAssembly in Google Chrome prior to 69.0 3497 92 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17458</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	An object lifecycle issue in Blink could lead to a use after free in WebAudio in Google Chrome prior to 69 0 3497 81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-17457</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	JavaScript alert handling in Prompts in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6160</a> <a href="#">B D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0 3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20070</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6167</a> <a href="#">B D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficiently strict origin checks during JIT payment app installation in Payments in Google Chrome prior to 70 0 3538 67 allowed a remote attacker to install a service worker for a domain that can host attacker controlled files via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-20071</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Insufficient data validation in V8 builtins string generator could lead to out of bounds read and write access in V8 in Google Chrome prior to 62.0 3202.94 and allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15428</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	A missing check for whether a property of a JS object is private in V8 in Google Chrome prior to 55.0 2883.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2016-9651</a> <a href="#">REDHAT</a> <a href="#">B D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	A memory corruption bug in WebAssembly could lead to out of bounds read and write through V8 in WebAssembly in Google Chrome prior to 62.0 3202.62 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15401</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Using an ID that can be controlled by a compromised renderer which allows any frame to overwrite the page_state of any other frame in the same process in Navigation in Google Chrome on Chrome OS prior to 62.0.3202.74 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15402</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Insufficient data validation in crosh could lead to a command injection under chronos privileges in Networking in Google Chrome on Chrome OS prior to 61.0 3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15403</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	An ability to process crash dumps under root privileges and inappropriate symlinks handling could lead to a local privilege escalation in Crash Reporting in Google Chrome on Chrome OS prior to 61.0.3163.113 allowed a local attacker to perform privilege escalation via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15404</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
google -- chrome	Inappropriate symlink handling and a race condition in the stateful recovery feature implementation could lead to a persistence established by a malicious code running with root privileges in cryptohomed in Google Chrome on Chrome OS prior to 61.0 3163.113 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2017-15405</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
				<a href="#">CVE-2018-6179</a>

google -- chrome	Insufficient enforcement of file access permission in the activeTab case in Extensions in Google Chrome prior to 68.0 3440.75 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.	2019-01-09	not yet calculated	B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A precision error in Skia in Google Chrome prior to 68.0 3440.75 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6153</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Eliding from the wrong side in an infobar in DevTools in Google Chrome prior to 68.0 3440.75 allowed an attacker who convinced a user to install a malicious extension to Hide Chrome Security UI via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6178</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6175</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Integer overflows in Swiftshader in Google Chrome prior to 68.0 3440.75 potentially allowed a remote attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6174</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6173</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6172</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A bad cast in PDFium in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6170</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Lack of timeout on extension install prompt in Extensions in Google Chrome prior to 68.0 3440.75 allowed a remote attacker to trigger installation of an unwanted extension via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6169</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A race condition in Oilpan in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6158</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	Bad cast in DevTools in Google Chrome on Win, Linux, Mac, Chrome OS prior to 66.0 3359.117 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6151</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO DEBIAN</a>
google -- chrome	A use after free in ResourceCoordinator in Google Chrome prior to 69.0 3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16085</a> B D <a href="#">REDHAT CONFIRM</a> <a href="#">MISC GENTOO</a>
google -- chrome	A missing check for popup window handling in Fullscreen in Google Chrome on macOS prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML	2019-01-09	not yet calculated	<a href="#">CVE-2018-16080</a> B D <a href="#">REDHAT</a>



	page.			<a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Unsafe handling of credit card details in Autofill in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16078</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Incorrect handling of asynchronous methods in Fullscreen in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to enter full screen without showing a warning via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6097</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A race condition between permission prompts and navigations in Prompts in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16079</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6100</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An asynchronous generator may return an incorrect state in V8 in Google Chrome prior to 66.0.3359.117 allowing a remote attacker to potentially exploit object corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6106</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	readAsText() can indefinitely read the file picked by the user, rather than only once at the time the file is picked in File API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to access data on the user file system without explicit consent via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6109</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Parsing documents as HTML in Downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to cause Chrome to execute scripts via a local non-HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6110</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An object lifetime issue in the developer tools network handler in Google Chrome prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6111</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Allowing the chrome debugger API to run on file:// URLs in DevTools in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system without file access permission via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16081</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	A JavaScript focused window could overlap the fullscreen notification in Fullscreen in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6096</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An out of bounds read in Swiftshader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16082</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	An out of bounds read in forward error correction code in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16083</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">EXPLOIT-DB</a>
				<a href="#">CVE-2018-</a>

google -- chrome	Making URLs clickable and allowing them to be styled in DevTools in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6112</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Improper handling of pending navigation entries in Navigation in Google Chrome on iOS prior to 66.0 3359.117 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6113</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect enforcement of CSP for <object> tags in Blink in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6114</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Confusing settings in Autofill in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6117</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6120</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A missing check for JS-simulated input events in Blink in Google Chrome prior to 69.0 3497.81 allowed a remote attacker to download arbitrary files with no user input via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16088</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Lack of proper state tracking in Permissions in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16087</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Missing bounds check in PDFium in Google Chrome prior to 69.0 3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16076</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Insufficient origin checks in Blink in Google Chrome prior to 66.0 3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6093</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Lack of secure text entry mode in Browser UI in Google Chrome on Mac prior to 67.0.3396.62 allowed a local attacker to obtain potentially sensitive information from process memory via a local process.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6147</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Early free of object in use in IndexedDB in Google Chrome prior to 67.0 3396.62 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6127</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Off-by-one error in PDFium in Google Chrome prior to 67.0 3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6144</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient validation in V8 in Google Chrome prior to 67.0 3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6143</a> <a href="#">B.D</a> <a href="#">SECTRAK</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>

				<a href="#">DEBIAN</a>
google -- chrome	Insufficient validation of an image filter in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6141</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Allowing the chrome debugger API to attach to Web UI pages in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6140</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient target checks on the chrome.debugger API in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6139</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	CSS Paint API in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6137</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Lack of clearing the previous site before loading alerts from a new one in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6135</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6133</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6126</a> <a href="#">B.D</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	Service Workers can intercept any request made by an <embed> or <object> tag in Fetch API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6091</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Type confusion in ReadableStreams in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6124</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6123</a> <a href="#">B.D</a> <a href="#">SECTrack</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	A Javascript reentrancy issues that caused a use-after-free in V8 in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16065</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>

google -- chrome	A use after free in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16066</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Missing validation in Mojo in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16068</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	A use after free in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16071</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	A missing origin check related to HLS manifests in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass same origin policy via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16072</a> <a href="#">B.D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a>
google -- chrome	Type confusion could lead to a heap out-of-bounds write in V8 in Google Chrome prior to 64.0.3282.168 allowing a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6056</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficiently sanitized distributed objects in Updater in Google Chrome on macOS prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via an executable file.	2019-01-09	not yet calculated	<a href="#">CVE-2018-6084</a> <a href="#">B.D</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
google -- chrome	A use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16067</a> <a href="#">B.D</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">GENTOO</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient data validation on image data in PDFium in Google Chrome prior to 51.0.2704.63 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.	2019-01-09	not yet calculated	<a href="#">CVE-2016-10403</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ibm -- api_connect	BM API Connect 5.0 0 0 through 5 0 8.4 is affected by a vulnerability in the role-based access control in the management server that could allow an authenticated user to obtain highly sensitive information. BM X-Force ID: 153175.	2019-01-08	not yet calculated	<a href="#">CVE-2018-1932</a> <a href="#">CONFIRM</a> <a href="#">B.D</a> <a href="#">XF</a>
ibm -- i_access_for_windows	An untrusted search path vulnerability in IBM i Access for Windows versions 7.1 and earlier on Windows can allow arbitrary code execution via a Trojan horse DLL in the current working directory, related to use of the LoadLibrary function. IBM X-Force ID: 152079.	2019-01-04	not yet calculated	<a href="#">CVE-2018-1888</a> <a href="#">B.D</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- jazz_reporting_service	BM Jazz Reporting Service (JRS) 6 0.3, 6 0.4, 6 0.5, and 6 0.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152785.	2019-01-08	not yet calculated	<a href="#">CVE-2018-1918</a> <a href="#">CONFIRM</a> <a href="#">B.D</a> <a href="#">XF</a>
ibm -- spectrum_scale	BM Spectrum Scale (GPFS) 4.1.1, 4.2 0, 4 2.1, 4 2.2, 4.2.3, and 5 0 0 where the use of Local Read Only Cache (LROC) is enabled may caused read operation on a file to return data from a different file. IBM X-Force ID: 154440.	2019-01-08	not yet calculated	<a href="#">CVE-2018-1993</a> <a href="#">B.D</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
imperva -- securesphere	Imperva SecureSphere running v12.0.0.50 is vulnerable to local arbitrary code execution, escaping sealed-mode.	2019-01-10	not yet calculated	<a href="#">CVE-2018-5412</a> <a href="#">EXPLOIT-DB</a>
imperva -- securesphere	Imperva SecureSphere running v13.0, v12 0, or v11.5 allows low privileged users to add SSH login keys to the admin user, resulting in privilege escalation.	2019-01-10	not yet calculated	<a href="#">CVE-2018-5413</a> <a href="#">EXPLOIT-DB</a>
imperva -- securesphere_gateway	Imperva SecureSphere gateway (GW) running v13, for both pre-First Time Login or post-First Time Login (FTL), if the attacker knows the basic authentication passwords, the GW may be vulnerable to RCE through specially crafted requests, from the web access management interface.	2019-01-10	not yet calculated	<a href="#">CVE-2018-5403</a> <a href="#">EXPLOIT-DB</a>
intel -- nuc_firmware	Improper setting of device configuration in system firmware for Intel(R) NUC kits may allow a privileged user to potentially enable escalation of privilege via physical access.	2019-01-10	not yet calculated	<a href="#">CVE-2017-3718</a> <a href="#">CONFIRM</a>
intel -- optane_ssd_dc_p4800x	Firmware update routine in bootloader for Intel(R) Optane(TM) SSD DC P4800X before version E2010435 may allow a privileged user to	2019-01-	not yet	<a href="#">CVE-2018-12167</a>

	potentially enable a denial of service via local access.	10	calculated	<a href="#">CONFIRM</a>
intel -- optane_ssd_dc_p4800x	Insufficient write protection in firmware for Intel(R) Optane(TM) SSD DC P4800X before version E2010435 may allow a privileged user to potentially enable a denial of service via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-12166</a> <a href="#">CONFIRM</a>
intel -- proset/wireless_wifi_software	Improper directory permissions in the ZeroConfig service in Intel(R) PROSet/Wireless WiFi Software before version 20.90.0.7 may allow an authorized user to potentially enable escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-12177</a> <a href="#">CONFIRM</a>
intel -- sgx_sdk_and_platform_software_for_window	Improper file verification in install routine for Intel(R) SGX SDK and Platform Software for Windows before 2.2.100 may allow an escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-18098</a> <a href="#">CONFIRM</a>
intel -- ssd_data_center_tool_for_windows	Improper directory permissions in the installer for the Intel(R) SSD Data Center Tool for Windows before v3.0.17 may allow authenticated users to potentially enable an escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2018-3703</a> <a href="#">CONFIRM</a>
intel -- system_support_utility_for_windows	Insufficient path checking in Intel(R) System Support Utility for Windows before 2.5.0.15 may allow an authenticated user to potentially enable an escalation of privilege via local access.	2019-01-10	not yet calculated	<a href="#">CVE-2019-0088</a> <a href="#">CONFIRM</a>
irssi -- irssi	Irssi 1.1.x before 1.1.2 has a use after free when hidden lines are expired from the scroll buffer.	2019-01-09	not yet calculated	<a href="#">CVE-2019-5882</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
japan_atomic_energy_agency -- mapping_tool	Untrusted search path vulnerability in Installer of Mapping Tool 2 0.1.6 and 2 0.1.7 allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16176</a> <a href="#">MISC</a> <a href="#">JVN</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Jira Plugin 3 0.1 and earlier in JiraSite.java that allows attackers with Overall/Read access to have Jenkins connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000412</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Crowd 2 Integration Plugin 2 0.0 and earlier in CrowdSecurityRealm.java that allows attackers to have Jenkins perform a connection test, connecting to an attacker-specified server with attacker-specified credentials and connection settings.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000422</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/model/Api.java that allows attackers to specify URLs to Jenkins that result in rendering arbitrary attacker-controlled HTML by Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000407</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A denial of service vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/security/HudsonPrivateSecurityRealm.java that allows attackers without Overall/Read permission to access a specific URL on instances using the built-in Jenkins user database security realm that results in the creation of an ephemeral user record in memory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000408</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A session fixation vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/security/HudsonPrivateSecurityRealm.java that prevented Jenkins from invalidating the existing session and creating a new one when a user signed up for a new user account.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000409</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Git Changelog Plugin 2.6 and earlier in GitChangelogSummaryDecorator/summary.jelly, GitChangelogLeftsideBuildDecorator/badge.jelly, GitLogJiraFilterPostPublisher/config.jelly, GitLogBasicChangelogPostPublisher/config.jelly that allows attackers able to control the Git history parsed by the plugin to have Jenkins render arbitrary HTML on some pages.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000426</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins SonarQube Scanner Plugin 2 8 and earlier in SonarInstallation.java that allows attackers with local file system access to obtain the credentials used to connect to SonarQube.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000425</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Crowd 2 Integration Plugin 2 0.0 and earlier in CrowdSecurityRealm.java, CrowdConfigurationService.java that allows attackers with local file system access to obtain the credentials used to connect to Crowd 2.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000423</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Mesos Plugin 0.17.1 and earlier in MesosCloud.java that allows attackers with Overall/Read access to initiate a test connection to an attacker-specified Mesos server with attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000421</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability exists in Jenkins JUnit Plugin 1.25 and earlier in TestObject.java that allows setting the description of a test result.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000411</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins Mesos Plugin 0.17.1 and earlier in MesosCloud.java that allows attackers with Overall/Read access to obtain credentials IDs for credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000420</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins HipChat Plugin 2.2.0 and earlier in HipChatNotifier.java that allows attackers with Overall/Read access to obtain credentials IDs for credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000419</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An improper authorization vulnerability exists in Jenkins HipChat Plugin 2.2.0 and earlier in HipChatNotifier.java that allows attackers with Overall/Read access to send test notifications to an attacker-specified HipChat server with attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000418</a> <a href="#">CONFIRM</a>
	A cross-site request forgery vulnerability exists in Jenkins Email			



jenkins -- jenkins	Extension Template Plugin 1.0 and earlier in ExtEmailTemplateManagement.java that allows creating or removing templates.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000417 CONFIRM</a>
jenkins -- jenkins	A reflected cross-site scripting vulnerability exists in Jenkins Job Config History Plugin 2.18 and earlier in all Jelly files that shows arbitrary attacker-specified HTML in Jenkins to users with Job/Configure access.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000416 CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier, and the Stapler framework used by these releases, in core/src/main/java/org/kohsuke/stapler/RequestImpl.java, core/src/main/java/hudson/model/Descriptor.java that allows attackers with Overall/Administer permission or access to the local file system to obtain credentials entered by users if the form submission could not be successfully processed.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000410 CONFIRM</a>
jenkins -- jenkins	A cross-site request forgery vulnerability exists in Jenkins Config File Provider Plugin 3.1 and earlier in ConfigFilesManagement.java, FolderConfigFileAction.java that allows creating and editing configuration file definitions.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000414 CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Config File Provider Plugin 3.1 and earlier in configfiles.jelly, providerlist.jelly that allows users with the ability to configure configuration files to insert arbitrary HTML into some pages in Jenkins.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000413 CONFIRM</a>
jenkins -- jenkins	A cross-site scripting vulnerability exists in Jenkins Rebuilder Plugin 1.28 and earlier in RebuildAction/BooleanParameterValue.jelly, RebuildAction/ExtendedChoiceParameterValue.jelly, RebuildAction/FileParameterValue.jelly, RebuildAction/LabelParameterValue.jelly, RebuildAction/ListSubversionTagsParameterValue.jelly, RebuildAction/MavenMetadataParameterValue.jelly, RebuildAction/NodeParameterValue.jelly, RebuildAction/PasswordParameterValue.jelly, RebuildAction/RandomStringParameterValue.jelly, RebuildAction/RunParameterValue.jelly, RebuildAction/StringParameterValue.jelly, RebuildAction/TextParameterValue.jelly, RebuildAction/ValidatingStringParameterValue.jelly that allows users with Job/Configuration permission to insert arbitrary HTML into rebuild forms.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000415 CONFIRM</a>
jenkins -- jenkins	An insufficiently protected credentials vulnerability exists in Jenkins Artifactory Plugin 2.16.1 and earlier in ArtifactoryBuilder.java, CredentialsConfig.java that allows attackers with local file system access to obtain old credentials configured for the plugin before it integrated with Credentials Plugin.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000424 CONFIRM</a>
jenkins -- jenkins	A path traversal vulnerability exists in Jenkins 2.145 and earlier, LTS 2.138.1 and earlier in core/src/main/java/hudson/model/FileParameterValue.java that allows attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build.	2019-01-09	not yet calculated	<a href="#">CVE-2018-1000406 CONFIRM</a>
jpccert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to conduct Python code injection attacks via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16168 MISC</a>
jpccert_coordination_center -- logontracer	Cross-site scripting vulnerability in LogonTracer 1.2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16165 MISC</a>
jpccert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to conduct XML External Entity (XXE) attacks via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16166 MISC</a>
jpccert_coordination_center -- logontracer	LogonTracer 1.2.0 and earlier allows remote attackers to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16167 MISC</a>
lib60870 -- lib60870	An issue was discovered in lib60870 2.1.1. LinkLayer_setAddress in link_layer/link_layer.c has a NULL pointer dereference.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6137 MISC</a>
libiec61850 -- libiec61850	An issue has been found in lib EC61850 v1.3.1. Ethernet_setProtocolFilter in hal/ethernet/linux/ethernet_linux.c has a SEGV, as demonstrated by sv_subscriber_example.c and sv_subscriber.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6136 MISC</a>
libiec61850 -- libiec61850	An issue has been found in lib EC61850 v1.3.1. Memory_malloc and Memory_calloc in hal/memory/lib_memory.c have memory leaks when called from mms/iso_mms/common/mms_value.c, server/mms_mapping/mms_mapping.c, and server/mms_mapping/mms_sv.c (via common/string_utilities.c), as demonstrated by iec61850_9_2_LE_example.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6138 MISC</a>
libiec61850 -- libiec61850	An issue has been found in lib EC61850 v1.3.1. Memory_malloc in hal/memory/lib_memory.c has a memory leak when called from Asn1PrimitiveValue_create in mms/asn1/asn1_ber_primitive_value.c, as demonstrated by goose_publisher_example.c and iec61850_9_2_LE_example.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6135 MISC</a>
libpng -- libpng	png_create_info_struct in png.c in libpng 1.6.36 has a memory leak, as demonstrated by pngcp.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6129 MISC</a>
libtiff -- libtiff	The T_FFFdOpen function in tif_unix.c in LibTiff 4.0.10 has a memory leak, as demonstrated by pal2rgb.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6128 MISC</a>
linux -- linux_kernel	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of	2019-01-07	not yet calculated	<a href="#">CVE-2019-5489 MISC</a>

	the fcore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.			MISC MISC MISC
linux -- linux_kernel	EARCLNK ESPCMS-P8 has SQL injection in the install_pack/index.php?ac=Member&at=verifyAccount verify_key parameter. install_pack/espcms_public/espcms_db.php may allow retrieving sensitive information from the ESPCMS database.	2019-01-07	not yet calculated	CVE-2019-5488 MISC
lockon -- ec-cube	Open redirect vulnerability in EC-CUBE (EC-CUBE 3.0.0, EC-CUBE 3.0.1, EC-CUBE 3.0.2, EC-CUBE 3.0.3, EC-CUBE 3.0.4, EC-CUBE 3.0.5, EC-CUBE 3.0.6, EC-CUBE 3.0.7, EC-CUBE 3.0.8, EC-CUBE 3.0.9, EC-CUBE 3.0.10, EC-CUBE 3.0.11, EC-CUBE 3.0.12, EC-CUBE 3.0.12-p1, EC-CUBE 3.0.13, EC-CUBE 3.0.14, EC-CUBE 3.0.15, EC-CUBE 3.0.16) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-16191 JVN MISC
mate_desktop_environment -- mate-screensaver	mate-screensaver before 1.20.2 in MATE Desktop Environment allows physically proximate attackers to view screen content and possibly control applications. By unplugging and re-plugging or power-cycling external output devices (such as additionally attached graphical outputs via HDMI, VGA, DVI, etc.) the content of a screensaver-locked session can be revealed. In some scenarios, the attacker can execute applications, such as by clicking with a mouse.	2019-01-09	not yet calculated	CVE-2018-20681 MISC MISC MISC MISC
mcafee -- web_gateway	Improper input validation in the proxy component of McAfee Web Gateway 7.8.2.0 and later allows remote attackers to cause a denial of service via a crafted HTTP request parameter.	2019-01-09	not yet calculated	CVE-2019-3581 CONFIRM
micronet -- inplc	Nplc-RT 3.08 and earlier allows remote attackers to bypass authentication to execute an arbitrary command through the protocol-compliant traffic. This is a different vulnerability than CVE-2018-0670.	2019-01-09	not yet calculated	CVE-2018-0669 MISC JVN
micronet -- inplc	Buffer overflow in INplc-RT 3.08 and earlier allows remote attackers to cause denial-of-service (DoS) condition that may result in executing arbitrary code via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0668 MISC JVN
micronet -- inplc	Privilege escalation vulnerability in Nplc-RT 3.08 and earlier allows an attacker with administrator rights to execute arbitrary code on the Windows system via unspecified vectors.	2019-01-09	not yet calculated	CVE-2018-0671 MISC JVN
micronet -- inplc	Nplc-RT 3.08 and earlier allows remote attackers to bypass authentication to execute an arbitrary command through the protocol-compliant traffic. This is a different vulnerability than CVE-2018-0669.	2019-01-09	not yet calculated	CVE-2018-0670 MISC JVN
micronet -- inplc	Untrusted search path vulnerability in Installer of Nplc SDK Express 3.08 and earlier and Installer of Nplc SDK Pro+ 3.08 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	CVE-2018-0667 MISC JVN
microsoft -- net_framework	An information disclosure vulnerability exists in .NET Framework and .NET Core which allows bypassing Cross-origin Resource Sharing (CORS) configurations, aka ".NET Framework Information Disclosure Vulnerability." This affects Microsoft .NET Framework 2.0, Microsoft .NET Framework 3.0, Microsoft .NET Framework 4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET Framework 4.6, Microsoft .NET Framework 4.6.4/4.6.1/4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.7.1/4.7.2, .NET Core 2.1, Microsoft .NET Framework 4.7.1/4.7.2, Microsoft .NET Framework 3.5, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4.6.4/4.6.1/4.6.2, .NET Core 2.2, Microsoft .NET Framework 4.7.2.	2019-01-08	not yet calculated	CVE-2019-0545 B.D REDHAT CONFIRM
microsoft -- asp_net_core	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka "ASP.NET Core Denial of Service Vulnerability." This affects ASP.NET Core 2.2, ASP.NET Core 2.1. This CVE ID is unique from CVE-2019-0564.	2019-01-08	not yet calculated	CVE-2019-0548 B.D REDHAT CONFIRM
microsoft -- edge	An elevation of privilege vulnerability exists in Microsoft Edge Browser Broker COM object, aka "Microsoft Edge Elevation of Privilege Vulnerability." This affects Microsoft Edge.	2019-01-08	not yet calculated	CVE-2019-0566 B.D CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0567.	2019-01-08	not yet calculated	CVE-2019-0568 B.D CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0568.	2019-01-08	not yet calculated	CVE-2019-0539 B.D CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2019-0539, CVE-2019-0568.	2019-01-08	not yet calculated	CVE-2019-0567 B.D CONFIRM
microsoft -- exchange_server	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka "Microsoft Exchange Memory Corruption Vulnerability." This affects Microsoft Exchange Server.	2019-01-08	not yet calculated	CVE-2019-0586 B.D CONFIRM
microsoft -- exchange_server	An information disclosure vulnerability exists when the Microsoft Exchange PowerShell API grants calendar contributors more view permissions than intended, aka "Microsoft Exchange Information Disclosure Vulnerability." This affects Microsoft Exchange Server.	2019-01-08	not yet calculated	CVE-2019-0588 B.D CONFIRM
microsoft -- multiple_products	An information disclosure vulnerability exists when Microsoft Word macro buttons are used improperly, aka "Microsoft Word Information Disclosure Vulnerability." This affects Microsoft Word, Office 365 ProPlus, Microsoft Office, Word.	2019-01-08	not yet calculated	CVE-2019-0561 B.D CONFIRM
	A remote code execution vulnerability exists in the way that the			CVE-2019-

microsoft -- multiple_products	MSHTML engine improperly validates input, aka "MSHTML Engine Remote Code Execution Vulnerability." This affects Microsoft Office, Microsoft Office Word Viewer, Internet Explorer 9, Internet Explorer 11, Microsoft Excel Viewer, Internet Explorer 10, Office 365 ProPlus.	2019-01-08	not yet calculated	<a href="#">0541</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft Word software when it fails to properly handle objects in memory, aka "Microsoft Word Remote Code Execution Vulnerability." This affects Word, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft SharePoint, Microsoft Office Online Server, Microsoft Word, Microsoft SharePoint Server.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0585</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- multiple_products	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint Server, Microsoft SharePoint, Microsoft Business Productivity Servers. This CVE ID is unique from CVE-2019-0556, CVE-2019-0557.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0558</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint. This CVE ID is unique from CVE-2019-0557, CVE-2019-0558.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0556</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft SharePoint Elevation of Privilege Vulnerability." This affects Microsoft SharePoint Server, Microsoft SharePoint.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0562</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint. This CVE ID is unique from CVE-2019-0556, CVE-2019-0558.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0557</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- skype_for_android	An elevation of privilege vulnerability exists when Skype for Android fails to properly handle specific authentication requests, aka "Skype for Android Elevation of Privilege Vulnerability." This affects Skype 8.35.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0622</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- visual_studio	A remote code execution vulnerability exists in Visual Studio when the C++ compiler improperly handles specific combinations of C++ constructs, aka "Visual Studio Remote Code Execution Vulnerability." This affects Microsoft Visual Studio.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0546</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- visual_studio	An information disclosure vulnerability exists when Visual Studio improperly discloses arbitrary file contents if the victim opens a malicious .vscontent file, aka "Microsoft Visual Studio Information Disclosure Vulnerability." This affects Microsoft Visual Studio.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0537</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0572, CVE-2019-0573, CVE-2019-0574.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0571</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Runtime improperly handles objects in memory, aka "Windows Runtime Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0570</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0536, CVE-2019-0549, CVE-2019-0554.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0569</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0538</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka "Windows Hyper-V Remote Code Execution Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019. This CVE ID is unique from CVE-2019-0551.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0550</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2019-0536, CVE-2019-0554, CVE-2019-0569.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0549</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when Windows improperly handles authentication requests, aka "Microsoft Windows Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0543</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
	An elevation of privilege vulnerability exists in the Microsoft XmlDocument class that could allow an attacker to escape from the			

microsoft -- windows	AppContainer sandbox in the browser, aka "Microsoft XmlDocument Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2012, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0555</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0536, CVE-2019-0549, CVE-2019-0569.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0554</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when Windows Subsystem for Linux improperly handles objects in memory, aka "Windows Subsystem for Linux Information Disclosure Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0553</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0572, CVE-2019-0574.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0573</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege exists in Windows COM Desktop Broker, aka "Windows COM Elevation of Privilege Vulnerability." This affects Windows Server 2012 R2, Windows RT 8.1, Windows Server 2019, Windows Server 2016, Windows 8.1, Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0552</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when Windows Hyper-V on a host server fails to properly validate input from an authenticated user on a guest operating system, aka "Windows Hyper-V Remote Code Execution Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE D is unique from CVE-2019-0550.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0551</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0573, CVE-2019-0574.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0572</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0576</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists when the Windows Data Sharing Service improperly handles file operations, aka "Windows Data Sharing Service Elevation of Privilege Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers. This CVE ID is unique from CVE-2019-0571, CVE-2019-0572, CVE-2019-0573.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0574</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0577</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0581</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0582</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0578</a> <a href="#">B.D</a> <a href="#">CONFIRM</a>

microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0579</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0580</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0583</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0575, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0584</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka "Jet Database Engine Remote Code Execution Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0538, CVE-2019-0576, CVE-2019-0577, CVE-2019-0578, CVE-2019-0579, CVE-2019-0580, CVE-2019-0581, CVE-2019-0582, CVE-2019-0583, CVE-2019-0584.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0575</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE D is unique from CVE-2019-0549, CVE-2019-0554, CVE-2019-0569.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0536</a> <a href="#">B D</a> <a href="#">CONFIRM</a>
mizuho_bank -- mizuho_direct_app_for_android	The Mizuho Direct App for Android version 3.13.0 and earlier does not verify server certificates, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16179</a> <a href="#">MISC</a> <a href="#">MISC</a>
modulemd -- modulemd	modulemd 1.3.1 and earlier uses an unsafe function for processing externally provided data, leading to remote code execution.	2019-01-10	not yet calculated	<a href="#">CVE-2017-1002157</a> <a href="#">CONFIRM</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows an attacker on the same network segment to execute arbitrary OS commands via SOAP interface of UPnP.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16195</a> <a href="#">MISC</a> <a href="#">JVN</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allow an attacker on the same network segment to obtain information registered on the device via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16192</a> <a href="#">MISC</a> <a href="#">JVN</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Cross-site scripting vulnerability in Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16193</a> <a href="#">MISC</a> <a href="#">JVN</a>
nec -- aterm_wf1200cr_and_aterm_wg1200cr	Aterm WF1200CR and Aterm WG1200CR (Aterm WF1200CR firmware Ver1.1.1 and earlier, Aterm WG1200CR firmware Ver1.0.1 and earlier) allows authenticated attackers to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16194</a> <a href="#">MISC</a> <a href="#">JVN</a>
nelson -- open_source_erp	Nelson Open Source ERP v6.3.1 allows SQL Injection via the db/utlis/query/data.xml query parameter.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5893</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
netapp -- oncommand_unified_manager_for_7-mode	OnCommand Unified Manager for 7-Mode (core package) prior to 5.2.4 uses cookies that lack the secure attribute in certain circumstances making it vulnerable to impersonation via man-in-the-middle (MITM) attacks.	2019-01-07	not yet calculated	<a href="#">CVE-2018-5481</a> <a href="#">CONFIRM</a>
nippon_telegraph_and_telephone_west_corporation -- security_measures_tool	Untrusted search path vulnerability in The installer of Windows10 Fall Creators Update Modify module for Security Measures tool allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16177</a> <a href="#">MISC</a> <a href="#">JVN</a>
				<a href="#">CVE-2018-</a>



npm -- cordova-plugin-ionic-webview	Directory traversal vulnerability in cordova-plugin-ionic-webview versions prior to 2.2.0 (not including 2.0.0-beta.0, 2.0.0-beta.1, 2.0.0-beta.2, and 2.1.0-0) allows remote attackers to access arbitrary files via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">16202</a> <a href="#">MISC</a> <a href="#">JVN</a> <a href="#">MISC</a>
openssh -- openssh	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename.	2019-01-10	not yet calculated	<a href="#">CVE-2018-20685</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
panasonic -- bn-sdwb3_firmware	Buffer overflow in BN-SDWB3 firmware version 1.0.9 and earlier allows an attacker on the same network segment to execute arbitrary code via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0678</a> <a href="#">JVN</a> <a href="#">MISC</a>
panasonic -- bn-sdwb3_firmware	BN-SDWB3 firmware version 1.0.9 and earlier allows attacker with administrator rights on the same network segment to execute arbitrary OS commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0677</a> <a href="#">JVN</a> <a href="#">MISC</a>
panasonic -- bn-sdwb3_firmware	BN-SDWB3 firmware version 1.0.9 and earlier allows an attacker on the same network segment to bypass authentication to access to the management screen and execute an arbitrary command via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0676</a> <a href="#">JVN</a> <a href="#">MISC</a>
panasonic -- multiple_pcs	An unquoted search path vulnerability in some pre-installed applications on Panasonic PC run on Windows 7 (32bit), Windows 7 (64bit), Windows 8 (64bit), Windows 8.1 (64bit), Windows 10 (64bit) delivered in or later than October 2009 allow local users to gain privileges via a Trojan horse executable file and execute arbitrary code with elevated privileges.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16183</a> <a href="#">JVN</a> <a href="#">MISC</a>
pgpool -- global_development_group_pgpooladmin	PgpoolAdmin 4.0 and earlier allows remote attackers to bypass the login authentication and obtain the administrative privilege of the PostgreSQL database via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16203</a> <a href="#">JVN</a> <a href="#">MISC</a>
phpscriptsmall.com -- advance_peer_to_peer_mlm_script	The Admin Panel of PHP Scripts Mall Advance Peer to Peer MLM Script v1.7.0 allows remote attackers to bypass intended access restrictions by directly navigating to admin/dashboard.php or admin/user.php, as demonstrated by disclosure of information about users and staff.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6126</a> <a href="#">MISC</a>
phpscriptsmall.com -- citysearch_/hotfrog/_gelbeseiten_clone_script	PHP Scripts Mall Citysearch / Hotfrog / Gelbeseiten Clone Script 2.0.1 has Reflected XSS via the srch parameter, as demonstrated by restaurants-details.php.	2019-01-12	not yet calculated	<a href="#">CVE-2019-6248</a> <a href="#">MISC</a>
pivotal -- concourse	Pivotal Concourse, all versions prior to 4.2.2, puts the user access token in a url during the login flow. A remote attacker who gains access to a user's browser history could obtain the access token and use it to authenticate as the user.	2019-01-11	not yet calculated	<a href="#">CVE-2019-3803</a> <a href="#">CONFIRM</a>
policykit -- policykit	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6133</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
qibosoft -- qibosoft	qibosoft through V7 allows remote attackers to read arbitrary files via the member/index.php main parameter, as demonstrated by SSRF to a URL on the same web site to read a .sql file.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5725</a> <a href="#">MISC</a>
rakuten_securities -- market_speed	Untrusted search path vulnerability in the installer of MARKET SPEED Ver.16.4 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16182</a> <a href="#">JVN</a> <a href="#">MISC</a>
red_hat -- satellite	A cross-site scripting (XSS) flaw was found in the katello component of Satellite. An attacker with privilege to create/edit organizations and locations is able to execute a XSS attacks against other users through the Subscriptions or the Red Hat Repositories wizards. This can possibly lead to malicious code execution and extraction of the anti-CSRF token of higher privileged users. Versions before 3.9.0 are vulnerable.	2019-01-12	not yet calculated	<a href="#">CVE-2018-16887</a> <a href="#">CONFIRM</a>
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.6 to V2.2, D5500 V1.6 to V2.2, D5510 V1.6 to V2.2, and the display versions with RICOH Interactive Whiteboard Controller Type1 V1.6 to V2.2 attached (D5520, D6500, D6510, D7500, D8400) allows remote attackers to execute arbitrary commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16184</a> <a href="#">JVN</a> <a href="#">MISC</a>
ricoh -- interactive_whiteboard	The RICOH Interactive Whiteboard D2200 V1.3 to V2.2, D5500 V1.3 to V2.2, D5510 V1.3 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.3 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) does not verify its server certificates, which allows man-in-the-middle attackers to eversdrop on encrypted communication.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16187</a> <a href="#">JVN</a> <a href="#">MISC</a>
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.1 to V2.2, D5500 V1.1 to V2.2, D5510 V1.1 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.1 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) uses hard-coded credentials, which may allow an attacker on the same network segments to login to the administrators settings screen and change the configuration.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16186</a> <a href="#">JVN</a> <a href="#">MISC</a>
ricoh -- interactive_whiteboard	RICOH Interactive Whiteboard D2200 V1.1 to V2.2, D5500 V1.1 to V2.2, D5510 V1.1 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1 V1.1 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137.0 attached (D5520, D6510, D7500, D8400) allows remote attackers to execute a malicious program.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16185</a> <a href="#">JVN</a> <a href="#">MISC</a>
	SQL injection vulnerability in the RICOH Interactive Whiteboard D2200 V1.3 to V2.2, D5500 V1.3 to V2.2, D5510 V1.3 to V2.2, the display versions with RICOH Interactive Whiteboard Controller Type1			<a href="#">CVE-2018-</a>

ricoh -- interactive_whiteboard	V1 3 to V2.2 attached (D5520, D6500, D6510, D7500, D8400), and the display versions with RICOH Interactive Whiteboard Controller Type2 V3.0 to V3.1.10137 0 attached (D5520, D6510, D7500, D8400) allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">16188</a> <a href="#">JVN</a> <a href="#">MISC</a>
sap -- business_objects_mobile_for_android	SAP Business Objects Mobile for Android (before 6 3.5) application allows an attacker to provide malicious input in the form of a SAP BI link, preventing legitimate users from accessing the application by crashing it.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0240</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- bw/4hana	Under some circumstances, masterdata maintenance in SAP BW/4HANA (fixed in DW4CORE version 1.0 (SP08)) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0243</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- cloud_connector	SAP Cloud Connector, before version 2.11.3, allows an attacker to inject code that can be executed by the application. An attacker could thereby control the behavior of the application.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0247</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- cloud_connector	SAP Cloud Connector, before version 2.11.3, does not perform any authentication checks for functionalities that require user identity.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0246</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- commerce	SAP Commerce (previously known as SAP Hybris Commerce), before version 6.7, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0238</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- crm_webclient_ui	SAP CRM WebClient UI (fixed in SAPSCORE 1.12; S4FND 1 02; WEBCU F 7 31, 7.46, 7.47, 7.48, 8 0, 8 01) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0244</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- crm_webclient_ui	SAP CRM WebClient UI (fixed in SAPSCORE 1.12; S4FND 1 02; WEBCU F 7 31, 7.46, 7.47, 7.48, 8 0, 8 01) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0245</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- enterprise_financial_services	SAP Enterprise Financial Services (fixed in SAPSCORE 1.13, 1.14, 1.15; S4CORE 1.01, 1.02, 1 03; EA-F NSERV 1.10, 2 0, 5 0, 6 0, 6 03, 6.04, 6.05, 6 06, 6.16, 6.17, 6.18, 8.0; Bank/CFM 4.63_20) does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges.	2019-01-08	not yet calculated	<a href="#">CVE-2018-2484</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- financial_consolidation_cube_designer	A security weakness in SAP Financial Consolidation Cube Designer (BOBJ_EADES fixed in versions 8.0, 10.1) may allow an attacker to discover the password hash of an admin user.	2019-01-08	not yet calculated	<a href="#">CVE-2018-2499</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- gateway_of_abap_application_server	Under certain conditions SAP Gateway of ABAP Application Server (fixed in SAP_GWFND 7.5, 7.51, 7.52, 7.53; SAP_BASIS 7 5) allows an attacker to access information which would otherwise be restricted.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0248</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- landscape_management	Under certain conditions SAP Landscape Management (VCM 3.0) allows an attacker to access information which would otherwise be restricted.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0249</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- work_and_inventory_manager	SAP Work and Inventory Manager (Agentry_SDK , before 7.0, 7.1) allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0241</a> <a href="#">B.D</a> <a href="#">MISC</a> <a href="#">MISC</a>
seiko_epson -- printers_and_scanners	HTTP header injection vulnerability in SEIKO EPSON printers and scanners (DS-570W firmware versions released prior to 2018 March 13, DS-780N firmware versions released prior to 2018 March 13, EP-10VA firmware versions released prior to 2017 September 4, EP-30VA firmware versions released prior to 2017 June 19, EP-707A firmware versions released prior to 2017 August 1, EP-708A firmware versions released prior to 2017 August 7, EP-709A firmware versions released prior to 2017 June 12, EP-777A firmware versions released prior to 2017 August 1, EP-807AB/AW/AR firmware versions released prior to 2017 August 1, EP-808AB/AW/AR firmware versions released prior to 2017 August 7, EP-879AB/AW/AR firmware versions released prior to 2017 June 12, EP-907F firmware versions released prior to 2017 August 1, EP-977A3 firmware versions released prior to 2017 August 1, EP-978A3 firmware versions released prior to 2017 August 7, EP-979A3 firmware versions released prior to 2017 June 12, EP-M570T firmware versions released prior to 2017 September 6, EW-M5071FT firmware versions released prior to 2017 November 2, EW-M660FT firmware versions released prior to 2018 April 19, EW-M770T firmware versions released prior to 2017 September 6, PF-70 firmware versions released prior to 2018 April 20, PF-71 firmware versions released prior to 2017 July 18, PF-81 firmware versions released prior to 2017 September 14, PX-048A firmware versions released prior to 2017 July 4, PX-049A firmware versions released prior to 2017 September 11, PX-437A firmware versions released prior to 2017 July 24, PX-M350F firmware versions released prior to 2018 February 23, PX-M5040F firmware versions released prior to 2017 November 20, PX-M5041F firmware versions released prior to 2017 November 20, PX-M650A firmware versions released prior to 2017 October 17, PX-M650F firmware versions released prior to 2017 October 17, PX-M680F firmware versions released prior to 2017 June 29, PX-M7050F firmware versions released prior to 2017 October 13, PX-M7050FP firmware versions released prior to 2017 October 13, PX-M7050FX firmware versions released prior to 2017	2019-01-09	not yet calculated	<a href="#">CVE-2018-0689</a> <a href="#">JVN</a> <a href="#">MISC</a>

	November 7, PX-M7070FX firmware versions released prior to 2017 April 27, PX-M740F firmware versions released prior to 2017 December 4, PX-M741F firmware versions released prior to 2017 December 4, PX-M780F firmware versions released prior to 2017 June 29, PX-M781F firmware versions released prior to 2017 June 27, PX-M840F firmware versions released prior to 2017 November 16, PX-M840FX firmware versions released prior to 2017 December 8, PX-M860F firmware versions released prior to 2017 October 25, PX-S05B/W firmware versions released prior to 2018 March 9, PX-S350 firmware versions released prior to 2018 February 23, PX-S5040 firmware versions released prior to 2017 November 20, PX-S7050 firmware versions released prior to 2018 February 21, PX-S7050PS firmware versions released prior to 2018 February 21, PX-S7050X firmware versions released prior to 2017 November 7, PX-S7070X firmware versions released prior to 2017 April 27, PX-S740 firmware versions released prior to 2017 December 3, PX-S840 firmware versions released prior to 2017 November 16, PX-S840X firmware versions released prior to 2017 December 8, PX-S860 firmware versions released prior to 2017 December 7) may allow a remote attackers to lead a user to a phishing site or execute an arbitrary script on the user's web browser.			
seiko_epson -- printers_and_scanners	Open redirect vulnerability in SE KO EPSON printers and scanners (DS-570W firmware versions released prior to 2018 March 13, DS-780N firmware versions released prior to 2018 March 13, EP-10VA firmware versions released prior to 2017 September 4, EP-30VA firmware versions released prior to 2017 June 19, EP-707A firmware versions released prior to 2017 August 1, EP-708A firmware versions released prior to 2017 August 7, EP-709A firmware versions released prior to 2017 June 12, EP-777A firmware versions released prior to 2017 August 1, EP-807AB/AW/AR firmware versions released prior to 2017 August 1, EP-808AB/AW/AR firmware versions released prior to 2017 August 7, EP-879AB/AW/AR firmware versions released prior to 2017 June 12, EP-907F firmware versions released prior to 2017 August 1, EP-977A3 firmware versions released prior to 2017 August 1, EP-978A3 firmware versions released prior to 2017 August 7, EP-979A3 firmware versions released prior to 2017 June 12, EP-M570T firmware versions released prior to 2017 September 6, EW-M5071FT firmware versions released prior to 2017 November 2, EW-M660FT firmware versions released prior to 2018 April 19, EW-M770T firmware versions released prior to 2017 September 6, PF-70 firmware versions released prior to 2018 April 20, PF-71 firmware versions released prior to 2017 July 18, PF-81 firmware versions released prior to 2017 September 14, PX-048A firmware versions released prior to 2017 July 4, PX-049A firmware versions released prior to 2017 September 11, PX-437A firmware versions released prior to 2017 July 24, PX-M350F firmware versions released prior to 2018 February 23, PX-M5040F firmware versions released prior to 2017 November 20, PX-M5041F firmware versions released prior to 2017 November 20, PX-M650A firmware versions released prior to 2017 October 17, PX-M650F firmware versions released prior to 2017 October 17, PX-M680F firmware versions released prior to 2017 June 29, PX-M7050F firmware versions released prior to 2017 October 13, PX-M7050FP firmware versions released prior to 2017 October 13, PX-M7050FX firmware versions released prior to 2017 November 7, PX-M7070FX firmware versions released prior to 2017 April 27, PX-M740F firmware versions released prior to 2017 December 4, PX-M741F firmware versions released prior to 2017 December 4, PX-M780F firmware versions released prior to 2017 June 29, PX-M781F firmware versions released prior to 2017 June 27, PX-M840F firmware versions released prior to 2017 November 16, PX-M840FX firmware versions released prior to 2017 December 8, PX-M860F firmware versions released prior to 2017 October 25, PX-S05B/W firmware versions released prior to 2018 March 9, PX-S350 firmware versions released prior to 2018 February 23, PX-S5040 firmware versions released prior to 2017 November 20, PX-S7050 firmware versions released prior to 2018 February 21, PX-S7050PS firmware versions released prior to 2018 February 21, PX-S7050X firmware versions released prior to 2017 November 7, PX-S7070X firmware versions released prior to 2017 April 27, PX-S740 firmware versions released prior to 2017 December 3, PX-S840 firmware versions released prior to 2017 November 16, PX-S840X firmware versions released prior to 2017 December 8, PX-S860 firmware versions released prior to 2017 December 7) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the web interface of the affected product.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0688</a> <a href="#">JVN</a> <a href="#">MISC</a>
shopxo -- shopxo	An issue was discovered in ShopXO 1.2.0. In the UnlinkDir method of the FileUtil.php file, the input parameters are not checked, resulting in input mishandling by the rmdir method. Attackers can delete arbitrary files by using "." directory traversal.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5887</a> <a href="#">MISC</a>
shopxo -- shopxo	An issue was discovered in ShopXO 1.2.0. In the application/install/controller/index.php file, there is no validation lock file in the Add method, which allows an attacker to reinstall the database. The attacker can write arbitrary code to database.php during system reinstallation.	2019-01-10	not yet calculated	<a href="#">CVE-2019-5886</a> <a href="#">MISC</a>
svgpp -- svgpp	An issue was discovered in Anti-Grain Geometry (AGG) 2.4 as used in SVG++ (aka svgpp) 1.2.3. A heap-based buffer overflow bug in svgpp_agg_render may lead to code execution. In the render_scanlines_aa_solid function, the blend_hline function is called repeatedly multiple times. blend_hline is equivalent to a loop containing write operations. Each call writes a piece of heap data, and multiple calls overwrite the data in the heap.	2019-01-12	not yet calculated	<a href="#">CVE-2019-6247</a> <a href="#">MISC</a>
svgpp -- svgpp	An issue was discovered in SVG++ (aka svgpp) 1.2.3. After calling the gil::get_color function in Generic Image Library in Boost, the return code is used as an address, leading to an Access Violation because of an out-of-bounds read.	2019-01-12	not yet calculated	<a href="#">CVE-2019-6246</a> <a href="#">MISC</a>
svgpp -- svgpp	An issue was discovered in Anti-Grain Geometry (AGG) 2.4 as used in SVG++ (aka svgpp) 1.2.3. In the function agg::cell_aa::not_equal, dx is assigned to (x2 - x1). If dx >= dx_limit, which is (16384 << poly_subpixel_shift), this function will call itself recursively. There can	2019-01-12	not yet calculated	<a href="#">CVE-2019-6245</a>

	be a situation where $(x2 - x1)$ is always bigger than $dx\_limit$ during the recursion, leading to continual stack consumption.			MISC
systemd-journald -- systemd-journald	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16866</a> B.D <a href="#">CONFIRM</a> UBUNTU MISC
systemd-journald -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16865</a> B.D <a href="#">CONFIRM</a> UBUNTU MISC
systemd-journald -- systemd-journald	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.	2019-01-11	not yet calculated	<a href="#">CVE-2018-16864</a> B.D <a href="#">CONFIRM</a> UBUNTU MISC
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an attacker on the same network segment to bypass access restriction to access the information and files stored on the affected device.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16197</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier may allow an attacker on the same network segment to access a non-documented developer screen to perform operations on the affected device.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16198</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Cross-site scripting vulnerability in Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an remote attacker to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16199</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier allows an attacker on the same network segment to execute arbitrary OS commands.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16200</a> MISC JVN
toshiba -- toshiba_home_gateway_hem-gw16a_and_hem-gw26a	Toshiba Home gateway HEM-GW16A 1.2.9 and earlier, Toshiba Home gateway HEM-GW26A 1.2.9 and earlier uses hard-coded credentials, which may allow an attacker on the same network segment to login to the administrators settings screen and change the configuration or execute arbitrary OS commands.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16201</a> MISC JVN
traccar -- traccar_server	In Traccar Server version 4.2, protocol/SpotProtocolDecoder.java might allow XXE attacks.	2019-01-09	not yet calculated	<a href="#">CVE-2019-5748</a> MISC MISC
usualtoolcms -- usualtoolcms	An issue was discovered in UsualToolCMS 8.0. cmsadmin/a_sqlbackx.php?t=sql allows CSRF attacks that can execute SQL statements, and consequently execute arbitrary PHP code by writing that code into a php file.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6244</a> MISC
weseek -- growi	Cross-site scripting vulnerability in GROWI v3.2.3 and earlier allows remote attackers to inject arbitrary web script or HTML via New Page modal.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16205</a> JVN MISC
weseek -- growi	Cross-site scripting vulnerability in GROWI v3.2.3 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0698</a> JVN MISC
windows -- dhcp_client	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka "Windows DHCP Client Remote Code Execution Vulnerability." This affects Windows 10, Windows 10 Servers.	2019-01-08	not yet calculated	<a href="#">CVE-2019-0547</a> B.D <a href="#">CONFIRM</a>
winscp -- winscp	In WinSCP before 5.14 beta, due to missing validation, the scp implementation would accept arbitrary files sent by the server, potentially overwriting unrelated files. This affects TSCPFileSystem::SCPSink in core/ScpFileSystem.cpp.	2019-01-10	not yet calculated	<a href="#">CVE-2018-20684</a> B.D MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the RTSE dissector and other ASN.1 dissectors could crash. This was addressed in epan/charsets.c by adding a get_t61_string length check.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5718</a> B.D MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the ISAKMP dissector could crash. This was addressed in epan/dissectors/packet-isakmp.c by properly handling the case of a missing decryption data block.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5719</a> MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5 and 2.4.0 to 2.4.11, the P_MUL dissector could crash. This was addressed in epan/dissectors/packet-p_mul.c by rejecting the invalid sequence number of zero.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5717</a> B.D MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.4.0 to 2.4.11, the ENIP dissector could crash. This was addressed in epan/dissectors/packet-enip.c by changing the memory-management approach so that a use-after-free is avoided.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5721</a> MISC MISC MISC
wireshark -- wireshark	In Wireshark 2.6.0 to 2.6.5, the 6LoWPAN dissector could crash. This was addressed in epan/dissectors/packet-6lowpan.c by avoiding use of a TVB before its creation.	2019-01-08	not yet calculated	<a href="#">CVE-2019-5716</a> B.D MISC MISC

				MISC
wordpress -- wordpress	Cross-site scripting vulnerability in WordPress plugin spam-byebye 2.2.1 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-12	not yet calculated	<a href="#">CVE-2018-16206</a> JVN MISC
wordpress -- wordpress	SQL injection vulnerability in the LearnPress prior to version 3.1.0 allows attacker with administrator rights to execute arbitrary SQL commands via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16175</a> JVN MISC
wordpress -- wordpress	Open redirect vulnerability in LearnPress prior to version 3.1.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16174</a> JVN MISC
wordpress -- wordpress	Cross-site scripting vulnerability in LearnPress prior to version 3.1.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16173</a> JVN MISC
wordpress -- wordpress	The "Social Pug - Easy Social Share Buttons" plugin before 1.2.6 for WordPress allows XSS via the wp-admin/admin.php?page=dpsp-toolkit&dpsp_message_class parameter.	2019-01-09	not yet calculated	<a href="#">CVE-2016-10736</a> MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Event Calendar WD version 1.1.21 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16164</a> JVN MISC MISC MISC
wordpress -- wordpress	Cross-site scripting vulnerability in Google XML Sitemaps Version 4.0.9 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16204</a> JVN MISC
xiaocms -- xiaocms	An issue was discovered in XiaoCms 20141229. It allows admin/index.php?c=database table[] SQL injection. This can be used for PHP code execution via " NTO UTF LE" with a .php filename.	2019-01-11	not yet calculated	<a href="#">CVE-2019-6127</a> MISC
xterm.js -- xterm.js	A remote code execution vulnerability exists in Xterm.js when the component mishandles special characters, aka "Xterm Remote Code Execution Vulnerability." This affects xterm.js.	2019-01-09	not yet calculated	<a href="#">CVE-2019-0542</a> B.D MISC
yamaha -- multiple_routers	Yamaha routers RT57i Rev 8.00.95 and earlier, RT58i Rev 9.01.51 and earlier, NVR500 Rev.11.00.36 and earlier, RTX810 Rev.11.01.31 and earlier, allow an administrative user to embed arbitrary scripts to the configuration data through a certain form field of the configuration page, which may be executed on another administrative user's web browser. This is a different vulnerability from CVE-2018-0666.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0665</a> MISC MISC JVN MISC
yamaha -- multiple_routers	Yamaha routers RT57i Rev 8.00.95 and earlier, RT58i Rev 9.01.51 and earlier, NVR500 Rev.11.00.36 and earlier, RTX810 Rev.11.01.31 and earlier, allow an administrative user to embed arbitrary scripts to the configuration data through a certain form field of the configuration page, which may be executed on another administrative user's web browser. This is a different vulnerability from CVE-2018-0665.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0666</a> MISC MISC JVN MISC
yokogawa -- multiple_products	Buffer overflow in the license management function of YOKOGAWA products (iDefine for ProSafe-RS R1.16.3 and earlier, STARDOM VDS R7.50 and earlier, STARDOM FCN/FCJ Simulator R4.20 and earlier, ASTPLANNER R15.01 and earlier, TriFellows V5.04 and earlier) allows remote attackers to stop the license management function or execute an arbitrary program via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-0651</a> B.D MISC MISC
yokogawa -- multiple_products	Multiple Yokogawa products that contain Vnet/ P Open Communication Driver (CENTUM CS 3000(R3.05.00 - R3.09.50), CENTUM CS 3000 Entry Class(R3.05.00 - R3.09.50), CENTUM VP(R4.01.00 - R6.03.10), CENTUM VP Entry Class(R4.01.00 - R6.03.10), Exaopc(R3.10.00 - R3.75.00), PRM(R2.06.00 - R3.31.00), ProSafe-RS(R1.02.00 - R4.02.00), FAST/TOOLS(R9.02.00 - R10.02.00), B/M9000 VP(R6.03.01 - R8.01.90)) allows remote attackers to cause a denial of service attack that may result in stopping Vnet/IP Open Communication Driver's communication via unspecified vectors.	2019-01-09	not yet calculated	<a href="#">CVE-2018-16196</a> B.D MISC MISC

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED



#### SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)



**From:** [US-CERT](#)  
**To:** [Tanner McGinnis](#)  
**Subject:** SB19-007: Vulnerability Summary for the Week of December 31, 2018  
**Date:** Monday, January 07, 2019 11:13:21 AM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## **[SB19-007: Vulnerability Summary for the Week of December 31, 2018](#)**

01/07/2019 06:55 AM EST

Original release date: January 07, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
There were no high vulnerabilities recorded this week.				

[Back to top](#)

## **Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
douco -- doupdp	An issue was discovered in DouCo DouPHP 1.5 20181221. It allows full path disclosure in "Smarty error: unable to read resource" error messages for a crafted installation page.	2018-12-28	<a href="#">5.0</a>	<a href="#">CVE-2018-20566 MISC</a>
f5 -- big-ip_access_policy_manager	A cross-site request forgery (CSRF) vulnerability in the APM webtop 11.2.1 or greater may allow attacker to force an APM webtop session to log out and require re-authentication.	2018-12-28	<a href="#">4.3</a>	<a href="#">CVE-2018-15334 BID CONFIRM</a>
freedesktop -- poppler	A reachable Object::getString assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to construction of invalid rich media annotation assets in the AnnotRichMedia class in Annot.c.	2018-12-28	<a href="#">4.3</a>	<a href="#">CVE-2018-20551 MISC MISC</a>
freedesktop -- poppler	A reachable Object::dictLookup assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to the lack of a check for the dict data type, as demonstrated by use of the FileSpec class (in FileSpec.cc) in pdfdetach.	2019-01-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20650 MISC MISC</a>
libming -- libming	A heap-based buffer over-read was discovered in decompileJUMP function in util/decompile.c of libming v0.4.8. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by swftocxx.	2018-12-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20591 MISC</a>
tinyexr_project -- tinyexr	An attempted excessive memory allocation was discovered in the function tinyexr::Allocatelmage in tinyexr.h in tinyexr v0.9.5. Remote	2019-01-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20652</a>

	attackers could leverage this vulnerability to cause a denial-of-service via crafted input, which leads to an out-of-memory exception.			<a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 has ?do=user_addpost CSRF.	2018-12-30	<a href="#">6.8</a>	<a href="#">CVE-2018-20598</a> <a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 allows remote attackers to execute arbitrary PHP code by entering this code during an index.php sadmin_fileedit action.	2018-12-30	<a href="#">6.5</a>	<a href="#">CVE-2018-20599</a> <a href="#">MISC</a>
ucms_project -- ucms	sadmin/cedit.php in UCMS 1.4.7 has XSS via an index.php sadmin_cedit action.	2018-12-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20600</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/page.php?rec=edit has XSS via the page_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20557</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/system.php?rec=update has XSS via the site_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20558</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/product.php?rec=update has XSS via the name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20559</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/show.php?rec=update has XSS via the show_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20560</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/article.php?rec=update has XSS via the title parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20561</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/article_category.php?rec=update has XSS via the cat_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20562</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/mobile.php?rec=system&act=update has XSS via the mobile_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20563</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/product_category.php?rec=update has XSS via the cat_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20564</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/nav.php?rec=update has XSS via the nav_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20565</a> <a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 has XSS via the dir parameter in an index.php sadmin_fileedit action.	2018-12-30	<a href="#">3.5</a>	<a href="#">CVE-2018-20597</a> <a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 has XSS via the description parameter in an index.php list_editpost action.	2018-12-30	<a href="#">3.5</a>	<a href="#">CVE-2018-20601</a> <a href="#">MISC</a>
website_seller_script_project -- website_seller_script	PHP Scripts Mall Website Seller Script 2 0.5 has XSS via a Profile field such as Company Address, a related issue to CVE-2018-15896.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20530</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- gate-e1_and_gate-e2	Pluto Safety PLC Gateway Ethernet devices ABB GATE-E1 and GATE-E2 all versions do not allow authentication to be configured on administrative telnet or web interfaces, which could enable various effects vectors, including conducting device resets, reading or modifying registers, and changing configuration settings such as IP addresses.	2019-01-03	not yet calculated	<a href="#">CVE-2018-18995</a> <a href="#">BID</a> <a href="#">MISC</a>
abb -- gate-e1_and_gate-e2	Pluto Safety PLC Gateway Ethernet devices in ABB GATE-E1 and GATE-E2 all versions allows an unauthenticated attacker using the administrative web interface to insert an HTML/Javascript payload into any of the device properties, which may allow an attacker to display/execute the payload in a	2019-01-03	not yet calculated	<a href="#">CVE-2018-18997</a> <a href="#">BID</a> <a href="#">MISC</a>

	visitor browser.			
ansible -- ansible	ansible before versions 2.5.14, 2.6.11, 2.7.5 is vulnerable to a information disclosure flaw in vvv+ mode with no_log on that can lead to leakage of sensible data.	2019-01-03	not yet calculated	<a href="#">CVE-2018-16876</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ansible -- tower	Ansible Tower before version 3.3.3 does not set a secure channel as it is using the default insecure configuration channel settings for messaging celery workers from Rabbi MQ. This could lead in data leak of sensitive information such as passwords as well as denial of service attacks by deleting projects or inventory files.	2019-01-03	not yet calculated	<a href="#">CVE-2018-16879</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
apache -- netbeans	Apache NetBeans (incubating) 9.0 NetBeans Proxy Auto-Configuration (PAC) interpretation is vulnerable for remote command execution (RCE). Using the nashorn script engine the environment of the javascript execution for the Proxy Auto-Configuration leaks privileged objects, that can be used to circumvent the execution limits. If a different script engine was used, no execution limits were in place. Both vectors allow remote code execution.	2018-12-31	not yet calculated	<a href="#">CVE-2018-17191</a> <a href="#">BID</a> <a href="#">MISC</a>
aria2 -- aria2	aria2c in aria2 1.33.1, when --log is used, can store an HTTP Basic Authentication username and password in a file, which might allow local users to obtain sensitive information by reading this file.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3500</a> <a href="#">MISC</a>
artifex -- ghostscript	In Artifex Ghostscript before 9.26, a carefully crafted PDF file can trigger an extremely long running computation when parsing the file.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19478</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
august -- connect_devices	An issue was discovered on August Connect devices. Insecure data transfer between the August app and August Connect during configuration allows attackers to discover home Wi-Fi credentials. This data transfer uses an unencrypted access point for these credentials, and passes them in an HTTP POST, using the AugustWifiDevice class, with data encrypted with a fixed key found obfuscated in the app.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20100</a> <a href="#">MISC</a>
bento4 -- bento4	An issue was discovered in Bento4 1.5.1-627. The AP4_StcoAtom class in Core/AP4StcoAtom.cpp has an attempted excessive memory allocation when called from AP4_AtomFactory::CreateAtomFromStream in Core/AP4AtomFactory.cpp, as demonstrated by mp42hls.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20659</a> <a href="#">MISC</a>
bmc -- remedy	Remedy AR System Server in BMC Remedy 7.1 may fail to set the correct user context in certain impersonation scenarios, which can allow a user to act with the identity of a different user, because userdata.js in the WO:WorkOrderConsole component allows a username substitution involving a UserData_Init call.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19505</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">SECTRACK</a>
buck -- buck	Buck parser-cache command loads/saves state using Java serialized object. If the state information is maliciously crafted, deserializing it could lead to code execution. This issue affects Buck versions prior to v2018.06.25.01.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6331</a> <a href="#">MISC</a>
chinamobile_plc -- wireless_router_gpn2.4p21-c-cn_devices	ChinaMobile PLC Wireless Router GPN2.4P21-C-CN devices with firmware W2001EN-00 have XSS via the cgi-bin/webproc?getpage=html/index.html var:subpage parameter.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20326</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cim -- cim	public\install\install.php in CIM 0.9.3 allows remote attackers to reload the product via the public/install/step3 URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20614</a> <a href="#">MISC</a>
code42 -- code42_for_enterprise	The Code42 app before 6.8.4, as used in Code42 for Enterprise, on Linux installs with overly permissive permissions on the /usr/local/crashplan/log directory. This allows a user to manipulate symbolic links to escalate privileges, or show the contents of sensitive files that a regular user would not have access to.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20131</a> <a href="#">MISC</a>
core_ftp_server -- core_ftp_server	The server in Core FTP 2.0 build 653 on 32-bit platforms allows remote attackers to cause a denial of service (daemon crash) via a crafted XRMd command.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20658</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
	Prior to CouchDB version 2.3.0, CouchDB allowed for runtime-			

couchdb -- couchdb	configuration of key components of the database. In some cases, this lead to vulnerabilities where CouchDB admin users could access the underlying operating system as the CouchDB user. Together with other vulnerabilities, it allowed full system entry for unauthenticated users. Rather than waiting for new vulnerabilities to be discovered, and fixing them as they come up, the CouchDB development team decided to make changes to avoid this entire class of vulnerabilities.	2019-01-02	not yet calculated	<a href="#">CVE-2018-17188</a> <a href="#">MISC</a>
cuba_platform -- cuba_platform	The Reporting Addon (aka Reports Addon) through 2019-01-02 for CUBA Platform through 6.10.x has Persistent XSS via the "Reports > Reports" name field.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20663</a> <a href="#">MISC</a>
cuppacms -- cuppacms	CuppaCMS has XSS via an SVG document uploaded to the administrator/#/component/table_manager/view/cu_views URI.	2018-12-31	not yet calculated	<a href="#">CVE-2018-19918</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
d-link -- dir-818lw_and_dir-860l	On D-Link DIR-818LW Rev.A 2.05.B03 and DIR-860L Rev.B 2.03.B03 devices, unauthenticated remote OS command execution can occur in the soap.cgi service of the cgibin binary via an "&&" substring in the service parameter. NOTE: this issue exists because of an incomplete fix for CVE-2018-6530.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20114</a> <a href="#">MISC</a>
dolibarr -- dolibarr	A stored cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote authenticated users to inject arbitrary web script or HTML via the "address" (POST) or "town" (POST) parameter to adherents/type.php.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19992</a> <a href="#">MISC</a>
dolibarr -- dolibarr	A reflected cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote attackers to inject arbitrary web script or HTML via the transphrase parameter to public/notice.php.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19993</a> <a href="#">MISC</a>
dolibarr -- dolibarr	An error-based SQL injection vulnerability in product/card.php in Dolibarr version 8.0.2 allows remote authenticated users to execute arbitrary SQL commands via the desiredstock parameter.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19994</a> <a href="#">MISC</a>
dolibarr -- dolibarr	A stored cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote authenticated users to inject arbitrary web script or HTML via the "address" (POST) or "town" (POST) parameter to user/card.php.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19995</a> <a href="#">MISC</a> <a href="#">MISC</a>
dolibarr -- dolibarr	SQL injection vulnerability in user/card.php in Dolibarr version 8.0.2 allows remote authenticated users to execute arbitrary SQL commands via the employee parameter.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19998</a> <a href="#">MISC</a> <a href="#">MISC</a>
driveragent -- driveragent	DriverAgent 2.2015.7.14, which includes DrvAgent64 sys 1.0.0.1, allows a user to send an IOCTL (0x80002068) with a user defined buffer size. If the size of the buffer is less than 512 bytes, then the driver will overwrite the next pool header if there is one next to the user buffer's pool.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19523</a> <a href="#">MISC</a>
emc -- rsa_archer	RSA Archer versions prior to 6.5.0.1 contain an improper access control vulnerability. A remote malicious user could potentially exploit this vulnerability to bypass authorization checks and gain read access to restricted user information.	2019-01-03	not yet calculated	<a href="#">CVE-2018-15780</a> <a href="#">BID</a> <a href="#">FULLDISC</a>
epon -- cpe-wifi_devices	EPON CPE-WiFi devices 2.0.4-X000 are vulnerable to escalation of privileges by sending cooLogin=1, cooUser=admin, and timestamp=-1 cookies.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20512</a> <a href="#">MISC</a>
exiftool -- exiftool	ExifTool 8.32 allows local users to gain privileges by creating a %TEMP%\par-%username%\cache-exiftool-8.32 folder with a victim's username, and then copying a Trojan horse ws32_32.dll file into this new folder, aka DLL Hijacking. NOTE: 8.32 is an obsolete version from 2010 (9.x was released starting in 2012, and 10.x was released starting in 2015).	2019-01-02	not yet calculated	<a href="#">CVE-2018-20211</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
expressvpn -- expressvpn	An issue was discovered in ExpressVPN on Windows. The Xvpnd.exe process (which runs as a service with SYSTEM privileges) listens on TCP port 2015, which is used as an RPC interface for communication with the client side of the ExpressVPN application. A JSON-RPC protocol over HTTP is used for communication. The JSON-RPC XVPN.GetPreference and XVPN.SetPreference methods are vulnerable to path traversal, and allow reading and writing files on the file system on behalf of the service.	2019-01-02	not yet calculated	<a href="#">CVE-2018-15490</a> <a href="#">MISC</a>
f5 -- big-ip	When APM 13.0.0-13.1.x is deployed as an OAuth Resource Server, APM becomes a client application to an external OAuth authorization server. In certain cases when communication between the BIG-IP APM and the OAuth authorization server is lost, APM may not display the intended message in the failure response	2018-12-28	not yet calculated	<a href="#">CVE-2018-15335</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 11.2.1. and greater, unrestricted Snapshot File Access allows BIG-IP system's user with any role, including Guest Role, to have access and download previously generated and available snapshot files on the BIG-IP configuration utility such as QKView and TCPDumps.	2018-12-28	not yet calculated	<a href="#">CVE-2018-15333</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

f5 -- ip_infusion_zebos_and_ocnos	The BGP daemon (bgpd) in all IP Infusion ZebOS versions to 7.10.6 and all OcNOS versions to 1.3.3.145 allow remote attackers to cause a denial of service attack via an autonomous system (AS) path containing 8 or more autonomous system number (ASN) elements.	2018-12-28	not yet calculated	<a href="#">CVE-2018-17539</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the slf4j-ext class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14718</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the axis2-transport-jms class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19360</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the openjpa class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19361</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow attackers to conduct external XML entity (XXE) attacks by leveraging failure to block unspecified JDK classes from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14720</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to conduct server-side request forgery (SSRF) attacks by leveraging failure to block the axis2-jaxws class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14721</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the blaze-ds-opt and blaze-ds-core classes from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14719</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the jboss-common-core class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19362</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. It is an Out-of-Bounds Read Information Disclosure and crash due to a NULL pointer dereference when reading TIFF data during TIFF parsing.	2019-01-03	not yet calculated	<a href="#">CVE-2019-5007</a> <a href="#">CONFIRM</a>
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. It is a NULL pointer dereference during PDF parsing.	2019-01-03	not yet calculated	<a href="#">CVE-2019-5006</a> <a href="#">CONFIRM</a>
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. They allowed Denial of Service (application crash) via image data, because two bytes are written to the end of the allocated memory without judging whether this will cause corruption.	2019-01-03	not yet calculated	<a href="#">CVE-2019-5005</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD before 11.2-STABLE(r348229), 11.2-RELEASE-p7, 12.0-STABLE(r342228), and 12.0-RELEASE-p1, insufficient validation of network-provided data in bootpd may make it possible for a malicious attacker to craft a bootp packet which could cause a stack buffer overflow. It is possible that the buffer overflow could lead to a Denial of Service or remote code execution.	2019-01-03	not yet calculated	<a href="#">CVE-2018-17161</a> <a href="#">BID</a> <a href="#">FREEBSD</a>
frog -- frog_cms	FROG CMS 0.9.5 has XSS via the admin/?/snippet/add name parameter, which is mishandled during an edit action, a related issue to CVE-2018-10319.	2018-12-31	not yet calculated	<a href="#">CVE-2018-19844</a> <a href="#">MISC</a>
getsimple -- getsimple_cms	There is Stored XSS in GetSimple CMS 3.3.12 via the admin/edit.php "post-menu" parameter, a related issue to CVE-2018-16325.	2018-12-31	not yet calculated	<a href="#">CVE-2018-19845</a> <a href="#">MISC</a>
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20673</a> <a href="#">MISC</a>
gnu -- binutils	load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20671</a> <a href="#">MISC</a>



				MISC
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, has a memory leak via a crafted string, leading to a denial of service (memory consumption), as demonstrated by cxxfilt, a related issue to CVE-2018-12698.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20657</a> <a href="#">BID</a> <a href="#">MISC</a>
gnu -- binutils	In GNU Binutils 2.31.1, there is a use-after-free in the error function in elfcomm.c when called from the process_archive function in readelf.c via a crafted ELF file.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20623</a> <a href="#">BID</a> <a href="#">MISC</a>
gnu -- binutils	A NULL pointer dereference was discovered in elf_link_add_object_symbols in elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31.1. This occurs for a crafted ET_DYN with no program headers. A specially crafted ELF file allows remote attackers to cause a denial of service, as demonstrated by ld.	2019-01-01	not yet calculated	<a href="#">CVE-2018-20651</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
guardzilla -- gz180_devices	The remote upgrade feature in Guardzilla GZ180 devices allow command injection via a crafted new firmware version parameter.	2018-12-31	not yet calculated	<a href="#">CVE-2018-18600</a>
hhvm -- hhvm	The Memcache::getextendedstats function can be used to trigger an out-of-bounds read. Exploiting this issue requires control over memcached server hostnames and/or ports. This affects all supported versions of HHVM (3.30 and 3.27.4 and below).	2018-12-31	not yet calculated	<a href="#">CVE-2018-6340</a> <a href="#">MISC</a> <a href="#">MISC</a>
hhvm -- hhvm	A Malformed h2 frame can cause 'std::out_of_range' exception when parsing priority meta data. This behavior can lead to denial-of-service. This affects all supported versions of HHVM (3.25.2, 3.24.6, and 3.21.10 and below) when using the proxygen server to handle HTTP2 requests.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6335</a> <a href="#">MISC</a> <a href="#">MISC</a>
hhvm -- hhvm	folly::secureRandom will re-use a buffer between parent and child processes when fork() is called. That will result in multiple forked children producing repeat (or similar) results. This affects HHVM 3.26 prior to 3.26.3 and the folly library between v2017.12.11.00 and v2018.08.09.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6337</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
hhvm -- hhvm	Mul ipart-file uploads call variables to be improperly registered in the global scope. In cases where variables are not declared explicitly before being used this can lead to unexpected behavior. This affects all supported versions of HHVM prior to the patch (3.25.1, 3.24.5, and 3.21.9 and below).	2018-12-31	not yet calculated	<a href="#">CVE-2018-6334</a> <a href="#">MISC</a> <a href="#">MISC</a>
hsweb -- hsweb	A CSRF issue was discovered in web/authorization/oauth2/controller/OAuth2ClientController.java in hsweb 3.0.4 because the state parameter in the request is not compared with the state parameter in the session after user authentication is successful.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20595</a> <a href="#">MISC</a> <a href="#">MISC</a>
hsweb -- hsweb	An issue was discovered in hsweb 3.0.4. It is a reflected XSS vulnerability due to the absence of type parameter checking in FlowableModelManagerController.java.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20594</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- hg_products	There is an information leak vulnerability in some Huawei HG products. An attacker may obtain information about the HG device by exploiting this vulnerability.	2019-01-02	not yet calculated	<a href="#">CVE-2018-7900</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows full path disclosure via a dev.php?tools-ipaddr&api=Pcoln&uiP= URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20606</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to execute arbitrary PHP code by using root/run/adm.php to modify the boot/bootskip.php file.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20605</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to obtain potentially sensitive debugging information via the root/tools/adbug/binfo.php URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20607</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to read phpinfo output via the root/tools/adbug/binfo.php?phpinfo1 URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20608</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to obtain potentially sensitive configuration information via the root/tools/adbug/check.php URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20609</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows directory traversal via the root/run/adm.php efile parameter.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20610</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allow XSS via a crafted cookie to the root/tools/adbug/binfo.php?cookie URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20611</a> <a href="#">MISC</a>
	inxedu through 2018-12-24 has a SQL Injection vulnerability that can lead to information disclosure via the deleteFaveorite/			

inxedu -- inxedu	PATH_INFO. The vulnerable code location is com.inxedu.os.edu.controller.user.UserController#deleteFavorite (aka deleteFavorite in com/inxedu/os/edu/controller/user/UserController.java), where courseFavoritesService.deleteCourseFavoritesByld is mishandled during use of MyBatis. NOTE: UserController.java has a spelling variation in an annotation: a @RequestMapping("/deleteFavorite/{ids}") line followed by a "public ModelAndView deleteFavorite" line.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3576</a> <a href="#">MISC</a>
ivan_cordoba -- ivan_cordoba_generic_cms	Ivan Cordoba Generic Content Management System (CMS) through 2018-04-28 has XSS via the Administrator/add_pictures.php article ID.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20589</a> <a href="#">MISC</a>
ivan_cordoba -- ivan_cordoba_generic_cms	Ivan Cordoba Generic Content Management System (CMS) through 2018-04-28 has XSS via the Administrator/users.php user ID.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20590</a> <a href="#">MISC</a>
jasper -- jasper	JasPer 2.0.14 has a memory leak in base/jas_malloc.c in libjasper.a when "--output-format jp2" is used.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20622</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MLIST</a>
jspxcms -- jspxcms	Jjspxcms v9.0.0 allows SSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20596</a> <a href="#">MISC</a>
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows full path disclosure via the /install.php?s=/1 URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20602</a> <a href="#">MISC</a>
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows admin.php?s=/Member/add.html CSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20603</a> <a href="#">MISC</a>
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows Directory Traversal via crafted use of ../ in Template/edit/path URIs, as demonstrated by the admin.php?s=/Template/edit/path/*web*.*.*.*1.txt html URI to read the 1.txt file.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20604</a> <a href="#">MISC</a>
libming -- libming	An issue was discovered in libming 0.4.8. There is a heap-based buffer over-read in the function writePNG in the file util/dbl2png.c of the dbl2png command-line program. Because this is associated with an erroneous call to png_write_row in libpng, an out-of-bounds write might occur for some memory layouts.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3572</a> <a href="#">MISC</a>
libsixel -- libsixel	In libsixel v1.8.2, there is a heap-based buffer over-read in the function load_jpeg() in the file loader.c, as demonstrated by img2sixel.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3574</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel -- libsixel	In libsixel v1.8.2, there is an infinite loop in the function sixel_decode_raw_impl() in the file fromsixel.c, as demonstrated by sixel2png.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3573</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification rules allow bitwise logical operations that can be also applied to the can_dlc field. Because of a missing check, the CAN drivers may write arbitrary content beyond the data registers in the CAN controller's I/O memory when processing can-gw manipulated outgoing frames. This is related to cgw_csum_xor_rel. An unprivileged user can trigger a system crash (general protection fault).	2019-01-03	not yet calculated	<a href="#">CVE-2019-3701</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
mcafee -- application_control_and_change_control	A whitelist bypass vulnerability in McAfee Application Control / Change Control 7.0.1 and before allows execution bypass, for example, with simple DLL through interpreters such as PowerShell.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6668</a> <a href="#">CONFIRM</a>
mini-xml -- mini-xml	In Mini-XML (aka mxml) v2.12, there is stack-based buffer overflow in the scan_file function in mxmldoc.c.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mini-xml -- mini-xml	In Mini-XML (aka mxml) v2.12, there is a use-after-free in the mxmlAdd function of the mxml-node.c file. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted xml file, as demonstrated by mxmldoc.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20592</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
multiple_vendors -- multiple_products	An issue was discovered in osquery. A maliciously crafted Universal/fat binary can evade third-party code signing checks. By not completing full inspection of the Universal/fat binary, the user of the third-party tool will believe that the code is signed by Apple, but the malicious unsigned code will execute. This issue affects osquery prior to v3.2.7	2018-12-31	not yet calculated	<a href="#">CVE-2018-6336</a> <a href="#">MISC</a>

mybb -- mybb	The OUGC Awards plugin before 1.8.19 for MyBB allows XSS via a crafted award reason that is mishandled on the awards page or in a user profile.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3501</a> <a href="#">MISC</a> <a href="#">MISC</a>
nuclide -- nuclide	The hhvm-attach deep link handler in Nuclide did not properly sanitize the provided hostname parameter when rendering. As a result, a malicious URL could be used to render HTML and other content inside of the editor's context, which could potentially be chained to lead to code execution. This issue affected Nuclide prior to v0.290.0.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6333</a> <a href="#">MISC</a>
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_csv_decode2 function in ok_csv.c.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20617</a> <a href="#">MISC</a>
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer over-read in the ok_mo_decode2 function in ok_mo.c.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20618</a> <a href="#">MISC</a>
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_wav_decode_ms_adpcm_data function in ok_wav.c.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20616</a> <a href="#">MISC</a>
openrefine -- openrefine	OpenRefine through 3.1 allows arbitrary file write because Directory Traversal can occur during the import of a crafted project file.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3580</a> <a href="#">MISC</a>
otfcc -- otfcc	lib/support/unicodeconv/unicodeconv.c in libotfcc.a in otfcc v0.10.3-alpha has a buffer over-read.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20588</a> <a href="#">MISC</a>
poppler -- poppler	In Poppler 0.72.0, PDFDoc::setup in PDFDoc.cc allows attackers to cause a denial-of-service (application crash caused by Object.h SIGABRT, because of a wrong return value from PDFDoc::setup) by crafting a PDF file in which an xref data structure is mishandled during extractPDFSubtype processing.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20662</a> <a href="#">MISC</a> <a href="#">MISC</a>
proxygen -- proxygen	Proxygen fails to validate that a secondary auth manager is set before dereferencing it. That can cause a denial of service issue when parsing a Certificate/CertificateRequest HTTP2 Frame over a fizz (TLS 1.3) transport. This issue affects Proxygen releases starting from v2018.10.29.00 until the fix in v2018.11.19.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6343</a> <a href="#">MISC</a>
proxygen -- proxygen	A potential denial-of-service issue in the Proxygen handling of invalid HTTP2 priority settings (specifically a circular dependency). This affects Proxygen prior to v2018.12.31.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6346</a> <a href="#">MISC</a>
proxygen -- proxygen	An issue in the Proxygen handling of HTTP2 parsing of headers/trailers can lead to a denial-of-service attack. This affects Proxygen prior to v2018.12.31.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6347</a> <a href="#">MISC</a>
react -- react_applications	React applications which rendered to HTML using the ReactDOMServer API were not escaping user-supplied attribute names at render-time. That lack of escaping could lead to a cross-site scripting vulnerability. This issue affected minor releases 16.0.x, 16.1.x, 16.2.x, 16.3.x, and 16.4.x. It was fixed in 16.0.1, 16.1.2, 16.2.1, 16.3.3, and 16.4.2.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
react-dev-utils -- react-dev-utils	react-dev-utils on Windows allows developers to run a local webserver for accepting various commands, including a command to launch an editor. The input to that command was not properly sanitized, allowing an attacker who can make a network request to the server (either via CSRF or by direct request) to execute arbitrary commands on the targeted system. This issue affects multiple branches: 1.x.x prior to 1.0.4, 2.x.x prior to 2.0.2, 3.x.x prior to 3.1.2, 4.x.x prior to 4.2.2, and 5.x.x prior to 5.0.2.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6342</a> <a href="#">MISC</a> <a href="#">MISC</a>
simply-blog -- simply-blog	Simply-Blog through 2019-01-01 has SQL Injection via the admin/deleteCategories.php delete parameter.	2019-01-01	not yet calculated	<a href="#">CVE-2019-3494</a> <a href="#">MISC</a>
sqla_yaml_fixtures -- sqla_yaml_fixtures	Sqla_yaml_fixtures 0.9.1 allows local users to execute arbitrary python code via the fixture_text argument in sqla_yaml_fixtures load.	2019-01-03	not yet calculated	<a href="#">CVE-2019-3575</a> <a href="#">MISC</a>
technicolor -- mediaaccess_tg789vac_hp_devices	The admin web interface on Technicolor MediaAccess TG789vac v2 HP devices with firmware v16.3.7190-2761005-20161004084353 displays unsanitised user input, which allows an unauthenticated malicious user to embed JavaScript into the Log viewer interface via a crafted HTTP Referer header, aka XSS.	2019-01-03	not yet calculated	<a href="#">CVE-2018-8827</a> <a href="#">MISC</a>
telegram -- telegram_messaging_application_for_android	An exploitable information disclosure vulnerability exists in the "Secret Chats" functionality of the Telegram Android messaging application version 4.9.0. The "Secret Chats" functionality allows a user to delete all traces of a chat, either by using a time trigger or by direct request. There is a bug in this functionality that leaves behind photos taken and shared on the secret chats, even after the chats are deleted. These photos will be stored in	2019-01-03	not yet calculated	<a href="#">CVE-2018-3986</a> <a href="#">BID</a> <a href="#">MISC</a>

	the device and accessible to all applications installed on the Android device.			
temmoku -- temmoku	TEMMOKU T1.09 Beta allows admin/user/add CSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20613 MISC</a>
tobesoft -- xplatform	A vulnerability in the ExtCommon.dll user extension module version 9.2, 9.2.1, 9.2.2 of Xplatform ActiveX could allow attacker to perform a command injection attack. The vulnerability is due to insufficient input validation of command parameters. An crafted malicious parameters could cause arbitrary command to execute.	2019-01-02	not yet calculated	<a href="#">CVE-2018-5197 MISC MISC</a>
uwa -- uwa	UWA 2.3.11 allows index php? g=admin&c=admin&a=add_admin_do CSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20612 MISC</a>
vtiger -- vtiger_crm	Vtiger CRM 7.1.0 before Hotfix2 allows uploading files with the extension "php3" in the logo upload field, if the uploaded file is in PNG format and has a size of 150x40. One can put PHP code into the image; PHP code can be executed using "<? ?>" tags, as demonstrated by a CompanyDetailsSave action. This bypasses the bad-file-extensions protection mechanism. It is related to actions/CompanyDetailsSave.php, actions/UpdateCompanyLogo.php, and models/CompanyDetails.php.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5009 MISC MISC MISC EXPLOIT-DB</a>
waimai -- waimai_super_cms	An issue was discovered in Waimai Super Cms 20150505. web/Lib/Action/ProductAction.class.php allows blind SQL Injection via the id[0] parameter to the /product URI.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3577 MISC</a>
webroot -- brightcloud_sdk	An exploitable buffer overflow vulnerability exists in the HTTP header-parsing function of the Webroot BrightCloud SDK. The function bc_http_read_header incorrectly handles overlong headers, leading to arbitrary code execution. An unauthenticated attacker could impersonate a remote BrightCloud server to trigger this vulnerability.	2019-01-03	not yet calculated	<a href="#">CVE-2018-4012 MISC</a>
weixin-java-tools -- weixin-java-tools	An issue was discovered in weixin-java-tools v3.3.0. There is an XXE vulnerability in the getXmlDoc method of the BaseWxPayResult java file. NOTE: this issue exists because of an incomplete fix for CVE-2018-20318.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5312 MISC</a>
whatsapp -- whatsapp	A heap corruption in WhatsApp can be caused by a malformed RTP packet being sent after a call is established. The vulnerability can be used to cause denial of service. It affects WhatsApp for Android prior to v2.18.293, WhatsApp for iOS prior to v2.18.93, and WhatsApp for Windows Phone prior to v2.18.172.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6344 BID MISC</a>
yunucms -- yunucms	An issue was discovered in YUNUCMS V1.1.8. app/index/controller/Show.php has an XSS vulnerability via the index.php/index/show/index cw parameter.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5311 MISC</a>
yunucms -- yunucms	YUNUCMS 1.1.8 has XSS in app/admin/controller/System.php because crafted data can be written to the sys.php file, as demonstrated by site_title in an admin/system/basic POST request.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5310 MISC</a>
zoho_manageengine -- adselfservice	Zoho ManageEngine ADSelfService Plus 5.x before build 5703 has SSRF.	2019-01-03	not yet calculated	<a href="#">CVE-2019-3905 CONFIRM</a>
zoho_manageengine -- adselfservice	Zoho ManageEngine ADSelfService Plus 5.x before build 5701 has XXE via an uploaded product license.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20664 CONFIRM</a>

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)







**From:** [US-CERT](#)  
**To:** [wqultarte@ci.sunnyvale.ca.us](mailto:wqultarte@ci.sunnyvale.ca.us)  
**Subject:** SB19-007: Vulnerability Summary for the Week of December 31, 2018  
**Date:** Monday, January 07, 2019 9:25:41 AM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## **[SB19-007: Vulnerability Summary for the Week of December 31, 2018](#)**

01/07/2019 06:55 AM EST

Original release date: January 07, 2019

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## **High Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
There were no high vulnerabilities recorded this week.				

[Back to top](#)

## **Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
douco -- doupdp	An issue was discovered in DouCo DouPHP 1.5 20181221. It allows full path disclosure in "Smarty error: unable to read resource" error messages for a crafted installation page.	2018-12-28	<a href="#">5.0</a>	<a href="#">CVE-2018-20566 MISC</a>
f5 -- big-ip_access_policy_manager	A cross-site request forgery (CSRF) vulnerability in the APM webtop 11.2.1 or greater may allow attacker to force an APM webtop session to log out and require re-authentication.	2018-12-28	<a href="#">4.3</a>	<a href="#">CVE-2018-15334 BID CONFIRM</a>
freedesktop -- poppler	A reachable Object::getString assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to construction of invalid rich media annotation assets in the AnnotRichMedia class in Annot.c.	2018-12-28	<a href="#">4.3</a>	<a href="#">CVE-2018-20551 MISC MISC</a>
freedesktop -- poppler	A reachable Object::dictLookup assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to the lack of a check for the dict data type, as demonstrated by use of the FileSpec class (in FileSpec.cc) in pdfdetach.	2019-01-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20650 MISC MISC</a>
libming -- libming	A heap-based buffer over-read was discovered in decompileJUMP function in util/decompile.c of libming v0.4.8. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by swftocxx.	2018-12-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20591 MISC</a>
tinyexr_project -- tinyexr	An attempted excessive memory allocation was discovered in the function tinyexr::Allocatelmage in tinyexr.h in tinyexr v0.9.5. Remote	2019-01-01	<a href="#">4.3</a>	<a href="#">CVE-2018-20652</a>

	attackers could leverage this vulnerability to cause a denial-of-service via crafted input, which leads to an out-of-memory exception.			<a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 has ?do=user_addpost CSRF.	2018-12-30	<a href="#">6.8</a>	<a href="#">CVE-2018-20598</a> <a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 allows remote attackers to execute arbitrary PHP code by entering this code during an index.php sadmin_fileedit action.	2018-12-30	<a href="#">6.5</a>	<a href="#">CVE-2018-20599</a> <a href="#">MISC</a>
ucms_project -- ucms	sadmin/cedit.php in UCMS 1.4.7 has XSS via an index.php sadmin_cedit action.	2018-12-30	<a href="#">4.3</a>	<a href="#">CVE-2018-20600</a> <a href="#">MISC</a>

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/page.php?rec=edit has XSS via the page_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20557</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/system.php?rec=update has XSS via the site_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20558</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/product.php?rec=update has XSS via the name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20559</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/show.php?rec=update has XSS via the show_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20560</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/article.php?rec=update has XSS via the title parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20561</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/article_category.php?rec=update has XSS via the cat_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20562</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/mobile.php?rec=system&act=update has XSS via the mobile_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20563</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/product_category.php?rec=update has XSS via the cat_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20564</a> <a href="#">MISC</a>
douco -- doupHP	An issue was discovered in DouCo DouPHP 1.5 20181221. admin/nav.php?rec=update has XSS via the nav_name parameter.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20565</a> <a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 has XSS via the dir parameter in an index.php sadmin_fileedit action.	2018-12-30	<a href="#">3.5</a>	<a href="#">CVE-2018-20597</a> <a href="#">MISC</a>
ucms_project -- ucms	UCMS 1.4.7 has XSS via the description parameter in an index.php list_editpost action.	2018-12-30	<a href="#">3.5</a>	<a href="#">CVE-2018-20601</a> <a href="#">MISC</a>
website_seller_script_project -- website_seller_script	PHP Scripts Mall Website Seller Script 2 0.5 has XSS via a Profile field such as Company Address, a related issue to CVE-2018-15896.	2018-12-28	<a href="#">3.5</a>	<a href="#">CVE-2018-20530</a> <a href="#">MISC</a>

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abb -- gate-e1_and_gate-e2	Pluto Safety PLC Gateway Ethernet devices ABB GATE-E1 and GATE-E2 all versions do not allow authentication to be configured on administrative telnet or web interfaces, which could enable various effects vectors, including conducting device resets, reading or modifying registers, and changing configuration settings such as IP addresses.	2019-01-03	not yet calculated	<a href="#">CVE-2018-18995</a> <a href="#">BID</a> <a href="#">MISC</a>
abb -- gate-e1_and_gate-e2	Pluto Safety PLC Gateway Ethernet devices in ABB GATE-E1 and GATE-E2 all versions allows an unauthenticated attacker using the administrative web interface to insert an HTML/Javascript payload into any of the device properties, which may allow an attacker to display/execute the payload in a	2019-01-03	not yet calculated	<a href="#">CVE-2018-18997</a> <a href="#">BID</a> <a href="#">MISC</a>

	visitor browser.			
ansible -- ansible	ansible before versions 2.5.14, 2.6.11, 2.7.5 is vulnerable to a information disclosure flaw in vvv+ mode with no_log on that can lead to leakage of sensible data.	2019-01-03	not yet calculated	<a href="#">CVE-2018-16876</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
ansible -- tower	Ansible Tower before version 3.3.3 does not set a secure channel as it is using the default insecure configuration channel settings for messaging celery workers from RabbitMQ. This could lead in data leak of sensitive information such as passwords as well as denial of service attacks by deleting projects or inventory files.	2019-01-03	not yet calculated	<a href="#">CVE-2018-16879</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
apache -- netbeans	Apache NetBeans (incubating) 9.0 NetBeans Proxy Auto-Configuration (PAC) interpretation is vulnerable for remote command execution (RCE). Using the Nashorn script engine the environment of the JavaScript execution for the Proxy Auto-Configuration leaks privileged objects, that can be used to circumvent the execution limits. If a different script engine was used, no execution limits were in place. Both vectors allow remote code execution.	2018-12-31	not yet calculated	<a href="#">CVE-2018-17191</a> <a href="#">BID</a> <a href="#">MISC</a>
aria2 -- aria2	aria2c in aria2 1.33.1, when --log is used, can store an HTTP Basic Authentication username and password in a file, which might allow local users to obtain sensitive information by reading this file.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3500</a> <a href="#">MISC</a>
artifex -- ghostscript	In Artifex Ghostscript before 9.26, a carefully crafted PDF file can trigger an extremely long running computation when parsing the file.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19478</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
august -- connect_devices	An issue was discovered on August Connect devices. Insecure data transfer between the August app and August Connect during configuration allows attackers to discover home Wi-Fi credentials. This data transfer uses an unencrypted access point for these credentials, and passes them in an HTTP POST, using the AugustWifiDevice class, with data encrypted with a fixed key found obfuscated in the app.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20100</a> <a href="#">MISC</a>
bento4 -- bento4	An issue was discovered in Bento4 1.5.1-627. The AP4_StcoAtom class in Core/AP4StcoAtom.cpp has an attempted excessive memory allocation when called from AP4_AtomFactory::CreateAtomFromStream in Core/AP4AtomFactory.cpp, as demonstrated by mp42hls.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20659</a> <a href="#">MISC</a>
bmc -- remedy	Remedy AR System Server in BMC Remedy 7.1 may fail to set the correct user context in certain impersonation scenarios, which can allow a user to act with the identity of a different user, because UserData.js in the WO:WorkOrderConsole component allows a username substitution involving a UserData_Init call.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19505</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">SECTRACK</a>
buck -- buck	Buck parser-cache command loads/saves state using Java serialized object. If the state information is maliciously crafted, deserializing it could lead to code execution. This issue affects Buck versions prior to v2018.06.25.01.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6331</a> <a href="#">MISC</a>
chinamobile_plc -- wireless_router_gpn2.4p21-c-cn_devices	ChinaMobile PLC Wireless Router GPN2.4P21-C-CN devices with firmware W2001EN-00 have XSS via the cgi-bin/webproc?getpage=html/index.html var:subpage parameter.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20326</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
cim -- cim	public\install\install.php in CIM 0.9.3 allows remote attackers to reload the product via the public/install/step3 URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20614</a> <a href="#">MISC</a>
code42 -- code42_for_enterprise	The Code42 app before 6.8.4, as used in Code42 for Enterprise, on Linux installs with overly permissive permissions on the /usr/local/crashplan/log directory. This allows a user to manipulate symbolic links to escalate privileges, or show the contents of sensitive files that a regular user would not have access to.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20131</a> <a href="#">MISC</a>
core_ftp_server -- core_ftp_server	The server in Core FTP 2.0 build 653 on 32-bit platforms allows remote attackers to cause a denial of service (daemon crash) via a crafted XRMd command.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20658</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
	Prior to CouchDB version 2.3.0, CouchDB allowed for runtime-			

couchdb -- couchdb	configuration of key components of the database. In some cases, this lead to vulnerabilities where CouchDB admin users could access the underlying operating system as the CouchDB user. Together with other vulnerabilities, it allowed full system entry for unauthenticated users. Rather than waiting for new vulnerabilities to be discovered, and fixing them as they come up, the CouchDB development team decided to make changes to avoid this entire class of vulnerabilities.	2019-01-02	not yet calculated	<a href="#">CVE-2018-17188</a> <a href="#">MISC</a>
cuba_platform -- cuba_platform	The Reporting Addon (aka Reports Addon) through 2019-01-02 for CUBA Platform through 6.10.x has Persistent XSS via the "Reports > Reports" name field.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20663</a> <a href="#">MISC</a>
cuppacms -- cuppacms	CuppaCMS has XSS via an SVG document uploaded to the administrator/#/component/table_manager/view/cu_views URI.	2018-12-31	not yet calculated	<a href="#">CVE-2018-19918</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
d-link -- dir-818lw_and_dir-860l	On D-Link DIR-818LW Rev.A 2.05.B03 and DIR-860L Rev.B 2.03.B03 devices, unauthenticated remote OS command execution can occur in the soap.cgi service of the cgibin binary via an "&&" substring in the service parameter. NOTE: this issue exists because of an incomplete fix for CVE-2018-6530.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20114</a> <a href="#">MISC</a>
dolibarr -- dolibarr	A stored cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote authenticated users to inject arbitrary web script or HTML via the "address" (POST) or "town" (POST) parameter to adherents/type.php.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19992</a> <a href="#">MISC</a>
dolibarr -- dolibarr	A reflected cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote attackers to inject arbitrary web script or HTML via the transphrase parameter to public/notice.php.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19993</a> <a href="#">MISC</a>
dolibarr -- dolibarr	An error-based SQL injection vulnerability in product/card.php in Dolibarr version 8.0.2 allows remote authenticated users to execute arbitrary SQL commands via the desiredstock parameter.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19994</a> <a href="#">MISC</a>
dolibarr -- dolibarr	A stored cross-site scripting (XSS) vulnerability in Dolibarr 8.0.2 allows remote authenticated users to inject arbitrary web script or HTML via the "address" (POST) or "town" (POST) parameter to user/card.php.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19995</a> <a href="#">MISC</a> <a href="#">MISC</a>
dolibarr -- dolibarr	SQL injection vulnerability in user/card.php in Dolibarr version 8.0.2 allows remote authenticated users to execute arbitrary SQL commands via the employee parameter.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19998</a> <a href="#">MISC</a> <a href="#">MISC</a>
driveragent -- driveragent	DriverAgent 2.2015.7.14, which includes DrvAgent64 sys 1.0.0.1, allows a user to send an IOCTL (0x80002068) with a user defined buffer size. If the size of the buffer is less than 512 bytes, then the driver will overwrite the next pool header if there is one next to the user buffer's pool.	2019-01-03	not yet calculated	<a href="#">CVE-2018-19523</a> <a href="#">MISC</a>
emc -- rsa_archer	RSA Archer versions prior to 6.5.0.1 contain an improper access control vulnerability. A remote malicious user could potentially exploit this vulnerability to bypass authorization checks and gain read access to restricted user information.	2019-01-03	not yet calculated	<a href="#">CVE-2018-15780</a> <a href="#">BID</a> <a href="#">FULLDISC</a>
epon -- cpe-wifi_devices	EPON CPE-WiFi devices 2.0.4-X000 are vulnerable to escalation of privileges by sending cooLogin=1, cooUser=admin, and timestamp=-1 cookies.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20512</a> <a href="#">MISC</a>
exiftool -- exiftool	ExifTool 8.32 allows local users to gain privileges by creating a %TEMP%\par-%username%\cache-exiftool-8.32 folder with a victim's username, and then copying a Trojan horse ws32_32.dll file into this new folder, aka DLL Hijacking. NOTE: 8.32 is an obsolete version from 2010 (9.x was released starting in 2012, and 10.x was released starting in 2015).	2019-01-02	not yet calculated	<a href="#">CVE-2018-20211</a> <a href="#">MISC</a> <a href="#">FULLDISC</a>
expressvpn -- expressvpn	An issue was discovered in ExpressVPN on Windows. The Xvpnd.exe process (which runs as a service with SYSTEM privileges) listens on TCP port 2015, which is used as an RPC interface for communication with the client side of the ExpressVPN application. A JSON-RPC protocol over HTTP is used for communication. The JSON-RPC XVPN.GetPreference and XVPN.SetPreference methods are vulnerable to path traversal, and allow reading and writing files on the file system on behalf of the service.	2019-01-02	not yet calculated	<a href="#">CVE-2018-15490</a> <a href="#">MISC</a>
f5 -- big-ip	When APM 13.0.0-13.1.x is deployed as an OAuth Resource Server, APM becomes a client application to an external OAuth authorization server. In certain cases when communication between the BIG-IP APM and the OAuth authorization server is lost, APM may not display the intended message in the failure response	2018-12-28	not yet calculated	<a href="#">CVE-2018-15335</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
f5 -- big-ip	On versions 11.2.1. and greater, unrestricted Snapshot File Access allows BIG-IP system's user with any role, including Guest Role, to have access and download previously generated and available snapshot files on the BIG-IP configuration utility such as QKView and TCPDumps.	2018-12-28	not yet calculated	<a href="#">CVE-2018-15333</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

f5 -- ip_infusion_zebos_and_ocnos	The BGP daemon (bgpd) in all IP Infusion ZebOS versions to 7.10.6 and all OcNOS versions to 1.3.3.145 allow remote attackers to cause a denial of service attack via an autonomous system (AS) path containing 8 or more autonomous system number (ASN) elements.	2018-12-28	not yet calculated	<a href="#">CVE-2018-17539</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the slf4j-ext class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14718</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the axis2-transport-jms class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19360</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the openjpa class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19361</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow attackers to conduct external XML entity (XXE) attacks by leveraging failure to block unspecified JDK classes from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14720</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to conduct server-side request forgery (SSRF) attacks by leveraging failure to block the axis2-jaxws class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14721</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.7 might allow remote attackers to execute arbitrary code by leveraging failure to block the blaze-ds-opt and blaze-ds-core classes from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-14719</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
fasterxml -- jackson	FasterXML jackson-databind 2.x before 2.9.8 might allow attackers to have unspecified impact by leveraging failure to block the jboss-common-core class from polymorphic deserialization.	2019-01-02	not yet calculated	<a href="#">CVE-2018-19362</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. It is an Out-of-Bounds Read Information Disclosure and crash due to a NULL pointer dereference when reading TIFF data during TIFF parsing.	2019-01-03	not yet calculated	<a href="#">CVE-2019-5007</a> <a href="#">CONFIRM</a>
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. It is a NULL pointer dereference during PDF parsing.	2019-01-03	not yet calculated	<a href="#">CVE-2019-5006</a> <a href="#">CONFIRM</a>
foxit_software -- foxit_reader_and_phantompdf	An issue was discovered in Foxit Reader and PhantomPDF before 9.4 on Windows. They allowed Denial of Service (application crash) via image data, because two bytes are written to the end of the allocated memory without judging whether this will cause corruption.	2019-01-03	not yet calculated	<a href="#">CVE-2019-5005</a> <a href="#">CONFIRM</a>
freebsd -- freebsd	In FreeBSD before 11.2-STABLE(r348229), 11.2-RELEASE-p7, 12.0-STABLE(r342228), and 12.0-RELEASE-p1, insufficient validation of network-provided data in bootpd may make it possible for a malicious attacker to craft a bootp packet which could cause a stack buffer overflow. It is possible that the buffer overflow could lead to a Denial of Service or remote code execution.	2019-01-03	not yet calculated	<a href="#">CVE-2018-17161</a> <a href="#">BID</a> <a href="#">FREEBSD</a>
frog -- frog_cms	FROG CMS 0.9.5 has XSS via the admin/?/snippet/add name parameter, which is mishandled during an edit action, a related issue to CVE-2018-10319.	2018-12-31	not yet calculated	<a href="#">CVE-2018-19844</a> <a href="#">MISC</a>
getsimple -- getsimple_cms	There is Stored XSS in GetSimple CMS 3.3.12 via the admin/edit.php "post-menu" parameter, a related issue to CVE-2018-16325.	2018-12-31	not yet calculated	<a href="#">CVE-2018-19845</a> <a href="#">MISC</a>
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, contains an integer overflow vulnerability (for "Create an array for saving the template argument values") that can trigger a heap-based buffer overflow, as demonstrated by nm.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20673</a> <a href="#">MISC</a>
gnu -- binutils	load_specific_debug_section in objdump.c in GNU Binutils through 2.31.1 contains an integer overflow vulnerability that can trigger a heap-based buffer overflow via a crafted section size.	2019-01-04	not yet calculated	<a href="#">CVE-2018-20671</a> <a href="#">MISC</a>



				MISC
gnu -- binutils	The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.31.1, has a memory leak via a crafted string, leading to a denial of service (memory consumption), as demonstrated by cxxfilt, a related issue to CVE-2018-12698.	2019-01-02	not yet calculated	<a href="#">CVE-2018-20657</a> <a href="#">BID</a> <a href="#">MISC</a>
gnu -- binutils	In GNU Binutils 2.31.1, there is a use-after-free in the error function in elfcomm.c when called from the process_archive function in readelf.c via a crafted ELF file.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20623</a> <a href="#">BID</a> <a href="#">MISC</a>
gnu -- binutils	A NULL pointer dereference was discovered in elf_link_add_object_symbols in elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31.1. This occurs for a crafted ET_DYN with no program headers. A specially crafted ELF file allows remote attackers to cause a denial of service, as demonstrated by ld.	2019-01-01	not yet calculated	<a href="#">CVE-2018-20651</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
guardzilla -- gz180_devices	The remote upgrade feature in Guardzilla GZ180 devices allow command injection via a crafted new firmware version parameter.	2018-12-31	not yet calculated	<a href="#">CVE-2018-18600</a>
hhvm -- hhvm	The Memcache::getextendedstats function can be used to trigger an out-of-bounds read. Exploiting this issue requires control over memcached server hostnames and/or ports. This affects all supported versions of HHVM (3.30 and 3.27.4 and below).	2018-12-31	not yet calculated	<a href="#">CVE-2018-6340</a> <a href="#">MISC</a> <a href="#">MISC</a>
hhvm -- hhvm	A Malformed h2 frame can cause 'std::out_of_range' exception when parsing priority meta data. This behavior can lead to denial-of-service. This affects all supported versions of HHVM (3.25.2, 3.24.6, and 3.21.10 and below) when using the proxygen server to handle HTTP2 requests.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6335</a> <a href="#">MISC</a> <a href="#">MISC</a>
hhvm -- hhvm	folly::secureRandom will re-use a buffer between parent and child processes when fork() is called. That will result in multiple forked children producing repeat (or similar) results. This affects HHVM 3.26 prior to 3.26.3 and the folly library between v2017.12.11.00 and v2018.08.09.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6337</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
hhvm -- hhvm	Mul ipart-file uploads call variables to be improperly registered in the global scope. In cases where variables are not declared explicitly before being used this can lead to unexpected behavior. This affects all supported versions of HHVM prior to the patch (3.25.1, 3.24.5, and 3.21.9 and below).	2018-12-31	not yet calculated	<a href="#">CVE-2018-6334</a> <a href="#">MISC</a> <a href="#">MISC</a>
hsweb -- hsweb	A CSRF issue was discovered in web/authorization/oauth2/controller/OAuth2ClientController.java in hsweb 3.0.4 because the state parameter in the request is not compared with the state parameter in the session after user authentication is successful.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20595</a> <a href="#">MISC</a> <a href="#">MISC</a>
hsweb -- hsweb	An issue was discovered in hsweb 3.0.4. It is a reflected XSS vulnerability due to the absence of type parameter checking in FlowableModelManagerController.java.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20594</a> <a href="#">MISC</a> <a href="#">MISC</a>
huawei -- hg_products	There is an information leak vulnerability in some Huawei HG products. An attacker may obtain information about the HG device by exploiting this vulnerability.	2019-01-02	not yet calculated	<a href="#">CVE-2018-7900</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows full path disclosure via a dev.php?tools-ipaddr&api=Pcoln&uiP= URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20606</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to execute arbitrary PHP code by using root/run/adm.php to modify the boot/bootskip.php file.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20605</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to obtain potentially sensitive debugging information via the root/tools/adbug/binfo.php URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20607</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to read phpinfo output via the root/tools/adbug/binfo.php?phpinfo1 URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20608</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows remote attackers to obtain potentially sensitive configuration information via the root/tools/adbug/check.php URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20609</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allows directory traversal via the root/run/adm.php efile parameter.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20610</a> <a href="#">MISC</a>
imcat -- imcat	imcat 4.4 allow XSS via a crafted cookie to the root/tools/adbug/binfo.php?cookie URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20611</a> <a href="#">MISC</a>
	inxedu through 2018-12-24 has a SQL Injection vulnerability that can lead to information disclosure via the deleteFaveorite/			

inxedu -- inxedu	PATH_INFO. The vulnerable code location is com.inxedu.os.edu.controller.user.UserController#deleteFavorite (aka deleteFavorite in com/inxedu/os/edu/controller/user/UserController.java), where courseFavoritesService.deleteCourseFavoritesByld is mishandled during use of MyBatis. NOTE: UserController.java has a spelling variation in an annotation: a @RequestMapping("/deleteFavorite/{ids}") line followed by a "public ModelAndView deleteFavorite" line.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3576</a> <a href="#">MISC</a>
ivan_cordoba -- ivan_cordoba_generic_cms	Ivan Cordoba Generic Content Management System (CMS) through 2018-04-28 has XSS via the Administrator/add_pictures.php article ID.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20589</a> <a href="#">MISC</a>
ivan_cordoba -- ivan_cordoba_generic_cms	Ivan Cordoba Generic Content Management System (CMS) through 2018-04-28 has XSS via the Administrator/users.php user ID.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20590</a> <a href="#">MISC</a>
jasper -- jasper	JasPer 2.0.14 has a memory leak in base/jas_malloc.c in libjasper.a when "--output-format jp2" is used.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20622</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MLIST</a>
jspxcms -- jspxcms	Jjspxcms v9.0.0 allows SSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20596</a> <a href="#">MISC</a>
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows full path disclosure via the /install.php?s=/1 URI.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20602</a> <a href="#">MISC</a>
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows admin.php?s=/Member/add.html CSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20603</a> <a href="#">MISC</a>
lei_feng_tv -- lei_feng_tv_cms	Lei Feng TV CMS (aka LFCMS) 3.8.6 allows Directory Traversal via crafted use of ../ in Template/edit/path URIs, as demonstrated by the admin.php?s=/Template/edit/path/*web*.*.*.*1.txt html URI to read the 1.txt file.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20604</a> <a href="#">MISC</a>
libming -- libming	An issue was discovered in libming 0.4.8. There is a heap-based buffer over-read in the function writePNG in the file util/dbl2png.c of the dbl2png command-line program. Because this is associated with an erroneous call to png_write_row in libpng, an out-of-bounds write might occur for some memory layouts.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3572</a> <a href="#">MISC</a>
libsixel -- libsixel	In libsixel v1.8.2, there is a heap-based buffer over-read in the function load_jpeg() in the file loader.c, as demonstrated by img2sixel.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3574</a> <a href="#">MISC</a> <a href="#">MISC</a>
libsixel -- libsixel	In libsixel v1.8.2, there is an infinite loop in the function sixel_decode_raw_impl() in the file fromsixel.c, as demonstrated by sixel2png.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3573</a> <a href="#">MISC</a> <a href="#">MISC</a>
linux -- linux_kernel	An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification rules allow bitwise logical operations that can be also applied to the can_dlc field. Because of a missing check, the CAN drivers may write arbitrary content beyond the data registers in the CAN controller's I/O memory when processing can-gw manipulated outgoing frames. This is related to cgw_csum_xor_rel. An unprivileged user can trigger a system crash (general protection fault).	2019-01-03	not yet calculated	<a href="#">CVE-2019-3701</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
mcafee -- application_control_and_change_control	A whitelist bypass vulnerability in McAfee Application Control / Change Control 7.0.1 and before allows execution bypass, for example, with simple DLL through interpreters such as PowerShell.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6668</a> <a href="#">CONFIRM</a>
mini-xml -- mini-xml	In Mini-XML (aka mxml) v2.12, there is stack-based buffer overflow in the scan_file function in mxmldoc.c.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20593</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
mini-xml -- mini-xml	In Mini-XML (aka mxml) v2.12, there is a use-after-free in the mxmlAdd function of the mxml-node.c file. Remote attackers could leverage this vulnerability to cause a denial-of-service via a crafted xml file, as demonstrated by mxmldoc.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20592</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
multiple_vendors -- multiple_products	An issue was discovered in osquery. A maliciously crafted Universal/fat binary can evade third-party code signing checks. By not completing full inspection of the Universal/fat binary, the user of the third-party tool will believe that the code is signed by Apple, but the malicious unsigned code will execute. This issue affects osquery prior to v3.2.7	2018-12-31	not yet calculated	<a href="#">CVE-2018-6336</a> <a href="#">MISC</a>

mybb -- mybb	The OUGC Awards plugin before 1.8.19 for MyBB allows XSS via a crafted award reason that is mishandled on the awards page or in a user profile.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3501</a> <a href="#">MISC</a> <a href="#">MISC</a>
nuclide -- nuclide	The hhvm-attach deep link handler in Nuclide did not properly sanitize the provided hostname parameter when rendering. As a result, a malicious URL could be used to render HTML and other content inside of the editor's context, which could potentially be chained to lead to code execution. This issue affected Nuclide prior to v0.290.0.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6333</a> <a href="#">MISC</a>
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_csv_decode2 function in ok_csv.c.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20617</a> <a href="#">MISC</a>
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer over-read in the ok_mo_decode2 function in ok_mo.c.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20618</a> <a href="#">MISC</a>
ok-file-formats -- ok-file-formats	ok-file-formats through 2018-10-16 has a heap-based buffer overflow in the ok_wav_decode_ms_adpcm_data function in ok_wav.c.	2018-12-31	not yet calculated	<a href="#">CVE-2018-20616</a> <a href="#">MISC</a>
openrefine -- openrefine	OpenRefine through 3.1 allows arbitrary file write because Directory Traversal can occur during the import of a crafted project file.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3580</a> <a href="#">MISC</a>
otfcc -- otfcc	lib/support/unicodeconv/unicodeconv.c in libotfcc.a in otfcc v0.10.3-alpha has a buffer over-read.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20588</a> <a href="#">MISC</a>
poppler -- poppler	In Poppler 0.72.0, PDFDoc::setup in PDFDoc.cc allows attackers to cause a denial-of-service (application crash caused by Object.h SIGABRT, because of a wrong return value from PDFDoc::setup) by crafting a PDF file in which an xref data structure is mishandled during extractPDFSubtype processing.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20662</a> <a href="#">MISC</a> <a href="#">MISC</a>
proxygen -- proxygen	Proxygen fails to validate that a secondary auth manager is set before dereferencing it. That can cause a denial of service issue when parsing a Certificate/CertificateRequest HTTP2 Frame over a fizza (TLS 1.3) transport. This issue affects Proxygen releases starting from v2018.10.29.00 until the fix in v2018.11.19.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6343</a> <a href="#">MISC</a>
proxygen -- proxygen	A potential denial-of-service issue in the Proxygen handling of invalid HTTP2 priority settings (specifically a circular dependency). This affects Proxygen prior to v2018.12.31.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6346</a> <a href="#">MISC</a>
proxygen -- proxygen	An issue in the Proxygen handling of HTTP2 parsing of headers/trailers can lead to a denial-of-service attack. This affects Proxygen prior to v2018.12.31.00.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6347</a> <a href="#">MISC</a>
react -- react_applications	React applications which rendered to HTML using the ReactDOMServer API were not escaping user-supplied attribute names at render-time. That lack of escaping could lead to a cross-site scripting vulnerability. This issue affected minor releases 16.0.x, 16.1.x, 16.2.x, 16.3.x, and 16.4.x. It was fixed in 16.0.1, 16.1.2, 16.2.1, 16.3.3, and 16.4.2.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6341</a> <a href="#">MISC</a> <a href="#">MISC</a>
react-dev-utils -- react-dev-utils	react-dev-utils on Windows allows developers to run a local webserver for accepting various commands, including a command to launch an editor. The input to that command was not properly sanitized, allowing an attacker who can make a network request to the server (either via CSRF or by direct request) to execute arbitrary commands on the targeted system. This issue affects multiple branches: 1.x.x prior to 1.0.4, 2.x.x prior to 2.0.2, 3.x.x prior to 3.1.2, 4.x.x prior to 4.2.2, and 5.x.x prior to 5.0.2.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6342</a> <a href="#">MISC</a> <a href="#">MISC</a>
simply-blog -- simply-blog	Simply-Blog through 2019-01-01 has SQL Injection via the admin/deleteCategories.php delete parameter.	2019-01-01	not yet calculated	<a href="#">CVE-2019-3494</a> <a href="#">MISC</a>
sqla_yaml_fixtures -- sqla_yaml_fixtures	Sqla_yaml_fixtures 0.9.1 allows local users to execute arbitrary python code via the fixture_text argument in sqla_yaml_fixtures load.	2019-01-03	not yet calculated	<a href="#">CVE-2019-3575</a> <a href="#">MISC</a>
technicolor -- mediaaccess_tg789vac_hp_devices	The admin web interface on Technicolor MediaAccess TG789vac v2 HP devices with firmware v16.3.7190-2761005-20161004084353 displays unsanitised user input, which allows an unauthenticated malicious user to embed JavaScript into the Log viewer interface via a crafted HTTP Referer header, aka XSS.	2019-01-03	not yet calculated	<a href="#">CVE-2018-8827</a> <a href="#">MISC</a>
telegram -- telegram_messaging_application_for_android	An exploitable information disclosure vulnerability exists in the "Secret Chats" functionality of the Telegram Android messaging application version 4.9.0. The "Secret Chats" functionality allows a user to delete all traces of a chat, either by using a time trigger or by direct request. There is a bug in this functionality that leaves behind photos taken and shared on the secret chats, even after the chats are deleted. These photos will be stored in	2019-01-03	not yet calculated	<a href="#">CVE-2018-3986</a> <a href="#">BID</a> <a href="#">MISC</a>

	the device and accessible to all applications installed on the Android device.			
temmoku -- temmoku	TEMMOKU T1.09 Beta allows admin/user/add CSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20613 MISC</a>
tobesoft -- xplatform	A vulnerability in the ExtCommon.dll user extension module version 9.2, 9.2.1, 9.2.2 of Xplatform ActiveX could allow attacker to perform a command injection attack. The vulnerability is due to insufficient input validation of command parameters. An crafted malicious parameters could cause arbitrary command to execute.	2019-01-02	not yet calculated	<a href="#">CVE-2018-5197 MISC MISC</a>
uwa -- uwa	UWA 2.3.11 allows index php? g=admin&c=admin&a=add_admin_do CSRF.	2018-12-30	not yet calculated	<a href="#">CVE-2018-20612 MISC</a>
vtiger -- vtiger_crm	Vtiger CRM 7.1.0 before Hotfix2 allows uploading files with the extension "php3" in the logo upload field, if the uploaded file is in PNG format and has a size of 150x40. One can put PHP code into the image; PHP code can be executed using "<? ?>" tags, as demonstrated by a CompanyDetailsSave action. This bypasses the bad-file-extensions protection mechanism. It is related to actions/CompanyDetailsSave.php, actions/UpdateCompanyLogo.php, and models/CompanyDetails.php.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5009 MISC MISC MISC EXPLOIT-DB</a>
waimai -- waimai_super_cms	An issue was discovered in Waimai Super Cms 20150505. web/Lib/Action/ProductAction.class.php allows blind SQL Injection via the id[0] parameter to the /product URI.	2019-01-02	not yet calculated	<a href="#">CVE-2019-3577 MISC</a>
webroot -- brightcloud_sdk	An exploitable buffer overflow vulnerability exists in the HTTP header-parsing function of the Webroot BrightCloud SDK. The function bc_http_read_header incorrectly handles overlong headers, leading to arbitrary code execution. An unauthenticated attacker could impersonate a remote BrightCloud server to trigger this vulnerability.	2019-01-03	not yet calculated	<a href="#">CVE-2018-4012 MISC</a>
weixin-java-tools -- weixin-java-tools	An issue was discovered in weixin-java-tools v3.3.0. There is an XXE vulnerability in the getXmlDoc method of the BaseWxPayResult java file. NOTE: this issue exists because of an incomplete fix for CVE-2018-20318.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5312 MISC</a>
whatsapp -- whatsapp	A heap corruption in WhatsApp can be caused by a malformed RTP packet being sent after a call is established. The vulnerability can be used to cause denial of service. It affects WhatsApp for Android prior to v2.18.293, WhatsApp for iOS prior to v2.18.93, and WhatsApp for Windows Phone prior to v2.18.172.	2018-12-31	not yet calculated	<a href="#">CVE-2018-6344 BID MISC</a>
yunucms -- yunucms	An issue was discovered in YUNUCMS V1.1.8. app/index/controller/Show.php has an XSS vulnerability via the index.php/index/show/index cw parameter.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5311 MISC</a>
yunucms -- yunucms	YUNUCMS 1.1.8 has XSS in app/admin/controller/System.php because crafted data can be written to the sys.php file, as demonstrated by site_title in an admin/system/basic POST request.	2019-01-04	not yet calculated	<a href="#">CVE-2019-5310 MISC</a>
zoho_manageengine -- adselfservice	Zoho ManageEngine ADSelfService Plus 5.x before build 5703 has SSRF.	2019-01-03	not yet calculated	<a href="#">CVE-2019-3905 CONFIRM</a>
zoho_manageengine -- adselfservice	Zoho ManageEngine ADSelfService Plus 5.x before build 5701 has XXE via an uploaded product license.	2019-01-03	not yet calculated	<a href="#">CVE-2018-20664 CONFIRM</a>

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [www.us-cert.gov](http://www.us-cert.gov). If you need help or have questions, please send an email to [info@us-cert.gov](mailto:info@us-cert.gov). Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

#### OTHER RESOURCES:

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

#### STAY CONNECTED:



#### SUBSCRIBER SERVICES:

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)







**From:** [Hillis Financial Services](#)  
**To:** [kmcgraw@ci.sunnyvale.ca.us](mailto:kmcgraw@ci.sunnyvale.ca.us)  
**Subject:** Weekly Market Update Dated 12-31-2018  
**Date:** Monday, December 31, 2018 10:39:18 AM

---

Having trouble viewing this email? [Click here](#)



# Year-End Special Edition: A Look Back at 2018

**WEEKLY UPDATE - DECEMBER 31, 2018**

## In This Issue

Quote Of The Week

Recipe Of The Week

Healthy Lifestyle

The close of the year provides an opportunity for investors to step back and consider the wider financial landscape. This week, we're reviewing some key issues that defined 2018, as well as some factors that may influence financial markets in the coming year.

## Year in Review

Wall Street began 2018 in rally mode, as enthusiasm for the 2017 Tax Cuts and

Jobs Act spilled over into the New Year. Strong economic news encouraged investors, who put aside fears that rising inflation may lead to higher interest rates. What Wall Street did not see coming were the spring and summer trade disputes with China, Canada, Mexico, and the European Union. Fear of a global economic slowdown contributed to a sharp decline in stock prices in October. U.S. economic growth forecasts were tempered in November for 2019, with bull and bears engaged in a fierce tug-of-war as the year came to a close.<sup>[1]</sup>

## **Economic Growth**

After expanding at a middling 2.2% pace in the first quarter, the Gross Domestic Product (GDP) rose 4.2% in Q2 and 3.4% in Q3.<sup>[2]</sup> The Federal Reserve Bank of Atlanta forecasted a 2.7% increase for Q4, which will be released on January 30, 2019 by the Bureau of Economic Analysis.<sup>[3][4]</sup> The Congressional Budget Office expects GDP growth in 2019 to slow to 2.4% "as growth in business investment and government purchases slows."<sup>[5]</sup>

## **Interest Rates**

At the close of its September 2018 meeting, the Federal Reserve raised the federal funds rate to 2.25%, a full percentage point higher than it was a year earlier. Federal Reserve Chair Jerome Powell appeared to change his stance on monetary policy, saying interest rates were "just below" a neutral level. Previously, he indicated rates were a "long way" from neutral.<sup>[6]</sup>

## **Consumer Prices and Wage Growth**

The number of future interest rate hikes by the Fed may largely depend on its reading of inflation. An uptick in consumer prices or an increase in wage growth may prompt the Fed to consider additional hikes in 2019.<sup>[7]</sup>

## **Trade Talk Progress**

Tariffs were a highlight of 2018 news. On July 10, the Trump administration announced a list of tariffs on \$200 billion in Chinese goods.<sup>[8]</sup> The escalating trade dispute between the U.S. and China is an enormous overhang on the financial markets. The continuing impasse may affect economic growth and push consumer prices higher.

2018 also was a year in which a major trade pact started to come together. The United States-Mexico-Canada Agreement (USMCA) was approved in principle in October. However, the agreement must be approved by Congress and the legislative bodies of Mexico and Canada before it can take effect.<sup>[9]</sup>

## **U.S. Dollar**

Rising interest rates and robust domestic growth in 2018 lead to a

strengthening of the U.S. dollar. A strong U.S. dollar can negatively affect profits of U.S.-based multinational companies, since it can make their products more expensive to overseas buyers.<sup>[10]</sup> This will also be something to watch in the coming year.

## Real Estate

The trend of higher interest rates in 2018 was also felt in the real estate market. The average rate on a 30-year conventional home loan stood at 3.95% in January 2018. At year's end, it was hovering near 5% according to Freddie Mac.<sup>[11]</sup>

We hope you enjoyed this look back at 2018! Next week, we'll be back to covering the market numbers.



## Quote Of The Week



*"The habit of saving is itself an education; it fosters every virtue, teaches self-denial, cultivates the sense of order, trains to forethought, and so broadens the mind."*

- T.T. Munger

## Recipe Of The Week



### Beef Stroganoff



Serves 4



## Ingredients:

- 2 tablespoons olive oil
- 10 ounces cremini mushrooms (sliced)
- Kosher salt
- Pepper
- 1 pound lean beef sirloin (thinly sliced)
- 2 cloves garlic (finely chopped)
- 2 tablespoons Dijon mustard
- ½ cup dry white wine
- 3½ cups low-sodium beef broth
- 8 ounces fusilli pasta
- 3 tablespoons crème fraîche or sour cream

## Directions:

1. On medium heat, heat 1 tablespoon olive oil in large skillet.
2. Stir in cremini mushrooms, season with salt and pepper, and cook until browned, 5 minutes. Move to bowl.
3. Put the pan back on medium heat. Stir in 1 tablespoon olive oil, season thinly sliced lean beef sirloin with salt and pepper, and cook until no longer pink.
4. Add garlic, cook 1 minute, and stir in Dijon mustard.
5. Put in dry white wine, cook. Scrape up any browned bits.
6. Mix in low-sodium beef broth. Bring to a simmer.
7. Mix in fusilli pasta and mushroom with juices. Bring to a simmer again. Stir often until the pasta is al dente, 14-18 minutes.
8. Mix in crème fraîche or sour cream. Season with salt and pepper.

Recipe adapted from Good Housekeeping<sup>[12]</sup>



## Healthy Lifestyle



## Fibromyalgia: What is It, and How Do You Treat It?

You experience chronic muscle pain, fatigue, sleep problems, and tender areas. You may have fibromyalgia.

About 5 million Americans have fibromyalgia, a lifelong condition. Sufferers typically have stiff, sore muscles. The syndrome is not easily diagnosed, but doctors are able to develop treatment plans based on symptoms.

Health experts say your best approach for relief is to get moving. A few minor changes to your exercise routine can give you more energy and ease the pain.



For starters, gently rotate your joints until they move easily. Focusing on the big muscles (calves, thighs, hips, lower back, shoulders), stretch the full range of motion and hold for 30 seconds.

Walking and other aerobic activities can provide significant relief. The secret is to find something you enjoy doing and doing it for 30 minutes a day, five days a week.

Isometric exercises are great too. Isometrics consist of pushing and holding something against resistance. The chest press is one example. Holding your two hands clasped in front of you is a good one. Do five sets. A set is pressing and holding for 10-15 seconds.

Take it easy with workouts at first. Low- and moderate-intensity routines are the best way to get in the habit. Take it slow and easy.

Tips adapted from WebMD<sup>[15]</sup>

---

### ***Share the Wealth of Knowledge!***

*Please share this market update with family, friends, or colleagues. If you would like us to add them to our list, simply click on the "Forward email" link below.  
We love being introduced!*



---

Investing involves risk including the potential loss of principal. No investment strategy can guarantee a profit or protect against loss in periods of declining values.

Diversification does not guarantee profit nor is it guaranteed to protect assets.

International investing involves special risks such as currency fluctuation and political instability and may not be suitable for all investors.

The Standard & Poor's 500 (S&P 500) is an unmanaged group of securities considered to be representative of the stock market in general.

The Dow Jones Industrial Average is a price-weighted average of 30 significant stocks traded on the New York Stock Exchange and the NASDAQ. The DJIA was invented by Charles Dow back in 1896.

The Nasdaq Composite is an index of the common stocks and similar securities listed on the NASDAQ stock market and is considered a broad indicator of the performance of stocks of technology companies and growth companies.

The MSCI EAFE Index was created by Morgan Stanley Capital International (MSCI) that serves as a benchmark of the performance in major international equity markets as represented by 21 major MSCI indices from Europe, Australia, and Southeast Asia.

The 10-year Treasury Note represents debt owed by the United States Treasury to the public. Since the U.S. Government is seen as a risk-free borrower, investors use the 10-year Treasury Note as a benchmark for the long-term bond market.

Opinions expressed are subject to change without notice and are not intended as investment advice or to predict future performance.

Past performance does not guarantee future results.

You cannot invest directly in an index.

Consult your financial professional before making any investment decision.

Fixed income investments are subject to various risks including changes in interest rates, credit quality, inflation risk, market valuations, prepayments, corporate events, tax ramifications and other factors.

These are the views of Platinum Advisor Strategies, LLC, and not necessarily those of the named representative, Broker dealer or Investment Advisor, and should not be construed as investment advice. Neither the named representative nor the named Broker dealer or Investment Advisor gives tax or legal advice. All information is believed to be from reliable sources; however, we make no representation as to its completeness or accuracy. Please consult your financial advisor for further information.

By clicking on these links, you will leave our server, as the links are located on another server. We have not independently verified the information available through this link. The link is provided to you as a matter of interest. Please click on the links below to leave and proceed to the selected site.

[1] [www.cnn.com/2018/11/20/jp-morgan-sees-a-slowdown-coming-with-economy-growing-at-less-than-2-percent-in-2019.html](http://www.cnn.com/2018/11/20/jp-morgan-sees-a-slowdown-coming-with-economy-growing-at-less-than-2-percent-in-2019.html)

[2] [tradingeconomics.com/united-states/gdp-growth](http://tradingeconomics.com/united-states/gdp-growth)

[3] [www.frbatlanta.org/cqer/research/gdpnow.aspx](http://www.frbatlanta.org/cqer/research/gdpnow.aspx)

[4] [www.bea.gov/news/schedule](http://www.bea.gov/news/schedule)

[5] [www.cnn.com/2018/08/14/us-economy-seen-strong-in-2018-to-slow-in-2019-cbo.html](http://www.cnn.com/2018/08/14/us-economy-seen-strong-in-2018-to-slow-in-2019-cbo.html)

[6] [www.marketwatch.com/story/seemingly-dovish-powell-says-interest-rates-are-just-below-level-where-they-wont-stimulate-economy-2018-11-28](http://www.marketwatch.com/story/seemingly-dovish-powell-says-interest-rates-are-just-below-level-where-they-wont-stimulate-economy-2018-11-28)

[7] [www.marketwatch.com/story/seemingly-dovish-powell-says-interest-rates-are-just-below-level-where-they-wont-stimulate-economy-2018-11-28](http://www.marketwatch.com/story/seemingly-dovish-powell-says-interest-rates-are-just-below-level-where-they-wont-stimulate-economy-2018-11-28)

[8] [www.cnn.com/2018/07/10/white-house-releases-list-of-goods-hit-by-200-billion-in-tariffs.html](http://www.cnn.com/2018/07/10/white-house-releases-list-of-goods-hit-by-200-billion-in-tariffs.html)

[9] [www.businessinsider.com/us-canada-mexico-trade-deal-usmca-nafta-congress-vote-block-2018-10](http://www.businessinsider.com/us-canada-mexico-trade-deal-usmca-nafta-congress-vote-block-2018-10)

[10] [qz.com/1511247/the-us-dollars-unexpected-strength-stands-out-in-the-market-wreckage-of-2018/](http://qz.com/1511247/the-us-dollars-unexpected-strength-stands-out-in-the-market-wreckage-of-2018/)

[m.benzinga.com/article/12500556](http://m.benzinga.com/article/12500556)

[11] [www.freddiemac.com/pmms/archive.html](http://www.freddiemac.com/pmms/archive.html)

[12] [www.goodhousekeeping.com/food-recipes/easy/a24178537/beef-stroganoff-recipe/](http://www.goodhousekeeping.com/food-recipes/easy/a24178537/beef-stroganoff-recipe/)

[13] [www.irs.gov/newsroom/tax-reform-affects-if-and-how-taxpayers-itemize-their-deductions](http://www.irs.gov/newsroom/tax-reform-affects-if-and-how-taxpayers-itemize-their-deductions)

[14] [www.golfdigest.com/story/the-putting-alignment-mistake-youre-making-and-how-to-fix-it](http://www.golfdigest.com/story/the-putting-alignment-mistake-youre-making-and-how-to-fix-it)

[15] [www.webmd.com/fibromyalgia/default.htm](http://www.webmd.com/fibromyalgia/default.htm)

[16] [www.earthshare.org/market/](http://www.earthshare.org/market/)



**Jack Hillis**

**President**

Hillis Financial Services

333 W. Santa Clara Street, Suite 604

San Jose, CA 95113

408.282.7993

[john.hillis@lpl.com](mailto:john.hillis@lpl.com)

[www.hillisfinancial.com](http://www.hillisfinancial.com)

Copyright © 2018. All Rights Reserved.

The Financial Consultants of Hillis Financial Services are registered representatives with, and securities offered through LPL Financial, Member [FINRA/SIPC](#).

[Forward this email](#)



This email was sent to [kmcgraw@ci.sunnyvale.ca.us](mailto:kmcgraw@ci.sunnyvale.ca.us) by [john.hillis@lpl.com](mailto:john.hillis@lpl.com) | [Update Profile/Email Address](#) | Rapid removal with [SafeUnsubscribe™](#) | [About our service provider](#).

Hillis Financial Services | 333 W. Santa Clara Street | Suite 604 | San Jose | CA | 95113

From: [US-CERT](#)  
To: [Tanner McGinnis](#)  
Subject: SB18-351: Vulnerability Summary for the Week of December 10, 2018  
Date: Monday, December 17, 2018 12:26:07 PM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## SB18-351 Vulnerability Summary for the Week of December 10, 2018

12/17/2018 06:37 AM EST

Original release date: December 17, 2018

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka "Windows Kernel Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	2018-12-11	7.2	<a href="#">CVE-2018-8611</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8639.	2018-12-11	7.2	<a href="#">CVE-2018-8641</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2018-12-11	6.8	<a href="#">CVE-2018-17481</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Heap buffer overflow in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18335</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2018-12-11	6.8	<a href="#">CVE-2018-18336</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of stylesheets leading to a use after free in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18337</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect, thread-unsafe use of SkImage in Canvas in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18338</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect object lifecycle in WebAudio in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18339</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect object lifecycle in MediaRecorder in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18340</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	An integer overflow leading to a heap buffer overflow in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18341</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>



google -- chrome	Incorrect handing of paths leading to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18343</a> BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of alert box display in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to present confusing browser UI via a crafted HTML page.	2018-12-11	4.3	<a href="#">CVE-2018-18346</a> BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of failed navigations with invalid URLs in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to trick a user into executing javascript in an arbitrary origin via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18347</a> BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of Reflect.construct in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18359</a> BID REDHAT CONFIRM MISC DEBIAN
ibm -- marketing_platform	IBM Marketing Platform 9.1.0, 9.1.2, and 10.1 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 139029.	2018-12-07	5.5	<a href="#">CVE-2018-1424</a> CONFIRM BID XF
ibm -- marketing_platform	IBM Marketing Platform 9.1.0, 9.1.2 and 10.1 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 152855.	2018-12-07	5.5	<a href="#">CVE-2018-1920</a> CONFIRM BID XF
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8596.	2018-12-11	4.3	<a href="#">CVE-2018-8595</a> BID CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8595.	2018-12-11	4.3	<a href="#">CVE-2018-8596</a> BID CONFIRM

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8621, CVE-2018-8622.	2018-12-11	2.1	<a href="#">CVE-2018-8477</a> BID CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when Remote Procedure Call runtime improperly initializes objects in memory, aka "Remote Procedure Call runtime Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	2018-12-11	2.1	<a href="#">CVE-2018-8514</a> BID CONFIRM
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows Server 2012, Windows 7, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8477, CVE-2018-8622.	2018-12-11	2.1	<a href="#">CVE-2018-8621</a> BID CONFIRM
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8477, CVE-2018-8621.	2018-12-11	2.1	<a href="#">CVE-2018-8622</a> BID CONFIRM

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abisoft -- ticketly	AbiSoft Ticketly 1.0 is affected by multiple SQL Injection vulnerabilities through the parameters name, category_id and description in action/addproject.php; kind_id, priority_id, project_id, status_id and title in action/addticket.php; and kind_id and status_id in reports.php.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18923</a> MISC EXPLOIT-DB
abisoft -- ticketly	add_user in AbiSoft Ticketly 1.0 allows remote attackers to create administrator accounts via an action/add_user.php POST request.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18922</a> MISC
accusoft -- prizmdoc_html5_document_viewer	Accusoft PrizmDoc HTML5 Document Viewer before 13.5 contains an XML external entity (XXE) vulnerability, allowing an attacker to read arbitrary files or cause a denial of service (resource consumption).	2018-12-10	not yet calculated	<a href="#">CVE-2018-15805</a> CONFIRM MISC
apache -- ofbiz	In Apache OFBiz 16.11.01 to 16.11.04, the OFBiz HTTP engine (org.apache.ofbiz.service.engine.HttpEngine.java) handles requests for HTTP services via the /webtools/control/httpService endpoint. Both POST and GET requests to the httpService endpoint may contain three parameters: serviceName, serviceMode, and serviceContext. The exploitation occurs by having DOCTYPEs pointing to external references that trigger a payload that returns secret information from the host.	2018-12-13	not yet calculated	<a href="#">CVE-2018-8033</a> MLIST
apereo -- bedework -- bw-webdav	Apereo Bedework bw-webdav before 4.0.3 allows XXE attacks, as demonstrated by an invite-reply document that reads a local file, related to webdav/servlet/common/MethodBase.java and webdav/servlet/common/PostRequestPars.java.	2018-12-09	not yet calculated	<a href="#">CVE-2018-20000</a> MISC MISC
avanti_markets -- market_card	A vulnerability in the UPC bar code of the Avanti Markets MarketCard could allow an unauthenticated, local attacker to access funds within the customer's MarketCard balance, and also could lead to Customer Information Disclosure. The vulnerability is due to lack of proper validation of the UPC bar code present on the MarketCard. An attacker could exploit this vulnerability by generating a copy of a customer's bar code. An exploit could allow the attacker to access all funds located within the MarketCard or allow unauthenticated	2018-12-13	not yet calculated	<a href="#">CVE-2018-12076</a> MISC



	disclosure of information.			
bento4 -- bento4	An issue was discovered in EnsureCapacity in Core/Ap4Array.h in Bento4 1.5.1-627. Crafted MP4 input triggers an attempt at excessive memory allocation, as demonstrated by mp42hls.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20095</a> MISC
blackcat -- cms	Blackcat CMS 1.3.2 allows XSS via the willkommen.php?lang=DE page title at backend/pages/modify.php.	2018-12-10	not yet calculated	<a href="#">CVE-2018-16635</a> MISC
blinkforhome -- sync_module	A design flaw in the BlinkForHome (aka Blink For Home) Sync Module 2.10.4 and earlier allows attackers to disable cameras via Wi-Fi, because incident clips (triggered by the motion sensor) are not saved if the attacker's traffic (such as Dot11Deauth) successfully disconnects the Sync Module from the Wi-Fi network. (Access to live video from the app also becomes unavailable.)	2018-12-15	not yet calculated	<a href="#">CVE-2018-20161</a> MISC
cloud_foundry_foundation -- bits_service	Cloud Foundry Bits Service, versions prior to 2.18.0, includes an information disclosure vulnerability. A remote malicious user may execute a timing attack to brute-force the signing key, allowing them complete read and write access to the Bits Service storage.	2018-12-10	not yet calculated	<a href="#">CVE-2018-15800</a> CONFIRM
cloud_foundry_foundation -- uaa	Cloud Foundry UAA, all versions in v60.x, v61.x, v62.x, v63.x, and v64.x contain an authorization logic error. In environments with multiple identity providers that contain accounts across identity providers with the same username, a remote authenticated user with access to one of these accounts may be able to obtain a token for an account of the same username in the other identity provider.	2018-12-13	not yet calculated	<a href="#">CVE-2018-15754</a> CONFIRM
d-link -- dir-619l_and_dir-605l_devices	An issue was discovered in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 and DIR-605L Rev.B 2.12B1 devices. goform/formSysCmd allows remote authenticated users to execute arbitrary OS commands via the sysCmd POST parameter.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20057</a> MISC
d-link -- dir-619l_and_dir-605l_devices	An issue was discovered in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 and DIR-605L Rev.B 2.12B1 devices. There is a stack-based buffer overflow allowing remote attackers to execute arbitrary code without authentication via the goform/formLanguageChange currTime parameter.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20056</a> MISC
dedecms -- dedecms	An issue was discovered in DedeCMS V5.7 SP2. uploads/include/dialog/select_images_post.php allows remote attackers to upload and execute arbitrary PHP code via a double extension and a modified ".php" substring, in conjunction with the image/jpeg content type, as demonstrated by the filename=1.jpg.p*hp value.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20129</a> MISC
dell_emc -- idrac	Dell EMC iDRAC7/iDRAC8 versions prior to 2.61.60.60 contain an improper error handling vulnerability. An unauthenticated attacker with physical access to the system could potentially exploit this vulnerability to get access to the u-boot shell.	2018-12-13	not yet calculated	<a href="#">CVE-2018-15776</a> CONFIRM
dell_emc -- idrac	Dell EMC iDRAC7/iDRAC8 versions prior to 2.61.60.60 and iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22, and 3.23.23.23 contain a privilege escalation vulnerability. An authenticated malicious iDRAC user with operator privileges could potentially exploit a permissions check flaw in the Redfish interface to gain administrator access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-15774</a> CONFIRM
domainmod -- domainmod	DomainMOD 4.11.01 has XSS via the assets/add/category.php Category Name or Stakeholder field.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20011</a> MISC
domainmod -- domainmod	DomainMOD 4.11.01 has XSS via the assets/add/ssl-provider-account.php username field.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20010</a> MISC
domainmod -- domainmod	DomainMOD 4.11.01 has XSS via the assets/add/ssl-provider.php SSL Provider Name or SSL Provider URL field.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20009</a> MISC
doorgets -- doorgets	doorGets 7.0 allows remote attackers to write to arbitrary files via directory traversal, as demonstrated by a dg-user/?controller=theme&action=edit&name=doorgets&file=../../../../1.txt%00 URI with content in the theme_content_nofl parameter.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20064</a> MISC
eclipse -- mosquito	Eclipse Mosquito 1.5.x before 1.5.5 allows ACL bypass: if the option per_listener_settings was set to true, and the default listener was in use, and the default listener specified an acl_file, then the acl file was being ignored.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20145</a> MISC MISC MISC
edirectory -- edirectory	Cross site scripting vulnerability in eDirectory prior to 9.1 SP2	2018-12-12	not yet calculated	<a href="#">CVE-2018-17952</a> MISC
erpNext -- erpNext	A SQL injection issue was discovered in ERPNext 10.x and 11.x through 11.0.3-beta.29. This attack is only available to a logged-in user; however, many ERPNext sites allow account creation via the web. No special privileges are needed to conduct the attack. By calling a JavaScript function that calls a server-side Python function with carefully chosen arguments, a SQL attack can be carried out which allows SQL queries to be constructed to return any columns from any tables in the database. This is related to /api/resource/Item?fields= URIs, frappe.get_list, and frappe.call.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20061</a> MISC
evernote -- evernote	In Evernote before 7.6 on macOS, there is a local file path traversal issue in attachment previewing, aka MACOSNOTE-28634.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20058</a> CONFIRM
exiv2 -- exiv2	There is an infinite loop in Exiv2::Jp2Image::encodeJp2Header of jp2image.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20099</a> MISC MISC
exiv2 -- exiv2	There is a heap-based buffer over-read in the Exiv2::EXifToDataBuf function of pngimage.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20096</a> MISC MISC MISC
exiv2 -- exiv2	There is a SEGV in Exiv2::Internal::TiffParserWorker::findPrimaryGroups of tiffimage_int.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20097</a> MISC MISC
exiv2 -- exiv2	There is a heap-based buffer over-read in Exiv2::Jp2Image::encodeJp2Header of jp2image.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20098</a> MISC MISC
f5 -- big-ip	On BIG-IP 14.0.x, 13.x, 12.x, and 11.x, Enterprise Manager 3.1.1, BIG-IQ 6.x, 5.x, and 4.x, and iWorkflow 2.x, the passphrases for SNMPv3 users and trap destinations that are used for authentication and privacy are not handled by the BIG-IP system Secure Vault feature; they are written in the clear to the various configuration files.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15328</a> CONFIRM
fuel -- cms	XSS exists in FUEL CMS 1.4.3 via the Page title, Meta description, or Meta keywords during page data management, as demonstrated by the pages/edit/1/?lang=english URI.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20137</a> MISC
fuel -- cms	XSS exists in FUEL CMS 1.4.3 via the Header or Body in the Layout Variables during new-page creation, as demonstrated by the pages/edit/1/?lang=english URI.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20136</a> MISC
general_electric -- mark_vie	GE Mark VIe, EX2100e, EX2100e_Reg, and LS2100e Versions 03.03.28C to 05.02.04C, EX2100e All versions prior to v04.09.00C, EX2100e_Reg All versions prior to v04.09.00C, and LS2100e All versions prior to v04.09.00C	2018-12-14	not yet calculated	<a href="#">CVE-2018-19003</a>

	The affected versions of the application have a path traversal vulnerability that fails to restrict the ability of an attacker to gain access to restricted information.			MISC
general_electric -- proficy_cimplicity	XXE in GE Proficy Cimplicity GDS versions 9.0 R2, 9.5, 10.0	2018-12-07	not yet calculated	CVE-2018-15362 BID MISC MISC
geutebrueck_gmbh -- e2_camera_series	In Geutebrueck GmbH E2 Camera Series versions prior to 1.12.0.25 the DDNS configuration (in the Network Configuration panel) is vulnerable to an OS system command injection as root.	2018-12-14	not yet calculated	CVE-2018-19007 BID MISC
gnu -- binutils	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is an integer overflow and infinite loop caused by the IS_CONTAINED_BY_LMA macro in elf.c.	2018-12-07	not yet calculated	CVE-2018-19932 BID MISC MISC
gnu -- binutils	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is a heap-based buffer overflow in bfd_elf32_swap_phdr_in in elfcode.h because the number of program headers is not restricted.	2018-12-07	not yet calculated	CVE-2018-19931 BID MISC MISC
gnu -- binutils	The _bfd_generic_read_minisymbols function in syms.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31, has a memory leak via a crafted ELF file, leading to a denial of service (memory consumption), as demonstrated by nm.	2018-12-09	not yet calculated	CVE-2018-20002 BID MISC MISC
golang -- golang	The crypto/x509 package of Go before 1.10.6 and 1.11.x before 1.11.3 does not limit the amount of work performed for each chain verification, which might allow attackers to craft pathological inputs leading to a CPU denial of service. Go TLS servers accepting client certificates and TLS clients are affected.	2018-12-14	not yet calculated	CVE-2018-16875 CONFIRM MISC
golang -- golang	In Go before 1.10.6 and 1.11.x before 1.11.3, the "go get" command is vulnerable to directory traversal when executed with the import path of a malicious Go package which contains curly braces (both '{' and '}' characters). Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at https://golang.org/cmd/go/#hdr-Module_aware_go_get). The attacker can cause an arbitrary filesystem write, which can lead to code execution.	2018-12-14	not yet calculated	CVE-2018-16874 CONFIRM MISC
golang -- golang	In Go before 1.10.6 and 1.11.x before 1.11.3, the "go get" command is vulnerable to remote code execution when executed with the -u flag and the import path of a malicious Go package, or a package that imports it directly or indirectly. Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at https://golang.org/cmd/go/#hdr-Module_aware_go_get). Using custom domains, it's possible to arrange things so that a Git repository is cloned to a folder named ".git" by using a vanity import path that ends with "/.git". If the Git repository root contains a "HEAD" file, a "config" file, an "objects" directory, a "refs" directory, with some work to ensure the proper ordering of operations, "go get -u" can be tricked into considering the parent directory as a repository root, and running Git commands on it. That will use the "config" file in the original Git repository root for its configuration, and if that config file contains malicious commands, they will execute on the system running "go get -u".	2018-12-14	not yet calculated	CVE-2018-16873 CONFIRM MISC
google -- chrome	Failure to dismiss http auth dialogs on navigation in Network Authentication in Google Chrome on Android prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of an auto dialog via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18353 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of CSP enforcement during navigations in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18350 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2018-12-11	not yet calculated	CVE-2018-18355 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of bidirectional domain names with RTL characters in Omnibox in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2018-12-11	not yet calculated	CVE-2018-18348 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2018-12-11	not yet calculated	CVE-2018-18357 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Remote frame navigations was incorrectly permitted to local resources in Blink in Google Chrome prior to 71.0.3578.80 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.	2018-12-11	not yet calculated	CVE-2018-18349 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Lack of proper validation of ancestor frames site when sending lax cookies in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass SameSite cookie policy via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18351 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Service works could inappropriately gain access to cross origin audio in Media in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass same origin policy for audio content via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18352 BID REDHAT CONFIRM MISC DEBIAN
				CVE-2018-18345

google -- chrome	Incorrect handling of blob URLs in Site Isolation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker who had compromised the renderer process to bypass site isolation protections via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Execution of user supplied Javascript during object deserialization can update object length leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18342</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient validate of external protocols in Shell Integration in Google Chrome on Windows prior to 71.0.3578.80 allowed a remote attacker to launch external programs via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18354</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	An integer overflow in path handling lead to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18356</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Lack of special casing of localhost in WPAD files in Google Chrome prior to 71.0.3578.80 allowed an attacker on the local network segment to proxy resources on localhost via a crafted WPAD file.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18358</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Inappropriate allowance of the setDownloadBehavior devtools protocol feature in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker with control of an installed extension to access files on the local file system via a crafted Chrome Extension.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18344</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Execution of user supplied Javascript during array deserialization leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-17480</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
grafana -- grafana	Grafana before 4.6.5 and 5.x before 5.3.3 allows remote authenticated users to read arbitrary files by leveraging Editor or Admin permissions.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19039</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
haproxy -- haproxy	An issue was discovered in dns.c in HAProxy through 1.8.14. In the case of a compressed pointer, a crafted packet can trigger infinite recursion by making the pointer point to itself, or create a long chain of valid pointers resulting in stack exhaustion.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20103</a> <a href="#">MISC</a>
haproxy -- haproxy	An out-of-bounds read in dns_validate_dns_response in dns.c was discovered in HAProxy through 1.8.14. Due to a missing check when validating DNS responses, remote attackers might be able read the 16 bytes corresponding to an AAAA record from the non-initialized part of the buffer, possibly accessing anything that was left on the stack, or even past the end of the 8193-byte buffer, depending on the value of accepted_payload_size.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20102</a> <a href="#">MISC</a>
hashicorp -- consul	HashiCorp Consul 0.5.1 through 1.4.0 can use cleartext agent-to-agent RPC communication because the verify_outgoing setting is improperly documented. NOTE: the vendor has provided reconfiguration steps that do not require a software upgrade.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19653</a> <a href="#">MISC</a> <a href="#">MISC</a>
i-doit -- i-doit_open	i-doit open 1.11.2 allows Remote Code Execution because ZIP archives are mishandled. It has an upload feature that allows an authenticated user with the administrator role to upload arbitrary files to the main website directory. Exploitation involves uploading a ".php" file within a ".zip" file because a ZIP archive is accepted by /admin/?req=modules&action=add as a plugin, and extracted to the main directory. In order for the ".zip" file to be accepted, it must also contain a package.json file.	2018-12-15	not yet calculated	<a href="#">CVE-2018-20159</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 140760.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1478</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 140757.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1476</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 140969.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1484</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 does not renew a session variable after a successful authentication which could lead to session fixation/hijacking vulnerability. This could force a user to utilize a cookie that may be known to an attacker. IBM X-Force ID: 140970.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1485</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 140763.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1481</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 does not set the 'HttpOnly' attribute on authorization tokens or session cookies. If a Cross-Site Scripting vulnerability also existed attackers may be able to get the cookie values via malicious JavaScript and then hijack the user session. IBM X-Force ID: 140762.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1480</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 is vulnerable to HTTP response splitting attacks, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject arbitrary HTTP headers and cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning or cross-site scripting, and possibly obtain sensitive information. IBM X-force ID: 140692.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1474</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
	IBM Business Automation Workflow 18.0.0.0 and 18.0.0.1 is vulnerable to			

ibm -- business_automation_workflow	cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 150947.	2018-12-14	not yet calculated	<a href="#">CVE-2018-1848</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- connections	IBM Connections 5.0, 5.5, and 6.0 is vulnerable to possible host header injection attack that could cause navigation to the attacker's domain. IBM X-Force ID: 152456.	2018-12-07	not yet calculated	<a href="#">CVE-2018-1896</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- curam_social_program_management	IBM Curam Social Program Management 6.0.5, 6.1.1, 6.2.0, 7.0.1, and 7.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152529.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1900</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- curam_social_program_management	IBM Curam Social Program Management 7.0.3 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-force ID: 144951.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1671</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- curam_social_program_management	IBM Curam Social Program Management 6.0.5, 6.1.1, 6.2.0, 7.0.1, and 7.0.3 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 144747.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1654</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateways 7.5, 7.5.1, 7.5.2, 7.6, and 2018.4 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 144889.	2018-12-07	not yet calculated	<a href="#">CVE-2018-1663</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateway 7.1.0.0 through 7.1.0.19, 7.2.0.0 through 7.2.0.16, 7.5.0.0 through 7.5.1.17, 7.5.0.0 through 7.5.1.9, 7.5.2.0 through 7.5.2.9, and 7.6.0.0 through 7.6.0.2 and IBM MQ Appliance 8.0.0.0 through 8.0.0.8 and 9.0.1 through 9.0.5 could allow a local user to cause a denial of service through unknown vectors. IBM X-Force ID: 144724.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1652</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateway 7.6.0.0 through 7.6.0.10, 7.5.2.0 through 7.5.2.17, 7.5.1.0 through 7.5.1.17, 7.5.0.0 through 7.5.0.18, and 7.7.0.0 through 7.7.1.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 144893.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1667</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateway 7.6.0.0 through 7.6.0.10, 7.5.2.0 through 7.5.2.17, 7.5.1.0 through 7.5.1.17, 7.5.0.0 through 7.5.0.18, and 7.7.0.0 through 7.7.1.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 144891.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1665</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows 11.1 (includes DB2 Connect Server) contains a denial of service vulnerability. A remote, authenticated DB2 user could exploit this vulnerability by issuing a specially-crafted SELECT statement with TRUNCATE function. IBM X-Force ID: 154032.	2018-12-14	not yet calculated	<a href="#">CVE-2018-1977</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- mq_console_rest_api	A problem within the IBM MQ 9.0.2, 9.0.3, 9.0.4, 9.0.5, and 9.1.0.0 Console REST API Could allow attackers to execute a denial of service attack preventing users from logging into the MQ Console REST API. IBM X-Force ID: 151969.	2018-12-07	not yet calculated	<a href="#">CVE-2018-1883</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- operational_decision_management	IBM Operational Decision Management 8.5, 8.6, 8.7, 8.8, and 8.9 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 150170.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1821</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 148419.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1740</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 150017.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1813</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 144726.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1653</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 150018.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1814</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 for Enterprise Single-Sign On is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 150019.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1815</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 does not set the secure attribute on authorization tokens or session cookies. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 149703.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1804</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 152021.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1886</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 152078.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1887</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 generates an error message that includes sensitive information about its environment, users, or associated data. IBM X-Force ID: 149704.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1805</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 149702.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1803</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_guardium	IBM Security Guardium 10 and 10.5 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption	2018-12-13	not yet calculated	<a href="#">CVE-2018-1818</a> <a href="#">XF</a>

	of internal data. IBM X-Force ID: 150022.			<a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10 and 10.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 150021.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1817</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10 and 10.5 uses a one-way cryptographic hash against an input that should not be reversible, such as a password, but the software does not also use a salt as part of the input. IBM X-Force ID: 124743.	2018-12-13	not yet calculated	<a href="#">CVE-2017-1268</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console is vulnerable to cross-site request forgery, caused by improper validation of user-supplied input. By persuading a user to visit a malicious URL, a remote attacker could send a specially-crafted request. An attacker could exploit this vulnerability to perform CSRF attack and update available applications. IBM X-Force ID: 152992.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1926</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 9 could allow sensitive information to be available caused by mishandling of data by the application based on an incorrect return by the <code>HttpServletRequest.authenticate()</code> API when an unprotected URI is accessed. IBM X-Force ID: 153629.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1957</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to temporarily gain elevated privileges on the system, caused by incorrect cached value being used. IBM X-Force ID: 152530.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1901</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow remote attackers to execute arbitrary Java code through an administrative client class with a serialized object from untrusted sources. IBM X-Force ID: 152533.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1904</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
imanager -- imanager	Cross site scripting vulnerability in iManager prior to 3.1 SP2.	2018-12-12	not yet calculated	<a href="#">CVE-2018-17949</a> <a href="#">MISC</a>
intel -- parallel_studio	Improper directory permissions in the installer for the Intel Parallel Studio before 2019 Gold may allow authenticated users to potentially enable an escalation of privilege via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-3704</a> <a href="#">CONFIRM</a>
intel -- quickassist_technology_for_linux	Improper memory handling in Intel QuickAssist Technology for Linux (all versions) may allow an authenticated user to potentially enable a denial of service via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18096</a> <a href="#">CONFIRM</a>
intel -- quickassist_technology_for_linux	Improper configuration of hardware access in Intel QuickAssist Technology for Linux (all versions) may allow an authenticated user to potentially enable a denial of service via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-12206</a> <a href="#">CONFIRM</a>
intel -- solid_state_drive_toolbox	Improper directory permissions in Intel Solid State Drive Toolbox before 3.5.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18097</a> <a href="#">CONFIRM</a>
intel -- system_defense_utility	Improper directory permissions in the installer for the Intel System Defense Utility (all versions) may allow authenticated users to potentially enable an escalation of privilege via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-3705</a> <a href="#">CONFIRM</a>
intel -- vtune_amplifier	Improper file permissions in the installer for Intel VTune Amplifier 2018 Update 3 and before may allow unprivileged user to potentially gain privileged access via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18093</a> <a href="#">CONFIRM</a>
intel -- x86_platforms	An issue was discovered in Xen through 4.11.x on Intel x86 platforms allowing guest OS users to cause a denial of service (host OS hang) because Xen does not work around Intel's mishandling of certain HLE transactions associated with the KACQUIRE instruction prefix.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19967</a> <a href="#">BID</a> <a href="#">MISC</a>
jenkins -- jenkins	A data modification vulnerability exists in Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in User.java, <code>IdStrategy.java</code> that allows attackers to submit crafted user names that can cause an improper migration of user record storage formats, potentially preventing the victim from logging into Jenkins.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000863</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Pipeline: Groovy Plugin 2.59 and earlier in <code>groovy-sandbox/src/main/java/org/kohsuke/groovy/sandbox/SandboxTransformer.java</code> , <code>groovy-cps/lib/src/main/java/com/cloudbees/groovy/cps/SandboxCpsTransformer.java</code> that allows attackers with <code>Job/Configure</code> permission, or unauthorized attackers with <code>SCM commit</code> privileges and corresponding pipelines based on Jenkinsfiles set up in Jenkins, to execute arbitrary code on the Jenkins master JVM	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000866</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A denial of service vulnerability exists in Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in <code>CronTab.java</code> that allows attackers with <code>Overall/Read</code> permission to have a request handling thread enter an infinite loop.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000864</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Script Security Plugin 1.47 and earlier in <code>groovy-sandbox/src/main/java/org/kohsuke/groovy/sandbox/SandboxTransformer.java</code> that allows attackers with <code>Job/Configure</code> permission to execute arbitrary code on the Jenkins master JVM, if plugins using the Groovy sandbox are installed.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000865</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A code execution vulnerability exists in the Stapler web framework used by Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in <code>stapler/core/src/main/java/org/kohsuke/stapler/MetaClass.java</code> that allows attackers to invoke some methods on Java objects by accessing crafted URLs that were not intended to be invoked this way.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000861</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in <code>DirectoryBrowserSupport.java</code> that allows attackers with the ability to control build output to browse the file system on agents running builds beyond the duration of the build using the workspace browser.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000862</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
jooan -- ja-q1h_wi-fi_camera	Mishandling of an empty string on the Jooan JA-Q1H Wi-Fi camera with firmware 21.0.0.91 allows remote attackers to cause a denial of service (crash and reboot) via the <code>ONVIF GetStreamUri</code> method and <code>GetVideoEncoderConfigurationOptions</code> method.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20050</a> <a href="#">MISC</a>
jooan -- ja-q1h_wi-fi_camera	Mishandling of <code>&gt;'&gt;</code> on the Jooan JA-Q1H Wi-Fi camera with firmware 21.0.0.91 allows remote attackers to cause a denial of service (crash and reboot) via certain <code>ONVIF</code> methods such as <code>CreateUsers</code> , <code>SetImagingSettings</code> , <code>GetStreamUri</code> , and so on.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20051</a> <a href="#">MISC</a>
katello -- katello	A SQL injection flaw was found in katello's errata-related API. An authenticated remote attacker can craft input data to force a malformed SQL query to the backend database, which will leak internal IDs. This issue is related to an incomplete fix for CVE-2016-3072. Version 3.10 and older is vulnerable.	2018-12-13	not yet calculated	<a href="#">CVE-2018-14623</a> <a href="#">CONFIRM</a>
kt -- mc01507l_z-wave_s0_devices	An issue was discovered on KT MC01507L Z-Wave S0 devices. It occurs because HPKP is not implemented. The communication architecture is APP > Server > Controller (HUB) > Node (products which are controlled by HUB). The prerequisite is that the attacker is on the same network as the target HUB, and can use IP Changer to change destination IP addresses (of all packets whose destination IP address is Server) to a proxy-server IP address. This allows sniffing of cleartext between Server and Controller. The cleartext command data is transmitted to Controller using the proxy server's fake certificate, and it is able to control each Node of the HUB. Also, by operating HUB in Z-Wave Pairing Mode, it is possible to obtain the Z-Wave network key.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19982</a> <a href="#">MISC</a>



libav -- libav	In Libav 12.3, there is a floating point exception in the range_decode_culshift function (called from range_decode_bits) in libavcodec/apedec.c that will lead to remote denial of service via crafted input.	2018-12-09	not yet calculated	<a href="#">CVE-2018-20001</a> MISC
linux -- kernel	The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFDIO_ ioctl calls, as demonstrated by allowing local users to write data into holes in a tmpfs file (if the user has read-only access to that file, and that file contains holes), related to fs/userfaultfd.c and mm/userfaultfd.c.	2018-12-12	not yet calculated	<a href="#">CVE-2018-18397</a> MISC MISC MISC MISC
mcafee -- agent	Privilege escalation vulnerability in McAfee Agent (MA) for Linux 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to perform arbitrary command execution via specific conditions.	2018-12-12	not yet calculated	<a href="#">CVE-2018-6705</a> CONFIRM
mcafee -- agent	Insecure handling of temporary files in non-Windows McAfee Agent 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows an Unprivileged User to introduce custom paths during agent installation in Linux via unspecified vectors.	2018-12-12	not yet calculated	<a href="#">CVE-2018-6706</a> CONFIRM
mcafee -- agent	Denial of Service through Resource Depletion vulnerability in the agent in non-Windows McAfee Agent (MA) 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to cause DoS, unexpected behavior, or potentially unauthorized code execution via knowledge of the internal trust mechanism.	2018-12-13	not yet calculated	<a href="#">CVE-2018-6707</a> CONFIRM
mcafee -- agent	Privilege escalation vulnerability in McAfee Agent (MA) for Linux 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to perform arbitrary command execution via specific conditions.	2018-12-12	not yet calculated	<a href="#">CVE-2018-6704</a> CONFIRM
mcafee -- agent	Use After Free in McAfee Common service in McAfee Agent (MA) 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted TCP packet.	2018-12-11	not yet calculated	<a href="#">CVE-2018-6703</a> CONFIRM
medtronic -- carelink_and_ensure_programmers	Medtronic CareLink 2090 Programmer CareLink 9790 Programmer 29901 Encore Programmer, all versions, The affected products do not encrypt or do not sufficiently encrypt the following sensitive information while at rest PII and PHI.	2018-12-14	not yet calculated	<a href="#">CVE-2018-18984</a> MISC
micro_focus -- fortify_software_security_center	A potential Remote Unauthorized Access in Micro Focus Fortify Software Security Center (SSC), versions 17.10, 17.20, 18.10 this exploitation could allow Remote Unauthorized Access	2018-12-13	not yet calculated	<a href="#">CVE-2018-7691</a> MISC EXPLOIT-DB
micro_focus -- fortify_software_security_center	A potential Remote Unauthorized Access in Micro Focus Fortify Software Security Center (SSC), versions 17.10, 17.20, 18.10 this exploitation could allow Remote Unauthorized Access	2018-12-13	not yet calculated	<a href="#">CVE-2018-7690</a> MISC EXPLOIT-DB
microsoft -- .net_framework	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka ".NET Framework Remote Code Injection Vulnerability." This affects Microsoft .NET Framework 4.6, Microsoft .NET Framework 3.5, Microsoft .NET Framework 4.7.4.7.1/4.7.2, Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7.1/4.7.1/4.7.2, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET Framework 4.7.1/4.7.2, Microsoft .NET Framework 4.7.2, Microsoft .NET Framework 4.6.2.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8540</a> BID CONFIRM
microsoft -- .net_framework	A denial of service vulnerability exists when .NET Framework improperly handles special web requests, aka ".NET Framework Denial Of Service Vulnerability." This affects Microsoft .NET Framework 4.6, Microsoft .NET Framework 3.5, Microsoft .NET Framework 4.7.4.7.1/4.7.2, Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7.1/4.7.1/4.7.2, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET Framework 4.7.1/4.7.2, Microsoft .NET Framework 4.7.2.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8517</a> BID CONFIRM
microsoft -- dynamics_nav	A cross site scripting vulnerability exists when Microsoft Dynamics NAV does not properly sanitize a specially crafted web request to an affected Dynamics NAV server, aka "Microsoft Dynamics NAV Cross Site Scripting Vulnerability." This affects Microsoft Dynamics NAV.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8651</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8624</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8618</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8617, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8583</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8629</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8617</a> BID CONFIRM
microsoft -- exchange_server	A tampering vulnerability exists when Microsoft Exchange Server fails to properly handle profile data, aka "Microsoft Exchange Server Tampering Vulnerability." This affects Microsoft Exchange Server.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8604</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka "Scripting Engine Memory Corruption Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8643</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka "Windows VBScript Engine Remote Code Execution Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8625</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists when the Internet Explorer VBScript execution policy does not properly restrict VBScript under specific conditions, aka "Internet Explorer Remote Code Execution Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8619</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka "Internet Explorer Memory Corruption Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8631</a> BID CONFIRM
	A remote code execution vulnerability exists in Microsoft Outlook software			<a href="#">CVE-2018-</a>

microsoft -- multiple_products	when it fails to properly handle objects in memory, aka "Microsoft Outlook Remote Code Execution Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Outlook.	2018-12-11	not yet calculated	<a href="#">8587 BID CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka "Microsoft Excel Remote Code Execution Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Excel. This CVE ID is unique from CVE-2018-8597.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8636 BID CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly handle objects in memory, aka "Microsoft PowerPoint Remote Code Execution Vulnerability." This affects Microsoft Office, Office 365 ProPlus, Microsoft PowerPoint, Microsoft SharePoint, Microsoft PowerPoint Viewer, Office Online Server, Microsoft SharePoint Server.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8628 BID CONFIRM</a>
microsoft -- multiple_products	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values, aka "Connected User Experiences and Telemetry Service Denial of Service Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8612 BID CONFIRM</a>
microsoft -- multiple_products	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka "Microsoft Excel Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Excel. This CVE ID is unique from CVE-2018-8627.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8598 BID CONFIRM</a>
microsoft -- multiple_products	An information disclosure vulnerability exists when Microsoft Excel software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka "Microsoft Excel Information Disclosure Vulnerability." This affects Microsoft Office, Office 365 ProPlus, Microsoft Excel, Microsoft Excel Viewer, Excel. This CVE ID is unique from CVE-2018-8598.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8627 BID CONFIRM</a>
microsoft -- multiple_products	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka "Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability." This affects Microsoft Visual Studio, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8599 BID CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka "Microsoft Excel Remote Code Execution Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Excel. This CVE ID is unique from CVE-2018-8636.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8597 BID CONFIRM</a>
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint.	2018-12-12	not yet calculated	<a href="#">CVE-2018-8650 BID CONFIRM</a>
microsoft -- sharepoint	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted authentication request to an affected SharePoint server, aka "Microsoft SharePoint Server Elevation of Privilege Vulnerability." This affects Microsoft SharePoint Server, Microsoft SharePoint.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8635 BID CONFIRM</a>
microsoft -- sharepoint	An information disclosure vulnerability exists where certain modes of the search function in Microsoft SharePoint Server are vulnerable to cross-site search attacks (a variant of cross-site request forgery, CSRF), aka "Microsoft SharePoint Information Disclosure Vulnerability." This affects Microsoft SharePoint.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8580 BID CONFIRM</a>
microsoft -- windows	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka "Windows Denial of Service Vulnerability." This affects Windows 10, Windows Server 2019.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8649 BID CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists in Windows where Microsoft text-to-speech fails to properly handle objects in the memory, aka "Microsoft Text-To-Speech Remote Code Execution Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8634 BID CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka "DirectX Information Disclosure Vulnerability." This affects Windows 10, Windows Server 2019.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8638 BID CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8641.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8639 BID CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists in Windows Domain Name System (DNS) servers when they fail to properly handle requests, aka "Windows DNS Server Heap Overflow Vulnerability." This affects Windows Server 2012 R2, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8626 BID CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists in Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass, aka "Win32k Information Disclosure Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8637 BID CONFIRM</a>
microsoft -- windows_azure_pack	A Cross-site Scripting (XSS) vulnerability exists when Windows Azure Pack does not properly sanitize user-provided input, aka "Windows Azure Pack Cross Site Scripting Vulnerability." This affects Windows Azure Pack Rollup 13.1.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8652 BID CONFIRM</a>
mini-xml -- mini-xml	An issue has been found in Mini-XML (aka mxml) 2.12. It is a use-after-free in mxmlWalkNext in mxml-search.c, as demonstrated by mxmldoc.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20005 MISC</a>
mini-xml -- mini-xml	An issue has been found in Mini-XML (aka mxml) 2.12. It is a stack-based buffer overflow in mxml_write_node in mxml-file.c via vectors involving a double-precision floating point number and the '<order type="real">' substring, as demonstrated by testxml.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20004 MISC</a>
netiq -- edirectory	Incorrect enforcement of authorization checks in eDirectory prior to 9.1 SP2	2018-12-12	not yet calculated	<a href="#">CVE-2018-17950 MISC</a>
nomachine -- nomachine	The nxfs.sys driver in the DokanFS library 0.6.0 in NoMachine before 6.4.6 on Windows 10 allows local users to cause a denial of service (BSOD) because uninitialized memory can be read.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20029 MISC</a>
nonecms -- nonecms	An issue was discovered in NoneCms V1.3. thinkphp/library/think/App.php allows remote attackers to execute arbitrary PHP code via crafted use of the filter parameter, as demonstrated by the s=index/thinkRequest/input&filter=phpinfo&data=1 query string.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20062 MISC</a>
nucleus -- cms	Nucleus CMS 3.70 allows HTML Injection via the index.php body parameter.	2018-12-10	not yet calculated	<a href="#">CVE-2018-16636 CONFIRM MISC</a>
	Open Dental before version 18.4 transmits the entire user database over the			<a href="#">CVE-2018-</a>

open_dental -- open_dental	network when a remote unauthenticated user accesses the command prompt. This allows the attacker to gain access to usernames, password hashes, privilege levels, and more.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15718</a> <a href="#">MISC</a>
open_dental -- open_dental	Open Dental before version 18.4 stores user passwords as base64 encoded MD5 hashes.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15717</a> <a href="#">MISC</a>
open_dental -- open_dental	Open Dental before version 18.4 installs a mysql database and uses the default credentials of "root" with a blank password. This allows anyone on the network with access to the server to access all database information.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15719</a> <a href="#">MISC</a>
openrefine -- openrefine	The data import functionality in OpenRefine through 3.1 allows an XML External Entity (XXE) attack through a crafted (zip) file, allowing attackers to read arbitrary files.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20157</a> <a href="#">MISC</a>
oracle -- secure_global_desktop	XSS exists in the Administration Console in Oracle Secure Global Desktop 4.4 20080807152602 (but was fixed in later versions including 5.4). helpwindow.jsp has reflected XSS via all parameters, as demonstrated by the sgadmin/faces/com_sun_web_ui/help/helpwindow.jsp windowTitle parameter.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19439</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">BID</a>
palo_alto_networks -- expedition_migration_tool	The Palo Alto Networks Expedition Migration tool 1.0.107 and earlier may allow an unauthenticated attacker with remote access to run system level commands on the device hosting this service/application.	2018-12-11	not yet calculated	<a href="#">CVE-2018-10143</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
perl -- perl	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	2018-12-07	not yet calculated	<a href="#">CVE-2018-18311</a> <a href="#">BID</a> <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
perl -- perl	Perl before 5.26.3 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	2018-12-07	not yet calculated	<a href="#">CVE-2018-18314</a> <a href="#">BID</a> <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
php -- php	ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19935</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
phpcmf -- phpcmf	PHPCMF 4.1.3 has XSS via the first input field to the index.php?s=member&c=register&m=index URI.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20012</a> <a href="#">MISC</a> <a href="#">MISC</a>
phpmyadmin -- phpmyadmin	phpMyAdmin 4.7.x and 4.8.x versions prior to 4.8.4 are affected by a series of CSRF flaws. By deceiving a user into clicking on a crafted URL, it is possible to perform harmful SQL operations such as renaming databases, creating new tables/routines, deleting designer pages, adding/deleting users, updating user passwords, killing SQL processes, etc.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19969</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
phpmyadmin -- phpmyadmin	In phpMyAdmin before 4.8.4, an XSS vulnerability was found in the navigation tree, where an attacker can deliver a payload to a user through a crafted database/table name.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19970</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
phpmyadmin -- phpmyadmin	An attacker can exploit phpMyAdmin before 4.8.4 to leak the contents of a local file because of an error in the transformation feature. The attacker must have access to the phpMyAdmin Configuration Storage tables, although these can easily be created in any database to which the attacker has access. An attacker must have valid credentials to log in to phpMyAdmin; this vulnerability does not allow an attacker to circumvent the login system.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19968</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
phpok -- phpok	An issue was discovered in PHPok v5.0.055. There is a Stored XSS vulnerability via the title parameter to api.php?c=post&f=save (reachable via the index.php?id=book URI).	2018-12-10	not yet calculated	<a href="#">CVE-2018-20006</a> <a href="#">MISC</a>
phpscriptsmail.com -- entrepreneur_b2b_script	PHP Scripts Mail Entrepreneur B2B Script 3.0.6 allows Stored XSS via Account Settings fields such as FirstName and LastName, a similar issue to CVE-2018-14541.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20138</a> <a href="#">MISC</a>
pippo -- pippo	jaxb/JaxbEngine.java in Pippo 1.11.0 allows XXE.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20059</a> <a href="#">CONFIRM</a>
pivotal -- rabbitmq_for_pcf	Pivotal RabbitMQ for PCF, all versions, uses a deterministically generated cookie that is shared between all machines when configured in a multi-tenant cluster. A remote attacker who can gain information about the network topology can guess this cookie and, if they have access to the right ports on any server in the MQ cluster can use this cookie to gain full control over the entire cluster.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1279</a> <a href="#">CONFIRM</a>
pixar -- tractor	Pixar's Tractor software, versions 2.2 and earlier, contain a stored cross-site scripting vulnerability in the field that allows a user to add a note to an existing node. The stored information is displayed when a user requests information about the node. An attacker could insert Javascript into this note field that is then saved and displayed to the end user. An attacker might include Javascript that could execute on an authenticated user's system that could lead to website redirects, session cookie hijacking, social engineering, etc. As this is stored with the information about the node, all other authenticated users with access to this data are also vulnerable.	2018-12-13	not yet calculated	<a href="#">CVE-2018-5411</a> <a href="#">BID</a> <a href="#">CERT-VN</a>
qemu -- qemu	A flaw was found in qemu Media Transfer Protocol (MTP) before version 3.1.0. A path traversal in the in usb_mtp_write_data function in hw/usb/dev-mtp.c due to an improper filename sanitization. When the guest device is mounted in read-write mode, this allows to read/write arbitrary files which may lead to DoS scenario OR possibly lead to code execution on the host.	2018-12-12	not yet calculated	<a href="#">CVE-2018-16867</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
qemu -- qemu	A flaw was found in qemu Media Transfer Protocol (MTP). The code opening files in usb_mtp_get_object and usb_mtp_get_partial_object and directories in usb_mtp_object_readaddr doesn't consider that the underlying filesystem may have changed since the time lstat(2) was called in usb_mtp_object_alloc, a classical TOCTTOU problem. An attacker with write access to the host filesystem shared with a guest can use this property to navigate the host filesystem in the context of the QEMU process and read any file the QEMU process has access to. Access to the filesystem may be local or via a network share protocol such as CIFS.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16872</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2018-</a>

qemu -- qemu	hw/9pfs/cofile.c and hw/9pfs/9p.c in QEMU can modify an fid path while it is being accessed by a second thread, leading to (for example) a use-after-free outcome.	2018-12-13	not yet calculated	<a href="#">19364 MLIST</a> <a href="#">MLIST</a> <a href="#">UBUNTU</a>
qemu -- qemu	v9fs_wstat in hw/9pfs/9p.c in QEMU allows guest OS users to cause a denial of service (crash) because of a race condition during file renaming.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19489 MLIST</a> <a href="#">XCONFIRM</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
qualcomm -- snapdragon	While generating trusted application id, An integer overflow can occur giving the trusted application an invalid identity in Snapdragon Mobile and Snapdragon Wear in versions MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 835 and SDA660.	2018-12-10	not yet calculated	<a href="#">CVE-2016-10502 BID</a> <a href="#">CONFIRM</a>
ricoh -- myprint	Hardcoded credentials in the Ricoh myPrint application 2.9.2.4 for Windows and 2.2.7 for Android give access to any externally disclosed myPrint WSDL API, as demonstrated by discovering API secrets of related Google cloud printers, encrypted passwords of mail servers, and names of printed files.	2018-12-14	not yet calculated	<a href="#">CVE-2018-18006 MISC</a> <a href="#">FULLDISC</a>
s-cms -- s-cms	S-CMS V3.0 has SQL injection via the S_id parameter, as demonstrated by the /1/?type=productinfo&S_id=140 URI.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20018 MISC</a>
sap -- business_one_service_layer	TRACE method is enabled in SAP Business One Service Layer . Attacker can use XST (Cross Site Tracing) attack if frontend applications that are using Service Layer has a XSS vulnerability. This has been fixed in SAP Business One Service Layer (B1_ON_HANA, versions 9.2, 9.3).	2018-12-11	not yet calculated	<a href="#">CVE-2018-2502 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- commerce	SAP Commerce does not sufficiently validate user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability in storefronts that are based on the product. Fixed in versions (SAP Hybris Commerce, versions 6.2, 6.3, 6.4, 6.5, 6.6, 6.7).	2018-12-11	not yet calculated	<a href="#">CVE-2018-2505 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- hana	The security audit log of SAP HANA, versions 1.0 and 2.0, does not log SELECT events if these events are part of a statement with the syntax CREATE TABLE <table_name> AS SELECT.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2497 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- marketing	SAP Marketing (UICUAN (1.20, 1.30, 1.40), SAPSCORE (1.13, 1.14)) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2486 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- mobile_secure_android_client	Under certain conditions SAP Mobile Secure Android client (before version 6.60.19942.0 SP28 1711) allows an attacker to access information which would otherwise be restricted.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2500 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver AS Java Web Container service does not validate against whitelist the HTTP host header which can result in HTTP Host Header Manipulation or Cross-Site Scripting (XSS) vulnerability. This is fixed in versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2504 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver	By default, the SAP NetWeaver AS Java keystore service does not sufficiently restrict the access to resources that should be protected. This has been fixed in SAP NetWeaver AS Java (ServerCore versions 7.11, 7.20, 7.30, 7.31, 7.40, 7.50).	2018-12-11	not yet calculated	<a href="#">CVE-2018-2503 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver	Necessary authorization checks for an authenticated user, resulting in escalation of privileges, have been fixed in SAP Basis AS ABAP of SAP NetWeaver 700 to 750, from 750 onwards delivered as ABAP Platform.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2494 MISC</a> <a href="#">MISC</a>
sap -- netweaver	SAML 2.0 functionality in SAP NetWeaver AS Java, does not sufficiently validate XML documents received from an untrusted source. This is fixed in versions 7.2, 7.30, 7.31, 7.40 and 7.50.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2492 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
semcms -- semcms	SEMCMS 3.5 has XSS via the first text box to the SEMCMS_Main.php URI.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20017 MISC</a>
siemens -- simatic	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels 4" - 22" (All versions < V15 Update 4), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions < V15 Update 4), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V15 Update 4), SIMATIC WinCC Runtime Advanced (All versions < V15 Update 4), SIMATIC WinCC Runtime Professional (All versions < V15 Update 4), SIMATIC WinCC (TIA Portal) (All versions < V15 Update 4), SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel) (All versions). The webserver of affected HMI devices may allow URL redirections to untrusted websites. An attacker must trick a valid user who is authenticated to the device into clicking on a malicious link to exploit the vulnerability. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13813 BID</a> <a href="#">CONFIRM</a>
siemens -- simatic	A vulnerability has been identified in SIMATIC S7-1200 (All versions), SIMATIC S7-1500 (All Versions < V2.6). An attacker could exhaust the available connection pool of an affected device by opening a sufficient number of connections to the device. Successful exploitation requires an attacker to be able to send packets to port 102/tcp of the affected device. No user interaction and no user privileges are required to exploit the vulnerability. The vulnerability, if exploited, could cause a Denial-of-Service condition impacting the availability of the system. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13815 BID</a> <a href="#">CONFIRM</a>
siemens -- simatic	A vulnerability has been identified in SIMATIC HMI Comfort Panels 4" - 22" (All versions < V15 Update 4), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions < V15 Update 4), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V15 Update 4), SIMATIC WinCC Runtime Advanced (All versions < V15 Update 4), SIMATIC WinCC Runtime Professional (All versions < V15 Update 4), SIMATIC WinCC (TIA Portal) (All versions < V15 Update 4), SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel) (All versions). A directory traversal vulnerability could allow to download arbitrary files from the device. The security vulnerability could be exploited by an attacker with network access to the integrated web server. No user interaction and no authentication is required to exploit the vulnerability. The vulnerability impacts the confidentiality of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13812 BID</a> <a href="#">CONFIRM</a>
	A vulnerability has been identified in SIMATIC HMI Comfort Panels 4" - 22" (All versions < V14), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions < V14), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F,			

siemens -- simatic	KTP900 and KTP900F (All versions < V14), SIMATIC WinCC Runtime Advanced (All versions < V14), SIMATIC WinCC Runtime Professional (All versions < V14), SIMATIC WinCC (TIA Portal) (All versions < V14), SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel) (All versions). The integrated web server (port 80/tcp and port 443/tcp) of the affected devices could allow an attacker to inject HTTP headers. An attacker must trick a valid user who is authenticated to the device into clicking on a malicious link to exploit the vulnerability. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13814</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- simatic_it	A vulnerability has been identified in SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (Versions V7.1 < V7.1 Upd3), SIMATIC IT UA Discrete Manufacturing (Versions < V1.2), SIMATIC IT UA Discrete Manufacturing (Versions V1.2), SIMATIC IT UA Discrete Manufacturing (Versions V1.3), SIMATIC IT UA Discrete Manufacturing (Versions V2.3), SIMATIC IT UA Discrete Manufacturing (Versions V2.4). An attacker with network access to the installation could bypass the application-level authentication. In order to exploit the vulnerability, an attacker must obtain network access to an affected installation and must obtain a valid username to the system. Successful exploitation requires no user privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13804</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- simatic_s7-400_products	A vulnerability has been identified in SIMATIC S7-400 (incl. F) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-400H V4.5 and below (All versions), SIMATIC S7-400H V6 (All versions), SIMATIC S7-410 (All versions < V8.2.1). Sending of specially crafted packets to port 102/tcp via Ethernet interface via PROFIBUS or Multi Point Interfaces (MPI) could cause a Denial-of-Service condition on affected devices. Flashing with a firmware image may be required to recover the CPU. Successful exploitation requires an attacker to have network access to port 102/tcp via Ethernet interface or to be able to send messages via PROFIBUS or Multi Point Interfaces (MPI) to the device. No user interaction is required. If no access protection is configured, no privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the core functionality of the CPU, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16557</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
siemens -- simatic_s7-400_products	A vulnerability has been identified in SIMATIC S7-400 (incl. F) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-400H V4.5 and below (All versions), SIMATIC S7-400H V6 (All versions), SIMATIC S7-410 (All versions < V8.2.1). Specially crafted packets sent to port 102/tcp via Ethernet interface, via PROFIBUS, or via Multi Point Interfaces (MPI) could cause the affected devices to go into defect mode. Manual reboot is required to resume normal operation. Successful exploitation requires an attacker to be able to send specially crafted packets to port 102/tcp via Ethernet interface, via PROFIBUS or Multi Point Interfaces (MPI). No user interaction and no user privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the core functionality of the CPU, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16558</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
siemens -- simatic_step_7_tia_portal	A vulnerability has been identified in SIMATIC STEP 7 (TIA Portal) (All Versions < V15.1). Password hashes with insufficient computational effort could allow an attacker to access to a project file and reconstruct passwords. The vulnerability could be exploited by an attacker with local access to the project file. No user interaction is required to exploit the vulnerability. The vulnerability could allow the attacker to obtain certain passwords from the project. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13811</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). The integrated VNC server on port 5900/tcp of the affected products could allow a remote attacker to cause a Denial-of-Service condition of the VNC server. Please note that this vulnerability is only exploitable if port 5900/tcp is manually opened in the firewall configuration of network port X130. The security vulnerability could be exploited by an attacker with network access to the affected devices and port. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise availability of the VNC server. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11464</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). Specially crafted network packets sent to port 102/tcp (ISO-TSAP) could allow a remote attacker to either cause a Denial-of-Service condition of the integrated software firewall or allow to execute code in the context of the software firewall. The security vulnerability could be exploited by an attacker with network access to the affected systems on port 102/tcp. Successful exploitation requires no user privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11466</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker could use ioctl calls to do out of bounds reads, arbitrary writes, or execute code in kernel mode. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11465</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A buffer overflow in the service command application could allow a local attacker to execute code with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11463</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). By sending a specially crafted authentication request to the affected systems a remote attacker could escalate his privileges to an elevated user account but not to root. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no privileges and no user	2018-12-12	not yet calculated	<a href="#">CVE-2018-11462</a> <a href="#">BID</a> <a href="#">CONFIRM</a>



	interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). The integrated VNC server on port 5900/tcp of the affected products could allow a remote attacker to execute code with privileged permissions on the system by sending specially crafted network requests to port 5900/tcp. Please note that this vulnerability is only exploitable if port 5900/tcp is manually opened in the firewall configuration of network port X130. The security vulnerability could be exploited by an attacker with network access to the affected devices and port. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the VNC server. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11458</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). The integrated web server on port 4842/tcp of the affected products could allow a remote attacker to execute code with privileged permissions on the system by sending specially crafted network requests to port 4842/tcp. Please note that this vulnerability is only exploitable if port 4842/tcp is manually opened in the firewall configuration of network port X130. The security vulnerability could be exploited by an attacker with network access to the affected devices on port 4842/tcp. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the web server. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11457</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker with user privileges could use the service command application for privilege escalation to an elevated user but not root. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11461</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker could modify a user-writable configuration file so that after reboot or manual initiation the system reloads the modified configuration file and attacker-controlled code is executed with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected system. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11459</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker with elevated user privileges (manufact) could modify a Cramfs archive so that after reboot the system loads the modified Cramfs file and attacker-controlled code is executed with root privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires elevated user privileges (manufact) but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11460</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- tim_1531_irc	A vulnerability has been identified in TIM 1531 IRC (All version < V2.0). The devices was missing proper authentication on port 102/tcp, although configured. Successful exploitation requires an attacker to be able to send packets to port 102/tcp of the affected device. No user interaction and no user privileges are required to exploit the vulnerability. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-13816</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- scalance	A vulnerability has been identified in SCALANCE S602 (All versions < V4.0.1.1), SCALANCE S612 (All versions < V4.0.1.1), SCALANCE S623 (All versions < V4.0.1.1), SCALANCE S627-2M (All versions < V4.0.1.1). The integrated web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. The user must be logged into the web interface in order for the exploitation to succeed. At the stage of publishing this security advisory no public exploitation is known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16555</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
sigma_design -- z-wave_devices	An issue was discovered on Sigma Design Z-Wave S0 through S2 devices. An attacker first prepares a Z-Wave frame-transmission program (e.g., Z-Wave PC Controller, OpenZWave, CC1110, etc.). Next, the attacker conducts a DoS attack against the Z-Wave S0 Security version product by continuously sending divided "Nonce Get (0x98 0x81)" frames. The reason for dividing the "Nonce Get" frame is that, in security version S0, when a node receives a "Nonce Get" frame, the node produces a random new nonce and sends it to the Src node of the received "Nonce Get" frame. After the nonce value is generated and transmitted, the node transitions to wait mode. At this time, when "Nonce Get" is received again, the node discards the previous nonce value and generates a random nonce again. Therefore, because the frame is encrypted with previous nonce value, the received normal frame cannot be decrypted.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19983</a> <a href="#">MISC</a>
signal -- messenger_for_android	Signal Messenger for Android 4.24.8 may expose private information when using "disappearing messages." If a user uses the photo feature available in the "attach file" menu, then Signal will leave the picture in its own cache directory, which is available to any application on the system.	2018-12-10	not yet calculated	<a href="#">CVE-2018-3988</a> <a href="#">BID</a> <a href="#">MISC</a>
sonarsource -- sonarqube	A vulnerability in the API of SonarSource SonarQube before 7.4 could allow an authenticated user to discover sensitive information such as valid user-account logins in the web application. The vulnerability occurs because of improperly configured access controls that cause the API to return the external identity field to non-administrator users. The attacker could use this information in subsequent attacks against the system.	2018-12-14	not yet calculated	<a href="#">CVE-2018-19413</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- managed_file_transfer_command_center_and_tibco_managed_file_transfer_internet_server	The Administrator Service component of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center, and TIBCO Managed File Transfer Internet Server contains vulnerabilities where an authenticated user with specific privileges can gain access to credentials to other systems. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions up to and including 7.3.2; 8.0.0; 8.0.1; 8.0.2; 8.1.0, and TIBCO Managed File Transfer Internet Server: versions up to and including 7.3.2; 8.0.0; 8.0.1; 8.0.2; 8.1.0.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19810</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
urllib3 -- urllib3	urllib3 before version 1.23 does not remove the Authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or	2018-12-	not yet	<a href="#">CVE-2018-20060</a> <a href="#">MISC</a>

	scheme). This can allow for credentials in the Authorization header to be exposed to unintended hosts or transmitted in cleartext.	11	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
usualtoolcms -- usualtoolcms	An issue was discovered in UsualToolCMS v8.0. cmsadmin/a_sqlback.php allows remote attackers to delete arbitrary files via a backname[] directory-traversal pathname followed by a crafted substring.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20128</a> <a href="#">MISC</a>
verynginx -- verynginx	VeryNginx 0.3.3 allows remote attackers to bypass the Web Application Firewall feature because there is no error handler (for get_uni_args or get_post_args) to block the API misuse described in CVE-2018-9230.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19991</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, crafted URLs could trigger XSS for certain use cases involving plugins.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20150</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could modify new comments made by users with greater privileges, possibly causing XSS.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20153</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, authors could bypass intended restrictions on post types via crafted input.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20152</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, when the Apache HTTP Server is used, authors could upload crafted files that bypass intended MIME type restrictions, leading to XSS, as demonstrated by a .jpg file without JPEG data.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20149</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, the user-activation page could be read by a search engine's web crawler if an unusual configuration were chosen. The search engine could then index and display a user's e-mail address and (rarely) the password that was generated by default.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20151</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Maintenance Mode plugin before 2.0.7 for WordPress allows remote authenticated subscriber users to bypass intended access restrictions on changes to plugin settings.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20155</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could conduct PHP object injection attacks via crafted metadata in a wp.getMediaItem XMLRPC call. This is caused by mishandling of serialized data at phar:// URLs in the wp_get_attachment_thumb_file function in wp-includes/post.php.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20148</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Maintenance Mode plugin before 2.0.7 for WordPress allows remote authenticated "site administrator" users to execute arbitrary PHP code throughout a multisite network.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20156</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Maintenance Mode plugin before 2.0.7 for WordPress allows remote authenticated users to discover all subscriber e-mail addresses.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20154</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, authors could modify metadata to bypass intended restrictions on deleting files.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20147</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The codexion "Import users from CSV with meta" plugin before 1.12.1 for WordPress allows XSS via the value of a cell.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20101</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing 64-bit PV guest OS users to cause a denial of service (host OS crash) because #GP[0] can occur after a non-canonical address is passed to the TLB flushing code. NOTE: this issue exists because of an incorrect CVE-2017-5754 (aka MeltDown) mitigation.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19965</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen 4.11.x allowing x86 guest OS users to cause a denial of service (host OS hang) because the p2m lock remains unavailable indefinitely in certain error conditions.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19964</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen 4.11 allowing HVM guest OS users to cause a denial of service (host OS crash) or possibly gain host OS privileges because x86 IOREQ server resource accounting (for external emulators) was mishandled.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19963</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x on AMD x86 platforms, possibly allowing guest OS users to gain host OS privileges because small IOMMU mappings are unsafely combined into larger ones.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19962</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service (host OS crash) or possibly gain host OS privileges because of an interpretation conflict for a union data structure associated with shadow paging. NOTE: this issue exists because of an incorrect fix for CVE-2017-15595.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19966</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x on AMD x86 platforms, possibly allowing guest OS users to gain host OS privileges because TLB flushes do not always occur after IOMMU mapping changes.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19961</a> <a href="#">BID</a> <a href="#">MISC</a>
xxl-conf -- xxl-conf	An issue was discovered in XXL-CONF 1.6.0. There is a path traversal vulnerability via ../ in the keys parameter that can download any configuration file, related to ConfController.java and PropUtil.java.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20094</a> <a href="#">MISC</a>
yzmcms -- yzmcms	YzmCMS v5.2 has admin/role/add.html CSRF.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20015</a> <a href="#">MISC</a>
zoho_manageengine -- adaudit	Zoho ManageEngine ADAudit before 5.1 build 5120 allows remote attackers to cause a denial of service (stack-based buffer overflow) via the 'Domain Name' field when adding a new domain.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19118</a> <a href="#">CONFIRM</a>
zzzphp -- cms	An issue was discovered in zzzphp cms 1.5.8. del_file in /admin/save.php allows remote attackers to delete arbitrary files via a mixed-case extension and an extra ' character, because (for example) "php" is blocked but path=F:/1.php succeeds.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20127</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [s-ce.t go.](#) If you need help or have questions, please send an email to [Lo@ s-ce.t go.](#) Do not reply to this message since this email was sent from a notification-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas.us-cert.gov to your address book.

OTHER RESOURCES  
[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED  


SUBSCRIBER SERVICES  
[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [lmogninis@sunrival.ca.gov](mailto:lmogninis@sunrival.ca.gov) using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) - 2 5 Murray Lane SW Bldg 10 - Washington, DC 20598 - (888) 282-0870



From: [US-CERT](#)  
To: [uscert@ic.sunnyvale.ca.us](#)  
Subject: SB18-351: Vulnerability Summary for the Week of December 10, 2018  
Date: Monday, December 17, 2018 11:37:44 AM

U.S. Department of Homeland Security US-CERT



National Cyber Awareness System:

## SB18-351 Vulnerability Summary for the Week of December 10, 2018

12/17/2018 06:37 AM EST

Original release date: December 17, 2018

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the [National Institute of Standards and Technology](#) (NIST) [National Vulnerability Database](#) (NVD) in the past week. The NVD is sponsored by the [Department of Homeland Security](#) (DHS) [National Cybersecurity and Communications Integration Center](#) (NCCIC) / [United States Computer Emergency Readiness Team](#) (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) [National Vulnerability Database](#) (NVD). In some cases, the vulnerabilities in the Bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

## High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka "Windows Kernel Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	2018-12-11	7.2	<a href="#">CVE-2018-8611</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
microsoft -- windows_10	An elevation of privilege vulnerability exists in Windows when the Windows kernel-mode driver fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8639.	2018-12-11	7.2	<a href="#">CVE-2018-8641</a> <a href="#">BID</a> <a href="#">CONFIRM</a>

[Back to top](#)

## Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- chrome	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2018-12-11	6.8	<a href="#">CVE-2018-17481</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Heap buffer overflow in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18335</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	2018-12-11	6.8	<a href="#">CVE-2018-18336</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect handling of stylesheets leading to a use after free in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18337</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect, thread-unsafe use of SkImage in Canvas in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18338</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect object lifecycle in WebAudio in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18339</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Incorrect object lifecycle in MediaRecorder in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18340</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	An integer overflow leading to a heap buffer overflow in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18341</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>

google -- chrome	Incorrect handing of paths leading to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18343</a> BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of alert box display in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to present confusing browser UI via a crafted HTML page.	2018-12-11	4.3	<a href="#">CVE-2018-18346</a> BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of failed navigations with invalid URLs in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to trick a user into executing javascript in an arbitrary origin via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18347</a> BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of Reflect.construct in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	2018-12-11	6.8	<a href="#">CVE-2018-18359</a> BID REDHAT CONFIRM MISC DEBIAN
ibm -- marketing_platform	IBM Marketing Platform 9.1.0, 9.1.2, and 10.1 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 139029.	2018-12-07	5.5	<a href="#">CVE-2018-1424</a> CONFIRM BID XF
ibm -- marketing_platform	IBM Marketing Platform 9.1.0, 9.1.2 and 10.1 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 152855.	2018-12-07	5.5	<a href="#">CVE-2018-1920</a> CONFIRM BID XF
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8596.	2018-12-11	4.3	<a href="#">CVE-2018-8595</a> BID CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka "Windows GDI Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8595.	2018-12-11	4.3	<a href="#">CVE-2018-8596</a> BID CONFIRM

[Back to top](#)

## Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8621, CVE-2018-8622.	2018-12-11	2.1	<a href="#">CVE-2018-8477</a> BID CONFIRM
microsoft -- windows_10	An information disclosure vulnerability exists when Remote Procedure Call runtime improperly initializes objects in memory, aka "Remote Procedure Call runtime Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers.	2018-12-11	2.1	<a href="#">CVE-2018-8514</a> BID CONFIRM
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows Server 2012, Windows 7, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8477, CVE-2018-8622.	2018-12-11	2.1	<a href="#">CVE-2018-8621</a> BID CONFIRM
microsoft -- windows_7	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2012, Windows 8.1, Windows Server 2008 R2. This CVE ID is unique from CVE-2018-8477, CVE-2018-8621.	2018-12-11	2.1	<a href="#">CVE-2018-8622</a> BID CONFIRM

[Back to top](#)

## Severity Not Yet Assigned

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abisoft -- ticketly	AbiSoft Ticketly 1.0 is affected by multiple SQL Injection vulnerabilities through the parameters name, category_id and description in action/addproject.php; kind_id, priority_id, project_id, status_id and title in action/addticket.php; and kind_id and status_id in reports.php.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18923</a> MISC EXPLOIT-DB
abisoft -- ticketly	add_user in AbiSoft Ticketly 1.0 allows remote attackers to create administrator accounts via an action/add_user.php POST request.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18922</a> MISC
accusoft -- prizmdoc_html5_document_viewer	Accusoft PrizmDoc HTML5 Document Viewer before 13.5 contains an XML external entity (XXE) vulnerability, allowing an attacker to read arbitrary files or cause a denial of service (resource consumption).	2018-12-10	not yet calculated	<a href="#">CVE-2018-15805</a> CONFIRM MISC
apache -- ofbiz	In Apache OFBiz 16.11.01 to 16.11.04, the OFBiz HTTP engine (org.apache.ofbiz.service.engine.HttpEngine.java) handles requests for HTTP services via the /webtools/control/httpService endpoint. Both POST and GET requests to the httpService endpoint may contain three parameters: serviceName, serviceMode, and serviceContext. The exploitation occurs by having DOCTYPEs pointing to external references that trigger a payload that returns secret information from the host.	2018-12-13	not yet calculated	<a href="#">CVE-2018-8033</a> MLIST
apereo -- bedework -- bw-webdav	Apereo Bedework bw-webdav before 4.0.3 allows XXE attacks, as demonstrated by an invite-reply document that reads a local file, related to webdav/servlet/common/MethodBase.java and webdav/servlet/common/PostRequestPars.java.	2018-12-09	not yet calculated	<a href="#">CVE-2018-20000</a> MISC MISC
avanti_markets -- market_card	A vulnerability in the UPC bar code of the Avanti Markets MarketCard could allow an unauthenticated, local attacker to access funds within the customer's MarketCard balance, and also could lead to Customer Information Disclosure. The vulnerability is due to lack of proper validation of the UPC bar code present on the MarketCard. An attacker could exploit this vulnerability by generating a copy of a customer's bar code. An exploit could allow the attacker to access all funds located within the MarketCard or allow unauthenticated	2018-12-13	not yet calculated	<a href="#">CVE-2018-12076</a> MISC



	disclosure of information.			
bento4 -- bento4	An issue was discovered in EnsureCapacity in Core/Ap4Array.h in Bento4 1.5.1-627. Crafted MP4 input triggers an attempt at excessive memory allocation, as demonstrated by mp42hls.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20095</a> MISC
blackcat -- cms	Blackcat CMS 1.3.2 allows XSS via the willkommen.php?lang=DE page title at backend/pages/modify.php.	2018-12-10	not yet calculated	<a href="#">CVE-2018-16635</a> MISC
blinkforhome -- sync_module	A design flaw in the BlinkForHome (aka Blink For Home) Sync Module 2.10.4 and earlier allows attackers to disable cameras via Wi-Fi, because incident clips (triggered by the motion sensor) are not saved if the attacker's traffic (such as Dot11Deauth) successfully disconnects the Sync Module from the Wi-Fi network. (Access to live video from the app also becomes unavailable.)	2018-12-15	not yet calculated	<a href="#">CVE-2018-20161</a> MISC
cloud_foundry_foundation -- bits_service	Cloud Foundry Bits Service, versions prior to 2.18.0, includes an information disclosure vulnerability. A remote malicious user may execute a timing attack to brute-force the signing key, allowing them complete read and write access to the Bits Service storage.	2018-12-10	not yet calculated	<a href="#">CVE-2018-15800</a> CONFIRM
cloud_foundry_foundation -- uaa	Cloud Foundry UAA, all versions in v60.x, v61.x, v62.x, v63.x, and v64.x contain an authorization logic error. In environments with multiple identity providers that contain accounts across identity providers with the same username, a remote authenticated user with access to one of these accounts may be able to obtain a token for an account of the same username in the other identity provider.	2018-12-13	not yet calculated	<a href="#">CVE-2018-15754</a> CONFIRM
d-link -- dir-619l_and_dir-605l_devices	An issue was discovered in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 and DIR-605L Rev.B 2.12B1 devices. goform/formSysCmd allows remote authenticated users to execute arbitrary OS commands via the sysCmd POST parameter.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20057</a> MISC
d-link -- dir-619l_and_dir-605l_devices	An issue was discovered in /bin/boa on D-Link DIR-619L Rev.B 2.06B1 and DIR-605L Rev.B 2.12B1 devices. There is a stack-based buffer overflow allowing remote attackers to execute arbitrary code without authentication via the goform/formLanguageChange currTime parameter.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20056</a> MISC
dedecms -- dedecms	An issue was discovered in DedeCMS V5.7 SP2. uploads/include/dialog/select_images_post.php allows remote attackers to upload and execute arbitrary PHP code via a double extension and a modified ".php" substring, in conjunction with the image/jpeg content type, as demonstrated by the filename=1.jpg.p*hp value.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20129</a> MISC
dell_emc -- idrac	Dell EMC iDRAC7/iDRAC8 versions prior to 2.61.60.60 contain an improper error handling vulnerability. An unauthenticated attacker with physical access to the system could potentially exploit this vulnerability to get access to the u-boot shell.	2018-12-13	not yet calculated	<a href="#">CVE-2018-15776</a> CONFIRM
dell_emc -- idrac	Dell EMC iDRAC7/iDRAC8 versions prior to 2.61.60.60 and iDRAC9 versions prior to 3.20.21.20, 3.21.24.22, 3.21.26.22, and 3.23.23.23 contain a privilege escalation vulnerability. An authenticated malicious iDRAC user with operator privileges could potentially exploit a permissions check flaw in the Redfish interface to gain administrator access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-15774</a> CONFIRM
domainmod -- domainmod	DomainMOD 4.11.01 has XSS via the assets/add/category.php Category Name or Stakeholder field.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20011</a> MISC
domainmod -- domainmod	DomainMOD 4.11.01 has XSS via the assets/add/ssl-provider-account.php username field.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20010</a> MISC
domainmod -- domainmod	DomainMOD 4.11.01 has XSS via the assets/add/ssl-provider.php SSL Provider Name or SSL Provider URL field.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20009</a> MISC
doorgets -- doorgets	doorGets 7.0 allows remote attackers to write to arbitrary files via directory traversal, as demonstrated by a dg-user/?controller=theme&action=edit&name=doorgets&file=../../../../1.txt%00 URI with content in the theme_content_nofl parameter.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20064</a> MISC
eclipse -- mosquito	Eclipse Mosquito 1.5.x before 1.5.5 allows ACL bypass: if the option per_listener_settings was set to true, and the default listener was in use, and the default listener specified an acl_file, then the acl file was being ignored.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20145</a> MISC MISC MISC
edirectory -- edirectory	Cross site scripting vulnerability in eDirectory prior to 9.1 SP2	2018-12-12	not yet calculated	<a href="#">CVE-2018-17952</a> MISC
erpNext -- erpNext	A SQL injection issue was discovered in ERPNext 10.x and 11.x through 11.0.3-beta.29. This attack is only available to a logged-in user; however, many ERPNext sites allow account creation via the web. No special privileges are needed to conduct the attack. By calling a JavaScript function that calls a server-side Python function with carefully chosen arguments, a SQL attack can be carried out which allows SQL queries to be constructed to return any columns from any tables in the database. This is related to /api/resource/Item?fields= URIs, frappe.get_list, and frappe.call.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20061</a> MISC
evernote -- evernote	In Evernote before 7.6 on macOS, there is a local file path traversal issue in attachment previewing, aka MACOSNOTE-28634.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20058</a> CONFIRM
exiv2 -- exiv2	There is an infinite loop in Exiv2::Jp2Image::encodeJp2Header of jp2image.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20099</a> MISC MISC
exiv2 -- exiv2	There is a heap-based buffer over-read in the Exiv2::EXifToDataBuf function of pngimage.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20096</a> MISC MISC MISC
exiv2 -- exiv2	There is a SEGV in Exiv2::Internal::TiffParserWorker::findPrimaryGroups of tiffimage_int.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20097</a> MISC MISC
exiv2 -- exiv2	There is a heap-based buffer over-read in Exiv2::Jp2Image::encodeJp2Header of jp2image.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20098</a> MISC MISC
f5 -- big-ip	On BIG-IP 14.0.x, 13.x, 12.x, and 11.x, Enterprise Manager 3.1.1, BIG-IQ 6.x, 5.x, and 4.x, and iWorkflow 2.x, the passphrases for SNMPv3 users and trap destinations that are used for authentication and privacy are not handled by the BIG-IP system Secure Vault feature; they are written in the clear to the various configuration files.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15328</a> CONFIRM
fuel -- cms	XSS exists in FUEL CMS 1.4.3 via the Page title, Meta description, or Meta keywords during page data management, as demonstrated by the pages/edit/1/?lang=english URI.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20137</a> MISC
fuel -- cms	XSS exists in FUEL CMS 1.4.3 via the Header or Body in the Layout Variables during new-page creation, as demonstrated by the pages/edit/1/?lang=english URI.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20136</a> MISC
general_electric -- mark_vie	GE Mark VIe, EX2100e, EX2100e_Reg, and LS2100e Versions 03.03.28C to 05.02.04C, EX2100e All versions prior to v04.09.00C, EX2100e_Reg All versions prior to v04.09.00C, and LS2100e All versions prior to v04.09.00C	2018-12-14	not yet calculated	<a href="#">CVE-2018-19003</a>

	The affected versions of the application have a path traversal vulnerability that fails to restrict the ability of an attacker to gain access to restricted information.			MISC
general_electric -- proficy_cimplicity	XXE in GE Proficy Cimplicity GDS versions 9.0 R2, 9.5, 10.0	2018-12-07	not yet calculated	CVE-2018-15362 BID MISC MISC
geutebrueck_gmbh -- e2_camera_series	In Geutebrueck GmbH E2 Camera Series versions prior to 1.12.0.25 the DDNS configuration (in the Network Configuration panel) is vulnerable to an OS system command injection as root.	2018-12-14	not yet calculated	CVE-2018-19007 BID MISC
gnu -- binutils	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is an integer overflow and infinite loop caused by the IS_CONTAINED_BY_LMA macro in elf.c.	2018-12-07	not yet calculated	CVE-2018-19932 BID MISC MISC
gnu -- binutils	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils through 2.31. There is a heap-based buffer overflow in bfd_elf32_swap_phdr_in in elfcode.h because the number of program headers is not restricted.	2018-12-07	not yet calculated	CVE-2018-19931 BID MISC MISC
gnu -- binutils	The _bfd_generic_read_minisymbols function in syms.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.31, has a memory leak via a crafted ELF file, leading to a denial of service (memory consumption), as demonstrated by nm.	2018-12-09	not yet calculated	CVE-2018-20002 BID MISC MISC
golang -- golang	The crypto/x509 package of Go before 1.10.6 and 1.11.x before 1.11.3 does not limit the amount of work performed for each chain verification, which might allow attackers to craft pathological inputs leading to a CPU denial of service. Go TLS servers accepting client certificates and TLS clients are affected.	2018-12-14	not yet calculated	CVE-2018-16875 CONFIRM MISC
golang -- golang	In Go before 1.10.6 and 1.11.x before 1.11.3, the "go get" command is vulnerable to directory traversal when executed with the import path of a malicious Go package which contains curly braces (both '{' and '}' characters). Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at https://golang.org/cmd/go/#hdr-Module_aware_go_get). The attacker can cause an arbitrary filesystem write, which can lead to code execution.	2018-12-14	not yet calculated	CVE-2018-16874 CONFIRM MISC
golang -- golang	In Go before 1.10.6 and 1.11.x before 1.11.3, the "go get" command is vulnerable to remote code execution when executed with the -u flag and the import path of a malicious Go package, or a package that imports it directly or indirectly. Specifically, it is only vulnerable in GOPATH mode, but not in module mode (the distinction is documented at https://golang.org/cmd/go/#hdr-Module_aware_go_get). Using custom domains, it's possible to arrange things so that a Git repository is cloned to a folder named ".git" by using a vanity import path that ends with "/.git". If the Git repository root contains a "HEAD" file, a "config" file, an "objects" directory, a "refs" directory, with some work to ensure the proper ordering of operations, "go get -u" can be tricked into considering the parent directory as a repository root, and running Git commands on it. That will use the "config" file in the original Git repository root for its configuration, and if that config file contains malicious commands, they will execute on the system running "go get -u".	2018-12-14	not yet calculated	CVE-2018-16873 CONFIRM MISC
google -- chrome	Failure to dismiss http auth dialogs on navigation in Network Authentication in Google Chrome on Android prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of an auto dialog via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18353 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of CSP enforcement during navigations in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass content security policy via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18350 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2018-12-11	not yet calculated	CVE-2018-18355 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of bidirectional domain names with RTL characters in Omnibox in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2018-12-11	not yet calculated	CVE-2018-18348 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.	2018-12-11	not yet calculated	CVE-2018-18357 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Remote frame navigations was incorrectly permitted to local resources in Blink in Google Chrome prior to 71.0.3578.80 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.	2018-12-11	not yet calculated	CVE-2018-18349 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Lack of proper validation of ancestor frames site when sending lax cookies in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass SameSite cookie policy via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18351 BID REDHAT CONFIRM MISC DEBIAN
google -- chrome	Service works could inappropriately gain access to cross origin audio in Media in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass same origin policy for audio content via a crafted HTML page.	2018-12-11	not yet calculated	CVE-2018-18352 BID REDHAT CONFIRM MISC DEBIAN
				CVE-2018-18345

google -- chrome	Incorrect handling of blob URLs in Site Isolation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker who had compromised the renderer process to bypass site isolation protections via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Execution of user supplied Javascript during object deserialization can update object length leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18342</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Insufficient validate of external protocols in Shell Integration in Google Chrome on Windows prior to 71.0.3578.80 allowed a remote attacker to launch external programs via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18354</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	An integer overflow in path handling lead to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18356</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Lack of special casing of localhost in WPAD files in Google Chrome prior to 71.0.3578.80 allowed an attacker on the local network segment to proxy resources on localhost via a crafted WPAD file.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18358</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Inappropriate allowance of the setDownloadBehavior devtools protocol feature in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker with control of an installed extension to access files on the local file system via a crafted Chrome Extension.	2018-12-11	not yet calculated	<a href="#">CVE-2018-18344</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
google -- chrome	Execution of user supplied Javascript during array deserialization leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.	2018-12-11	not yet calculated	<a href="#">CVE-2018-17480</a> <a href="#">BID</a> <a href="#">REDHAT</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
grafana -- grafana	Grafana before 4.6.5 and 5.x before 5.3.3 allows remote authenticated users to read arbitrary files by leveraging Editor or Admin permissions.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19039</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
haproxy -- haproxy	An issue was discovered in dns.c in HAProxy through 1.8.14. In the case of a compressed pointer, a crafted packet can trigger infinite recursion by making the pointer point to itself, or create a long chain of valid pointers resulting in stack exhaustion.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20103</a> <a href="#">MISC</a>
haproxy -- haproxy	An out-of-bounds read in dns_validate_dns_response in dns.c was discovered in HAProxy through 1.8.14. Due to a missing check when validating DNS responses, remote attackers might be able read the 16 bytes corresponding to an AAAA record from the non-initialized part of the buffer, possibly accessing anything that was left on the stack, or even past the end of the 8193-byte buffer, depending on the value of accepted_payload_size.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20102</a> <a href="#">MISC</a>
hashicorp -- consul	HashiCorp Consul 0.5.1 through 1.4.0 can use cleartext agent-to-agent RPC communication because the verify_outgoing setting is improperly documented. NOTE: the vendor has provided reconfiguration steps that do not require a software upgrade.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19653</a> <a href="#">MISC</a> <a href="#">MISC</a>
i-doit -- i-doit_open	i-doit open 1.11.2 allows Remote Code Execution because ZIP archives are mishandled. It has an upload feature that allows an authenticated user with the administrator role to upload arbitrary files to the main website directory. Exploitation involves uploading a ".php" file within a ".zip" file because a ZIP archive is accepted by /admin/?req=modules&action=add as a plugin, and extracted to the main directory. In order for the ".zip" file to be accepted, it must also contain a package.json file.	2018-12-15	not yet calculated	<a href="#">CVE-2018-20159</a> <a href="#">MISC</a> <a href="#">EXPLOIT-DB</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 140760.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1478</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 140757.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1476</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 140969.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1484</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 does not renew a session variable after a successful authentication which could lead to session fixation/hijacking vulnerability. This could force a user to utilize a cookie that may be known to an attacker. IBM X-Force ID: 140970.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1485</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 140763.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1481</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 does not set the 'HttpOnly' attribute on authorization tokens or session cookies. If a Cross-Site Scripting vulnerability also existed attackers may be able to get the cookie values via malicious JavaScript and then hijack the user session. IBM X-Force ID: 140762.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1480</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- bigfix_platform	IBM BigFix Platform 9.2.0 through 9.2.14 and 9.5 through 9.5.9 is vulnerable to HTTP response splitting attacks, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to inject arbitrary HTTP headers and cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning or cross-site scripting, and possibly obtain sensitive information. IBM X-force ID: 140692.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1474</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
	IBM Business Automation Workflow 18.0.0.0 and 18.0.0.1 is vulnerable to			

ibm -- business_automation_workflow	cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 150947.	2018-12-14	not yet calculated	<a href="#">CVE-2018-1848</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- connections	IBM Connections 5.0, 5.5, and 6.0 is vulnerable to possible host header injection attack that could cause navigation to the attacker's domain. IBM X-Force ID: 152456.	2018-12-07	not yet calculated	<a href="#">CVE-2018-1896</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- curam_social_program_management	IBM Curam Social Program Management 6.0.5, 6.1.1, 6.2.0, 7.0.1, and 7.0.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 152529.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1900</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- curam_social_program_management	IBM Curam Social Program Management 7.0.3 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-force ID: 144951.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1671</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- curam_social_program_management	IBM Curam Social Program Management 6.0.5, 6.1.1, 6.2.0, 7.0.1, and 7.0.3 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 144747.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1654</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateways 7.5, 7.5.1, 7.5.2, 7.6, and 2018.4 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 144889.	2018-12-07	not yet calculated	<a href="#">CVE-2018-1663</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateway 7.1.0.0 through 7.1.0.19, 7.2.0.0 through 7.2.0.16, 7.5.0.0 through 7.5.1.17, 7.5.0.0 through 7.5.1.9, 7.5.2.0 through 7.5.2.9, and 7.6.0.0 through 7.6.0.2 and IBM MQ Appliance 8.0.0.0 through 8.0.0.8 and 9.0.1 through 9.0.5 could allow a local user to cause a denial of service through unknown vectors. IBM X-Force ID: 144724.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1652</a> <a href="#">XF</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateway 7.6.0.0 through 7.6.0.10, 7.5.2.0 through 7.5.2.17, 7.5.1.0 through 7.5.1.17, 7.5.0.0 through 7.5.0.18, and 7.7.0.0 through 7.7.1.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 144893.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1667</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- datapower_gateway	IBM DataPower Gateway 7.6.0.0 through 7.6.0.10, 7.5.2.0 through 7.5.2.17, 7.5.1.0 through 7.5.1.17, 7.5.0.0 through 7.5.0.18, and 7.7.0.0 through 7.7.1.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 144891.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1665</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- db2	IBM DB2 for Linux, UNIX and Windows 11.1 (includes DB2 Connect Server) contains a denial of service vulnerability. A remote, authenticated DB2 user could exploit this vulnerability by issuing a specially-crafted SELECT statement with TRUNCATE function. IBM X-Force ID: 154032.	2018-12-14	not yet calculated	<a href="#">CVE-2018-1977</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- mq_console_rest_api	A problem within the IBM MQ 9.0.2, 9.0.3, 9.0.4, 9.0.5, and 9.1.0.0 Console REST API Could allow attackers to execute a denial of service attack preventing users from logging into the MQ Console REST API. IBM X-Force ID: 151969.	2018-12-07	not yet calculated	<a href="#">CVE-2018-1883</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- operational_decision_management	IBM Operational Decision Management 8.5, 8.6, 8.7, 8.8, and 8.9 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 150170.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1821</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 148419.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1740</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 uses incomplete blacklisting for input validation which allows attackers to bypass application controls resulting in direct impact to the system and data integrity. IBM X-Force ID: 150017.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1813</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 144726.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1653</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 150018.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1814</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 for Enterprise Single-Sign On is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 150019.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1815</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 does not set the secure attribute on authorization tokens or session cookies. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 149703.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1804</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 152021.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1886</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 152078.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1887</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 generates an error message that includes sensitive information about its environment, users, or associated data. IBM X-Force ID: 149704.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1805</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_access_manager_appliance	IBM Security Access Manager Appliance 9.0.1.0, 9.0.2.0, 9.0.3.0, 9.0.4.0, and 9.0.5.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 149702.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1803</a> <a href="#">CONFIRM</a> <a href="#">XF</a>
ibm -- security_guardium	IBM Security Guardium 10 and 10.5 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption	2018-12-13	not yet calculated	<a href="#">CVE-2018-1818</a> <a href="#">XF</a>

	of internal data. IBM X-Force ID: 150022.			<a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10 and 10.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 150021.	2018-12-13	not yet calculated	<a href="#">CVE-2018-1817</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- security_guardium	IBM Security Guardium 10 and 10.5 uses a one-way cryptographic hash against an input that should not be reversible, such as a password, but the software does not also use a salt as part of the input. IBM X-Force ID: 124743.	2018-12-13	not yet calculated	<a href="#">CVE-2017-1268</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console is vulnerable to cross-site request forgery, caused by improper validation of user-supplied input. By persuading a user to visit a malicious URL, a remote attacker could send a specially-crafted request. An attacker could exploit this vulnerability to perform CSRF attack and update available applications. IBM X-Force ID: 152992.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1926</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 9 could allow sensitive information to be available caused by mishandling of data by the application based on an incorrect return by the <code>HttpServletRequest.authenticate()</code> API when an unprotected URI is accessed. IBM X-Force ID: 153629.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1957</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to temporarily gain elevated privileges on the system, caused by incorrect cached value being used. IBM X-Force ID: 152530.	2018-12-12	not yet calculated	<a href="#">CVE-2018-1901</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow remote attackers to execute arbitrary Java code through an administrative client class with a serialized object from untrusted sources. IBM X-Force ID: 152533.	2018-12-11	not yet calculated	<a href="#">CVE-2018-1904</a> <a href="#">BID</a> <a href="#">XF</a> <a href="#">CONFIRM</a>
imanager -- imanager	Cross site scripting vulnerability in iManager prior to 3.1 SP2.	2018-12-12	not yet calculated	<a href="#">CVE-2018-17949</a> <a href="#">MISC</a>
intel -- parallel_studio	Improper directory permissions in the installer for the Intel Parallel Studio before 2019 Gold may allow authenticated users to potentially enable an escalation of privilege via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-3704</a> <a href="#">CONFIRM</a>
intel -- quickassist_technology_for_linux	Improper memory handling in Intel QuickAssist Technology for Linux (all versions) may allow an authenticated user to potentially enable a denial of service via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18096</a> <a href="#">CONFIRM</a>
intel -- quickassist_technology_for_linux	Improper configuration of hardware access in Intel QuickAssist Technology for Linux (all versions) may allow an authenticated user to potentially enable a denial of service via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-12206</a> <a href="#">CONFIRM</a>
intel -- solid_state_drive_toolbox	Improper directory permissions in Intel Solid State Drive Toolbox before 3.5.7 may allow an authenticated user to potentially enable escalation of privilege via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18097</a> <a href="#">CONFIRM</a>
intel -- system_defense_utility	Improper directory permissions in the installer for the Intel System Defense Utility (all versions) may allow authenticated users to potentially enable an escalation of privilege via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-3705</a> <a href="#">CONFIRM</a>
intel -- vtune_amplifier	Improper file permissions in the installer for Intel VTune Amplifier 2018 Update 3 and before may allow unprivileged user to potentially gain privileged access via local access.	2018-12-13	not yet calculated	<a href="#">CVE-2018-18093</a> <a href="#">CONFIRM</a>
intel -- x86_platforms	An issue was discovered in Xen through 4.11.x on Intel x86 platforms allowing guest OS users to cause a denial of service (host OS hang) because Xen does not work around Intel's mishandling of certain HLE transactions associated with the KACQUIRE instruction prefix.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19967</a> <a href="#">BID</a> <a href="#">MISC</a>
jenkins -- jenkins	A data modification vulnerability exists in Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in User.java, <code>IdStrategy.java</code> that allows attackers to submit crafted user names that can cause an improper migration of user record storage formats, potentially preventing the victim from logging into Jenkins.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000863</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Pipeline: Groovy Plugin 2.59 and earlier in <code>groovy-sandbox/src/main/java/org/kohsuke/groovy/sandbox/SandboxTransformer.java</code> , <code>groovy-cps/lib/src/main/java/com/cloudbees/groovy/cps/SandboxCpsTransformer.java</code> that allows attackers with <code>Job/Configure</code> permission, or unauthorized attackers with SCM commit privileges and corresponding pipelines based on Jenkinsfiles set up in Jenkins, to execute arbitrary code on the Jenkins master JVM	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000866</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A denial of service vulnerability exists in Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in <code>CronTab.java</code> that allows attackers with <code>Overall/Read</code> permission to have a request handling thread enter an infinite loop.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000864</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A sandbox bypass vulnerability exists in Script Security Plugin 1.47 and earlier in <code>groovy-sandbox/src/main/java/org/kohsuke/groovy/sandbox/SandboxTransformer.java</code> that allows attackers with <code>Job/Configure</code> permission to execute arbitrary code on the Jenkins master JVM, if plugins using the Groovy sandbox are installed.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000865</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	A code execution vulnerability exists in the Stapler web framework used by Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in <code>stapler/core/src/main/java/org/kohsuke/stapler/MetaClass.java</code> that allows attackers to invoke some methods on Java objects by accessing crafted URLs that were not intended to be invoked this way.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000861</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
jenkins -- jenkins	An information exposure vulnerability exists in Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in <code>DirectoryBrowserSupport.java</code> that allows attackers with the ability to control build output to browse the file system on agents running builds beyond the duration of the build using the workspace browser.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1000862</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
jooan -- ja-q1h_wi-fi_camera	Mishandling of an empty string on the Jooan JA-Q1H Wi-Fi camera with firmware 21.0.0.91 allows remote attackers to cause a denial of service (crash and reboot) via the <code>ONVIF GetStreamUri</code> method and <code>GetVideoEncoderConfigurationOptions</code> method.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20050</a> <a href="#">MISC</a>
jooan -- ja-q1h_wi-fi_camera	Mishandling of <code>&gt;'</code> on the Jooan JA-Q1H Wi-Fi camera with firmware 21.0.0.91 allows remote attackers to cause a denial of service (crash and reboot) via certain <code>ONVIF</code> methods such as <code>CreateUsers</code> , <code>SetImagingSettings</code> , <code>GetStreamUri</code> , and so on.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20051</a> <a href="#">MISC</a>
katello -- katello	A SQL injection flaw was found in katello's errata-related API. An authenticated remote attacker can craft input data to force a malformed SQL query to the backend database, which will leak internal IDs. This issue is related to an incomplete fix for CVE-2016-3072. Version 3.10 and older is vulnerable.	2018-12-13	not yet calculated	<a href="#">CVE-2018-14623</a> <a href="#">CONFIRM</a>
kt -- mc01507l_z-wave_s0_devices	An issue was discovered on KT MC01507L Z-Wave S0 devices. It occurs because HPKP is not implemented. The communication architecture is APP > Server > Controller (HUB) > Node (products which are controlled by HUB). The prerequisite is that the attacker is on the same network as the target HUB, and can use IP Changer to change destination IP addresses (of all packets whose destination IP address is Server) to a proxy-server IP address. This allows sniffing of cleartext between Server and Controller. The cleartext command data is transmitted to Controller using the proxy server's fake certificate, and it is able to control each Node of the HUB. Also, by operating HUB in Z-Wave Pairing Mode, it is possible to obtain the Z-Wave network key.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19982</a> <a href="#">MISC</a>



libav -- libav	In Libav 12.3, there is a floating point exception in the range_decode_culshift function (called from range_decode_bits) in libavcodec/apedec.c that will lead to remote denial of service via crafted input.	2018-12-09	not yet calculated	<a href="#">CVE-2018-20001</a> MISC
linux -- kernel	The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFDIO_ ioctl calls, as demonstrated by allowing local users to write data into holes in a tmpfs file (if the user has read-only access to that file, and that file contains holes), related to fs/userfaultfd.c and mm/userfaultfd.c.	2018-12-12	not yet calculated	<a href="#">CVE-2018-18397</a> MISC MISC MISC MISC
mcafee -- agent	Privilege escalation vulnerability in McAfee Agent (MA) for Linux 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to perform arbitrary command execution via specific conditions.	2018-12-12	not yet calculated	<a href="#">CVE-2018-6705</a> CONFIRM
mcafee -- agent	Insecure handling of temporary files in non-Windows McAfee Agent 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows an Unprivileged User to introduce custom paths during agent installation in Linux via unspecified vectors.	2018-12-12	not yet calculated	<a href="#">CVE-2018-6706</a> CONFIRM
mcafee -- agent	Denial of Service through Resource Depletion vulnerability in the agent in non-Windows McAfee Agent (MA) 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to cause DoS, unexpected behavior, or potentially unauthorized code execution via knowledge of the internal trust mechanism.	2018-12-13	not yet calculated	<a href="#">CVE-2018-6707</a> CONFIRM
mcafee -- agent	Privilege escalation vulnerability in McAfee Agent (MA) for Linux 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows local users to perform arbitrary command execution via specific conditions.	2018-12-12	not yet calculated	<a href="#">CVE-2018-6704</a> CONFIRM
mcafee -- agent	Use After Free in McAfee Common service in McAfee Agent (MA) 5.0.0 through 5.0.6, 5.5.0, and 5.5.1 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted TCP packet.	2018-12-11	not yet calculated	<a href="#">CVE-2018-6703</a> CONFIRM
medtronic -- carelink_and_ensure_programmers	Medtronic CareLink 2090 Programmer CareLink 9790 Programmer 29901 Encore Programmer, all versions, The affected products do not encrypt or do not sufficiently encrypt the following sensitive information while at rest PII and PHI.	2018-12-14	not yet calculated	<a href="#">CVE-2018-18984</a> MISC
micro_focus -- fortify_software_security_center	A potential Remote Unauthorized Access in Micro Focus Fortify Software Security Center (SSC), versions 17.10, 17.20, 18.10 this exploitation could allow Remote Unauthorized Access	2018-12-13	not yet calculated	<a href="#">CVE-2018-7691</a> MISC EXPLOIT-DB
micro_focus -- fortify_software_security_center	A potential Remote Unauthorized Access in Micro Focus Fortify Software Security Center (SSC), versions 17.10, 17.20, 18.10 this exploitation could allow Remote Unauthorized Access	2018-12-13	not yet calculated	<a href="#">CVE-2018-7690</a> MISC EXPLOIT-DB
microsoft -- .net_framework	A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly, aka ".NET Framework Remote Code Injection Vulnerability." This affects Microsoft .NET Framework 4.6, Microsoft .NET Framework 3.5, Microsoft .NET Framework 4.7.4.7.1/4.7.2, Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7.1/4.7.1/4.7.2, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET Framework 4.7.1/4.7.2, Microsoft .NET Framework 4.7.2, Microsoft .NET Framework 4.6.2.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8540</a> BID CONFIRM
microsoft -- .net_framework	A denial of service vulnerability exists when .NET Framework improperly handles special web requests, aka ".NET Framework Denial Of Service Vulnerability." This affects Microsoft .NET Framework 4.6, Microsoft .NET Framework 3.5, Microsoft .NET Framework 4.7.4.7.1/4.7.2, Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7.1/4.7.1/4.7.2, Microsoft .NET Framework 3.5.1, Microsoft .NET Framework 4.6.2/4.7.1/4.7.2, Microsoft .NET Framework 4.5.2, Microsoft .NET Framework 4.7.1/4.7.2, Microsoft .NET Framework 4.7.2.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8517</a> BID CONFIRM
microsoft -- dynamics_nav	A cross site scripting vulnerability exists when Microsoft Dynamics NAV does not properly sanitize a specially crafted web request to an affected Dynamics NAV server, aka "Microsoft Dynamics NAV Cross Site Scripting Vulnerability." This affects Microsoft Dynamics NAV.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8651</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8624</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8618</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8617, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8583</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8617, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8629</a> BID CONFIRM
microsoft -- edge_and_chakracore	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka "Chakra Scripting Engine Memory Corruption Vulnerability." This affects Microsoft Edge, ChakraCore. This CVE ID is unique from CVE-2018-8583, CVE-2018-8618, CVE-2018-8624, CVE-2018-8629.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8617</a> BID CONFIRM
microsoft -- exchange_server	A tampering vulnerability exists when Microsoft Exchange Server fails to properly handle profile data, aka "Microsoft Exchange Server Tampering Vulnerability." This affects Microsoft Exchange Server.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8604</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka "Scripting Engine Memory Corruption Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8643</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka "Windows VBScript Engine Remote Code Execution Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8625</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists when the Internet Explorer VBScript execution policy does not properly restrict VBScript under specific conditions, aka "Internet Explorer Remote Code Execution Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8619</a> BID CONFIRM
microsoft -- internet_explorer	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka "Internet Explorer Memory Corruption Vulnerability." This affects Internet Explorer 9, Internet Explorer 11, Internet Explorer 10.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8631</a> BID CONFIRM
	A remote code execution vulnerability exists in Microsoft Outlook software			<a href="#">CVE-2018-</a>

microsoft -- multiple_products	when it fails to properly handle objects in memory, aka "Microsoft Outlook Remote Code Execution Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Outlook.	2018-12-11	not yet calculated	<a href="#">8587 BID CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka "Microsoft Excel Remote Code Execution Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Excel. This CVE ID is unique from CVE-2018-8597.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8636 BID CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft PowerPoint software when the software fails to properly handle objects in memory, aka "Microsoft PowerPoint Remote Code Execution Vulnerability." This affects Microsoft Office, Office 365 ProPlus, Microsoft PowerPoint, Microsoft SharePoint, Microsoft PowerPoint Viewer, Office Online Server, Microsoft SharePoint Server.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8628 BID CONFIRM</a>
microsoft -- multiple_products	A Denial Of Service vulnerability exists when Connected User Experiences and Telemetry Service fails to validate certain function values, aka "Connected User Experiences and Telemetry Service Denial of Service Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8612 BID CONFIRM</a>
microsoft -- multiple_products	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka "Microsoft Excel Information Disclosure Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Excel. This CVE ID is unique from CVE-2018-8627.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8598 BID CONFIRM</a>
microsoft -- multiple_products	An information disclosure vulnerability exists when Microsoft Excel software reads out of bound memory due to an uninitialized variable, which could disclose the contents of memory, aka "Microsoft Excel Information Disclosure Vulnerability." This affects Microsoft Office, Office 365 ProPlus, Microsoft Excel, Microsoft Excel Viewer, Excel. This CVE ID is unique from CVE-2018-8598.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8627 BID CONFIRM</a>
microsoft -- multiple_products	An elevation of privilege vulnerability exists when the Diagnostics Hub Standard Collector Service improperly impersonates certain file operations, aka "Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability." This affects Microsoft Visual Studio, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8599 BID CONFIRM</a>
microsoft -- multiple_products	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka "Microsoft Excel Remote Code Execution Vulnerability." This affects Office 365 ProPlus, Microsoft Office, Microsoft Excel. This CVE ID is unique from CVE-2018-8636.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8597 BID CONFIRM</a>
microsoft -- sharepoint	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka "Microsoft Office SharePoint XSS Vulnerability." This affects Microsoft SharePoint.	2018-12-12	not yet calculated	<a href="#">CVE-2018-8650 BID CONFIRM</a>
microsoft -- sharepoint	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted authentication request to an affected SharePoint server, aka "Microsoft SharePoint Server Elevation of Privilege Vulnerability." This affects Microsoft SharePoint Server, Microsoft SharePoint.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8635 BID CONFIRM</a>
microsoft -- sharepoint	An information disclosure vulnerability exists where certain modes of the search function in Microsoft SharePoint Server are vulnerable to cross-site search attacks (a variant of cross-site request forgery, CSRF), aka "Microsoft SharePoint Information Disclosure Vulnerability." This affects Microsoft SharePoint.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8580 BID CONFIRM</a>
microsoft -- windows	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka "Windows Denial of Service Vulnerability." This affects Windows 10, Windows Server 2019.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8649 BID CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists in Windows where Microsoft text-to-speech fails to properly handle objects in the memory, aka "Microsoft Text-To-Speech Remote Code Execution Vulnerability." This affects Windows Server 2016, Windows 10, Windows Server 2019, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8634 BID CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka "DirectX Information Disclosure Vulnerability." This affects Windows 10, Windows Server 2019.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8638 BID CONFIRM</a>
microsoft -- windows	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka "Win32k Elevation of Privilege Vulnerability." This affects Windows 7, Windows Server 2012 R2, Windows RT 8.1, Windows Server 2008, Windows Server 2019, Windows Server 2012, Windows 8.1, Windows Server 2016, Windows Server 2008 R2, Windows 10, Windows 10 Servers. This CVE ID is unique from CVE-2018-8641.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8639 BID CONFIRM</a>
microsoft -- windows	A remote code execution vulnerability exists in Windows Domain Name System (DNS) servers when they fail to properly handle requests, aka "Windows DNS Server Heap Overflow Vulnerability." This affects Windows Server 2012 R2, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8626 BID CONFIRM</a>
microsoft -- windows	An information disclosure vulnerability exists in Windows kernel that could allow an attacker to retrieve information that could lead to a Kernel Address Space Layout Randomization (KASLR) bypass, aka "Win32k Information Disclosure Vulnerability." This affects Windows 10 Servers, Windows 10, Windows Server 2019.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8637 BID CONFIRM</a>
microsoft -- windows_azure_pack	A Cross-site Scripting (XSS) vulnerability exists when Windows Azure Pack does not properly sanitize user-provided input, aka "Windows Azure Pack Cross Site Scripting Vulnerability." This affects Windows Azure Pack Rollup 13.1.	2018-12-11	not yet calculated	<a href="#">CVE-2018-8652 BID CONFIRM</a>
mini-xml -- mini-xml	An issue has been found in Mini-XML (aka mxml) 2.12. It is a use-after-free in mxmlWalkNext in mxml-search.c, as demonstrated by mxmldoc.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20005 MISC</a>
mini-xml -- mini-xml	An issue has been found in Mini-XML (aka mxml) 2.12. It is a stack-based buffer overflow in mxml_write_node in mxml-file.c via vectors involving a double-precision floating point number and the '<order type="real">' substring, as demonstrated by testxml.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20004 MISC</a>
netiq -- edirectory	Incorrect enforcement of authorization checks in eDirectory prior to 9.1 SP2	2018-12-12	not yet calculated	<a href="#">CVE-2018-17950 MISC</a>
nomachine -- nomachine	The nxfs.sys driver in the DokanFS library 0.6.0 in NoMachine before 6.4.6 on Windows 10 allows local users to cause a denial of service (BSOD) because uninitialized memory can be read.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20029 MISC</a>
nonecms -- nonecms	An issue was discovered in NoneCms V1.3. thinkphp/library/think/App.php allows remote attackers to execute arbitrary PHP code via crafted use of the filter parameter, as demonstrated by the s=index/thinkRequest/input&filter=phpinfo&data=1 query string.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20062 MISC</a>
nucleus -- cms	Nucleus CMS 3.70 allows HTML Injection via the index.php body parameter.	2018-12-10	not yet calculated	<a href="#">CVE-2018-16636 CONFIRM MISC</a>
	Open Dental before version 18.4 transmits the entire user database over the			<a href="#">CVE-2018-</a>

open_dental -- open_dental	network when a remote unauthenticated user accesses the command prompt. This allows the attacker to gain access to usernames, password hashes, privilege levels, and more.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15718</a> <a href="#">MISC</a>
open_dental -- open_dental	Open Dental before version 18.4 stores user passwords as base64 encoded MD5 hashes.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15717</a> <a href="#">MISC</a>
open_dental -- open_dental	Open Dental before version 18.4 installs a mysql database and uses the default credentials of "root" with a blank password. This allows anyone on the network with access to the server to access all database information.	2018-12-12	not yet calculated	<a href="#">CVE-2018-15719</a> <a href="#">MISC</a>
openrefine -- openrefine	The data import functionality in OpenRefine through 3.1 allows an XML External Entity (XXE) attack through a crafted (zip) file, allowing attackers to read arbitrary files.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20157</a> <a href="#">MISC</a>
oracle -- secure_global_desktop	XSS exists in the Administration Console in Oracle Secure Global Desktop 4.4 20080807152602 (but was fixed in later versions including 5.4). helpwindow.jsp has reflected XSS via all parameters, as demonstrated by the sgadmin/faces/com_sun_web_ui/help/helpwindow.jsp windowTitle parameter.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19439</a> <a href="#">MISC</a> <a href="#">FULLDISC</a> <a href="#">BID</a>
palo_alto_networks -- expedition_migration_tool	The Palo Alto Networks Expedition Migration tool 1.0.107 and earlier may allow an unauthenticated attacker with remote access to run system level commands on the device hosting this service/application.	2018-12-11	not yet calculated	<a href="#">CVE-2018-10143</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
perl -- perl	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	2018-12-07	not yet calculated	<a href="#">CVE-2018-18311</a> <a href="#">BID</a> <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
perl -- perl	Perl before 5.26.3 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	2018-12-07	not yet calculated	<a href="#">CVE-2018-18314</a> <a href="#">BID</a> <a href="#">SECTrack</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">FEDORA</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">UBUNTU</a> <a href="#">UBUNTU</a> <a href="#">DEBIAN</a>
php -- php	ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19935</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">DEBIAN</a>
phpcmf -- phpcmf	PHPCMF 4.1.3 has XSS via the first input field to the index.php?s=member&c=register&m=index URI.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20012</a> <a href="#">MISC</a> <a href="#">MISC</a>
phpmyadmin -- phpmyadmin	phpMyAdmin 4.7.x and 4.8.x versions prior to 4.8.4 are affected by a series of CSRF flaws. By deceiving a user into clicking on a crafted URL, it is possible to perform harmful SQL operations such as renaming databases, creating new tables/routines, deleting designer pages, adding/deleting users, updating user passwords, killing SQL processes, etc.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19969</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
phpmyadmin -- phpmyadmin	In phpMyAdmin before 4.8.4, an XSS vulnerability was found in the navigation tree, where an attacker can deliver a payload to a user through a crafted database/table name.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19970</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
phpmyadmin -- phpmyadmin	An attacker can exploit phpMyAdmin before 4.8.4 to leak the contents of a local file because of an error in the transformation feature. The attacker must have access to the phpMyAdmin Configuration Storage tables, although these can easily be created in any database to which the attacker has access. An attacker must have valid credentials to log in to phpMyAdmin; this vulnerability does not allow an attacker to circumvent the login system.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19968</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
phpok -- phpok	An issue was discovered in PHPok v5.0.055. There is a Stored XSS vulnerability via the title parameter to api.php?c=post&f=save (reachable via the index.php?id=book URI).	2018-12-10	not yet calculated	<a href="#">CVE-2018-20006</a> <a href="#">MISC</a>
phpscriptsmail.com -- entrepreneur_b2b_script	PHP Scripts Mail Entrepreneur B2B Script 3.0.6 allows Stored XSS via Account Settings fields such as FirstName and LastName, a similar issue to CVE-2018-14541.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20138</a> <a href="#">MISC</a>
pippo -- pippo	jaxb/JaxbEngine.java in Pippo 1.11.0 allows XXE.	2018-12-11	not yet calculated	<a href="#">CVE-2018-20059</a> <a href="#">CONFIRM</a>
pivotal -- rabbitmq_for_pcf	Pivotal RabbitMQ for PCF, all versions, uses a deterministically generated cookie that is shared between all machines when configured in a multi-tenant cluster. A remote attacker who can gain information about the network topology can guess this cookie and, if they have access to the right ports on any server in the MQ cluster can use this cookie to gain full control over the entire cluster.	2018-12-10	not yet calculated	<a href="#">CVE-2018-1279</a> <a href="#">CONFIRM</a>
pixar -- tractor	Pixar's Tractor software, versions 2.2 and earlier, contain a stored cross-site scripting vulnerability in the field that allows a user to add a note to an existing node. The stored information is displayed when a user requests information about the node. An attacker could insert Javascript into this note field that is then saved and displayed to the end user. An attacker might include Javascript that could execute on an authenticated user's system that could lead to website redirects, session cookie hijacking, social engineering, etc. As this is stored with the information about the node, all other authenticated users with access to this data are also vulnerable.	2018-12-13	not yet calculated	<a href="#">CVE-2018-5411</a> <a href="#">BID</a> <a href="#">CERT-VN</a>
qemu -- qemu	A flaw was found in qemu Media Transfer Protocol (MTP) before version 3.1.0. A path traversal in the in usb_mtp_write_data function in hw/usb/dev-mtp.c due to an improper filename sanitization. When the guest device is mounted in read-write mode, this allows to read/write arbitrary files which may lead to DoS scenario OR possibly lead to code execution on the host.	2018-12-12	not yet calculated	<a href="#">CVE-2018-16867</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>
qemu -- qemu	A flaw was found in qemu Media Transfer Protocol (MTP). The code opening files in usb_mtp_get_object and usb_mtp_get_partial_object and directories in usb_mtp_object_readir doesn't consider that the underlying filesystem may have changed since the time lstat(2) was called in usb_mtp_object_alloc, a classical TOCTTOU problem. An attacker with write access to the host filesystem shared with a guest can use this property to navigate the host filesystem in the context of the QEMU process and read any file the QEMU process has access to. Access to the filesystem may be local or via a network share protocol such as CIFS.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16872</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
				<a href="#">CVE-2018-</a>

qemu -- qemu	hw/9pfs/cofile.c and hw/9pfs/9p.c in QEMU can modify an fid path while it is being accessed by a second thread, leading to (for example) a use-after-free outcome.	2018-12-13	not yet calculated	<a href="#">19364 MLIST</a> <a href="#">MLIST</a> <a href="#">UBUNTU</a>
qemu -- qemu	v9fs_wstat in hw/9pfs/9p.c in QEMU allows guest OS users to cause a denial of service (crash) because of a race condition during file renaming.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19489 MLIST</a> <a href="#">XFD</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
qualcomm -- snapdragon	While generating trusted application id, An integer overflow can occur giving the trusted application an invalid identity in Snapdragon Mobile and Snapdragon Wear in versions MDM9206, MDM9607, MDM9650, SD 210/SD 212/SD 205, SD 835 and SDA660.	2018-12-10	not yet calculated	<a href="#">CVE-2016-10502 BID</a> <a href="#">CONFIRM</a>
ricoh -- myprint	Hardcoded credentials in the Ricoh myPrint application 2.9.2.4 for Windows and 2.2.7 for Android give access to any externally disclosed myPrint WSDL API, as demonstrated by discovering API secrets of related Google cloud printers, encrypted passwords of mail servers, and names of printed files.	2018-12-14	not yet calculated	<a href="#">CVE-2018-18006 MISC</a> <a href="#">FULLDISC</a>
s-cms -- s-cms	S-CMS V3.0 has SQL injection via the S_id parameter, as demonstrated by the /1/?type=productinfo&S_id=140 URI.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20018 MISC</a>
sap -- business_one_service_layer	TRACE method is enabled in SAP Business One Service Layer . Attacker can use XST (Cross Site Tracing) attack if frontend applications that are using Service Layer has a XSS vulnerability. This has been fixed in SAP Business One Service Layer (B1_ON_HANA, versions 9.2, 9.3).	2018-12-11	not yet calculated	<a href="#">CVE-2018-2502 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- commerce	SAP Commerce does not sufficiently validate user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability in storefronts that are based on the product. Fixed in versions (SAP Hybris Commerce, versions 6.2, 6.3, 6.4, 6.5, 6.6, 6.7).	2018-12-11	not yet calculated	<a href="#">CVE-2018-2505 BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- hana	The security audit log of SAP HANA, versions 1.0 and 2.0, does not log SELECT events if these events are part of a statement with the syntax CREATE TABLE <table_name> AS SELECT.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2497 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- marketing	SAP Marketing (UICUAN (1.20, 1.30, 1.40), SAPSCORE (1.13, 1.14)) does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2486 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- mobile_secure_android_client	Under certain conditions SAP Mobile Secure Android client (before version 6.60.19942.0 SP28 1711) allows an attacker to access information which would otherwise be restricted.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2500 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver	SAP NetWeaver AS Java Web Container service does not validate against whitelist the HTTP host header which can result in HTTP Host Header Manipulation or Cross-Site Scripting (XSS) vulnerability. This is fixed in versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2504 BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver	By default, the SAP NetWeaver AS Java keystore service does not sufficiently restrict the access to resources that should be protected. This has been fixed in SAP NetWeaver AS Java (ServerCore versions 7.11, 7.20, 7.30, 7.31, 7.40, 7.50).	2018-12-11	not yet calculated	<a href="#">CVE-2018-2503 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
sap -- netweaver	Necessary authorization checks for an authenticated user, resulting in escalation of privileges, have been fixed in SAP Basis AS ABAP of SAP NetWeaver 700 to 750, from 750 onwards delivered as ABAP Platform.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2494 MISC</a> <a href="#">MISC</a>
sap -- netweaver	SAML 2.0 functionality in SAP NetWeaver AS Java, does not sufficiently validate XML documents received from an untrusted source. This is fixed in versions 7.2, 7.30, 7.31, 7.40 and 7.50.	2018-12-11	not yet calculated	<a href="#">CVE-2018-2492 BID</a> <a href="#">MISC</a> <a href="#">MISC</a>
semcms -- semcms	SEMCMS 3.5 has XSS via the first text box to the SEMCMS_Main.php URI.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20017 MISC</a>
siemens -- simatic	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels 4" - 22" (All versions < V15 Update 4), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions < V15 Update 4), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V15 Update 4), SIMATIC WinCC Runtime Advanced (All versions < V15 Update 4), SIMATIC WinCC Runtime Professional (All versions < V15 Update 4), SIMATIC WinCC (TIA Portal) (All versions < V15 Update 4), SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel) (All versions). The webserver of affected HMI devices may allow URL redirections to untrusted websites. An attacker must trick a valid user who is authenticated to the device into clicking on a malicious link to exploit the vulnerability. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13813 BID</a> <a href="#">CONFIRM</a>
siemens -- simatic	A vulnerability has been identified in SIMATIC S7-1200 (All versions), SIMATIC S7-1500 (All Versions < V2.6). An attacker could exhaust the available connection pool of an affected device by opening a sufficient number of connections to the device. Successful exploitation requires an attacker to be able to send packets to port 102/tcp of the affected device. No user interaction and no user privileges are required to exploit the vulnerability. The vulnerability, if exploited, could cause a Denial-of-Service condition impacting the availability of the system. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13815 BID</a> <a href="#">CONFIRM</a>
siemens -- simatic	A vulnerability has been identified in SIMATIC HMI Comfort Panels 4" - 22" (All versions < V15 Update 4), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions < V15 Update 4), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V15 Update 4), SIMATIC WinCC Runtime Advanced (All versions < V15 Update 4), SIMATIC WinCC Runtime Professional (All versions < V15 Update 4), SIMATIC WinCC (TIA Portal) (All versions < V15 Update 4), SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel) (All versions). A directory traversal vulnerability could allow to download arbitrary files from the device. The security vulnerability could be exploited by an attacker with network access to the integrated web server. No user interaction and no authentication is required to exploit the vulnerability. The vulnerability impacts the confidentiality of the device. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13812 BID</a> <a href="#">CONFIRM</a>
	A vulnerability has been identified in SIMATIC HMI Comfort Panels 4" - 22" (All versions < V14), SIMATIC HMI Comfort Outdoor Panels 7" & 15" (All versions < V14), SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F,			

siemens -- simatic	KTP900 and KTP900F (All versions < V14), SIMATIC WinCC Runtime Advanced (All versions < V14), SIMATIC WinCC Runtime Professional (All versions < V14), SIMATIC WinCC (TIA Portal) (All versions < V14), SIMATIC HMI Classic Devices (TP/MP/OP/MP Mobile Panel) (All versions). The integrated web server (port 80/tcp and port 443/tcp) of the affected devices could allow an attacker to inject HTTP headers. An attacker must trick a valid user who is authenticated to the device into clicking on a malicious link to exploit the vulnerability. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13814</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- simatic_it	A vulnerability has been identified in SIMATIC IT LMS (All versions), SIMATIC IT Production Suite (Versions V7.1 < V7.1 Upd3), SIMATIC IT UA Discrete Manufacturing (Versions < V1.2), SIMATIC IT UA Discrete Manufacturing (Versions V1.2), SIMATIC IT UA Discrete Manufacturing (Versions V1.3), SIMATIC IT UA Discrete Manufacturing (Versions V2.3), SIMATIC IT UA Discrete Manufacturing (Versions V2.4). An attacker with network access to the installation could bypass the application-level authentication. In order to exploit the vulnerability, an attacker must obtain network access to an affected installation and must obtain a valid username to the system. Successful exploitation requires no user privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13804</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- simatic_s7-400_products	A vulnerability has been identified in SIMATIC S7-400 (incl. F) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-400H V4.5 and below (All versions), SIMATIC S7-400H V6 (All versions), SIMATIC S7-410 (All versions < V8.2.1). Sending of specially crafted packets to port 102/tcp via Ethernet interface via PROFIBUS or Multi Point Interfaces (MPI) could cause a Denial-of-Service condition on affected devices. Flashing with a firmware image may be required to recover the CPU. Successful exploitation requires an attacker to have network access to port 102/tcp via Ethernet interface or to be able to send messages via PROFIBUS or Multi Point Interfaces (MPI) to the device. No user interaction is required. If no access protection is configured, no privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the core functionality of the CPU, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16557</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
siemens -- simatic_s7-400_products	A vulnerability has been identified in SIMATIC S7-400 (incl. F) V6 and below (All versions), SIMATIC S7-400 PN/DP V7 (incl. F) (All versions), SIMATIC S7-400H V4.5 and below (All versions), SIMATIC S7-400H V6 (All versions), SIMATIC S7-410 (All versions < V8.2.1). Specially crafted packets sent to port 102/tcp via Ethernet interface, via PROFIBUS, or via Multi Point Interfaces (MPI) could cause the affected devices to go into defect mode. Manual reboot is required to resume normal operation. Successful exploitation requires an attacker to be able to send specially crafted packets to port 102/tcp via Ethernet interface, via PROFIBUS or Multi Point Interfaces (MPI). No user interaction and no user privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the core functionality of the CPU, compromising the availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16558</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
siemens -- simatic_step_7_tia_portal	A vulnerability has been identified in SIMATIC STEP 7 (TIA Portal) (All Versions < V15.1). Password hashes with insufficient computational effort could allow an attacker to access to a project file and reconstruct passwords. The vulnerability could be exploited by an attacker with local access to the project file. No user interaction is required to exploit the vulnerability. The vulnerability could allow the attacker to obtain certain passwords from the project. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-13811</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). The integrated VNC server on port 5900/tcp of the affected products could allow a remote attacker to cause a Denial-of-Service condition of the VNC server. Please note that this vulnerability is only exploitable if port 5900/tcp is manually opened in the firewall configuration of network port X130. The security vulnerability could be exploited by an attacker with network access to the affected devices and port. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise availability of the VNC server. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11464</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). Specially crafted network packets sent to port 102/tcp (ISO-TSAP) could allow a remote attacker to either cause a Denial-of-Service condition of the integrated software firewall or allow to execute code in the context of the software firewall. The security vulnerability could be exploited by an attacker with network access to the affected systems on port 102/tcp. Successful exploitation requires no user privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11466</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker could use ioctl calls to do out of bounds reads, arbitrary writes, or execute code in kernel mode. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11465</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A buffer overflow in the service command application could allow a local attacker to execute code with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11463</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). By sending a specially crafted authentication request to the affected systems a remote attacker could escalate his privileges to an elevated user account but not to root. The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no privileges and no user	2018-12-12	not yet calculated	<a href="#">CVE-2018-11462</a> <a href="#">BID</a> <a href="#">CONFIRM</a>



	interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.			
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). The integrated VNC server on port 5900/tcp of the affected products could allow a remote attacker to execute code with privileged permissions on the system by sending specially crafted network requests to port 5900/tcp. Please note that this vulnerability is only exploitable if port 5900/tcp is manually opened in the firewall configuration of network port X130. The security vulnerability could be exploited by an attacker with network access to the affected devices and port. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the VNC server. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11458</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). The integrated web server on port 4842/tcp of the affected products could allow a remote attacker to execute code with privileged permissions on the system by sending specially crafted network requests to port 4842/tcp. Please note that this vulnerability is only exploitable if port 4842/tcp is manually opened in the firewall configuration of network port X130. The security vulnerability could be exploited by an attacker with network access to the affected devices on port 4842/tcp. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the web server. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11457</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker with user privileges could use the service command application for privilege escalation to an elevated user but not root. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11461</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker could modify a user-writable configuration file so that after reboot or manual initiation the system reloads the modified configuration file and attacker-controlled code is executed with elevated privileges. The security vulnerability could be exploited by an attacker with local access to the affected system. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11459</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- sinumerik_controllers	A vulnerability has been identified in SINUMERIK 808D V4.7 (All versions), SINUMERIK 808D V4.8 (All versions), SINUMERIK 828D V4.7 (All versions < V4.7 SP6 HF1), SINUMERIK 840D sl V4.7 (All versions < V4.7 SP6 HF5), SINUMERIK 840D sl V4.8 (All versions < V4.8 SP3). A local attacker with elevated user privileges (manufact) could modify a CRAMFS archive so that after reboot the system loads the modified CRAMFS file and attacker-controlled code is executed with root privileges. The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires elevated user privileges (manufact) but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system. At the time of advisory publication no public exploitation of this security vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-11460</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- tim_1531_irc	A vulnerability has been identified in TIM 1531 IRC (All version < V2.0). The devices was missing proper authentication on port 102/tcp, although configured. Successful exploitation requires an attacker to be able to send packets to port 102/tcp of the affected device. No user interaction and no user privileges are required to exploit the vulnerability. At the time of advisory publication no public exploitation of this vulnerability was known.	2018-12-12	not yet calculated	<a href="#">CVE-2018-13816</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
siemens -- scalance	A vulnerability has been identified in SCALANCE S602 (All versions < V4.0.1.1), SCALANCE S612 (All versions < V4.0.1.1), SCALANCE S623 (All versions < V4.0.1.1), SCALANCE S627-2M (All versions < V4.0.1.1). The integrated web server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link. User interaction is required for a successful exploitation. The user must be logged into the web interface in order for the exploitation to succeed. At the stage of publishing this security advisory no public exploitation is known.	2018-12-13	not yet calculated	<a href="#">CVE-2018-16555</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
sigma_design -- z-wave_devices	An issue was discovered on Sigma Design Z-Wave S0 through S2 devices. An attacker first prepares a Z-Wave frame-transmission program (e.g., Z-Wave PC Controller, OpenZWave, CC1110, etc.). Next, the attacker conducts a DoS attack against the Z-Wave S0 Security version product by continuously sending divided "Nonce Get (0x98 0x81)" frames. The reason for dividing the "Nonce Get" frame is that, in security version S0, when a node receives a "Nonce Get" frame, the node produces a random new nonce and sends it to the Src node of the received "Nonce Get" frame. After the nonce value is generated and transmitted, the node transitions to wait mode. At this time, when "Nonce Get" is received again, the node discards the previous nonce value and generates a random nonce again. Therefore, because the frame is encrypted with previous nonce value, the received normal frame cannot be decrypted.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19983</a> <a href="#">MISC</a>
signal -- messenger_for_android	Signal Messenger for Android 4.24.8 may expose private information when using "disappearing messages." If a user uses the photo feature available in the "attach file" menu, then Signal will leave the picture in its own cache directory, which is available to any application on the system.	2018-12-10	not yet calculated	<a href="#">CVE-2018-3988</a> <a href="#">BID</a> <a href="#">MISC</a>
sonarsource -- sonarqube	A vulnerability in the API of SonarSource SonarQube before 7.4 could allow an authenticated user to discover sensitive information such as valid user-account logins in the web application. The vulnerability occurs because of improperly configured access controls that cause the API to return the external identity field to non-administrator users. The attacker could use this information in subsequent attacks against the system.	2018-12-14	not yet calculated	<a href="#">CVE-2018-19413</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
tibco -- managed_file_transfer_command_center_and_tibco_managed_file_transfer_internet_server	The Administrator Service component of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center, and TIBCO Managed File Transfer Internet Server contains vulnerabilities where an authenticated user with specific privileges can gain access to credentials to other systems. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions up to and including 7.3.2; 8.0.0; 8.0.1; 8.0.2; 8.1.0, and TIBCO Managed File Transfer Internet Server: versions up to and including 7.3.2; 8.0.0; 8.0.1; 8.0.2; 8.1.0.	2018-12-11	not yet calculated	<a href="#">CVE-2018-19810</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
urllib3 -- urllib3	urllib3 before version 1.23 does not remove the Authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or	2018-12-	not yet	<a href="#">CVE-2018-20060</a> <a href="#">MISC</a>

	scheme). This can allow for credentials in the Authorization header to be exposed to unintended hosts or transmitted in cleartext.	11	calculated	<a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
usualtoolcms -- usualtoolcms	An issue was discovered in UsualToolCMS v8.0. cmsadmin/a_sqlback.php allows remote attackers to delete arbitrary files via a backname[] directory-traversal pathname followed by a crafted substring.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20128</a> <a href="#">MISC</a>
verynginx -- verynginx	VeryNginx 0.3.3 allows remote attackers to bypass the Web Application Firewall feature because there is no error handler (for get_uni_args or get_post_args) to block the API misuse described in CVE-2018-9230.	2018-12-09	not yet calculated	<a href="#">CVE-2018-19991</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, crafted URLs could trigger XSS for certain use cases involving plugins.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20150</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could modify new comments made by users with greater privileges, possibly causing XSS.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20153</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, authors could bypass intended restrictions on post types via crafted input.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20152</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, when the Apache HTTP Server is used, authors could upload crafted files that bypass intended MIME type restrictions, leading to XSS, as demonstrated by a .jpg file without JPEG data.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20149</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, the user-activation page could be read by a search engine's web crawler if an unusual configuration were chosen. The search engine could then index and display a user's e-mail address and (rarely) the password that was generated by default.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20151</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Maintenance Mode plugin before 2.0.7 for WordPress allows remote authenticated subscriber users to bypass intended access restrictions on changes to plugin settings.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20155</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, contributors could conduct PHP object injection attacks via crafted metadata in a wp.getMediaItem XMLRPC call. This is caused by mishandling of serialized data at phar:// URLs in the wp_get_attachment_thumb_file function in wp-includes/post.php.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20148</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Maintenance Mode plugin before 2.0.7 for WordPress allows remote authenticated "site administrator" users to execute arbitrary PHP code throughout a multisite network.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20156</a> <a href="#">MISC</a>
wordpress -- wordpress	The WP Maintenance Mode plugin before 2.0.7 for WordPress allows remote authenticated users to discover all subscriber e-mail addresses.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20154</a> <a href="#">MISC</a>
wordpress -- wordpress	In WordPress before 4.9.9 and 5.x before 5.0.1, authors could modify metadata to bypass intended restrictions on deleting files.	2018-12-14	not yet calculated	<a href="#">CVE-2018-20147</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">MISC</a>
wordpress -- wordpress	The codexion "Import users from CSV with meta" plugin before 1.12.1 for WordPress allows XSS via the value of a cell.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20101</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing 64-bit PV guest OS users to cause a denial of service (host OS crash) because #GP[0] can occur after a non-canonical address is passed to the TLB flushing code. NOTE: this issue exists because of an incorrect CVE-2017-5754 (aka MeltDown) mitigation.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19965</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen 4.11.x allowing x86 guest OS users to cause a denial of service (host OS hang) because the p2m lock remains unavailable indefinitely in certain error conditions.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19964</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen 4.11 allowing HVM guest OS users to cause a denial of service (host OS crash) or possibly gain host OS privileges because x86 IOREQ server resource accounting (for external emulators) was mishandled.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19963</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x on AMD x86 platforms, possibly allowing guest OS users to gain host OS privileges because small IOMMU mappings are unsafely combined into larger ones.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19962</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x allowing x86 PV guest OS users to cause a denial of service (host OS crash) or possibly gain host OS privileges because of an interpretation conflict for a union data structure associated with shadow paging. NOTE: this issue exists because of an incorrect fix for CVE-2017-15595.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19966</a> <a href="#">BID</a> <a href="#">MISC</a>
xen -- xen	An issue was discovered in Xen through 4.11.x on AMD x86 platforms, possibly allowing guest OS users to gain host OS privileges because TLB flushes do not always occur after IOMMU mapping changes.	2018-12-07	not yet calculated	<a href="#">CVE-2018-19961</a> <a href="#">BID</a> <a href="#">MISC</a>
xxl-conf -- xxl-conf	An issue was discovered in XXL-CONF 1.6.0. There is a path traversal vulnerability via ../ in the keys parameter that can download any configuration file, related to ConfController.java and PropUtil.java.	2018-12-12	not yet calculated	<a href="#">CVE-2018-20094</a> <a href="#">MISC</a>
yzmcms -- yzmcms	YzmCMS v5.2 has admin/role/add.html CSRF.	2018-12-10	not yet calculated	<a href="#">CVE-2018-20015</a> <a href="#">MISC</a>
zoho_manageengine -- adaudit	Zoho ManageEngine ADAudit before 5.1 build 5120 allows remote attackers to cause a denial of service (stack-based buffer overflow) via the 'Domain Name' field when adding a new domain.	2018-12-13	not yet calculated	<a href="#">CVE-2018-19118</a> <a href="#">CONFIRM</a>
zzzphp -- cms	An issue was discovered in zzzphp cms 1.5.8. del_file in /admin/save.php allows remote attackers to delete arbitrary files via a mixed-case extension and an extra ' character, because (for example) "php" is blocked but path=F:/1.php succeeds.	2018-12-13	not yet calculated	<a href="#">CVE-2018-20127</a> <a href="#">MISC</a>

[Back to top](#)

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

A copy of this publication is available at [s-ce.l go.](#) If you need help or have quest ons, please send an email to [Lo@ s-ce.l go.](#) Do not reply to this message since this email was sent from a not fication-only address that is not monitored. To ensure you receive future US-CERT products, please add US-CERT@ncas-us-cert.gov o your address book.

OTHER RESOURCES

[Contact Us](#) | [Security Publications](#) | [Alerts and Tips](#) | [Related Resources](#)

STAY CONNECTED



SUBSCRIBER SERVICES

[Manage Preferences](#) | [Unsubscribe](#) | [Help](#)

This email was sent to [regularte@cd.sunnyvale.ca.us](mailto:regularte@cd.sunnyvale.ca.us) using GovDe lvery Commun cations Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 2 5 Murray Lane SW Bldg 10 · Washington, DC 20568 · (888) 282-0870



From:

[The Washington Post](#)

To:

[Anais Aquino](#)

Subject:

The Daily 202: Senate rebuke of Trump on Yemen shows Congress, not just the president, can offer moral leadership

Date:

Friday, December 14, 2018 7:07:37 AM

---

If you're having trouble reading this, [click here](#).

---

# The Daily 202



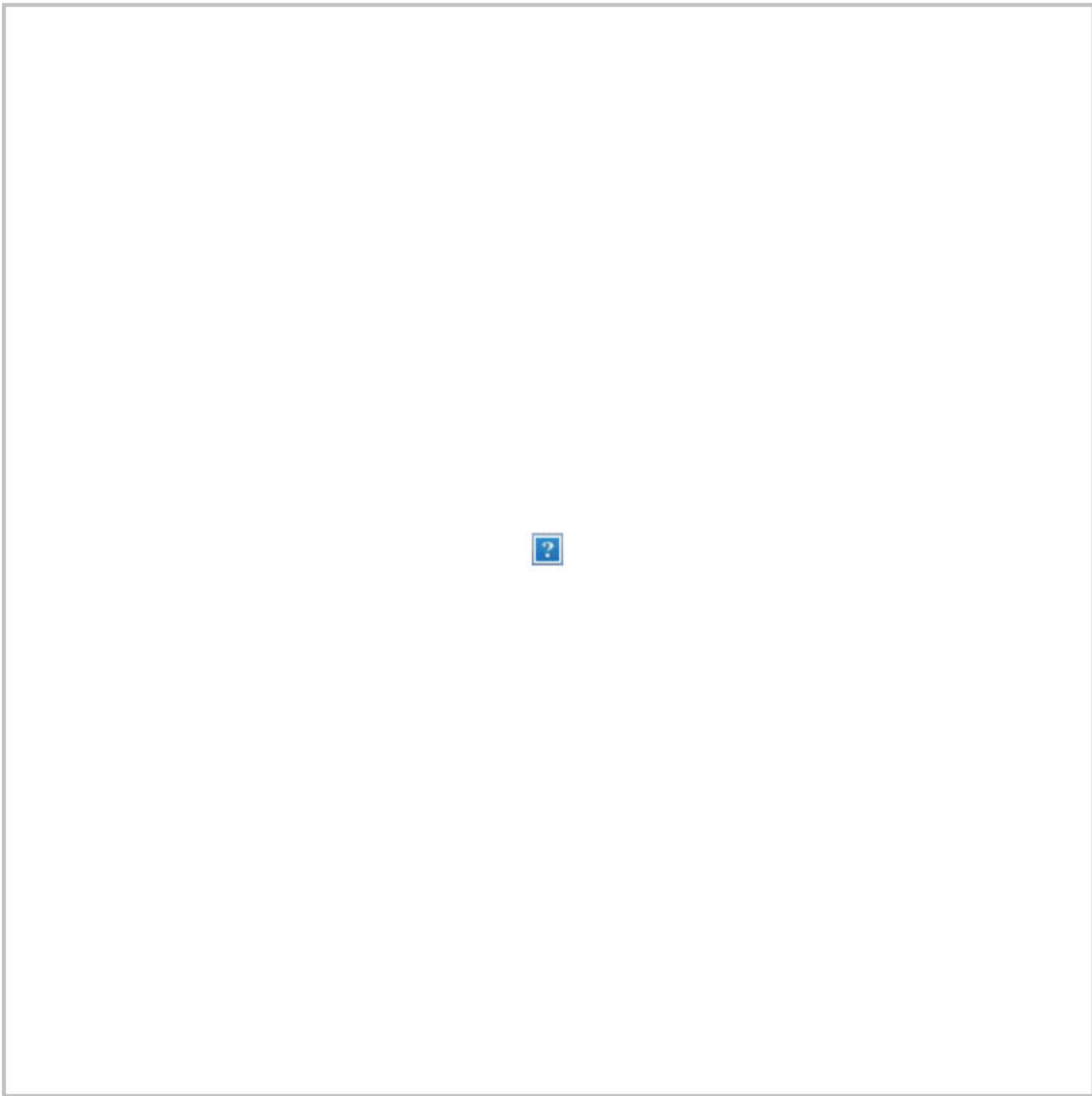
Share:  

 Listen to The Big Idea



## Senate rebuke of Trump on Yemen shows

# Congress, not just the president, can offer moral leadership



Senate rebukes Saudi Arabia, defies Trump with back-to-back votes



**BY JAMES HOHMANN**

*with Joanie Greve*

**THE BIG IDEA:** American presidents have historically embraced – sometimes with gusto and sometimes reluctantly – their unofficial role as chief spokesman



**for the free world, a soft power that comes with leading what Ronald Reagan called the “shining city upon a hill.” Not President Trump.**

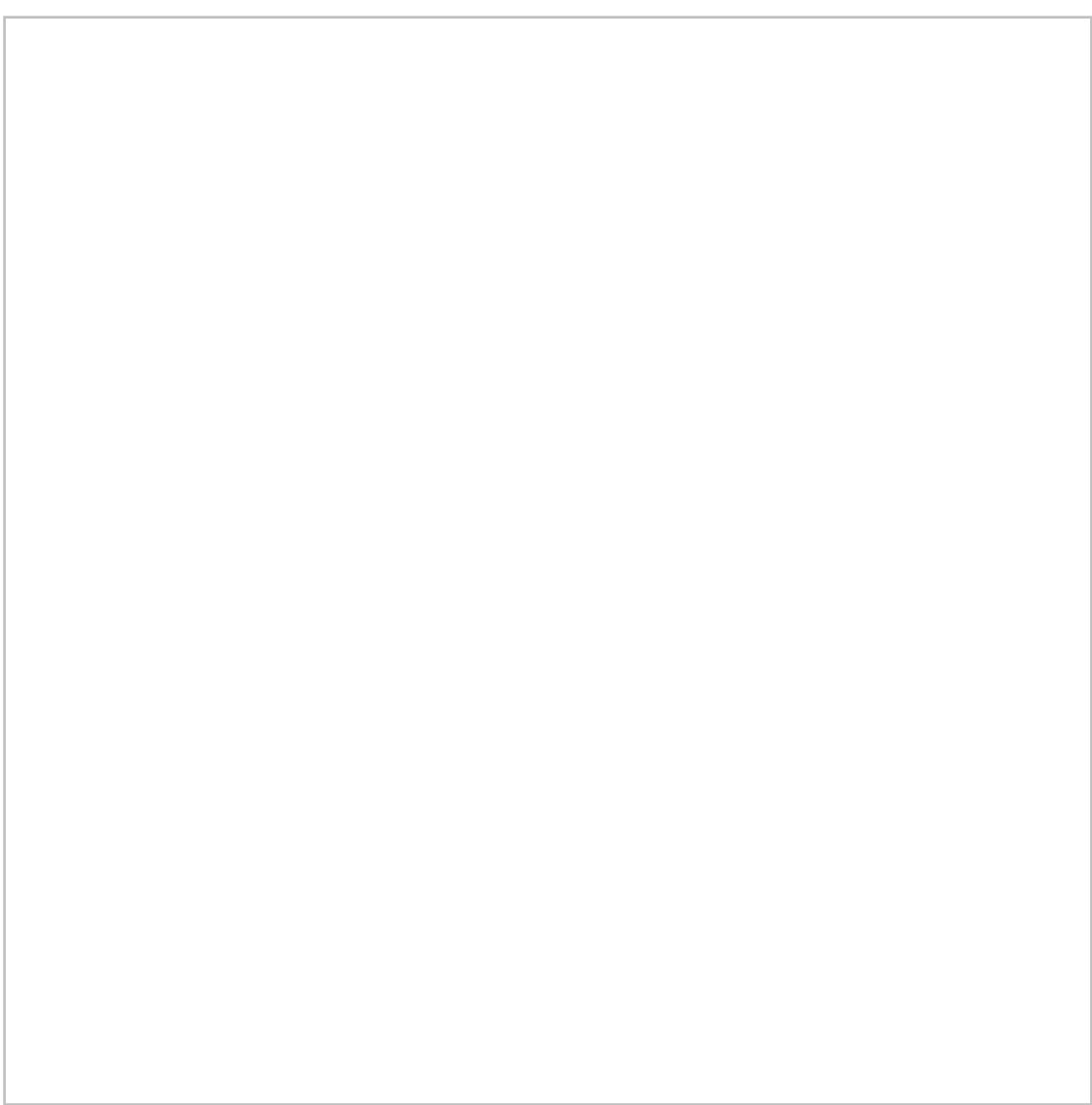
Trump, who spoke of “[American carnage](#)” in his inaugural address, seems plainly [uninterested](#) in seizing the mantle of moral leadership on the global stage. He’s consistently displayed a [Hobbesian](#) and Machiavellian approach to power politics during his nearly two years in office, [eschewing](#) the pillars of Lockean, Wilsonian and Reaganite thought while deemphasizing the promotion of democracy and human rights as aims of U.S. foreign policy.

His [blase responses](#) this fall to the [killing](#) of Washington Post contributing columnist Jamal Khashoggi and what the United Nations calls the world’s worst humanitarian crisis in Yemen have put in stark relief Trump’s abdication of that traditional moral leadership role.

**On Thursday afternoon, a bipartisan coalition in Congress moved to fill the void and perform this function of the presidency that Trump has essentially outsourced. [Senators voted 56-to-41](#) to cut off U.S. military support for Saudi Arabia’s often brutal conduct in the Yemen civil war. It’s the first time either chamber of Congress has asserted itself against the executive branch by using the War Powers Act, which became law during the depths of the Vietnam quagmire in 1973.**

A few minutes later, the Senate voted unanimously to approve a separate, [nonbinding resolution](#) that blames Crown Prince Mohammed bin Salman for what happened to Khashoggi. The CIA concluded that MBS, as he's known, probably ordered and monitored the dismemberment of the dissident journalist inside a Saudi consulate in Istanbul on Oct. 2. But Trump has touted the authoritarian prince's denials and sought to play down the expert assessment of his own intelligence community. There's even a tape.

“Unfortunately, at a moment in which it is most needed, the Trump administration has abdicated America’s moral leadership,” said Sen. Mark Warner (D-Va.), the vice chair of the Intelligence Committee. “In filling that void, and in light of the actions by the Saudis both in Yemen and in Khashoggi’s murder, the Senate must send a message that America’s moral voice will not be diminished.”



Sens. Bernie Sanders (I-Vt.), Mike Lee (R-Utah) and Chris Murphy (D-Conn.) celebrate at the Capitol after the Senate voted to end U.S. military support for the Saudi-led war in Yemen. (Jim Lo Scalzo/EPA-EFE)

**-- Thursday's vote was a personal and political triumph for three senators across the ideological spectrum who have made ending the war in Yemen their shared cause. Each believes strongly in the profound power of American moral leadership, and that Congress should reclaim the power to make war that the framers of the Constitution intended. Sen.**

Mike Lee (R-Utah), one of the most conservative members of the Senate, forged an alliance last year with Sen. Bernie Sanders (I-Vt.), a self-described democratic socialist, and Sen. Chris Murphy (D-Conn.), who is primarily known for advocating stricter gun control, to figure out ways to get the United States out of Yemen. They introduced the resolution that passed yesterday (with amendments) early in the year, but it was tabled in March. Khashoggi's heinous death created momentum to get it on the floor.

**“Today was a victory for the Constitution and the separation of powers,”** said Lee, who secured support from six of his GOP colleagues for the war powers resolution. “With this vote, we are one step closer to reviving our constitutional framework – where the power to declare war lies with Congress, not the executive branch – and we have taken a step towards removing ourselves from the spread of human suffering in Yemen.”

“For decades, under Republican presidents and Democratic presidents, Republican congresses and Democratic congresses, **the Congress of the United States has abdicated its constitutional responsibility for war-making,**” said Sanders. “It is not the president who has the responsibility under the Constitution to send our young men and women to war. It is the Congress. And we have got to take it back.”

“A bipartisan majority spoke with one voice that the status quo is over, and we will no longer accept the war crimes being committed in our name,” said Murphy. “The momentum is on one side, and it’s only growing.

**Congress has woken up** to the reality that the Saudi-led Coalition is using U.S. military support to kill thousands of civilians, bomb hospitals, block humanitarian aid and arm radical militias. The Saudis are important partners, but they need to realize that our partnership is not a blank check for them to fund extremists and murder civilians.”



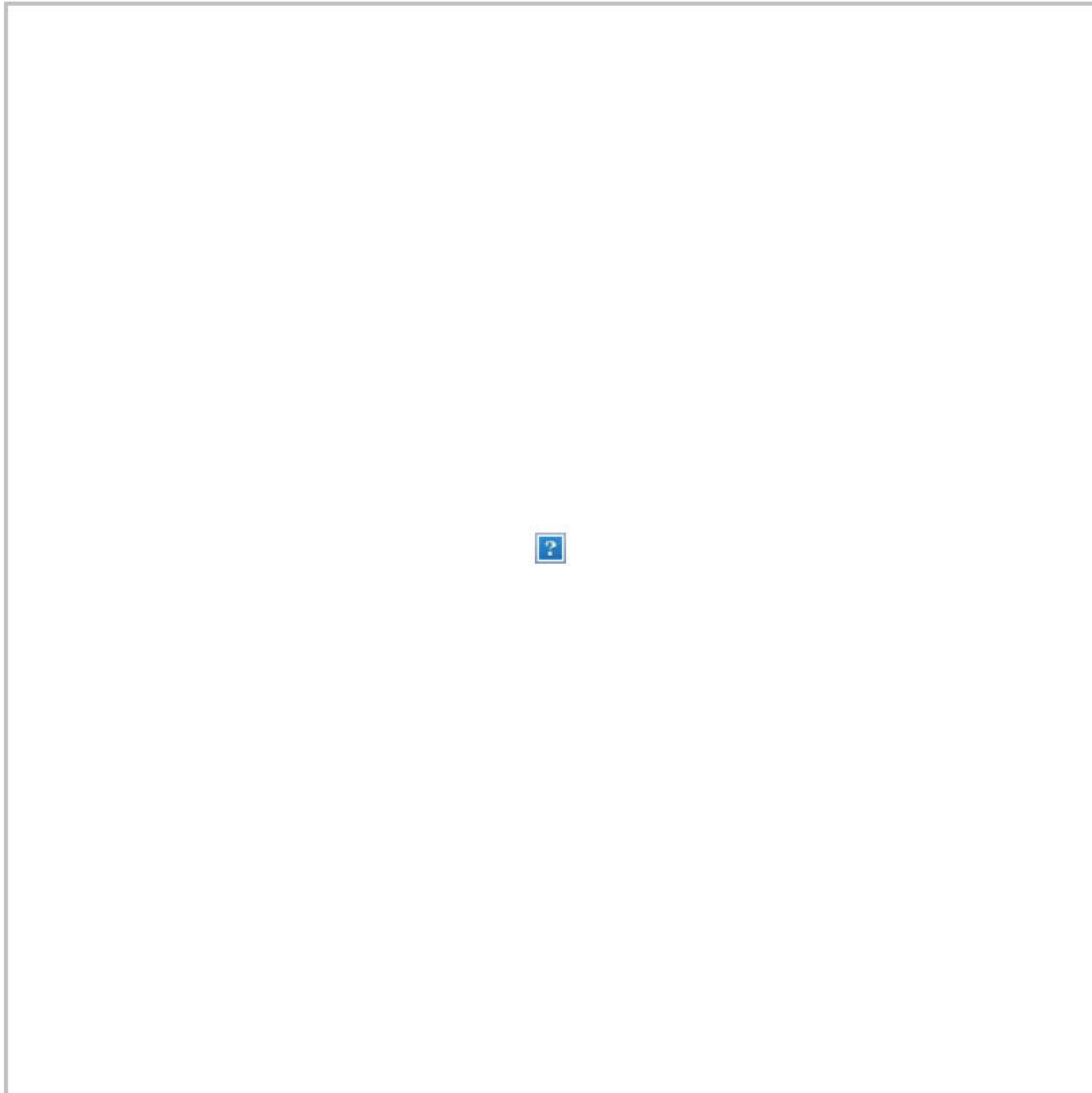


**-- House Republicans plan to ignore the war powers measure, and the White House has indicated Trump will disregard the nonbinding resolution, but the Senate debate appears to have had some impact at the negotiating table.**

A broader campaign of international pressure from the West has pushed the Saudis to make concessions in peace talks after four years of fighting. The United Nations has brokered negotiations in Sweden this week between Yemen's Saudi-backed government and the Houthis, the Iran-backed rebel group. **The two sides agreed yesterday to a cease-fire in the port city of Hodeida, which serves as a critical lifeline for humanitarian aid into the country.** They also apparently settled on terms for a prisoner swap. "We are living the beginning of the end of one of the biggest tragedies of the 21st century," U.N. Secretary-General António Guterres told reporters.

"Previous cease-fire agreements have collapsed quickly. But there has been greater international pressure on the warring sides in recent months to de-escalate the fighting, in part because of warnings by relief agencies that **more than 16 million people in Yemen — more than half of the country's population — are facing famine-like conditions,**" [Kareem Fahim and Missy Ryan report from Riyadh](#). **"More than 60,000 people,**

**combatants and civilians, have been killed in the conflict since 2016, according to an estimate by the Armed Conflict Location and Event Data Project.”**



Four-year-old Rakan used to weigh 40 pounds. Now he weighs 9 pounds.

**-- Many senators said they hope the resolution accelerates peace talks by putting Saudi Arabia on notice that they cannot count on unquestioning American support. “There must be a negotiated end to the fighting in Yemen, and the Saudi government must clearly understand that as a strategic ally of the United**

States, it has a responsibility to act in ways that promote democracy, human rights and stability in the region,” said Sen. Rob Portman (R-Ohio). “[W]e must send a message to the administration that we need a stronger response on this issue.”

“After reviewing the overwhelming evidence, it is clear that **the Saudi-led coalition’s actions in Yemen are no longer something we, as the leader of the free world, can support,**” added Sen. Joe Manchin (D-W.V.). “This resolution ... sends a clear message ... that the United States will no longer tolerate their disregard for human life.”



Women in war-torn Yemen uproot their families, and the children are traumatized

**-- Paul Ryan, doing the bidding of the administration in one of his final acts as speaker, jammed language into the farm bill on Wednesday that will prevent the House from using the War Powers Act during the remainder of the lame-duck session to cut off U.S. support for the Saudi effort in Yemen.**

“It's a common technique in the House: An unpopular measure is snuck into something that must pass. The

gimmick worked, but only because five Democrats who had worked on the farm bill broke with their party to support it,” [Dave Weigel reports](#). “In the new Democratic Party, that meant that five more Democrats were being talked about as targets for primary challenges. Alexandra Rojas, whose group Justice Democrats is recruiting challengers in 2020 House races, said the farm bill vote had galvanized activists who were on the verge of winning the Yemen fight.”



CONTENT FROM BANK OF AMERICA

## How to finance a cleaner planet



In 2018, Bank of America issued its fourth and largest green bond for \$2.25 billion. Learn more about this innovative way of financing a more sustainable future.

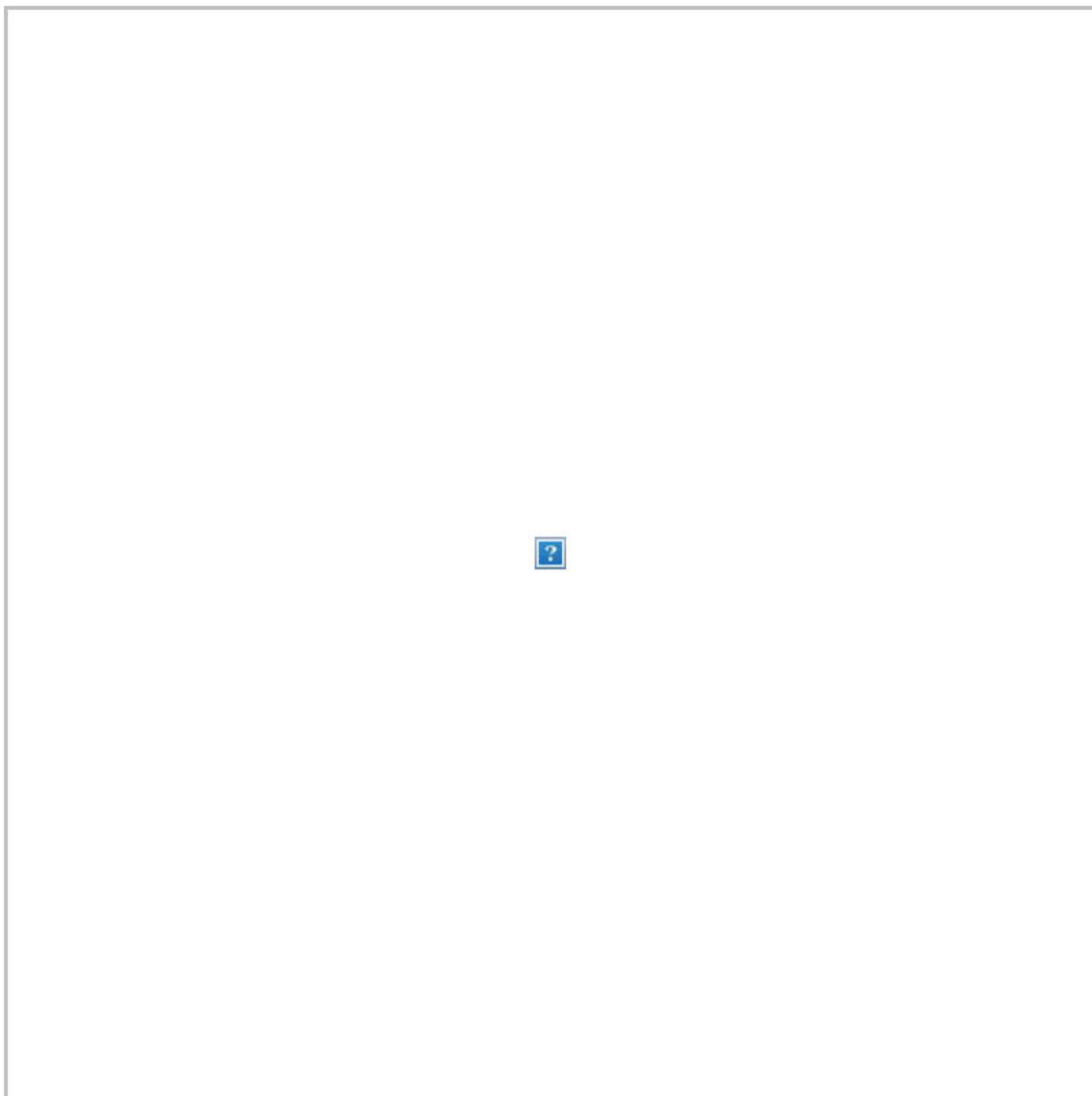


As war rages, children languish in Aden

-- But the comfortable margin in the Senate showed how much juice [the well-heeled Saudi lobby](#) has lost and could be a harbinger of what's to come once Democrats control the House, from implementing sanctions to curtailing arms sales to Riyadh.

“American foreign policy should be dictated by our national security interests and our values, not by the interests of the Saudi royal family,” said Sen. Maggie Hassan (D-N.H.).

“We won’t enable a president who chooses to cover up for Saudi leadership instead of standing up for American values,” added Sen. Tim Kaine (D-Va.).



As men fight and die in Yemen's civil war, wives and mothers are left to carry on

**-- How it's playing:**

- [The Washington Post Editorial Board](#): **“The Trump administration won’t stand for Khashoggi. It could at least stand for jailed Saudi women.”**
- Katherine Zoeph in [the New York Times](#): **“The Saudi Regime’s Other Victims. The murder of Khashoggi has focused attention on Saudi Arabia’s human rights abuses. We need to remember all of the thousands in prison.”**
- [The Wall Street Journal](#): **“Saudi Arabia Pumps Up Stock Market After Bad News**, Including Khashoggi Murder. The government of Crown Prince Mohammed bin Salman has spent billions to counter selloffs in recent months.”
- [The Fix](#): **“The entire Senate just said Trump is wrong about Khashoggi.”**
- [The Economist](#): **“Trump’s efforts to boost the Saudi alliance risk damaging it.”**
- [Washington Monthly](#): **“We Should Have Reevaluated Our Saudi Alliance Before Now.”**
- [The Nation](#): **“What the Hell Is Wrong With Paul Ryan?** It is outrageous that the House Speaker continues to block action to end US support for Saudi atrocities against Yemen.”
- [Breitbart](#): **“Paul Ryan’s Last Act: Protecting Barack Obama’s Illegal War in Yemen with Democrat Votes.”**
- [HuffPost](#): **“5 Democrats Bail Out Paul Ryan And Protect Saudi Arabia.”**
- Sen. Marco Rubio (R-Fla.) op-ed for [Fox News](#):

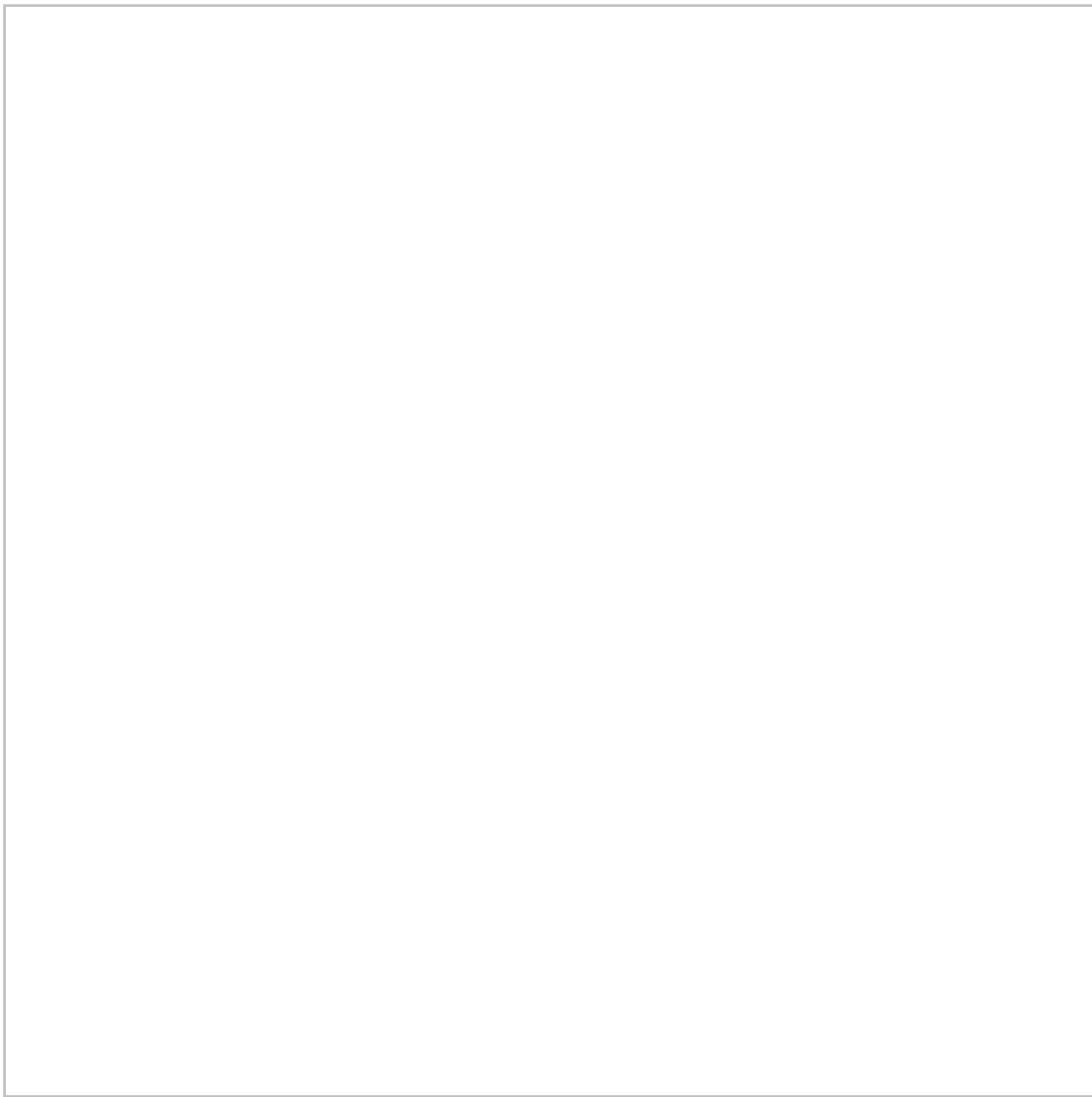
**“Hold Saudis accountable, but don't ignore Iran in Yemen.”**

- [Haaretz](#): “Benjamin Netanyahu on Khashoggi Murder: Destabilizing Saudi Arabia Would Destabilize the World.”
- John Hanna, who served as Vice President Dick Cheney’s national security adviser, writes in [Foreign Policy](#): **“Neither Side Gets the Khashoggi Debate Right.** The tribalism infecting U.S. domestic politics has unfortunately crept deep into the foreign-policy discourse.”

**-- This new street sign has just been erected outside our headquarters:**



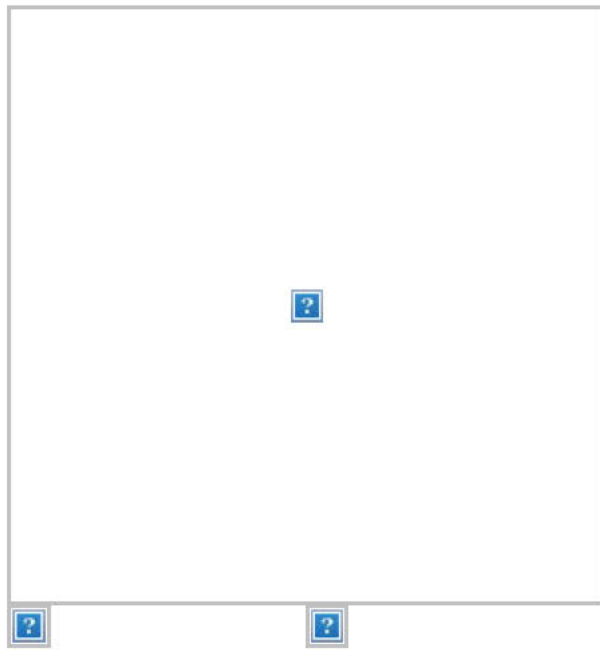




Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



**WHILE YOU WERE SLEEPING:**



Not just misleading. Not merely false. A lie. | Fact Checker

**-- Trump's insistence for much of the year that he had "no knowledge of any payments" to silence the women who allege they carried on extramarital affairs with him while the first lady was home caring for their infant son tops The Post Fact Checker's list of "the biggest Pinocchios of 2018." [Glenn Kessler explains](#):** "There has been no serial exaggerator in recent American politics like the president. He not only consistently makes false claims but also repeats them,

even though they have been proved wrong. The explosion of false and misleading statements from him in 2018 is well documented in our database: **In the seven weeks leading up the midterm elections, the president made 1,419 false or misleading claims — an average of 30 a day.** ... Meanwhile, the midterm election campaign, of course, was also an endless source of false claims, as an avalanche of negative ads tumbled across televisions screens. One of the president's ads is included on this list. Two potential opponents of the president in 2020 — Sens. Kamala D. Harris (D-Calif.) and [Bernie] — earn spots on our list. ...

**“Trump says many things that are factually incorrect, but he sometimes says things that are mind-blowingly false.** Despite having access to more information than anyone on Earth, he persists in making claims with literally no foundation. He has repeatedly claimed that U.S. Steel announced it is building new plants — anywhere from six to nine — but that's not true. He said that as president, Barack Obama, gave citizenship to 2,500 Iranians during the nuclear-deal negotiations, but that's not true. Over and over, Trump claimed that the Uzbek-born man who in 2017 was accused of killing eight people with a pickup truck in New York brought two dozen relatives to the United States through ‘chain migration.’ The real number is zero.

**“Trump and his aides claimed they did not have a**

**family separation policy, when in fact they did.** They said U.S. laws or court rulings forced them to separate families that crossed the border illegally, but that was not true. When a caravan of more than 5,000 migrants from Central America started making its way to the border, another series of dubious claims was spawned, including that people of Middle Eastern descent were involved. The president also falsely claimed that he had started building his border wall, but Congress has not appropriated the necessary funds.”





Sens. Bernie Sanders (I-Vt.) and Elizabeth Warren (D-Mass.) walk to the Senate floor after the weekly Democratic caucus policy luncheon. (Jonathan Ernst/Reuters)

## GET SMART FAST:

1. **Elizabeth Warren invited Bernie Sanders over for dinner at her D.C. condo to discuss their presidential ambitions.** Both acknowledged their likely 2020 bids, but neither senator sought the other's support or tried to dissuade the other from running. No staffers were allowed. ([New York Times](#))
2. **French police said they “neutralized” a person matching the description of the suspect in the Strasbourg Christmas market shooting.** An official in the Paris prosecutor's office told a French newspaper that the person caught was named Cherif Chekatt and that he's now dead. ([James McAuley](#))
3. **Actress Eliza Dushku received a confidential \$9.5 million settlement from CBS stemming from a sexual harassment complaint.** Dushku claimed she was retaliated against for confronting “Bull” actor Michael Weatherly about inappropriate comments he made. ([New York Times](#))
4. **News organizations with Australian operations largely declined to report on Cardinal George Pell's conviction on sexual abuse charges out of concern over the judge's gag order.** The judge in

the case, Peter Kidd, said some journalists are facing “the prospect of imprisonment and indeed substantial imprisonment” for violating the order. But many outlets outside of Australia, including The Washington Post, covered the conviction. ([Paul Farhi](#))

5. **The Kentucky Supreme Court unanimously struck down the state's pension reform law.** In a major defeat for Gov. Matt Bevin (R), the court ruled that the bill's speedy passage violated a provision in the Kentucky constitution requiring that lawmakers have a “fair opportunity” to consider legislation before voting on it. ([Louisville Courier Journal](#))
6. **Fed chairman Jay Powell has been emphasizing recently that the strong U.S. economy masks “important disparities by income, race and geography.”** In a sign of how economic benefits have not been evenly distributed, 4 in 10 American adults still say they could not cover a \$400 emergency expense. ([Heather Long](#))
7. **A former Special Forces soldier who was once awarded a Silver Star for his valor is facing a murder charge in connection to the 2010 killing of a suspected Taliban bombmaker.** Army Maj. Mathew L. Golsteyn allegedly said during a 2011

polygraph test while applying to the CIA that he killed the man, according to Army documents. ([Dan Lamothe](#))

8. **Indiana police said they prevented a potential mass shooting at a middle school after receiving a tip about the teenage suspect.** Officers exchanged gunfire with the suspect, who allegedly had plans to attack Dennis Intermediate School in Richmond, Ind., before he killed himself. ([Moriah Balingit and Mark Berman](#))
9. **A former Baylor University fraternity president who was accused of raping a young woman but received no jail time was barred from attending his commencement ceremony.** The University of Texas at Dallas added that Jacob Anderson is banned from campus following public outcry over his lenient sentence. ([Katie Mettler, Eli Rosenberg and Kristine Phillips](#))
10. **A California man who was trapped in the grease vent of a Chinese restaurant for two days was rescued by firefighters.** The man was hospitalized for dehydration and exhaustion but is expected to recover, while police officers have opened a trespassing and vandalism investigation. ([Amy B Wang](#))



Donald Trump takes the oath of office from Chief Justice John G. Roberts Jr. (Jim Bourg/Pool/AP)

## **THERE'S A BEAR IN THE WOODS:**

**-- Trump's 2017 inaugural committee is being investigated by federal prosecutors for possible misuse of funds. [The Wall Street Journal's Rebecca Davis O'Brien, Rebecca Ballhaus and Aruna Viswanatha report](#): "The criminal probe by the Manhattan U.S. attorney's office, which is in its early stages, also is**

**examining whether some of the committee's top donors gave money in exchange for access to the incoming Trump administration, policy concessions or to influence official administration positions.**

Giving money in exchange for political favors could run afoul of federal corruption laws. Diverting funds from the organization, which was registered as a nonprofit, could also violate federal law. ... **The investigation partly arises out of materials seized in the federal probe of former Trump lawyer Michael Cohen's business dealings** ... In April raids of Mr. Cohen's home, office and hotel room, [FBI] agents obtained a recorded conversation between Mr. Cohen and Stephanie Winston Wolkoff, a former adviser to Melania Trump, who worked on the inaugural events. In the recording, Ms. Wolkoff expressed concern about how the inaugural committee was spending money. ...

"The inaugural committee has publicly identified vendors accounting for \$61 million of the \$103 million it spent, and it hasn't provided details on those expenses, according to tax filings. As a nonprofit organization, the fund is only required to make public its top five vendors. **The committee raised more than double what former President Barack Obama's first inaugural fund reported raising in 2009, the previous record.**

[Trump's] funds came largely from wealthy donors and corporations who gave \$1 million or more — including casino billionaire Sheldon Adelson, AT&T Inc. and



Boeing Co.”

**-- The prosecutors are investigating whether the inaugural committee, as well as a pro-Trump super PAC, accepted illegal foreign donations, [according to the New York Times’s Sharon LaFraniere, Maggie Haberman and Adam Goldman](#).** “The inquiry focuses on whether people from Middle Eastern nations — including Qatar, Saudi Arabia and the United Arab Emirates — used straw donors to disguise their donations to the two funds. Federal law prohibits foreign contributions to federal campaigns, political action committees and inaugural funds. ... Thomas J. Barrack Jr., a billionaire financier and one of Mr. Trump’s closest friends, raised money for both funds. ... The super PAC, Rebuilding America Now, was formed in the summer of 2016 when Mr. Trump’s presidential campaign was short of cash and out of favor with many major Republican donors.”

**-- Multiple news outlets have now confirmed that Trump himself was at the August 2015 meeting where Cohen and National Enquirer publisher David Pecker discussed hush-money payments to the president's alleged mistresses.** The Wall Street Journal first reported the president’s attendance at the meeting last month. [NBC News’s Tom Winter reports:](#) “As part of a nonprosecution agreement disclosed Wednesday by federal prosecutors, American Media Inc., the Enquirer's parent company, admitted that ‘Pecker

offered to help deal with negative stories about that presidential candidate's relationships with women by, among other things, assisting the campaign in identifying such stories so they could be purchased and their publication avoided.' The 'statement of admitted facts' says that AMI admitted making a \$150,000 payment 'in concert with the campaign,' and says that Pecker, Cohen and 'at least one other member of the campaign' were in the meeting. According to a person familiar with the matter, the 'other member' was Trump."

**-- In his first interview since being sentenced, Cohen said of the hush-money payments that Trump "was very concerned about how this would affect the election."** [John Wagner reports](#): "Cohen, who has admitted facilitating payments to two women in violation of campaign finance laws, told ABC News that he knew what he was doing was wrong. Asked whether the president also knew it was wrong to make the payments, Cohen replied, 'Of course.' He added that the purpose was to 'help [Trump] and his campaign.' ... His comments, in an interview on 'Good Morning America,' are at odds with those of Trump on Thursday in tweets and a television interview."

**-- "[The president's] evolving strategy on the hush-money allegations is textbook Trump: Tell one version of events until it falls apart, then tell a new version, and so on — until the danger passes,"** [Philip](#)

[Rucker and John Wagner report](#). “The latest developments have exposed the depth of Trump’s efforts to deceive the public about the illegal hush-money payments, and some of his friends and advisers said privately that they fear those efforts could imperil the president. While there is a consensus view inside the White House that a sitting president will not be indicted, [a] former senior administration official described a deep uncertainty about other ways that Trump could be held liable. And **there is growing anxiety among Trump’s allies, including in Congress, that he could be vulnerable to the various investigations and, eventually, Democratic-led impeachment proceedings.**”

-- The escalating investigations, aided by cooperation from Trump’s former allies, have left the president feeling increasingly isolated. [The Los Angeles Times’s Chris Megerian and Eli Stokols report](#): “Several [people] close to the president ... said Trump already senses diminishing respect and worries about losing support from powerful financial donors and Republican lawmakers as his legal and political troubles worsen. ‘They’re still not saying it publicly, but most Republicans on the Hill understand ... that it’s not going to end well, that it’s going to be bad,’ said a longtime Republican operative close to party leadership.”

-- The latest developments in the Russia

**investigation have reinvigorated claims from Trump's critics that his election victory was illegitimate.** [Marc Fisher reports](#): "The evidence emerging in recent days and months that multiple crimes were committed in an effort to help Trump win the presidency is fueling arguments from Democrats and other Trump critics that the man in the Oval Office got the job through nefarious means. Even with no proof that those crimes swayed votes, the critics say, Trump has no moral hold on the office. ... Trump and his defenders retort that prosecutors so far have fallen well short of proving criminal deeds by the president himself. They say the legitimacy debate is just one more weapon in a bristling partisan arsenal deployed by Trump haters on the left."

**-- Another threat: House Minority Leader Nancy Pelosi said she expects a House committee to "take the first steps" toward getting Trump's tax returns after Democrats retake the chamber next month.** [John Wagner reports](#): "Pelosi said the decision on whether to initiate the process will fall to the Ways and Means Committee. Rep. Richard E. Neal (D-Mass.), who is expected to become chairman of the tax panel, has said he plans to insist that Trump release his tax returns. If Trump doesn't do so voluntarily, then Neal plans to file a legal request with the Treasury secretary that would require that the returns be disclosed to a small group of people on Capitol Hill. Neal has predicted that the matter would end up in federal court."



How Maria Butina forged ties with gun rights advocates and other U.S. conservatives

**-- The guilty plea of Russian agent Maria Butina has cast an unwanted spotlight on the National Rifle Association, a group she allegedly infiltrated at the highest levels and whose legal exposure remains unclear. [Rosalind S. Helderman, Tom Hamburger and Michelle Ye Hee Lee report](#): “One of Butina’s main targets was the NRA — a group she identified in a 2015 memo as an organization that 'had influence**



**over' the Republican Party**, according to court filings. Her relationships with the group, she wrote, could be used as the groundwork for an unofficial channel of communication to the next presidential administration. Later that year, she helped organize a delegation of top NRA leaders to visit Moscow, arranging for them to meet Russian government officials, and she attended the group's annual conventions as an honored guest. Butina and Alexander Torshin, a former Russian government official who helped direct her activities, then used their NRA connections to get access to GOP presidential candidates."

**"NRA officials, who did not return requests for comment Thursday, have repeatedly refused to answer questions about Butina or its interactions with Russian activists.** NRA spending on the 2016 elections surged in every category, with its political action committee and political nonprofit arm together shelling out \$54.4 million. The bulk of the money — \$30 million — went to efforts supporting Trump. That is triple the amount the group devoted to electing Republican Mitt Romney in the 2012 presidential race. ... The group's spending on federal races in 2018 plummeted to roughly \$9 million."

**-- Mueller's pattern of getting guilty pleas from cooperating witnesses may suggest his investigation is nearing its end. [Devlin Barrett reports](#):** "In the cases

of Cohen, former campaign adviser George Papadopoulos, former campaign chairman Paul Manafort, and former national security adviser Michael Flynn, Mueller has proceeded to the sentencing of each without first making him testify at trial against others. That's at odds with the common practice of prosecutors — which is to hold the stick of a tougher prison sentence over defendants until they have completed all of their cooperation, particularly any public testimony. While the recent legal action has led to speculation that prosecutors are narrowing in on the president in anticipation of more criminal charges, **Mueller's sentencing timeline suggests a different outcome to some legal experts — that the accounts of those cooperating witnesses will appear in a written report, not in court."**

**-- The House and Senate Intelligence Committees are looking to talk to several people who have been charged in Mueller's investigation. [CNN's Jeremy Herb and Manu Raju report](#):** "The [Senate] committee has been engaged in discussions with the special counsel and defense attorneys to get access to several cooperating Mueller witnesses in addition to Cohen, including Flynn, Papadopoulos and [Manafort's deputy Rick] Gates, according to a source familiar with the investigation. ... The expected incoming chairman of the House Intelligence Committee, Democratic Rep. Adam Schiff of California, has also expressed a desire to speak



again to Cohen, who testified behind closed doors before both intelligence panels last year. Schiff has said he's in touch with Cohen's legal team, too."

**-- Friends and associates of Michael Flynn agree that his public persona underwent a radical transformation in the past few years, but they are divided as to why. [Marc Fisher writes](#) in an in-depth piece on Trump's former national security adviser: "His friends and critics agree that after winning a reputation as a master intelligence officer on the battlefields of Iraq and Afghanistan, Flynn broke with lifelong patterns of behavior. Once discreet and apolitical, he morphed into a highly partisan alarm ringer. A man once trusted to cautiously analyze information began touting wild hearsay as fact. ... Did he gradually absorb a new, conspiracy-minded worldview, in part inspired by his son Michael Jr.'s embrace of fringy ideas? Did he discard lifelong habits because he'd been enraged to his core when President Barack Obama's administration in 2014 removed him as director of the Defense Intelligence Agency (DIA), his last and most senior military assignment? Or had Flynn, who retired as a lieutenant general, long harbored extreme views, successfully shielding his real opinions from those around him?"**



Children join a protest in the Senate Hart Building on the day of the court-imposed deadline for the Trump administration to return migrant children who were separated from their parents. (Salwan Georges/The Washington Post)

## **THE IMMIGRATION WARS:**

**-- Stories from the border: A 7-year-old girl from Guatemala died of dehydration and exhaustion after she was taken into Border Patrol custody last week. [Nick Miroff and Robert Moore report](#): “The child’s death is likely to intensify scrutiny of detention conditions at**



Border Patrol stations and CBP facilities that are increasingly overwhelmed by large numbers of families seeking asylum in the United States. According to CBP records, the girl and her father were taken into custody about 10 p.m. Dec. 6 south of Lordsburg, N.M., as part of a group of 163 people who approached U.S. agents to turn themselves in. More than eight hours later, the child began having seizures at 6:25 a.m., CBP records show. **Emergency responders, who arrived soon after, measured her body temperature at 105.7 degrees, and according to a statement from CBP, she ‘reportedly had not eaten or consumed water for several days.’** ... The agency is investigating the incident to ensure appropriate policies were followed.”

-- Trump pledged to do “whatever it takes to get border security,” even as he tried to shift blame toward Democrats for any potential government shutdown. [Erica Werner, Damian Paletta and John Wagner report](#): “In a video posted on Twitter, Trump attacked Democrats as ‘absolute hypocrites’ and claimed they’ve supported funding border barriers in the past but won’t do so now because of their opposition to him. The video showed images of people rushing the border and included clips of [Chuck Schumer], former secretary of state Hillary Clinton and [Barack Obama] speaking in opposition to illegal immigration and in favor of border security. ‘We need to have the wall. We need border security. Whatever it takes to get border security, I will do



it,' Trump says in the video. 'I pledged that a long time ago, and I will pledge it always.'" Reminder: Trump said just three days ago [he would be "proud"](#) to shut the government down over wall funding.

**-- Lawmakers say no progress has been made on a border wall deal since Trump had his contentious meeting with Schumer and Pelosi. [Politico's Sarah Ferris, Burgess Everett and Anthony Adragna report:](#)**

"Lawmakers say there is no public plan to prevent a partial government shuttering. And no secret plan either. 'There is no discernable plan. None that's been disclosed,' said Sen. John Cornyn, the Senate's No. 2 Republican, as he threw his hands into the air. ... The House isn't planning to return until the night of Dec. 19 — leaving only about 72 hours to reach a border wall deal that has eluded both parties for months. **Democrats say they're waiting on Republicans, and Republicans say they're waiting on Trump.**"

**-- In case you missed it: ICE has arrested 170 immigrants who sought to sponsor migrant children. [NBC News's Daniella Silva reports:](#)** "ICE said Tuesday that the arrests were of immigrants suspected of being in the United States illegally and took place from early July to November. They were the result of background checks conducted on potential sponsors of unaccompanied migrant children placed under the care of the Department of Health and Human Services. Nearly two thirds of those

arrested — 109 in total — had no criminal record, the agency said. Another 61 of those arrested did have criminal records, but ICE did not specify the crimes and said it could not break down convictions by violent and nonviolent offenses.”

**-- DHS issued a news release entitled, “Walls Work,” which included questionable claims about the progress being made on Trump’s border wall. [USA Today’s William Cummings reports](#): “DHS is committed to building wall and building wall quickly,’ reads the release, which eschews the use of articles in many instances. ‘We are not replacing short, outdated and ineffective wall with similar wall. Instead, under this President we are building a wall that is 30-feet high.’ ‘FACT: Prior to President Trump taking office, we have never built wall that high,’ the message adds. The government has built higher walls, but the statement presumably meant to specify it was referring to a border wall.”**



Ivanka Trump departs Air Force One with Jared Kushner in Coraopolis, Pa. (Keith Srakocic/AP)

## **WEST WING INTRIGUE:**

**-- Trump is considering his son-in-law Jared Kushner for White House chief of staff, according to [HuffPost's S.V. Date](#):** “[Kushner] met with Trump Wednesday about the job, a top Republican close to the White House [said]. He and two others close to Trump or the White House ... confirmed Kushner’s interest in the position. ... Kushner



has been pushing his own candidacy with Trump, citing his work on a criminal justice reform package and a claimed ability to work with Democrats, one person said. 'I don't know why he thinks that, when the Democrats are mainly going to be coming after Trump,' the source said. ... **Trump told reporters Thursday that he is down to five finalists.** 'We are interviewing people now for chief of staff,' he said at a photo opportunity with newly elected governors who were visiting the White House."

-- **Trump also met with former New Jersey governor Chris Christie about the job last night, [per Axios's Jonathan Swan](#).** "[Trump] considers him a top contender to replace John Kelly as chief of staff, according to a source. ... Trump has met with a couple of others, but the way he's discussed Christie to confidants make them think he's serious. His legal background may come in handy next year."

-- **Some advisers are encouraging Trump to consider young White House aide Johnny DeStefano for chief of staff. [The LA Times's Eli Stokols reports:](#)** "Several people close to the president are promoting [DeStefano], who was a political aide to former House Speaker John A. Boehner before joining the administration as Trump's director of personnel. He since has seen his portfolio expand and often travels with the president."

-- **The president's top aides remain deeply divided**

**over whether Trump's former deputy campaign manager David Bossie should be considered for the job.** [Politico's Gabby Orr, Andrew Restuccia and Rebecca Morin report](#): "Some White House allies say [Bossie] shot to the top of the list the minute Trump expressed an interest in having an effective political operator in the slot. His chances only improved, they add, when Rep. Mark Meadows (R-N.C.), head of the conservative Freedom Caucus, fell out of the running. But others quickly dismiss the speculation, saying the Trump world adviser can't overcome opposition within the first family and lingering concerns about a hotheadedness that kept him out of the West Wing to begin with."

**-- "Trump's hunt for a new chief of staff has taken on the feel of a reality TV show,"** [the AP's Catherine Lucey and Jonathan Lemire write](#). "No leading name has emerged in the days since Trump's preferred candidate to replace John Kelly bowed out. But the void has quickly filled with drama. ... Trump himself likes to feed the drama, dropping hints about the number of candidates in the running and bantering with journalists about who wants the job. The erratic search recalled the transition period before Trump took office, when prospective aides and television personalities paraded before a pack of journalists in the lobby of Trump Tower. Author Chris Whipple, an expert on chiefs of staff, called the search process 'sad to watch.'"





Pelosi 'comfortable' with term-limit deal

**IF YOU COME AT THE QUEEN, [YOU BEST NOT MISS:](#)**

**-- There are two deeply reported tick-tocks this morning on how Nancy Pelosi locked down the votes to become speaker. Both focus on the many strategic and tactical mistakes made by Rep. Seth Moulton (D-Mass.), the ringleader of the rebels trying to take her down. The hyper-ambitious Moulton has become a lightning rod, and Pelosi allies — including some of the**

biggest donors in the Democratic Party — are now determined to field a primary challenger against him in 2020.

-- **“Moulton had drawn up list of 58 Democrats who he knew wanted a new leader. Most of those, he said he believed, would sign a letter expressing opposition to Pelosi. ... Instead of 35 names, the rebels ultimately released a letter Nov. 19 with only 16 names,”** [Mike DeBonis and Robert Costa report](#). “‘A lot of summer soldiers around here,’ Moulton, a former Marine Corps officer, would say.

- “When during a CNN appearance he accused Pelosi of not moving aggressively on gun-control legislation during her previous time as speaker, her aides lined up gun-control advocates to criticize him.
- “He annoyed other members of the group by issuing a statement two days before the nominating vote declaring that he was willing to negotiate with Pelosi about the broader leadership team, upending their strategy.
- “Other members of the rebel group urged Rep. Kathleen Rice (D-N.Y.) to take a more aggressive role as a female face of the anti-Pelosi effort, but she bristled at being asked to step forward as a token woman — especially by Moulton, whom she blamed for strategic missteps.”

-- “Moulton told his colleagues that he’d win over the incoming freshmen, even referring to these lawmakers as ‘my candidates,’ according to multiple Democratic sources,” [per Politico’s Rachael Bade, Heather Caygle and John Bresnahan](#). “Moulton had a personal connection to the anti-Pelosi candidates who had military backgrounds. He campaigned with them, raised money for them and worked alongside VoteVets, a progressive political organization supporting veterans running for office, to try to get them elected. Moulton told these members-elect that Pelosi was going to be ousted and that it would be good for them politically to join the movement. But **Moulton oversold his sway, rebel sources complained**. Rep.-elect Mikie Sherrill, a former Navy helicopter pilot running in New Jersey, had released an ad against Pelosi and campaigned with Moulton. But she wouldn’t go anywhere near the letter. Several other freshmen who received help from Moulton also avoided the letter.

“**Pelosi had neutered Moulton right under his nose**. Just days after the election, she phoned VoteVets’ Chairman Jon Soltz and asked for his help wooing the incoming freshmen. Soltz had been working with Moulton but also had a close relationship with Pelosi. Soltz decided his group would remain neutral. But he gave the candidates advice that proved critical to helping Pelosi, sources said: Think about the long game. To be an effective legislator, you will have to work with the next



speaker — which more likely than not would be Pelosi. The advice worked. The candidates refused to sign the rebels' document. And when Moulton lobbied harder for their signatures, he repelled them even more. In fact, **some female veterans told other Democrats that they were annoyed with Moulton, these lawmakers said, concluding that they were being used for Moulton's own political gain. ...**

**“He asked for a meeting with Pelosi to start talks between the two sides — then misled his fellow rebels about who initiated the discussion, according to three sources familiar with the incident.** Moulton told [Rice] and Rep. Tim Ryan (D-Ohio) — perhaps Pelosi's staunchest critics in the group — that Pelosi requested the meeting. In reality, he had gone to Pelosi's staff and said he wanted to sit down. It created an awkward dynamic before a terrible meeting. Rice walked into Pelosi's office and said, ‘Thank you for calling this meeting.’ ‘I didn't ask for this meeting,’ Pelosi scoffed. An awkward silence ensued, and the meeting unraveled from there.”

**-- The term-limit deal Pelosi negotiated has once again cast a spotlight on her complicated relationship with her No. 2, Steny Hoyer (D-Md.). [The New York Times's Sheryl Gay Stolberg reports](#):** “The friction goes back decades. The last time Democrats took power from Republicans, in 2006, Ms. Pelosi backed

then-Representative John P. Murtha in his effort to oust Mr. Hoyer from the majority leader's slot. The putsch failed spectacularly, but she's ready to handcuff him again with a deal on term limits. ... Some see Mr. Hoyer as the ultimate corporate pol, out of sync with a Democratic caucus in which women, millennials and people of color are in ascendance, with the loudest new voices on the left. ... But over his more than 50 years in public life, 37 of them in Congress, Mr. Hoyer has proved himself a quiet survivor."





## **MIDTERMS FALLOUT:**

**-- GOP congressional candidate Mark Harris directed the hiring of the operative now at the center of election fraud allegations in North Carolina, despite warnings about his tactics.** [Amy Gardner and Beth Reinhard report](#): “Harris sought out the operative, Leslie McCrae Dowless, after losing a 2016 election in which Dowless had helped one of Harris’s opponents win an overwhelming share of the mail-in vote in a key county. State and local investigators say that whether Harris knew that his campaign may have engaged in improper tactics has become a focus of the expanding probes into whether election irregularities affected the 9th District election, in which Harris leads Democrat Dan McCready by 905 votes. That question is also roiling the state Republican Party, whose leaders had rallied around Harris, a 52-year-old evangelical pastor from the suburbs of Charlotte. **Party leaders are now backing away from Harris and trying to limit the fallout** of a scandal that has delayed certification of the last undecided federal contest of the 2018 election cycle. ...

**“Harris was warned about possible fraud on primary day in June 2016,** during his first bid for the 9th District congressional seat, according to people familiar with the conversation. The incumbent congressman and winner of the primary had received just one mail-in vote in rural

Bladen County. Harris, who came in second place, had won four. Johnson, the last-place contender, meanwhile, had received nearly all of them — 221. The only explanation, advisers told Harris that night in Charlotte, was that something shady had occurred on that third-place campaign, according to the people. A year later, they said, when Harris resolved to run for Congress again, the candidate personally directed the hiring of Dowless, an adept field operative and Bladen County native who had helped deliver that unusual result in 2016.”

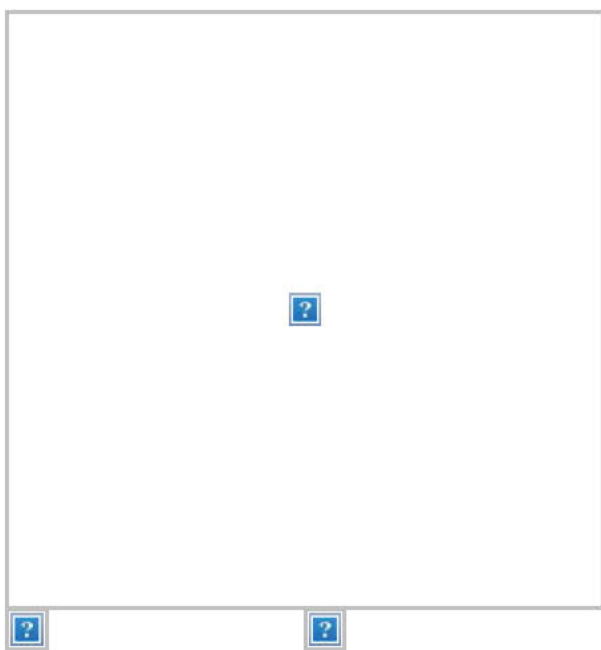
**-- Arizona Gov. Doug Ducey (R) is cooling on the idea of appointing former Senate candidate Martha McSally to John McCain’s old Senate seat if Sen. Jon Kyl (R) steps aside. [Sean Sullivan reports](#):** “Ducey has made no firm decision and McSally, who narrowly lost this year’s Senate race, remains a finalist. ... But her stock has fallen in the eyes of the governor, according to two people familiar with his thinking, as Ducey approaches one of the most significant decisions of his political career. Ducey’s choice would affect not only the future of the Senate but the 2020 elections in an increasingly competitive battleground state. It could also impact his relationship with [Mitch McConnell], a McSally advocate, as well as other party leaders who want to see more Republican women in Congress.”

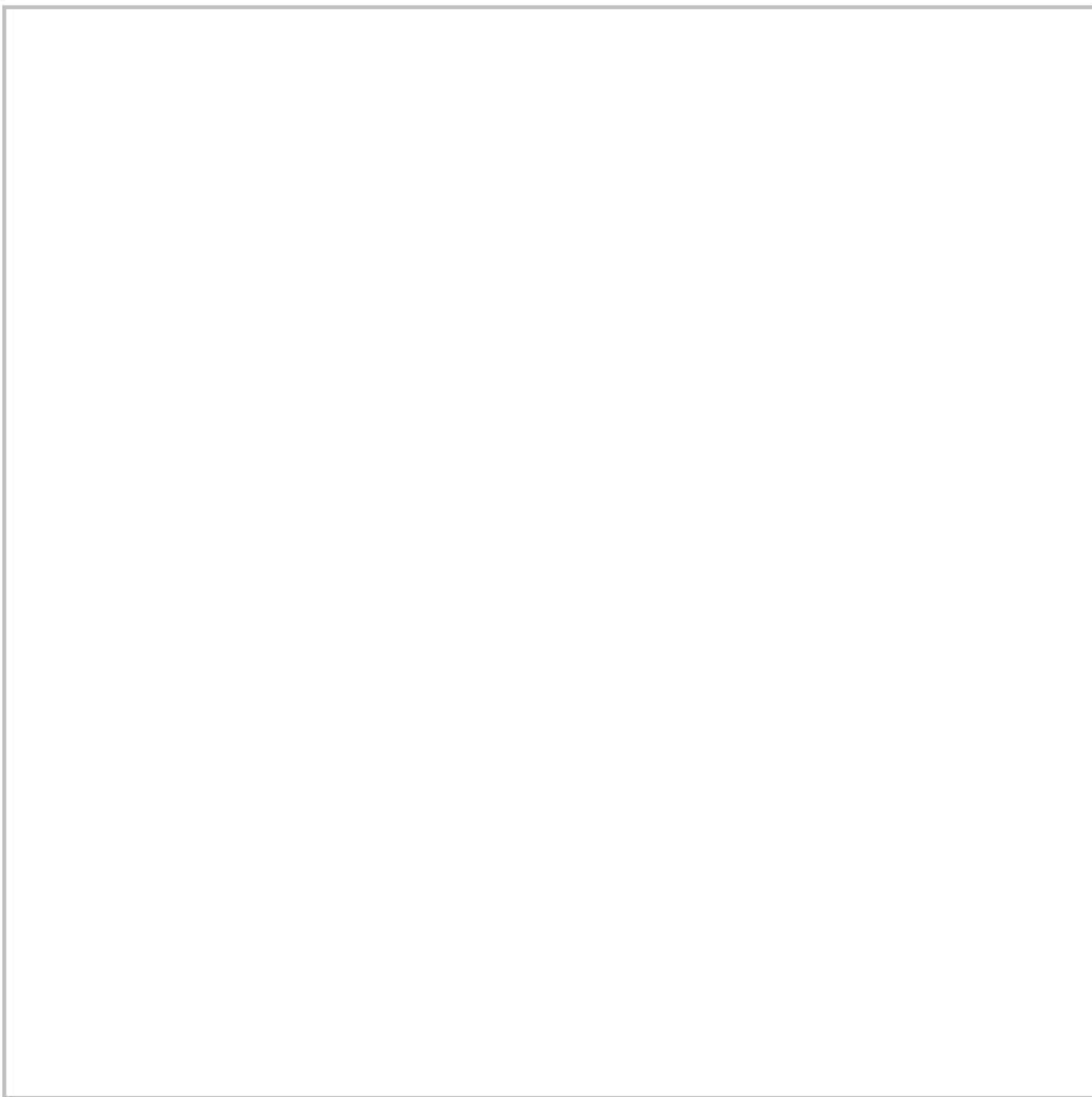
**-- A federal judge rejected GOP Rep. Bruce Poliquin’s**



**lawsuit challenging Maine's candidate-ranking system.** [The AP's Marina Villeneuve and Patrick Whittle report](#): "Poliquin sought to have the voting system declared unconstitutional after he lost the election to Democrat Jared Golden despite having the most first-place votes. Poliquin asked U.S. District Judge Lance Walker either to declare him the winner or order another election for the 2nd Congressional District. But Walker, appointed by [Trump], said states are given great leeway in how they conduct elections. Critics can question the wisdom of ranked-choice voting, Walker said, but such criticism 'falls short of constitutional impropriety.'"

**-- Kansas's incoming Democratic governor turned down a White House invitation to meet with Trump and other governors-elect,** [according to the Wichita Eagle's Jonathan Shorman and Bryan Lowry](#). "Trump campaigned aggressively for Gov-elect Laura Kelly's Republican opponent, Kansas Secretary of State Kris Kobach, this fall. ... Kelly's team said she was unable to travel to Washington because she is focused on the transition and the state budget. ... Kelly and every other newly elected governor was invited to attend the Thursday meeting to discuss shared state and federal priorities, including workforce development, infrastructure, support for veterans and military families and fighting the opioid crisis, according to the White House."





Blake Farenthold, pictured in 2017, resigned as a Republican congressman from Texas after sexual harassment accusations. (Susan Walsh/AP)

## **MORE FROM THE HILL:**

**-- The House and Senate quickly passed a bill aimed at overhauling how Congress handles sexual harassment complaints and sent the legislation to Trump's desk. [Elise Viebeck reports](#):** "Advocates welcomed the measure, which mandates an annual report of all settlements and awards and eliminates the



confidentiality agreements required for accusers at the beginning of the existing process. ... The measure approved on Thursday only requires lawmakers to pay for settlements involving harassment and retaliation, not discrimination. Cases in which a woman is fired for being pregnant, for example, would not trigger the liability. Republicans and Democrats in the lower chamber said they plan to introduce legislation next year to change this on the House side.” Why it matters: **Trump will now sign into law a bill made possible by the #MeToo movement, which was triggered in part by his electoral victory despite accusations of sexual misconduct and which he has [repeatedly mocked](#) over the past year.**

-- **House Republicans are increasing pressure on the Trump administration to end government funding for research using fetal tissue. [Amy Goldstein reports](#):** “[A] hearing before subcommittees of the House Oversight and Government Reform Committee grew testy at times over whether cells from sources other than aborted fetuses are as useful as fetal tissue in advancing therapies and possible cures for diseases from HIV to cancer. ... The hearing, which played to Republicans’ base of social and religious conservatives, comes amid moves by Trump health officials to rethink whether federal money should continue to support the research. In the past three months, the Department of Health and Human Services has [severed one contract](#) with a

California firm that has been a major supplier of such tissue for laboratories.”

**-- For the second consecutive year, the Senate will allow to lapse Barry Lee Myers’s nomination to lead the National Oceanic and Atmospheric Administration.** [The New York Times’s Lisa Friedman reports](#): “Democrats have said that Mr. Myers has significant conflicts of interest, including his past eagerness to privatize the National Weather Service. ... Republicans blamed Democrats for the delay. Mr. Trump had to renominate Mr. Myers in January after the Senate failed to act last year. Mr. Myers has twice been advanced by the Commerce Committee, said Senator John Thune of South Dakota, the Republican chairman.”

**-- Senate Armed Services Committee Chairman Jim Inhofe (R-Okla.) tried to defend his purchase (and rapid sale) of stock in a defense contractor after he voiced support for record Pentagon spending.** [Karoun Demirjian reports](#): “Inhofe said through spokeswoman Leacy Burke that the purchase was made without his knowledge by a third-party adviser, and that he had ‘no involvement’ in the transaction. ‘The Senator has called his financial adviser and they reversed, or busted, the transaction,’ Burke said, referring to a Wednesday letter in which Inhofe instructed adviser Keith Goddard ‘to no longer purchase defense or aerospace companies as part of my financial holdings.’”



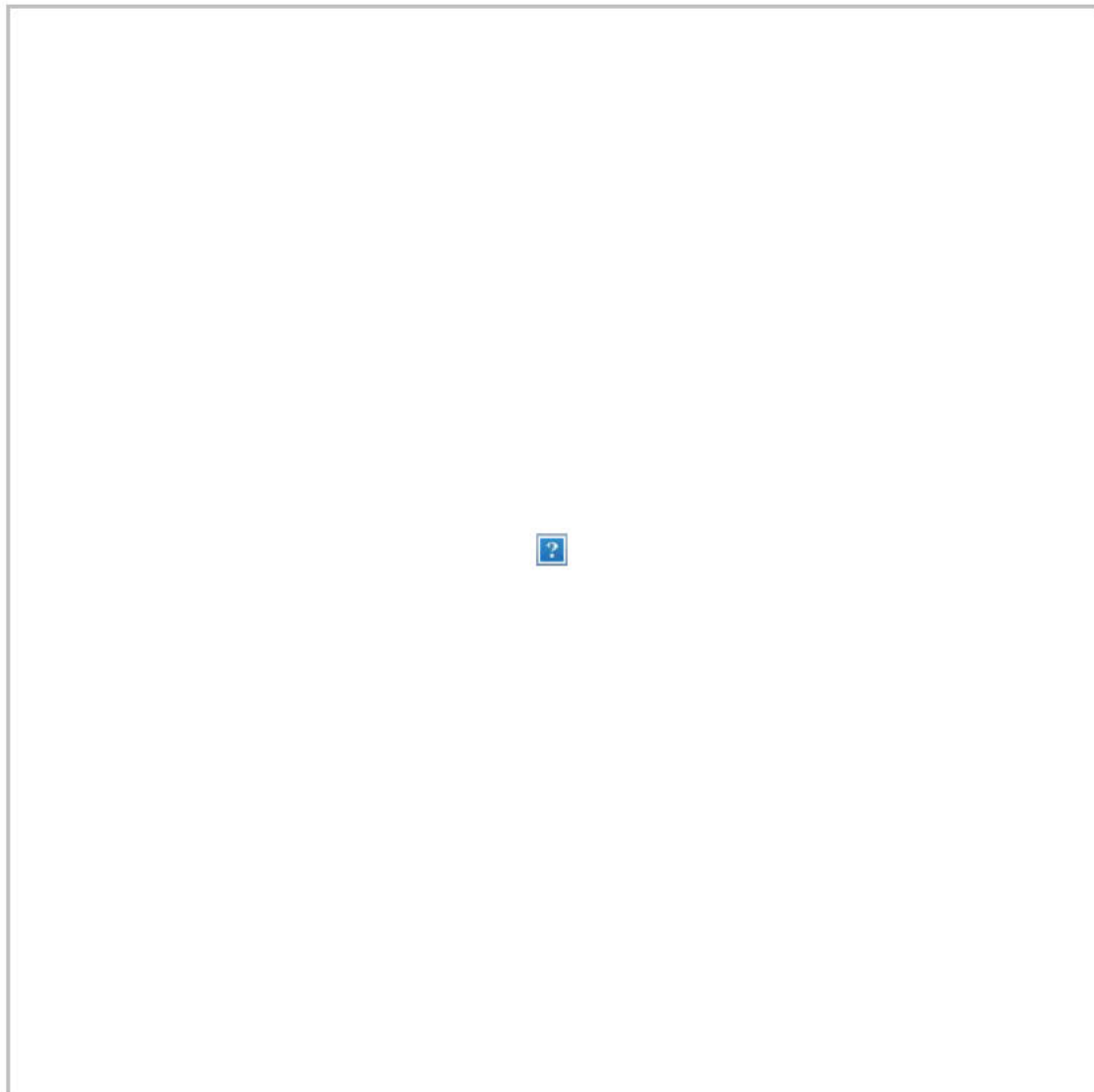
**-- Sens. Claire McCaskill (D-Mo.) and Jeff Flake (R-Ariz.) used their farewell addresses to blast the dysfunction of the Senate and politics generally. [NBC News's Allan Smith reports](#):** “Peter Morgan, an author, wrote that no family is complete without an embarrassing uncle,’ said [McCaskill]. ‘We have too many embarrassing uncles in the United States Senate. Lots of embarrassing stuff.’ She said that if senators ‘don’t have the strength to look in the mirror and fix’ the Senate, ‘the American people are going to grow more and more cynical, and they might do something crazy like elect a reality TV star president.’ McCaskill added: ‘The United States Senate is no longer the world’s greatest deliberative body. And everybody needs to quit saying it until we recover from this period of polarization and the fear of the political consequences of tough votes.’

**“Earlier, Flake used his final address on the Senate floor to warn of threats to America’s democracy ‘from within and without.’** ‘We of course are testing the institutions of American liberty in ways that none of us likely ever imagined we would — and in ways that we never should again,’ Flake said. ‘My colleagues, to say that our politics is not healthy is something of an understatement. I believe that we all know well that this is not a normal time, that the threats to our democracy from within and without are real, and none of us can say with confidence how the situation that we now find ourselves

in will turn out.’”

## **SOCIAL MEDIA SPEED READ:**

George Conway, who is married to White House adviser Kellyanne Conway, said he didn't believe Trump's comments about Michael Cohen:

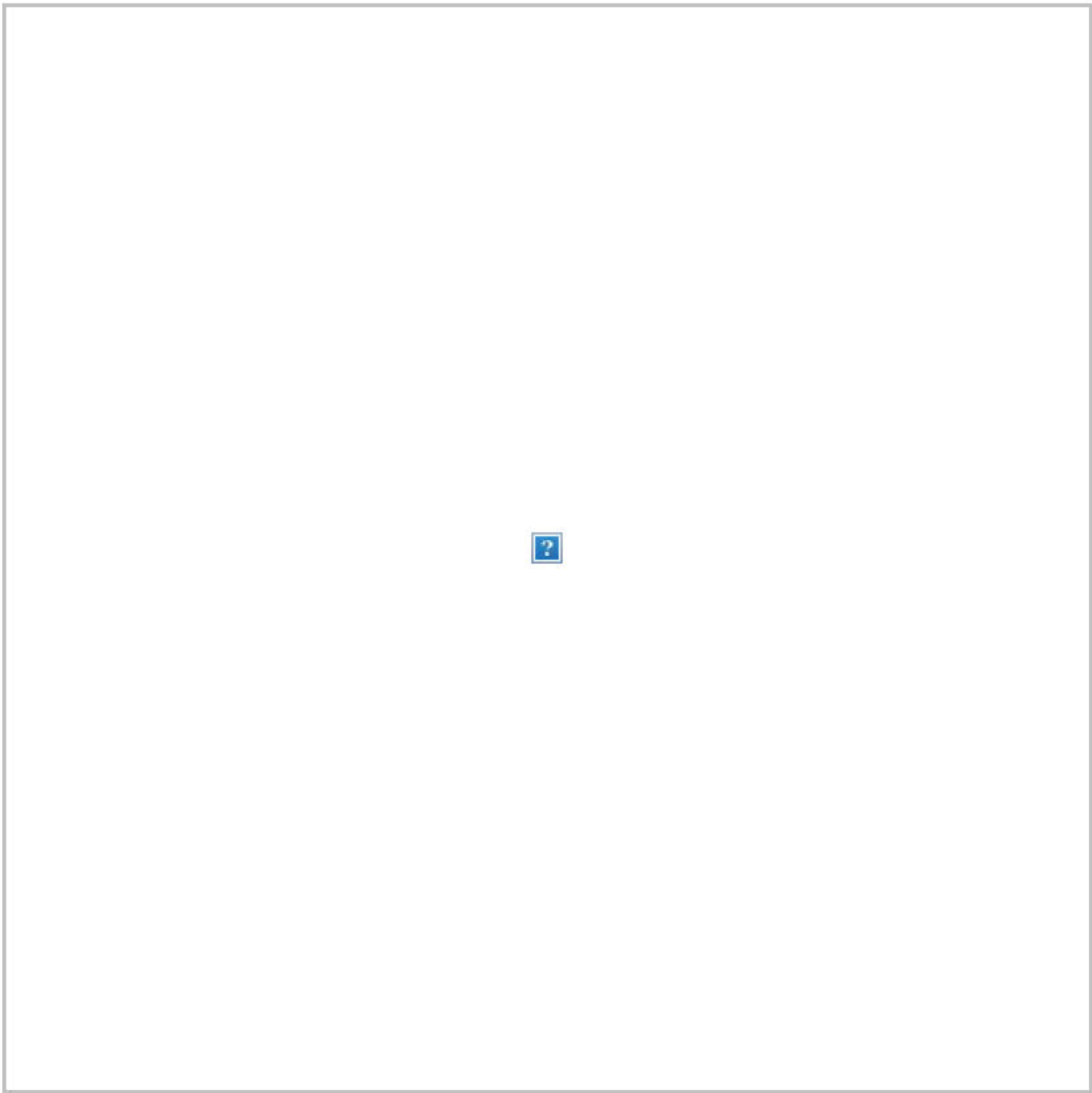


A former CIA director explained the three different types of Russian espionage after Butina's guilty plea:



Per a Washington Post reporter, a White House official challenged the HuffPost story that Kushner is under consideration for the chief of staff job:





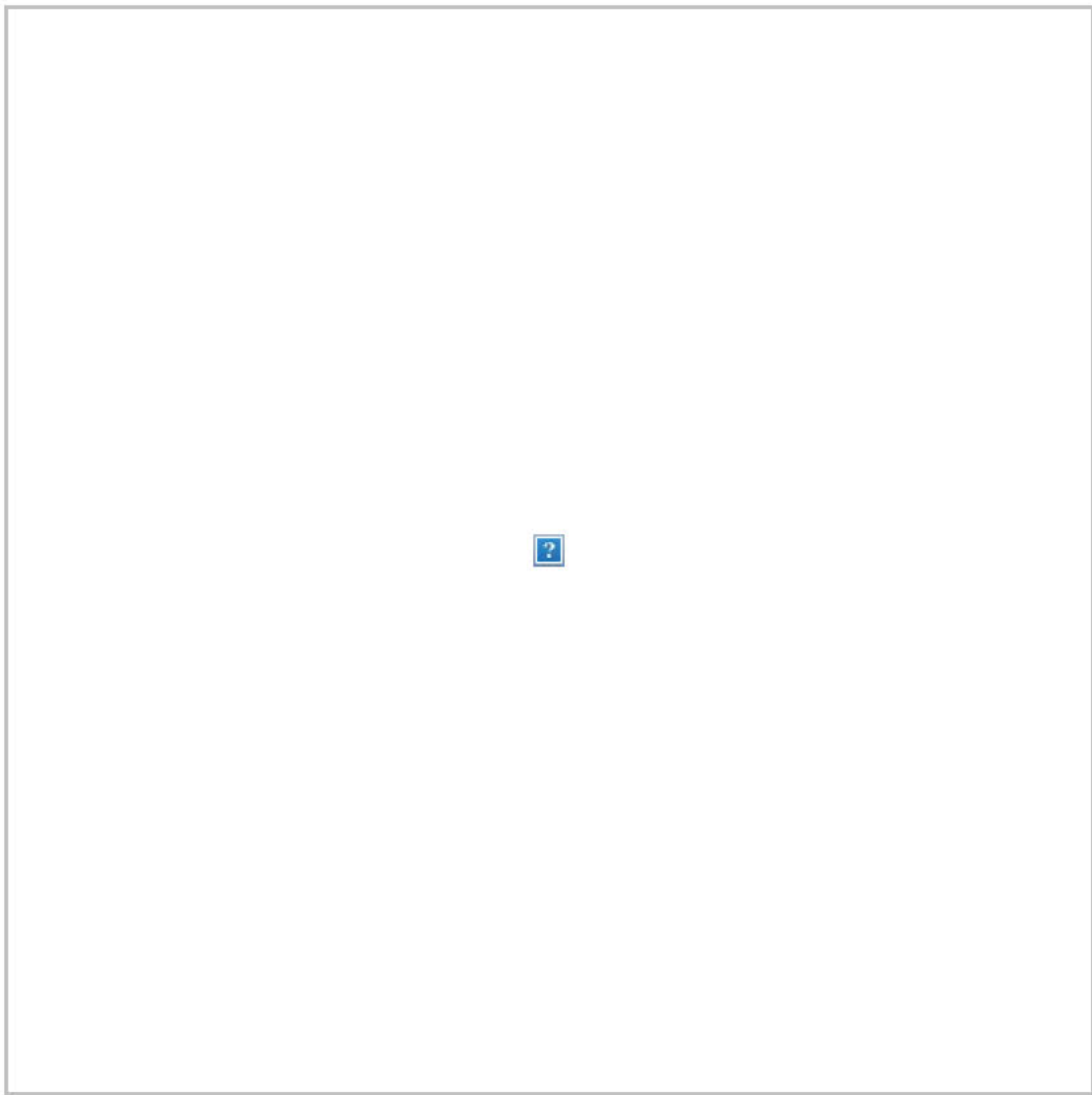
Trump's two chiefs of staff met again at the White House:



Former secretary of state John Kerry had harsh words for a Trump administration proposal to deport certain Vietnam War refugees:



A House Democrat also criticized the policy:

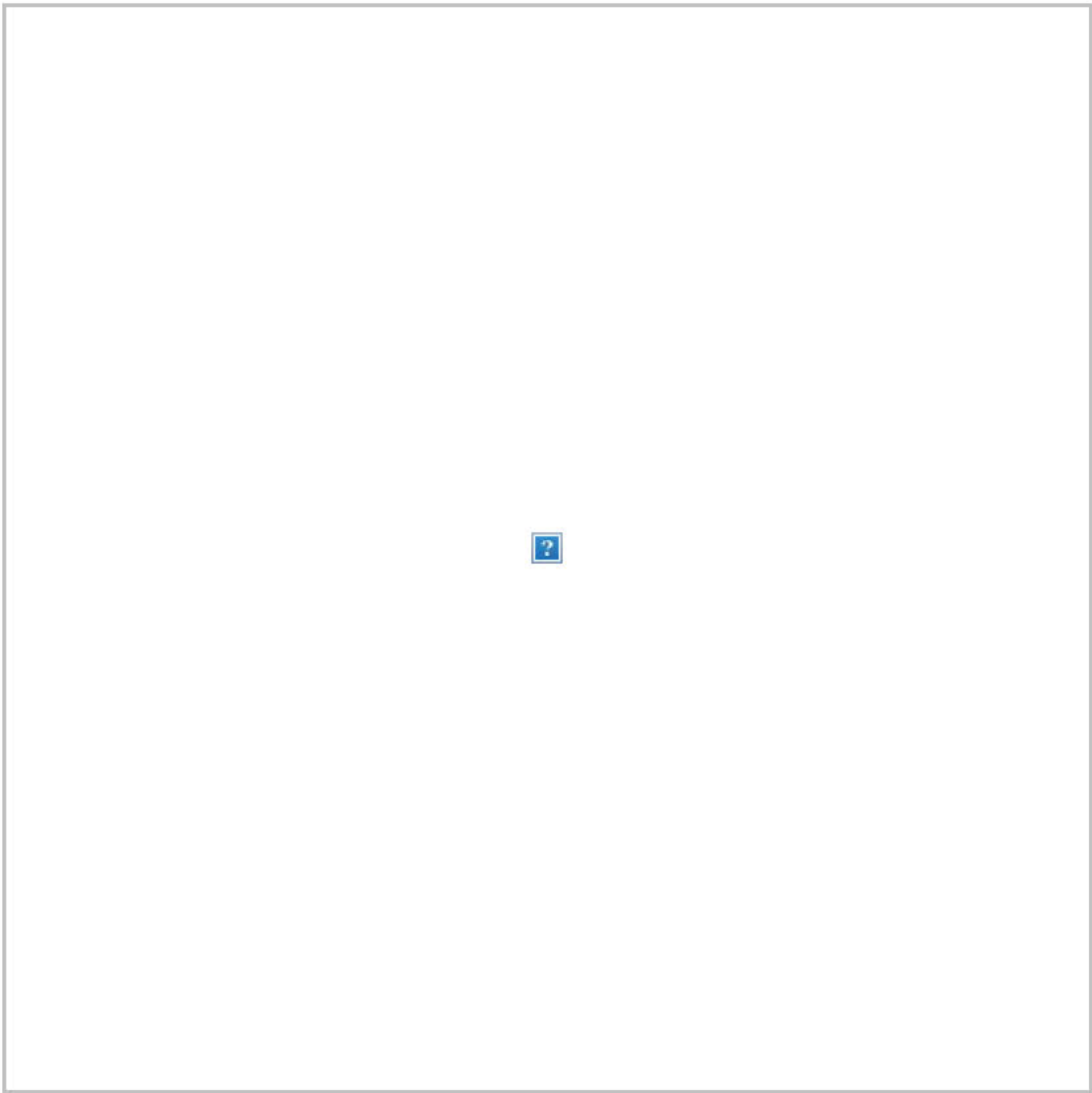


A Post reporter shared messages between a migrant who has repeatedly attempted to cross the southern border and his daughter:



A Post reporter attempted to fact-check Trump's comment about the renegotiated NAFTA covering the cost of a border wall:





A Post columnist mocked Trump for the suggestion:



Jim Comey slammed a top House Republican's description of the former FBI director's congressional testimony:



Sen. Jim Inhofe (R-Okla.) took a novel approach to answering reporters' tough questions about a stock purchase he made:

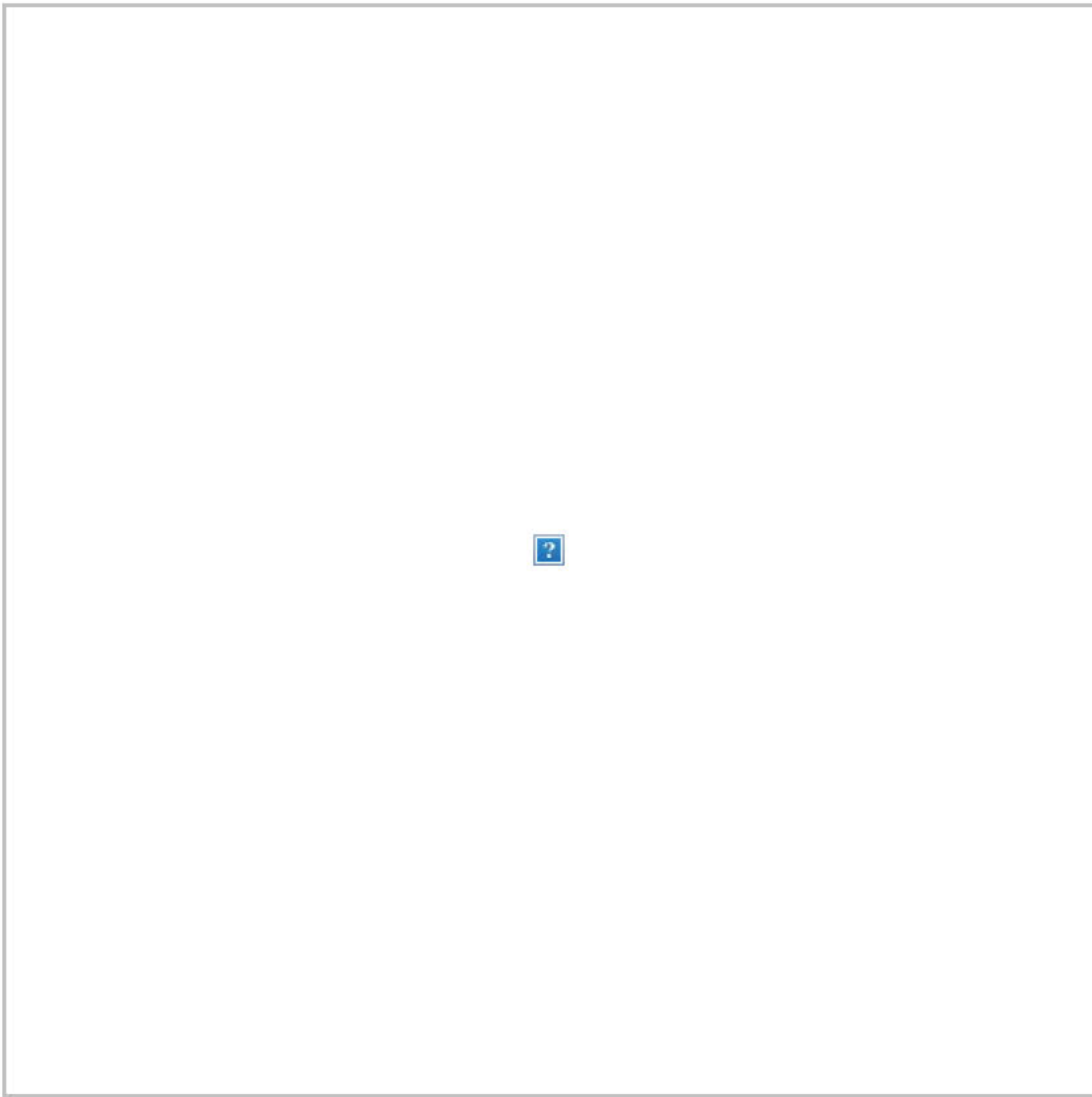


Sen. Marco Rubio (R-Fla.) argued against stock buybacks in a [piece](#) for the Atlantic:

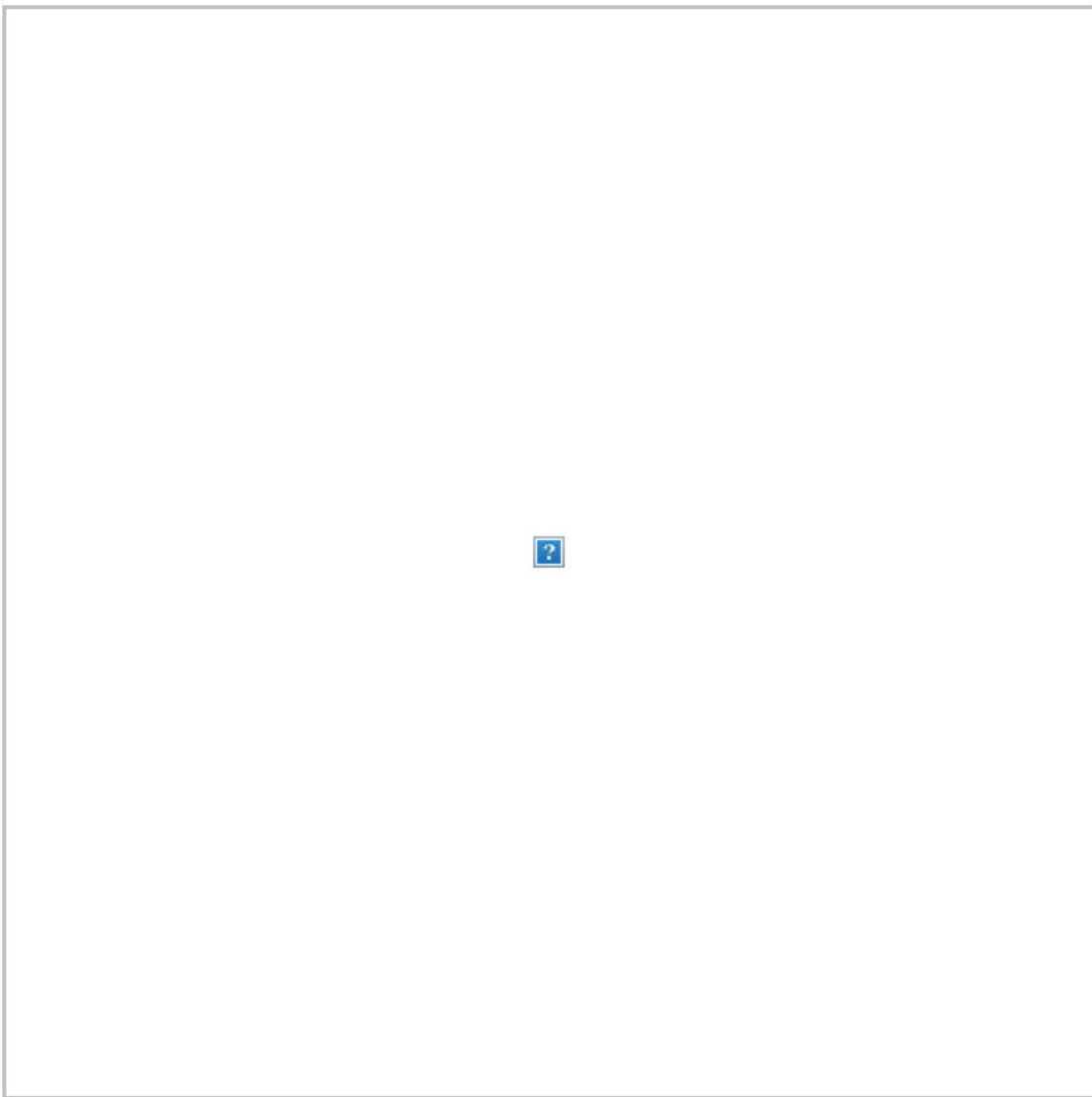


A former chief of staff to Joe Biden replied to Rubio:





Retweeting a story that identifies him as a "potential presidential candidate," Sen. Sherrod Brown (D-Ohio) went after an airline over tip jars:



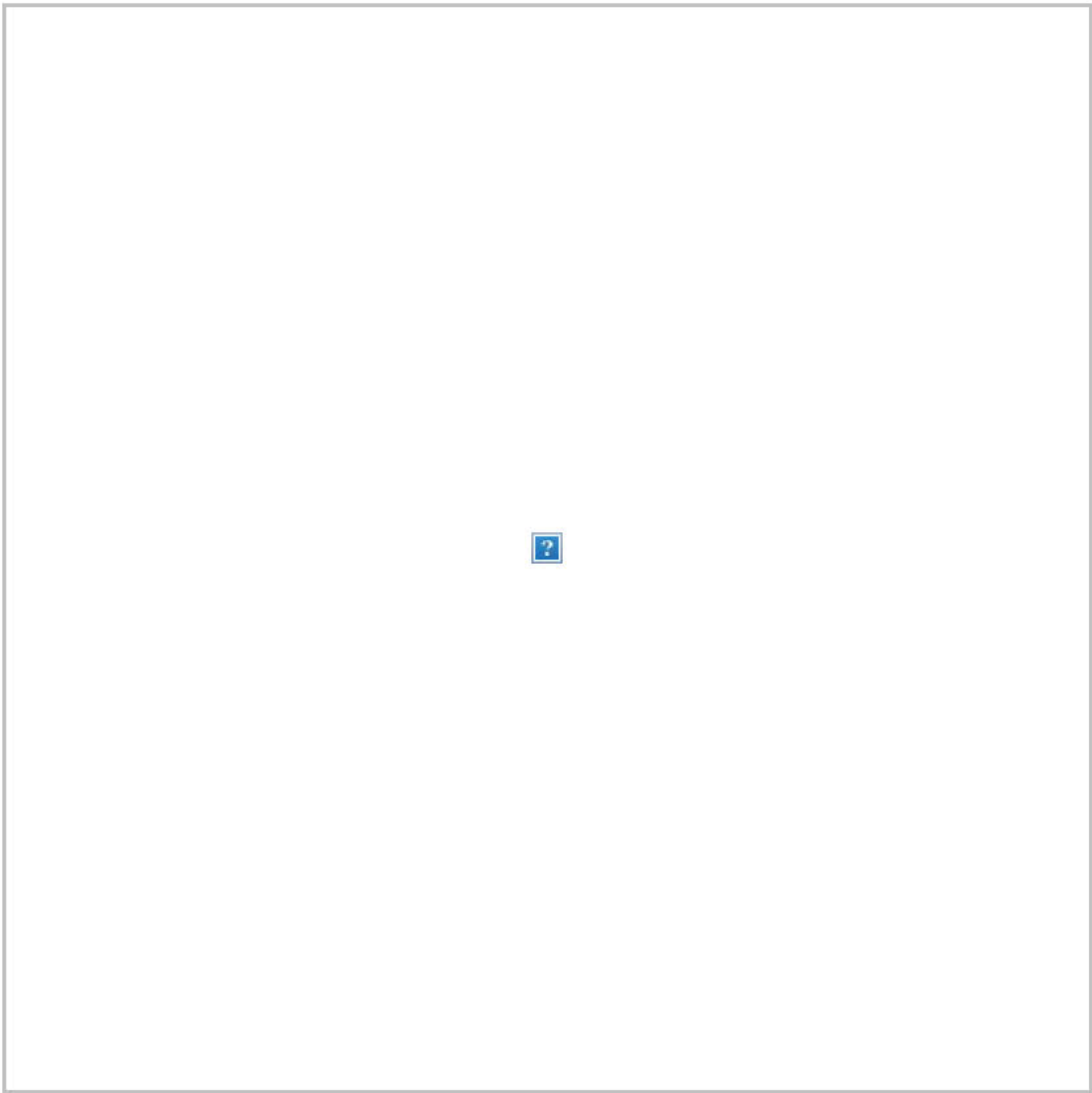
A Tennessee government agency issued this statement after a congressman-elect claimed vaccines might cause autism:



One of the co-founders of March for Our Lives was accepted to Harvard:

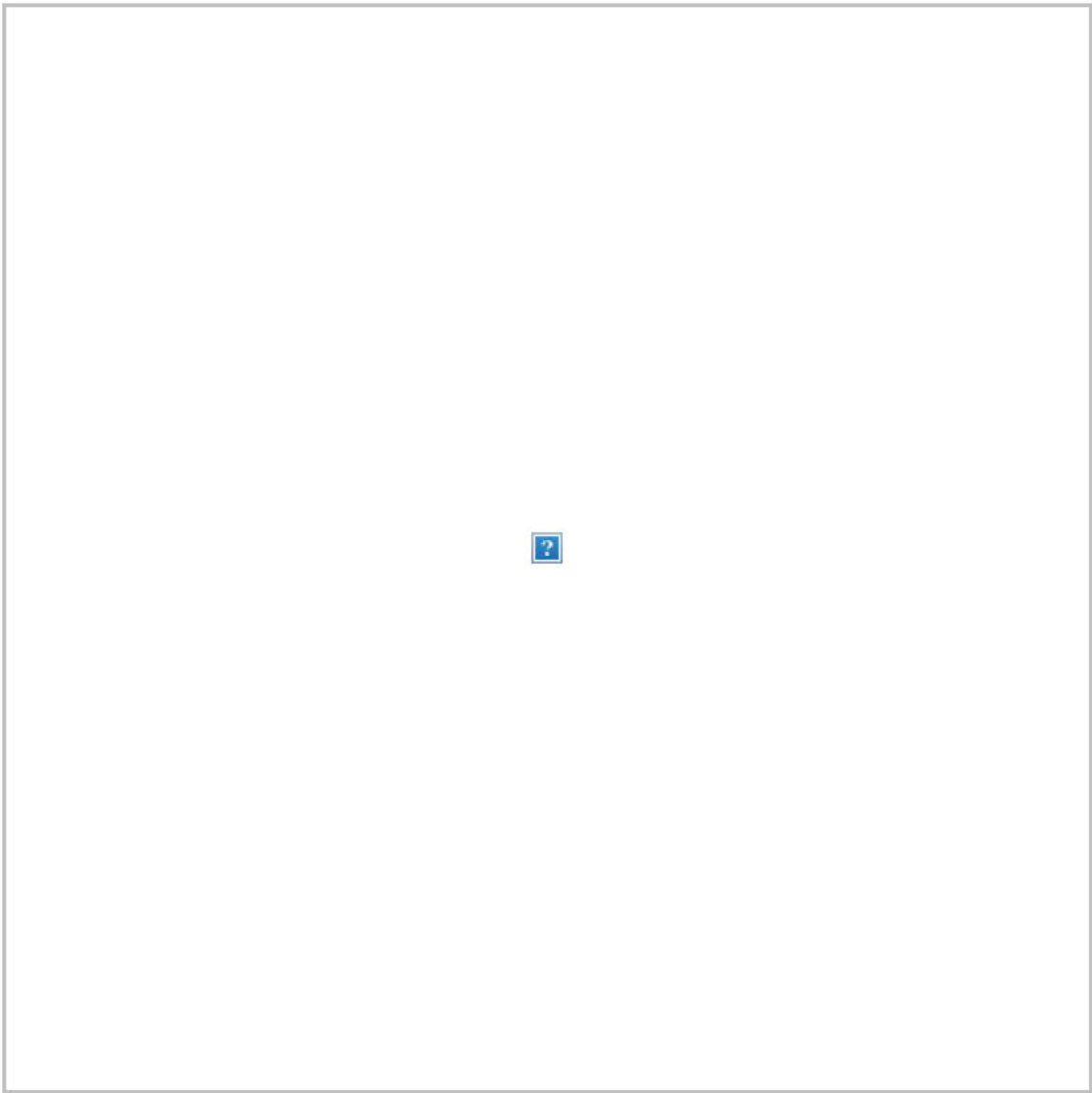


Rep.-elect Anthony Brindisi (D-N.Y.), [whom I profiled on Nov. 1](#), packed up his state assembly office in Albany and prepared to make the move to Washington:

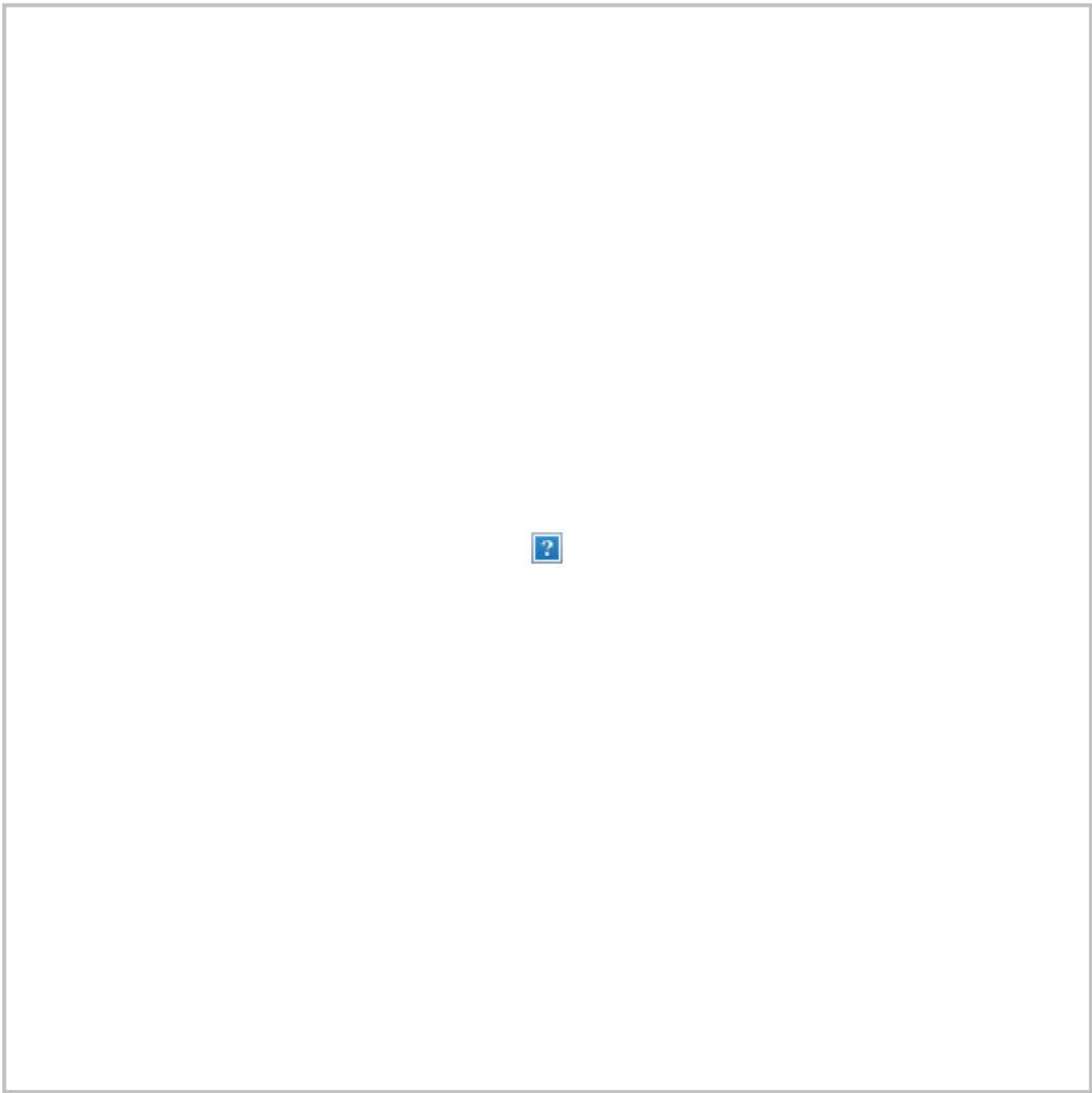


A new Senate caucus was formed:





Nancy Pelosi celebrated her fashion success:



And Sen. Jeff Flake requested a blanket imprinted with his tweets from the Daily Show:



The host responded with what the kids call a sick burn:



## **GOOD READS:**

-- "[The boy on the bridge](#)," by Jessica Contrera:

"There was no way she could have seen him, the boy on the bridge. Marisa Harris was driving her Ford Escape down a Northern Virginia highway, heading home after a peaceful afternoon hike at Burke Lake. Her boyfriend, Perry Muth, was stretched out in the passenger seat as they cruised east on Interstate 66 toward the bridge, an overpass suspended across the busy highway. ... The

boy on the bridge was 12. What led him there would always be a mystery to Marisa's family, even after police and prosecutors came to their conclusions. There was no fence on the part of the bridge he'd reached. There was a pedestrian sidewalk, and beside it, a three-foot, two-inch-tall guardrail. But there was nothing to stop the boy from climbing over it. And nothing to stop him from jumping — just as Marisa's car reached the spot below."

-- **BuzzFeed News**, "[The Cities Where The Cops See No Hate](#)," by **Peter Aldhous**: "Year after year, the vast majority of police departments across the country report zero hate crimes to the FBI. After sifting through more than 2,400 police incident reports from 2016 obtained from 10 of the largest such departments, BuzzFeed News identified 15 assaults in which the cops' own narratives suggested that the suspect may have been motivated by bias."

-- **New York Times**, "[How 'Baby, It's Cold Outside' Went From Parlor Act to Problematic](#)," by **Jacey Fortin**: "Rock Hudson did it with Mae West. Ray Charles did it with Betty Carter. Lady Gaga and Joseph Gordon-Levitt did it with a modern twist. And somewhere along the line, the 74-year-old song 'Baby, It's Cold Outside' became a holiday standard, in heavy radio rotation, playing overhead in department stores, and covered on Christmas albums. ... Now, a long-simmering debate over the lyrics has reached a boil. The annual holiday



culture wars and the reckoning over #MeToo have swirled together into a potent mix. Say — what's in this drink?"

#### **HOT ON THE LEFT:**

**"U.S. Budget Deficit Hits Widest on Record for Month of November," from Bloomberg News:**


"The U.S. posted the widest November budget deficit on record as spending doubled revenue. Outlays jumped 18 percent to \$411 billion last month, while receipts were little changed at \$206 billion, the Treasury Department said in a monthly report on Thursday. That left a \$205 billion shortfall, compared with a \$139 billion gap a year

#### **HOT ON THE RIGHT:**

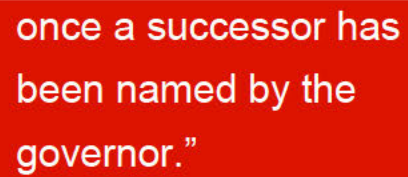
**"Florida Senate won't consider reinstating former Broward elections supervisor Brenda Snipes," from the South Florida Sun Sentinel:** "The Florida Senate has declined to take action on former Broward County elections head Brenda Snipes' suspension, paving the way for an ally of Republican Gov. Rick Scott to fill the remainder of her term, according to a memo on Thursday from Senate President Bill Galvano. Snipes had

earlier. The U.S. ran the largest deficit in six years in fiscal 2018, the first full year of Donald Trump's presidency when his Republican party enacted a tax-cut package and raised federal spending for the military and other priorities. The measures have added to the growing federal deficit, which is forecast to push past \$1 trillion by 2020 when the U.S. next holds presidential elections. In the first two months of the fiscal year that began Oct. 1, the gap widened to \$305.4 billion, compared with \$201.8 billion the same period a year earlier."

announced she would resign her post effective Jan. 4, amid an outcry over stumbles by her office during Florida's recount. A day after Scott suspended her from office on Nov. 30, Snipes she said she would withdraw her resignation. Citing 'misfeasance, incompetence and neglect of duty,' Scott installed Pete Antonacci, his former top lawyer, to fill the remainder of Snipes' term, which ends after the 2020 presidential election. ... Galvano, R-Bradenton, said legal precedent in Florida has established that Snipes cannot take back her resignation



once a successor has  
been named by the  
governor.”



## **DAYBOOK:**

**Trump** will receive his intelligence briefing and later attend two Christmas receptions with the first lady.

The president is also expected to spend 16 days at Mar-a-Lago over the Christmas and New Year’s holidays. It will be his longest sojourn to the “Southern White House” since his inauguration. ([Palm Beach Post](#))

Pelosi: 'Oval Office is an evidence-free zone'

### **QUOTE OF THE DAY:**

"I think the Oval Office is an evidence-free zone. You've got to have facts, data, evidence, truth in order to make an agreement on how you go forward." – Nancy Pelosi on Trump's argument that economic benefits from a renegotiated NAFTA would cover the cost of a border wall.





## **NEWS YOU CAN USE IF YOU LIVE IN D.C.:**

**-- Rain will become increasingly likely in Washington as the day goes on.** [The Capital Weather Gang forecasts](#): “Clouds thicken, with a few morning sprinkles possible. Steadier rain should hold off until later afternoon or perhaps into evening locally. We likely stay stuck in the 40s for high temperatures, with a very light but steady east-northeast breeze off the Bay and Atlantic. Monitor radar with us by midday for any rain timing and intensity updates.”

**-- The Metro board advanced measures to charge peak fares for special events and expand rush-hour service.** [Faiz Siddiqui reports](#): “But the board tabled action on a measure to continue the system’s early-closing hours for another year after board members representing the District threatened to veto it. ... Metro has proposed continuing the early closings to expand a preventive maintenance program implemented in the wake of its SafeTrack rehabilitation work.”

**-- A U-Va. professor retired after an internal investigation concluded he had inappropriate sexual contact with a student 17 years ago.** [Nick Anderson reports](#): “John Casey, an award-winning fiction writer,

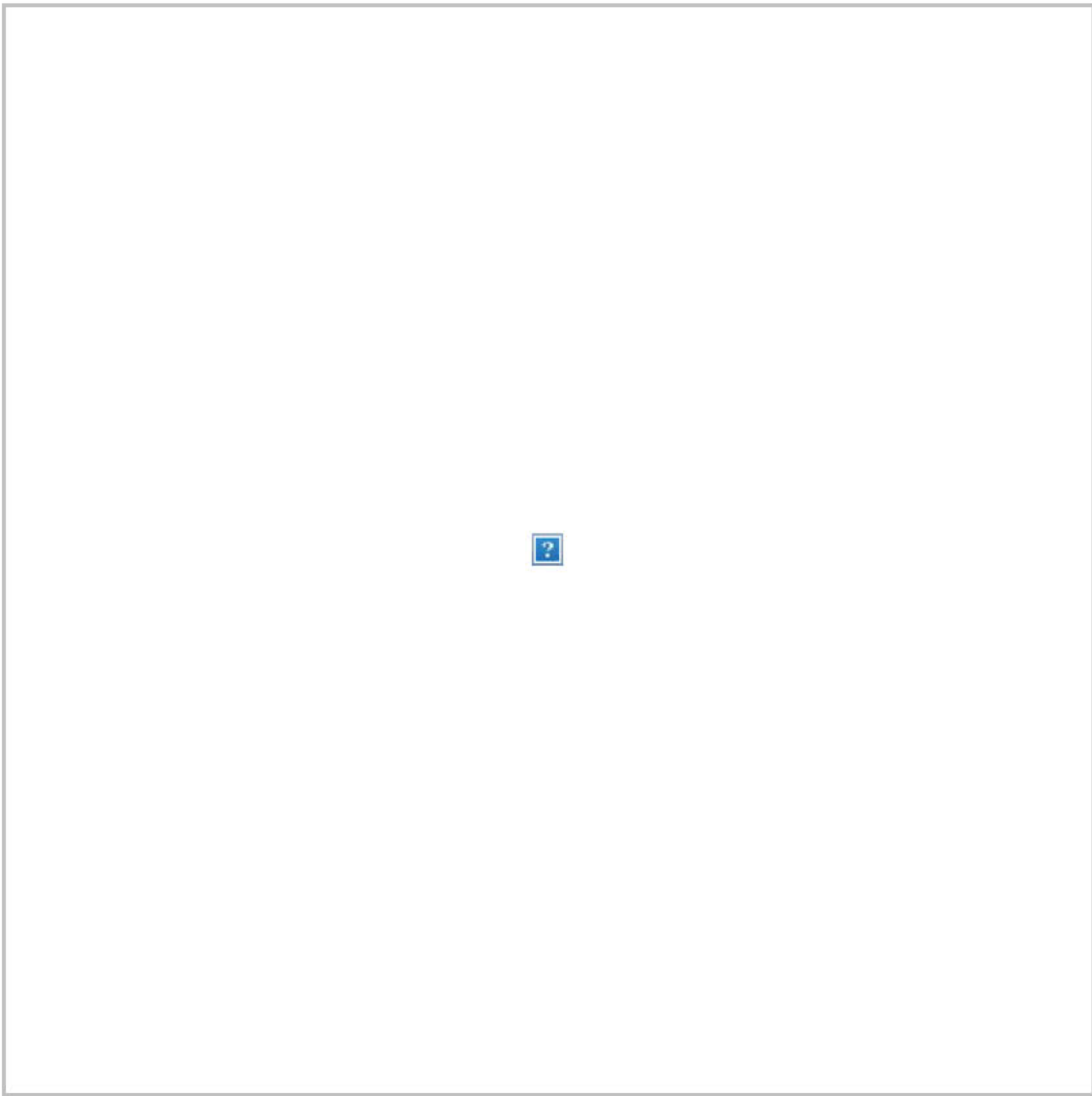


kissed and touched the student in an unwelcome manner one night in 2001, according to a letter summarizing conclusions last week from a disciplinary review panel. The investigation also determined Casey had sex with the student at a time when she was likely to have been enrolled in his class, according to the letter. The panel characterized his conduct as 'reprehensible,' according to the letter, and recommended termination. But the panel cleared Casey on a major charge: It concluded there was not enough evidence to support former student Lisa Schievelbein's allegation that the professor had sexual intercourse with her repeatedly without her consent."

**-- The earliest known painting of George Washington returned to his Mount Vernon estate for the first time since 1802.** The Charles Willson Peale painting is on loan from Washington and Lee University and will be on display for the next two years. ([Michael E. Ruane](#))

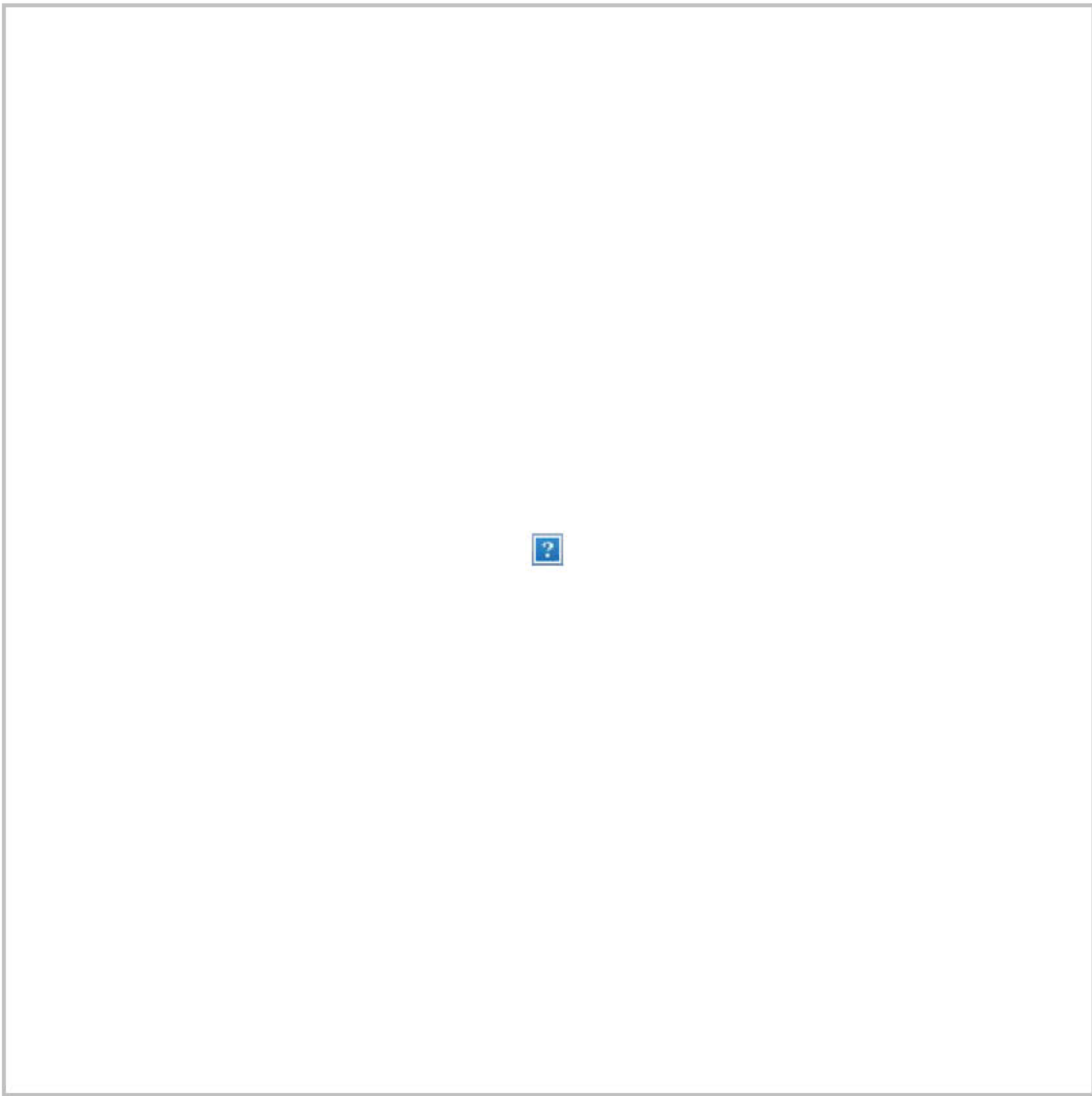
## **VIDEOS OF THE DAY:**

Stephen Colbert updated the presidential seal to reflect the latest developments from the Russia investigation:



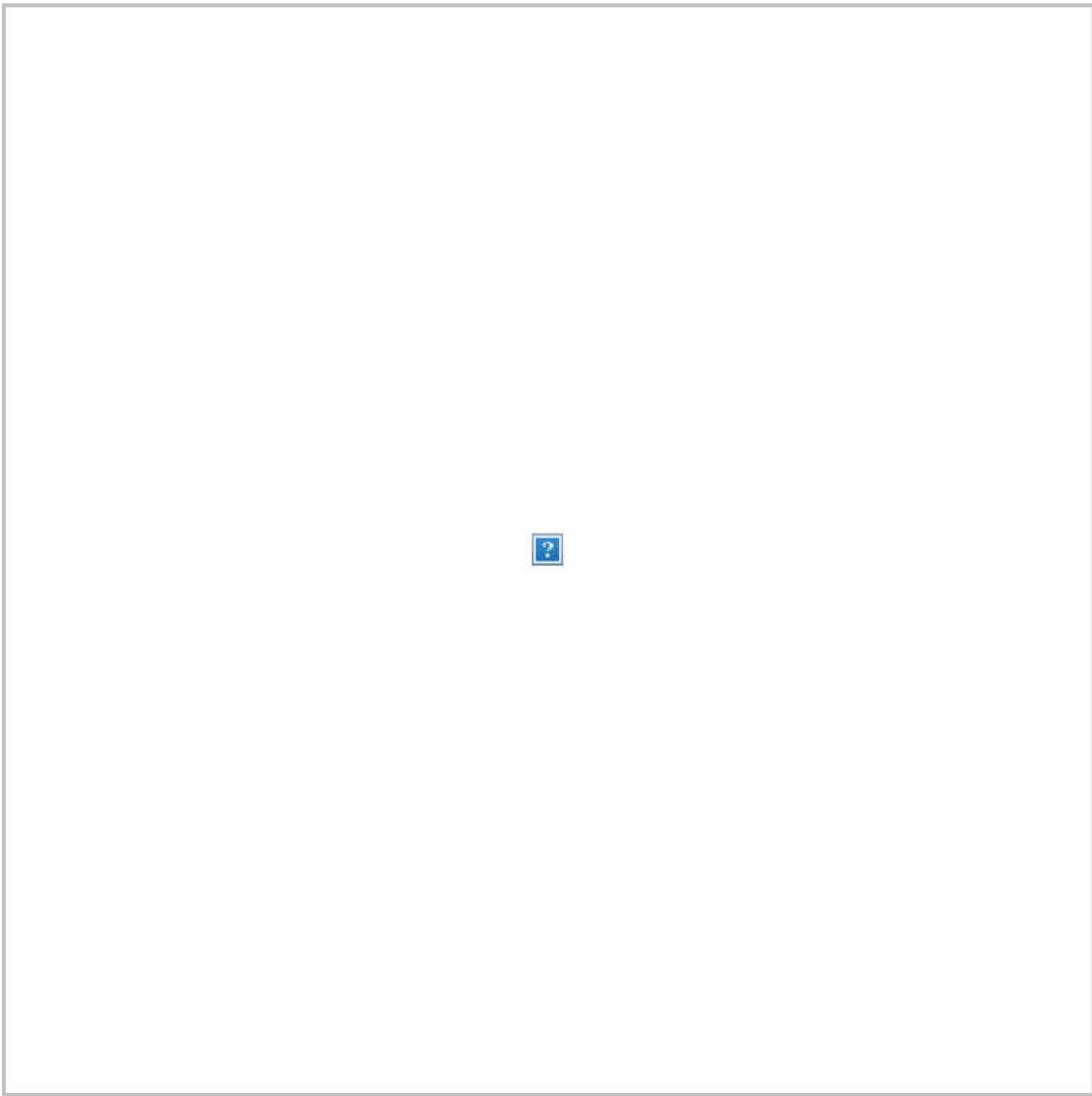
The Embarrassing President Feels Embarrassed

Melania Trump visited a D.C. children's hospital:



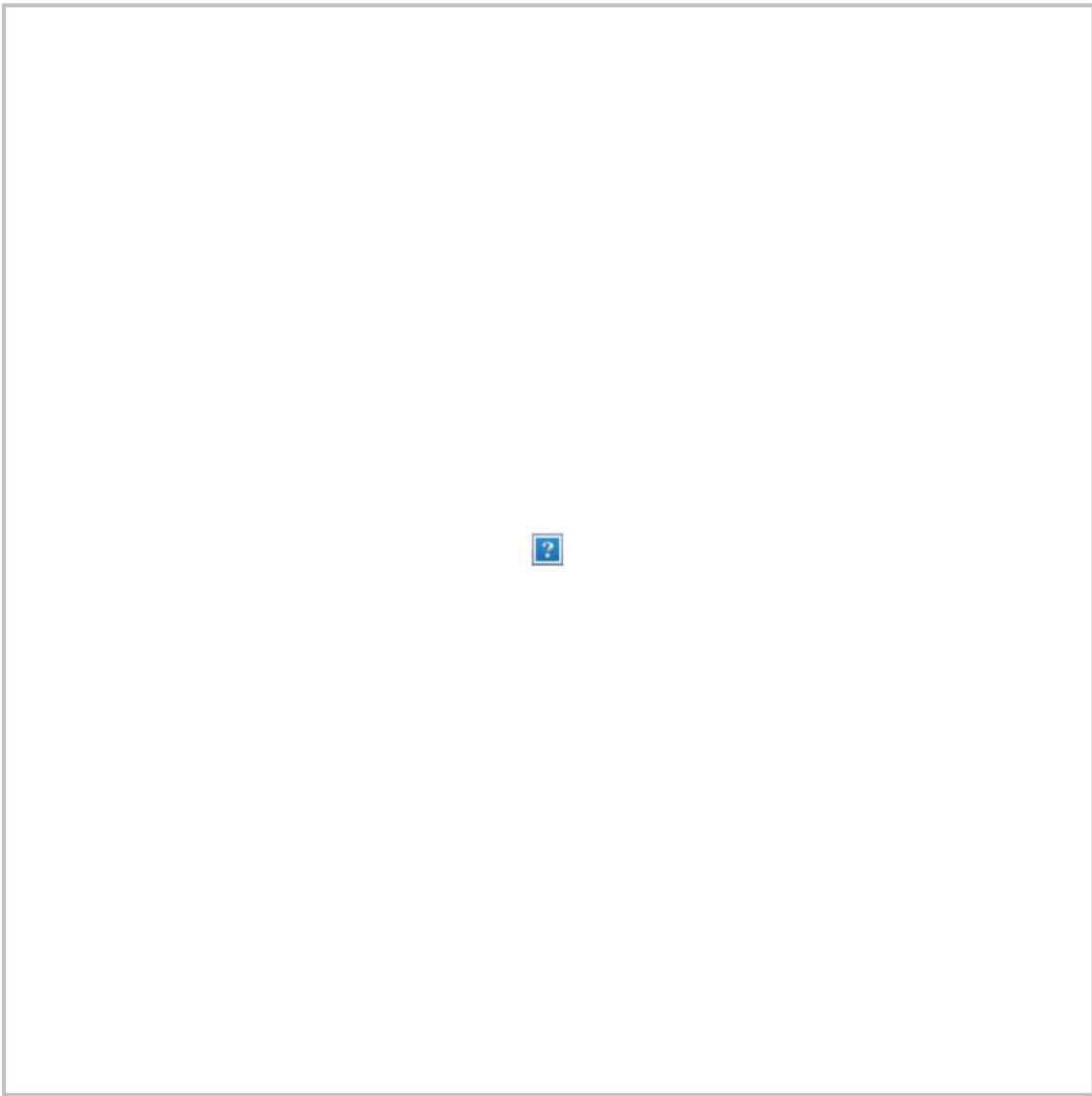
Melania Trump visits children's hospital

Virgin Galactic launched a spacecraft that reached an altitude of more than 50 miles, making it the first manned U.S. spacecraft to reach space since 2011:



Virgin Galactic launches the first manned U.S. spacecraft to reach space since 2011

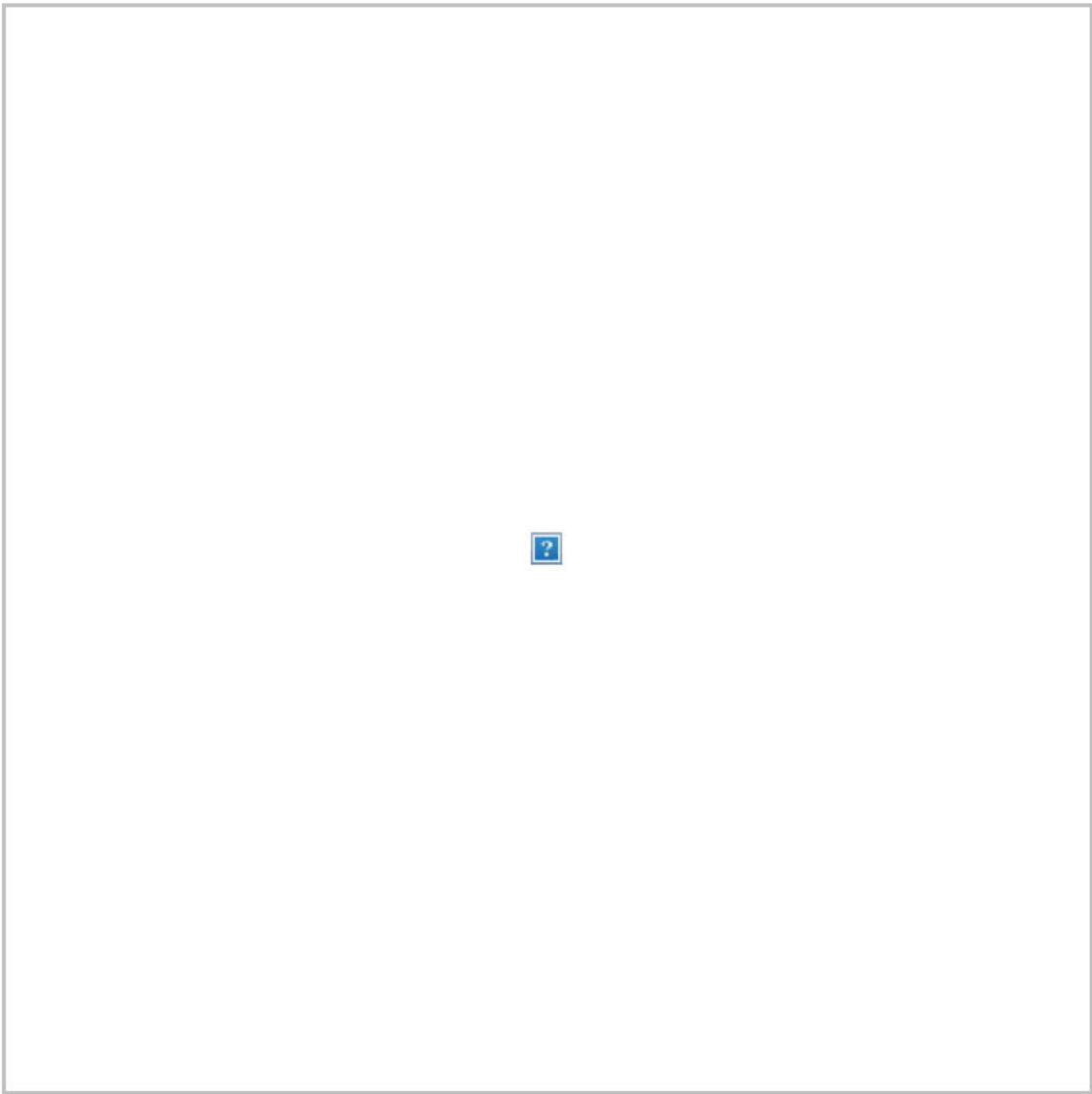
Miss USA apologized for comments she made about the English-speaking abilities of two Miss Universe contestants:



Miss USA apologizes for comments about Miss Universe contestants' English

**And officials at JFK Airport discovered live birds hidden in hair rollers:**





Airport officials discover 70 finches hidden in hair rollers

You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)

---

©2018 The Washington Post | 1301 K St NW, Washington DC 20071



From:

[The Washington Post](#)

To:

[Arnold Chu](#)

Subject:

The Daily 202: Senate rebuke of Trump on Yemen shows Congress, not just the president, can offer moral leadership

Date:

Friday, December 14, 2018 6:59:57 AM

---

If you're having trouble reading this, [click here](#).

---

# The Daily 202



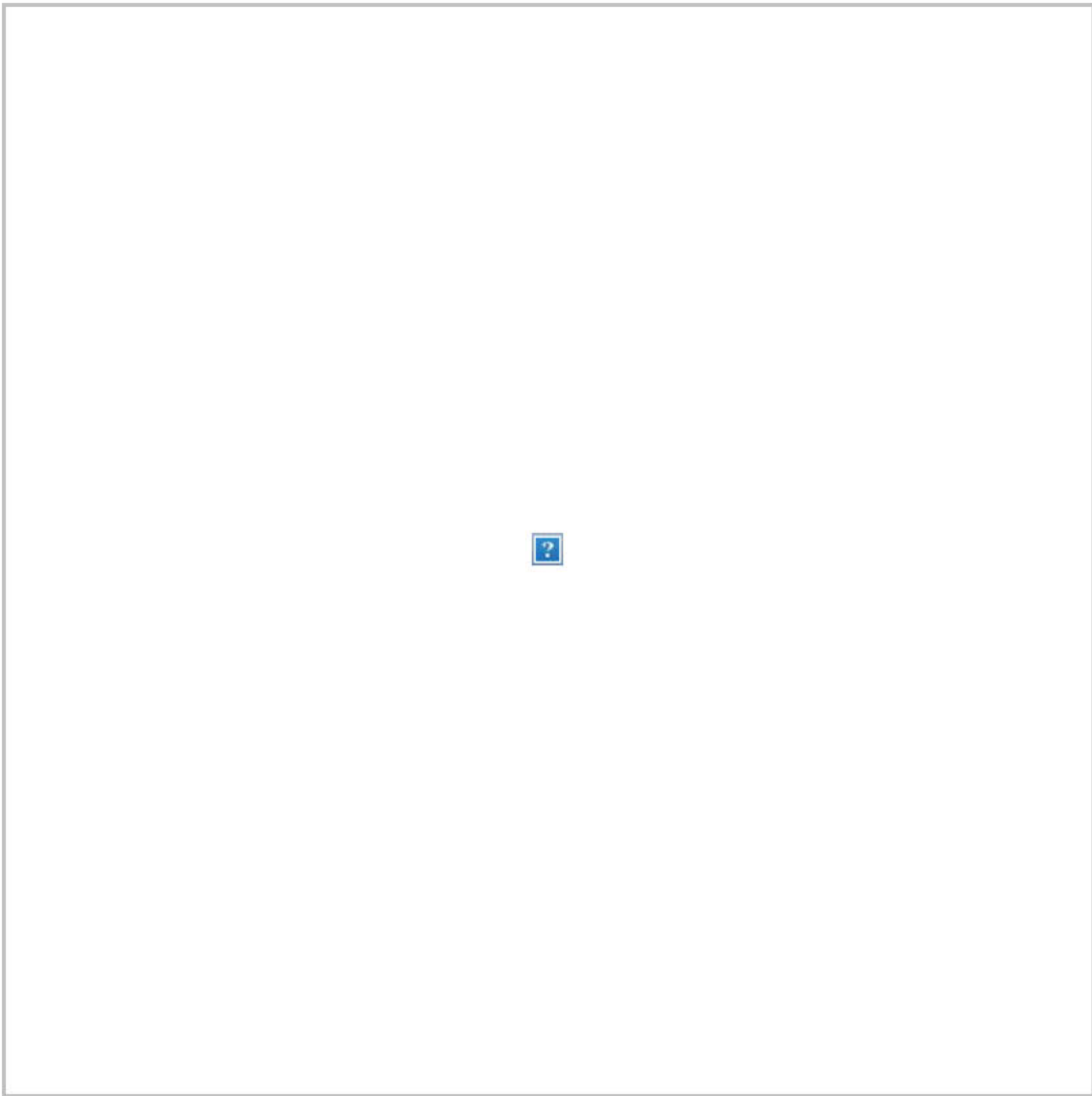
Share:  

 Listen to The Big Idea



## Senate rebuke of Trump on Yemen shows

# Congress, not just the president, can offer moral leadership



Senate rebukes Saudi Arabia, defies Trump with back-to-back votes



**BY JAMES HOHMANN**

*with Joanie Greve*

**THE BIG IDEA:** American presidents have historically embraced – sometimes with gusto and sometimes reluctantly – their unofficial role as chief spokesman

**for the free world, a soft power that comes with leading what Ronald Reagan called the “shining city upon a hill.” Not President Trump.**

Trump, who spoke of “[American carnage](#)” in his inaugural address, seems plainly [uninterested](#) in seizing the mantle of moral leadership on the global stage. He’s consistently displayed a [Hobbesian](#) and Machiavellian approach to power politics during his nearly two years in office, [eschewing](#) the pillars of Lockean, Wilsonian and Reaganite thought while deemphasizing the promotion of democracy and human rights as aims of U.S. foreign policy.

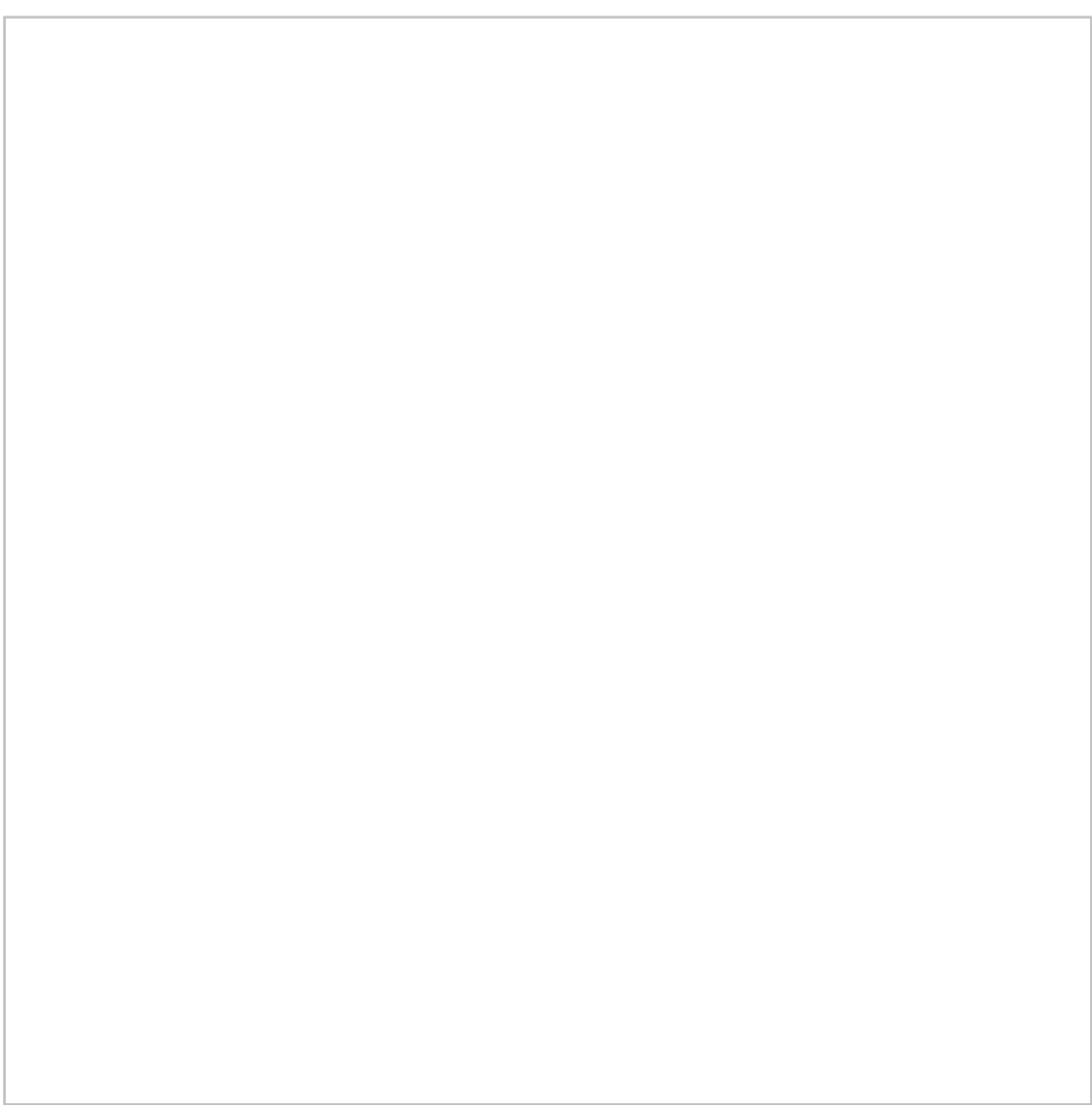
His [blase responses](#) this fall to the [killing](#) of Washington Post contributing columnist Jamal Khashoggi and what the United Nations calls the world’s worst humanitarian crisis in Yemen have put in stark relief Trump’s abdication of that traditional moral leadership role.

**On Thursday afternoon, a bipartisan coalition in Congress moved to fill the void and perform this function of the presidency that Trump has essentially outsourced. [Senators voted 56-to-41](#) to cut off U.S. military support for Saudi Arabia’s often brutal conduct in the Yemen civil war. It’s the first time either chamber of Congress has asserted itself against the executive branch by using the War Powers Act, which became law during the depths of the Vietnam quagmire in 1973.**

A few minutes later, the Senate voted unanimously to approve a separate, [nonbinding resolution](#) that blames Crown Prince Mohammed bin Salman for what happened to Khashoggi. The CIA concluded that MBS, as he's known, probably ordered and monitored the dismemberment of the dissident journalist inside a Saudi consulate in Istanbul on Oct. 2. But Trump has touted the authoritarian prince's denials and sought to play down the expert assessment of his own intelligence community. There's even a tape.

“Unfortunately, at a moment in which it is most needed, the Trump administration has abdicated America’s moral leadership,” said Sen. Mark Warner (D-Va.), the vice chair of the Intelligence Committee. “In filling that void, and in light of the actions by the Saudis both in Yemen and in Khashoggi’s murder, the Senate must send a message that America’s moral voice will not be diminished.”





Sens. Bernie Sanders (I-Vt.), Mike Lee (R-Utah) and Chris Murphy (D-Conn.) celebrate at the Capitol after the Senate voted to end U.S. military support for the Saudi-led war in Yemen. (Jim Lo Scalzo/EPA-EFE)

**-- Thursday's vote was a personal and political triumph for three senators across the ideological spectrum who have made ending the war in Yemen their shared cause. Each believes strongly in the profound power of American moral leadership, and that Congress should reclaim the power to make war that the framers of the Constitution intended. Sen.**

Mike Lee (R-Utah), one of the most conservative members of the Senate, forged an alliance last year with Sen. Bernie Sanders (I-Vt.), a self-described democratic socialist, and Sen. Chris Murphy (D-Conn.), who is primarily known for advocating stricter gun control, to figure out ways to get the United States out of Yemen. They introduced the resolution that passed yesterday (with amendments) early in the year, but it was tabled in March. Khashoggi's heinous death created momentum to get it on the floor.

**“Today was a victory for the Constitution and the separation of powers,”** said Lee, who secured support from six of his GOP colleagues for the war powers resolution. “With this vote, we are one step closer to reviving our constitutional framework – where the power to declare war lies with Congress, not the executive branch – and we have taken a step towards removing ourselves from the spread of human suffering in Yemen.”

“For decades, under Republican presidents and Democratic presidents, Republican congresses and Democratic congresses, **the Congress of the United States has abdicated its constitutional responsibility for war-making,**” said Sanders. “It is not the president who has the responsibility under the Constitution to send our young men and women to war. It is the Congress. And we have got to take it back.”

“A bipartisan majority spoke with one voice that the status quo is over, and we will no longer accept the war crimes being committed in our name,” said Murphy. “The momentum is on one side, and it’s only growing.

**Congress has woken up** to the reality that the Saudi-led Coalition is using U.S. military support to kill thousands of civilians, bomb hospitals, block humanitarian aid and arm radical militias. The Saudis are important partners, but they need to realize that our partnership is not a blank check for them to fund extremists and murder civilians.”

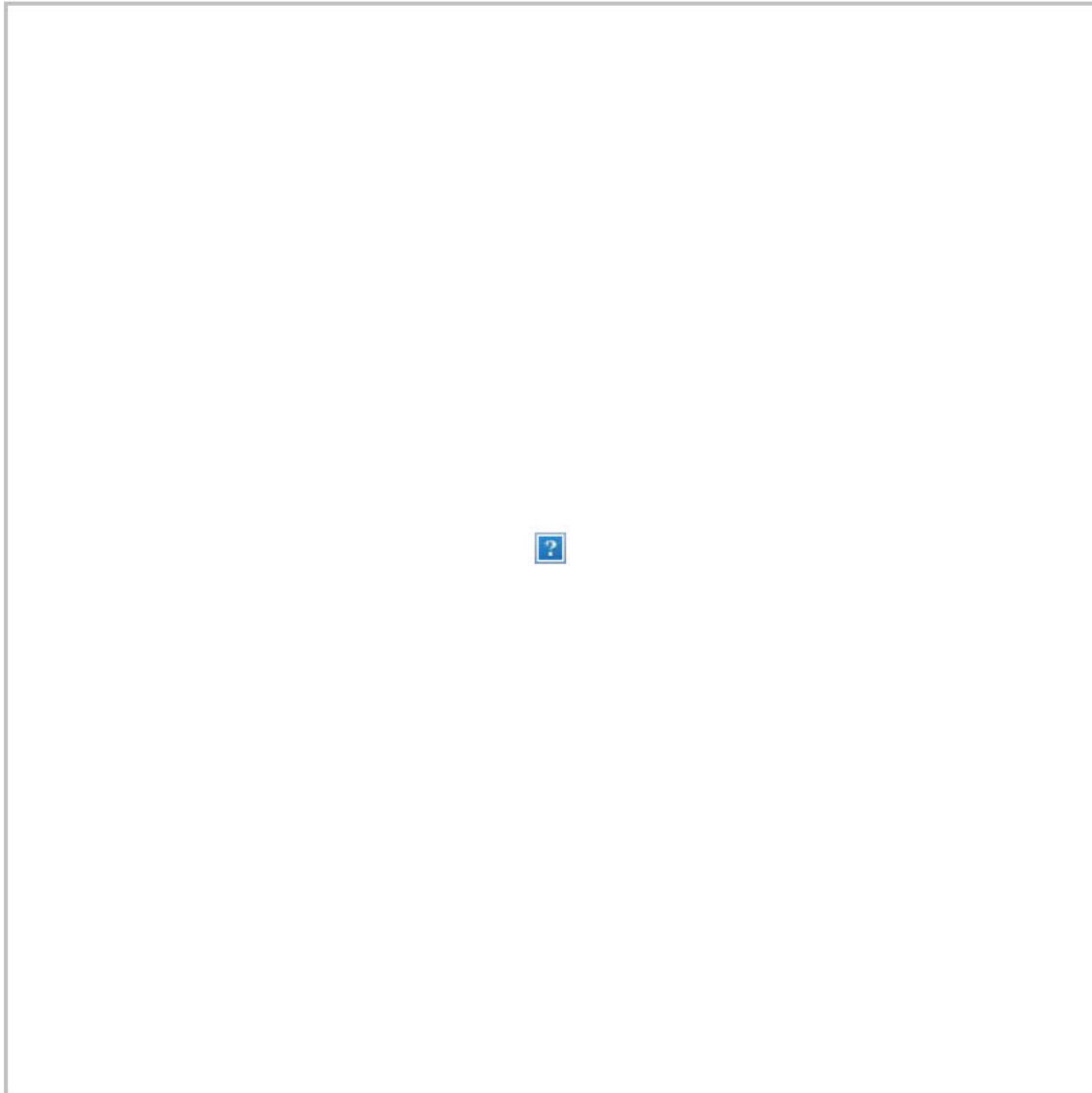


**-- House Republicans plan to ignore the war powers measure, and the White House has indicated Trump will disregard the nonbinding resolution, but the Senate debate appears to have had some impact at the negotiating table.**

A broader campaign of international pressure from the West has pushed the Saudis to make concessions in peace talks after four years of fighting. The United Nations has brokered negotiations in Sweden this week between Yemen's Saudi-backed government and the Houthis, the Iran-backed rebel group. **The two sides agreed yesterday to a cease-fire in the port city of Hodeida, which serves as a critical lifeline for humanitarian aid into the country.** They also apparently settled on terms for a prisoner swap. "We are living the beginning of the end of one of the biggest tragedies of the 21st century," U.N. Secretary-General António Guterres told reporters.

"Previous cease-fire agreements have collapsed quickly. But there has been greater international pressure on the warring sides in recent months to de-escalate the fighting, in part because of warnings by relief agencies that **more than 16 million people in Yemen — more than half of the country's population — are facing famine-like conditions,**" [Kareem Fahim and Missy Ryan report from Riyadh](#). **"More than 60,000 people,**

**combatants and civilians, have been killed in the conflict since 2016, according to an estimate by the Armed Conflict Location and Event Data Project.”**



Four-year-old Rakan used to weigh 40 pounds. Now he weighs 9 pounds.

**-- Many senators said they hope the resolution accelerates peace talks by putting Saudi Arabia on notice that they cannot count on unquestioning American support. “There must be a negotiated end to the fighting in Yemen, and the Saudi government must clearly understand that as a strategic ally of the United**



States, it has a responsibility to act in ways that promote democracy, human rights and stability in the region,” said Sen. Rob Portman (R-Ohio). “[W]e must send a message to the administration that we need a stronger response on this issue.”

“After reviewing the overwhelming evidence, it is clear that **the Saudi-led coalition’s actions in Yemen are no longer something we, as the leader of the free world, can support,**” added Sen. Joe Manchin (D-W.V.). “This resolution ... sends a clear message ... that the United States will no longer tolerate their disregard for human life.”



Women in war-torn Yemen uproot their families, and the children are traumatized

**-- Paul Ryan, doing the bidding of the administration in one of his final acts as speaker, jammed language into the farm bill on Wednesday that will prevent the House from using the War Powers Act during the remainder of the lame-duck session to cut off U.S. support for the Saudi effort in Yemen.**

“It's a common technique in the House: An unpopular measure is snuck into something that must pass. The

gimmick worked, but only because five Democrats who had worked on the farm bill broke with their party to support it,” [Dave Weigel reports](#). “In the new Democratic Party, that meant that five more Democrats were being talked about as targets for primary challenges. Alexandra Rojas, whose group Justice Democrats is recruiting challengers in 2020 House races, said the farm bill vote had galvanized activists who were on the verge of winning the Yemen fight.”



CONTENT FROM BANK OF AMERICA

## How to finance a cleaner planet

In 2018, Bank of America issued its fourth and largest green bond for \$2.25 billion. Learn more about this innovative way of financing a more sustainable future.

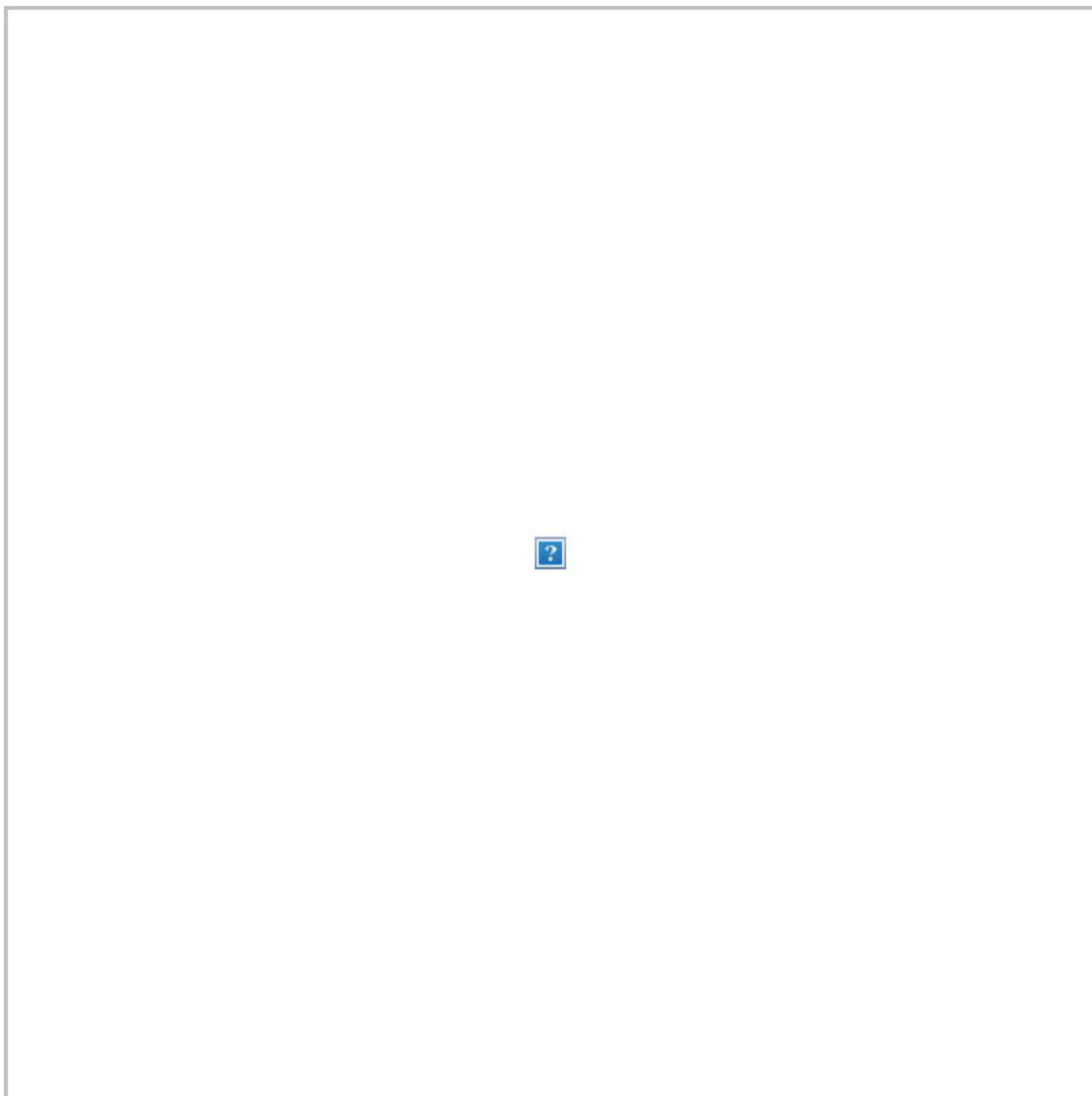


As war rages, children languish in Aden

-- But the comfortable margin in the Senate showed how much juice [the well-heeled Saudi lobby](#) has lost and could be a harbinger of what's to come once Democrats control the House, from implementing sanctions to curtailing arms sales to Riyadh.

“American foreign policy should be dictated by our national security interests and our values, not by the interests of the Saudi royal family,” said Sen. Maggie Hassan (D-N.H.).

“We won’t enable a president who chooses to cover up for Saudi leadership instead of standing up for American values,” added Sen. Tim Kaine (D-Va.).



As men fight and die in Yemen's civil war, wives and mothers are left to carry on

**-- How it's playing:**



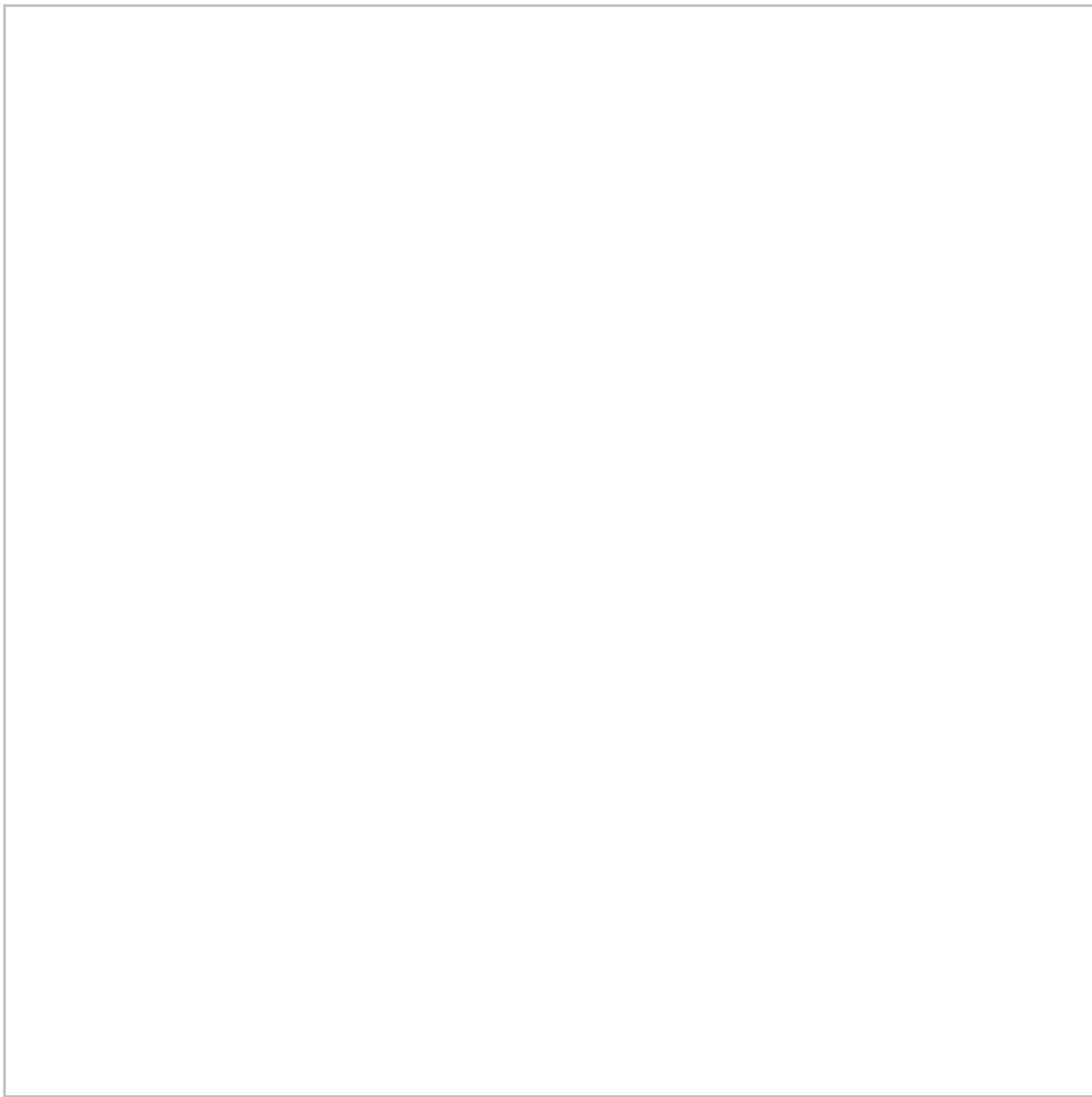
- [The Washington Post Editorial Board](#): **“The Trump administration won’t stand for Khashoggi. It could at least stand for jailed Saudi women.”**
- Katherine Zoeph in [the New York Times](#): **“The Saudi Regime’s Other Victims. The murder of Khashoggi has focused attention on Saudi Arabia’s human rights abuses. We need to remember all of the thousands in prison.”**
- [The Wall Street Journal](#): **“Saudi Arabia Pumps Up Stock Market After Bad News**, Including Khashoggi Murder. The government of Crown Prince Mohammed bin Salman has spent billions to counter selloffs in recent months.”
- [The Fix](#): **“The entire Senate just said Trump is wrong about Khashoggi.”**
- [The Economist](#): **“Trump’s efforts to boost the Saudi alliance risk damaging it.”**
- [Washington Monthly](#): **“We Should Have Reevaluated Our Saudi Alliance Before Now.”**
- [The Nation](#): **“What the Hell Is Wrong With Paul Ryan?** It is outrageous that the House Speaker continues to block action to end US support for Saudi atrocities against Yemen.”
- [Breitbart](#): **“Paul Ryan’s Last Act: Protecting Barack Obama’s Illegal War in Yemen with Democrat Votes.”**
- [HuffPost](#): **“5 Democrats Bail Out Paul Ryan And Protect Saudi Arabia.”**
- Sen. Marco Rubio (R-Fla.) op-ed for [Fox News](#):

**“Hold Saudis accountable, but don't ignore Iran in Yemen.”**

- [Haaretz](#): “Benjamin Netanyahu on Khashoggi Murder: Destabilizing Saudi Arabia Would Destabilize the World.”
- John Hanna, who served as Vice President Dick Cheney’s national security adviser, writes in [Foreign Policy](#): **“Neither Side Gets the Khashoggi Debate Right.** The tribalism infecting U.S. domestic politics has unfortunately crept deep into the foreign-policy discourse.”

**-- This new street sign has just been erected outside our headquarters:**

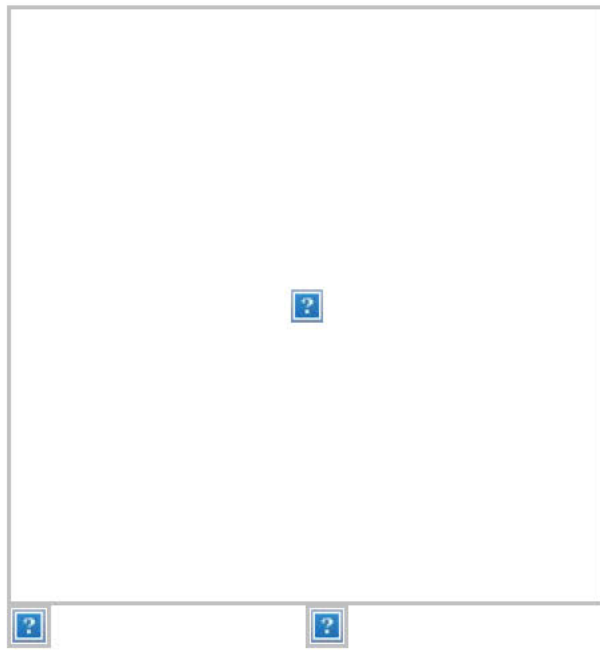




Subscribe on [Amazon Echo](#), [Google Home](#), [Apple HomePod](#) and other podcast players.

Welcome to the Daily 202, **PowerPost's** morning briefing for decision-makers.

[Sign up to receive the newsletter.](#)



**WHILE YOU WERE SLEEPING:**





Not just misleading. Not merely false. A lie. | Fact Checker

**-- Trump's insistence for much of the year that he had "no knowledge of any payments" to silence the women who allege they carried on extramarital affairs with him while the first lady was home caring for their infant son tops The Post Fact Checker's list of "the biggest Pinocchios of 2018." [Glenn Kessler explains](#):** "There has been no serial exaggerator in recent American politics like the president. He not only consistently makes false claims but also repeats them,

even though they have been proved wrong. The explosion of false and misleading statements from him in 2018 is well documented in our database: **In the seven weeks leading up the midterm elections, the president made 1,419 false or misleading claims — an average of 30 a day.** ... Meanwhile, the midterm election campaign, of course, was also an endless source of false claims, as an avalanche of negative ads tumbled across televisions screens. One of the president's ads is included on this list. Two potential opponents of the president in 2020 — Sens. Kamala D. Harris (D-Calif.) and [Bernie] — earn spots on our list. ...

**“Trump says many things that are factually incorrect, but he sometimes says things that are mind-blowingly false.** Despite having access to more information than anyone on Earth, he persists in making claims with literally no foundation. He has repeatedly claimed that U.S. Steel announced it is building new plants — anywhere from six to nine — but that's not true. He said that as president, Barack Obama, gave citizenship to 2,500 Iranians during the nuclear-deal negotiations, but that's not true. Over and over, Trump claimed that the Uzbek-born man who in 2017 was accused of killing eight people with a pickup truck in New York brought two dozen relatives to the United States through ‘chain migration.’ The real number is zero.

**“Trump and his aides claimed they did not have a**

**family separation policy, when in fact they did.** They said U.S. laws or court rulings forced them to separate families that crossed the border illegally, but that was not true. When a caravan of more than 5,000 migrants from Central America started making its way to the border, another series of dubious claims was spawned, including that people of Middle Eastern descent were involved. The president also falsely claimed that he had started building his border wall, but Congress has not appropriated the necessary funds.”



Sens. Bernie Sanders (I-Vt.) and Elizabeth Warren (D-Mass.) walk to the Senate floor after the weekly Democratic caucus policy luncheon. (Jonathan Ernst/Reuters)

## GET SMART FAST:

1. **Elizabeth Warren invited Bernie Sanders over for dinner at her D.C. condo to discuss their presidential ambitions.** Both acknowledged their likely 2020 bids, but neither senator sought the other's support or tried to dissuade the other from running. No staffers were allowed. ([New York Times](#))
2. **French police said they "neutralized" a person matching the description of the suspect in the Strasbourg Christmas market shooting.** An official in the Paris prosecutor's office told a French newspaper that the person caught was named Cherif Chekatt and that he's now dead. ([James McAuley](#))
3. **Actress Eliza Dushku received a confidential \$9.5 million settlement from CBS stemming from a sexual harassment complaint.** Dushku claimed she was retaliated against for confronting "Bull" actor Michael Weatherly about inappropriate comments he made. ([New York Times](#))
4. **News organizations with Australian operations largely declined to report on Cardinal George Pell's conviction on sexual abuse charges out of concern over the judge's gag order.** The judge in

the case, Peter Kidd, said some journalists are facing “the prospect of imprisonment and indeed substantial imprisonment” for violating the order. But many outlets outside of Australia, including The Washington Post, covered the conviction. ([Paul Farhi](#))

5. **The Kentucky Supreme Court unanimously struck down the state's pension reform law.** In a major defeat for Gov. Matt Bevin (R), the court ruled that the bill's speedy passage violated a provision in the Kentucky constitution requiring that lawmakers have a “fair opportunity” to consider legislation before voting on it. ([Louisville Courier Journal](#))
6. **Fed chairman Jay Powell has been emphasizing recently that the strong U.S. economy masks “important disparities by income, race and geography.”** In a sign of how economic benefits have not been evenly distributed, 4 in 10 American adults still say they could not cover a \$400 emergency expense. ([Heather Long](#))
7. **A former Special Forces soldier who was once awarded a Silver Star for his valor is facing a murder charge in connection to the 2010 killing of a suspected Taliban bombmaker.** Army Maj. Mathew L. Golsteyn allegedly said during a 2011



polygraph test while applying to the CIA that he killed the man, according to Army documents. ([Dan Lamothe](#))

8. **Indiana police said they prevented a potential mass shooting at a middle school after receiving a tip about the teenage suspect.** Officers exchanged gunfire with the suspect, who allegedly had plans to attack Dennis Intermediate School in Richmond, Ind., before he killed himself. ([Moriah Balingit and Mark Berman](#))
9. **A former Baylor University fraternity president who was accused of raping a young woman but received no jail time was barred from attending his commencement ceremony.** The University of Texas at Dallas added that Jacob Anderson is banned from campus following public outcry over his lenient sentence. ([Katie Mettler, Eli Rosenberg and Kristine Phillips](#))
10. **A California man who was trapped in the grease vent of a Chinese restaurant for two days was rescued by firefighters.** The man was hospitalized for dehydration and exhaustion but is expected to recover, while police officers have opened a trespassing and vandalism investigation. ([Amy B Wang](#))



Donald Trump takes the oath of office from Chief Justice John G. Roberts Jr. (Jim Bourg/Pool/AP)

## **THERE'S A BEAR IN THE WOODS:**

**-- Trump's 2017 inaugural committee is being investigated by federal prosecutors for possible misuse of funds. [The Wall Street Journal's Rebecca Davis O'Brien, Rebecca Ballhaus and Aruna Viswanatha report](#): "The criminal probe by the Manhattan U.S. attorney's office, which is in its early stages, also is**

**examining whether some of the committee's top donors gave money in exchange for access to the incoming Trump administration, policy concessions or to influence official administration positions.**

Giving money in exchange for political favors could run afoul of federal corruption laws. Diverting funds from the organization, which was registered as a nonprofit, could also violate federal law. ... **The investigation partly arises out of materials seized in the federal probe of former Trump lawyer Michael Cohen's business dealings** ... In April raids of Mr. Cohen's home, office and hotel room, [FBI] agents obtained a recorded conversation between Mr. Cohen and Stephanie Winston Wolkoff, a former adviser to Melania Trump, who worked on the inaugural events. In the recording, Ms. Wolkoff expressed concern about how the inaugural committee was spending money. ...

"The inaugural committee has publicly identified vendors accounting for \$61 million of the \$103 million it spent, and it hasn't provided details on those expenses, according to tax filings. As a nonprofit organization, the fund is only required to make public its top five vendors. **The committee raised more than double what former President Barack Obama's first inaugural fund reported raising in 2009, the previous record.**

[Trump's] funds came largely from wealthy donors and corporations who gave \$1 million or more — including casino billionaire Sheldon Adelson, AT&T Inc. and

Boeing Co.”

**-- The prosecutors are investigating whether the inaugural committee, as well as a pro-Trump super PAC, accepted illegal foreign donations, [according to the New York Times’s Sharon LaFraniere, Maggie Haberman and Adam Goldman](#).** “The inquiry focuses on whether people from Middle Eastern nations — including Qatar, Saudi Arabia and the United Arab Emirates — used straw donors to disguise their donations to the two funds. Federal law prohibits foreign contributions to federal campaigns, political action committees and inaugural funds. ... Thomas J. Barrack Jr., a billionaire financier and one of Mr. Trump’s closest friends, raised money for both funds. ... The super PAC, Rebuilding America Now, was formed in the summer of 2016 when Mr. Trump’s presidential campaign was short of cash and out of favor with many major Republican donors.”

**-- Multiple news outlets have now confirmed that Trump himself was at the August 2015 meeting where Cohen and National Enquirer publisher David Pecker discussed hush-money payments to the president's alleged mistresses.** The Wall Street Journal first reported the president’s attendance at the meeting last month. [NBC News’s Tom Winter reports:](#) “As part of a nonprosecution agreement disclosed Wednesday by federal prosecutors, American Media Inc., the Enquirer's parent company, admitted that ‘Pecker

offered to help deal with negative stories about that presidential candidate's relationships with women by, among other things, assisting the campaign in identifying such stories so they could be purchased and their publication avoided.' The 'statement of admitted facts' says that AMI admitted making a \$150,000 payment 'in concert with the campaign,' and says that Pecker, Cohen and 'at least one other member of the campaign' were in the meeting. According to a person familiar with the matter, the 'other member' was Trump."

**-- In his first interview since being sentenced, Cohen said of the hush-money payments that Trump "was very concerned about how this would affect the election."** [John Wagner reports](#): "Cohen, who has admitted facilitating payments to two women in violation of campaign finance laws, told ABC News that he knew what he was doing was wrong. Asked whether the president also knew it was wrong to make the payments, Cohen replied, 'Of course.' He added that the purpose was to 'help [Trump] and his campaign.' ... His comments, in an interview on 'Good Morning America,' are at odds with those of Trump on Thursday in tweets and a television interview."

**-- "[The president's] evolving strategy on the hush-money allegations is textbook Trump: Tell one version of events until it falls apart, then tell a new version, and so on — until the danger passes,"** [Philip](#)



[Rucker and John Wagner report](#). “The latest developments have exposed the depth of Trump’s efforts to deceive the public about the illegal hush-money payments, and some of his friends and advisers said privately that they fear those efforts could imperil the president. While there is a consensus view inside the White House that a sitting president will not be indicted, [a] former senior administration official described a deep uncertainty about other ways that Trump could be held liable. And **there is growing anxiety among Trump’s allies, including in Congress, that he could be vulnerable to the various investigations and, eventually, Democratic-led impeachment proceedings.**”

-- The escalating investigations, aided by cooperation from Trump’s former allies, have left the president feeling increasingly isolated. [The Los Angeles Times’s Chris Megerian and Eli Stokols report](#): “Several [people] close to the president ... said Trump already senses diminishing respect and worries about losing support from powerful financial donors and Republican lawmakers as his legal and political troubles worsen. ‘They’re still not saying it publicly, but most Republicans on the Hill understand ... that it’s not going to end well, that it’s going to be bad,’ said a longtime Republican operative close to party leadership.”

-- The latest developments in the Russia

**investigation have reinvigorated claims from Trump's critics that his election victory was illegitimate.** [Marc Fisher reports](#): "The evidence emerging in recent days and months that multiple crimes were committed in an effort to help Trump win the presidency is fueling arguments from Democrats and other Trump critics that the man in the Oval Office got the job through nefarious means. Even with no proof that those crimes swayed votes, the critics say, Trump has no moral hold on the office. ... Trump and his defenders retort that prosecutors so far have fallen well short of proving criminal deeds by the president himself. They say the legitimacy debate is just one more weapon in a bristling partisan arsenal deployed by Trump haters on the left."

**-- Another threat: House Minority Leader Nancy Pelosi said she expects a House committee to "take the first steps" toward getting Trump's tax returns after Democrats retake the chamber next month.** [John Wagner reports](#): "Pelosi said the decision on whether to initiate the process will fall to the Ways and Means Committee. Rep. Richard E. Neal (D-Mass.), who is expected to become chairman of the tax panel, has said he plans to insist that Trump release his tax returns. If Trump doesn't do so voluntarily, then Neal plans to file a legal request with the Treasury secretary that would require that the returns be disclosed to a small group of people on Capitol Hill. Neal has predicted that the matter would end up in federal court."



How Maria Butina forged ties with gun rights advocates and other U.S. conservatives

**-- The guilty plea of Russian agent Maria Butina has cast an unwanted spotlight on the National Rifle Association, a group she allegedly infiltrated at the highest levels and whose legal exposure remains unclear. [Rosalind S. Helderman, Tom Hamburger and Michelle Ye Hee Lee report](#): “One of Butina’s main targets was the NRA — a group she identified in a 2015 memo as an organization that 'had influence**

**over' the Republican Party**, according to court filings. Her relationships with the group, she wrote, could be used as the groundwork for an unofficial channel of communication to the next presidential administration. Later that year, she helped organize a delegation of top NRA leaders to visit Moscow, arranging for them to meet Russian government officials, and she attended the group's annual conventions as an honored guest. Butina and Alexander Torshin, a former Russian government official who helped direct her activities, then used their NRA connections to get access to GOP presidential candidates."

**"NRA officials, who did not return requests for comment Thursday, have repeatedly refused to answer questions about Butina or its interactions with Russian activists.** NRA spending on the 2016 elections surged in every category, with its political action committee and political nonprofit arm together shelling out \$54.4 million. The bulk of the money — \$30 million — went to efforts supporting Trump. That is triple the amount the group devoted to electing Republican Mitt Romney in the 2012 presidential race. ... The group's spending on federal races in 2018 plummeted to roughly \$9 million."

**-- Mueller's pattern of getting guilty pleas from cooperating witnesses may suggest his investigation is nearing its end. [Devlin Barrett reports](#):** "In the cases



of Cohen, former campaign adviser George Papadopoulos, former campaign chairman Paul Manafort, and former national security adviser Michael Flynn, Mueller has proceeded to the sentencing of each without first making him testify at trial against others. That's at odds with the common practice of prosecutors — which is to hold the stick of a tougher prison sentence over defendants until they have completed all of their cooperation, particularly any public testimony. While the recent legal action has led to speculation that prosecutors are narrowing in on the president in anticipation of more criminal charges, **Mueller's sentencing timeline suggests a different outcome to some legal experts — that the accounts of those cooperating witnesses will appear in a written report, not in court."**

**-- The House and Senate Intelligence Committees are looking to talk to several people who have been charged in Mueller's investigation. [CNN's Jeremy Herb and Manu Raju report](#):** "The [Senate] committee has been engaged in discussions with the special counsel and defense attorneys to get access to several cooperating Mueller witnesses in addition to Cohen, including Flynn, Papadopoulos and [Manafort's deputy Rick] Gates, according to a source familiar with the investigation. ... The expected incoming chairman of the House Intelligence Committee, Democratic Rep. Adam Schiff of California, has also expressed a desire to speak



again to Cohen, who testified behind closed doors before both intelligence panels last year. Schiff has said he's in touch with Cohen's legal team, too."

**-- Friends and associates of Michael Flynn agree that his public persona underwent a radical transformation in the past few years, but they are divided as to why. [Marc Fisher writes](#) in an in-depth piece on Trump's former national security adviser: "His friends and critics agree that after winning a reputation as a master intelligence officer on the battlefields of Iraq and Afghanistan, Flynn broke with lifelong patterns of behavior. Once discreet and apolitical, he morphed into a highly partisan alarm ringer. A man once trusted to cautiously analyze information began touting wild hearsay as fact. ... Did he gradually absorb a new, conspiracy-minded worldview, in part inspired by his son Michael Jr.'s embrace of fringy ideas? Did he discard lifelong habits because he'd been enraged to his core when President Barack Obama's administration in 2014 removed him as director of the Defense Intelligence Agency (DIA), his last and most senior military assignment? Or had Flynn, who retired as a lieutenant general, long harbored extreme views, successfully shielding his real opinions from those around him?"**



Children join a protest in the Senate Hart Building on the day of the court-imposed deadline for the Trump administration to return migrant children who were separated from their parents. (Salwan Georges/The Washington Post)

## **THE IMMIGRATION WARS:**

**-- Stories from the border: A 7-year-old girl from Guatemala died of dehydration and exhaustion after she was taken into Border Patrol custody last week. [Nick Miroff and Robert Moore report](#): “The child’s death is likely to intensify scrutiny of detention conditions at**



Border Patrol stations and CBP facilities that are increasingly overwhelmed by large numbers of families seeking asylum in the United States. According to CBP records, the girl and her father were taken into custody about 10 p.m. Dec. 6 south of Lordsburg, N.M., as part of a group of 163 people who approached U.S. agents to turn themselves in. More than eight hours later, the child began having seizures at 6:25 a.m., CBP records show. **Emergency responders, who arrived soon after, measured her body temperature at 105.7 degrees, and according to a statement from CBP, she ‘reportedly had not eaten or consumed water for several days.’** ... The agency is investigating the incident to ensure appropriate policies were followed.”

-- Trump pledged to do “whatever it takes to get border security,” even as he tried to shift blame toward Democrats for any potential government shutdown. [Erica Werner, Damian Paletta and John Wagner report](#): “In a video posted on Twitter, Trump attacked Democrats as ‘absolute hypocrites’ and claimed they’ve supported funding border barriers in the past but won’t do so now because of their opposition to him. The video showed images of people rushing the border and included clips of [Chuck Schumer], former secretary of state Hillary Clinton and [Barack Obama] speaking in opposition to illegal immigration and in favor of border security. ‘We need to have the wall. We need border security. Whatever it takes to get border security, I will do

it,' Trump says in the video. 'I pledged that a long time ago, and I will pledge it always.'" Reminder: Trump said just three days ago [he would be "proud"](#) to shut the government down over wall funding.

**-- Lawmakers say no progress has been made on a border wall deal since Trump had his contentious meeting with Schumer and Pelosi. [Politico's Sarah Ferris, Burgess Everett and Anthony Adragna report:](#)**

"Lawmakers say there is no public plan to prevent a partial government shuttering. And no secret plan either. 'There is no discernable plan. None that's been disclosed,' said Sen. John Cornyn, the Senate's No. 2 Republican, as he threw his hands into the air. ... The House isn't planning to return until the night of Dec. 19 — leaving only about 72 hours to reach a border wall deal that has eluded both parties for months. **Democrats say they're waiting on Republicans, and Republicans say they're waiting on Trump.**"

**-- In case you missed it: ICE has arrested 170 immigrants who sought to sponsor migrant children. [NBC News's Daniella Silva reports:](#)** "ICE said Tuesday that the arrests were of immigrants suspected of being in the United States illegally and took place from early July to November. They were the result of background checks conducted on potential sponsors of unaccompanied migrant children placed under the care of the Department of Health and Human Services. Nearly two thirds of those



arrested — 109 in total — had no criminal record, the agency said. Another 61 of those arrested did have criminal records, but ICE did not specify the crimes and said it could not break down convictions by violent and nonviolent offenses.”

**-- DHS issued a news release entitled, “Walls Work,” which included questionable claims about the progress being made on Trump’s border wall. [USA Today’s William Cummings reports](#): “DHS is committed to building wall and building wall quickly,’ reads the release, which eschews the use of articles in many instances. ‘We are not replacing short, outdated and ineffective wall with similar wall. Instead, under this President we are building a wall that is 30-feet high.’ ‘FACT: Prior to President Trump taking office, we have never built wall that high,’ the message adds. The government has built higher walls, but the statement presumably meant to specify it was referring to a border wall.”**





Ivanka Trump departs Air Force One with Jared Kushner in Coraopolis, Pa. (Keith Srakocic/AP)

## **WEST WING INTRIGUE:**

**-- Trump is considering his son-in-law Jared Kushner for White House chief of staff, according to [HuffPost's S.V. Date](#):** “[Kushner] met with Trump Wednesday about the job, a top Republican close to the White House [said]. He and two others close to Trump or the White House ... confirmed Kushner’s interest in the position. ... Kushner

has been pushing his own candidacy with Trump, citing his work on a criminal justice reform package and a claimed ability to work with Democrats, one person said. 'I don't know why he thinks that, when the Democrats are mainly going to be coming after Trump,' the source said. ... **Trump told reporters Thursday that he is down to five finalists.** 'We are interviewing people now for chief of staff,' he said at a photo opportunity with newly elected governors who were visiting the White House."

-- **Trump also met with former New Jersey governor Chris Christie about the job last night, [per Axios's Jonathan Swan](#).** "[Trump] considers him a top contender to replace John Kelly as chief of staff, according to a source. ... Trump has met with a couple of others, but the way he's discussed Christie to confidants make them think he's serious. His legal background may come in handy next year."

-- **Some advisers are encouraging Trump to consider young White House aide Johnny DeStefano for chief of staff. [The LA Times's Eli Stokols reports:](#)** "Several people close to the president are promoting [DeStefano], who was a political aide to former House Speaker John A. Boehner before joining the administration as Trump's director of personnel. He since has seen his portfolio expand and often travels with the president."

-- **The president's top aides remain deeply divided**

**over whether Trump's former deputy campaign manager David Bossie should be considered for the job.** [Politico's Gabby Orr, Andrew Restuccia and Rebecca Morin report](#): "Some White House allies say [Bossie] shot to the top of the list the minute Trump expressed an interest in having an effective political operator in the slot. His chances only improved, they add, when Rep. Mark Meadows (R-N.C.), head of the conservative Freedom Caucus, fell out of the running. But others quickly dismiss the speculation, saying the Trump world adviser can't overcome opposition within the first family and lingering concerns about a hotheadedness that kept him out of the West Wing to begin with."

**-- "Trump's hunt for a new chief of staff has taken on the feel of a reality TV show,"** [the AP's Catherine Lucey and Jonathan Lemire write](#). "No leading name has emerged in the days since Trump's preferred candidate to replace John Kelly bowed out. But the void has quickly filled with drama. ... Trump himself likes to feed the drama, dropping hints about the number of candidates in the running and bantering with journalists about who wants the job. The erratic search recalled the transition period before Trump took office, when prospective aides and television personalities paraded before a pack of journalists in the lobby of Trump Tower. Author Chris Whipple, an expert on chiefs of staff, called the search process 'sad to watch.'"





Pelosi 'comfortable' with term-limit deal

**IF YOU COME AT THE QUEEN, [YOU BEST NOT MISS:](#)**

**-- There are two deeply reported tick-tocks this morning on how Nancy Pelosi locked down the votes to become speaker. Both focus on the many strategic and tactical mistakes made by Rep. Seth Moulton (D-Mass.), the ringleader of the rebels trying to take her down. The hyper-ambitious Moulton has become a lightning rod, and Pelosi allies — including some of the**

biggest donors in the Democratic Party — are now determined to field a primary challenger against him in 2020.

-- **“Moulton had drawn up list of 58 Democrats who he knew wanted a new leader. Most of those, he said he believed, would sign a letter expressing opposition to Pelosi. ... Instead of 35 names, the rebels ultimately released a letter Nov. 19 with only 16 names,”** [Mike DeBonis and Robert Costa report](#). “‘A lot of summer soldiers around here,’ Moulton, a former Marine Corps officer, would say.

- “When during a CNN appearance he accused Pelosi of not moving aggressively on gun-control legislation during her previous time as speaker, her aides lined up gun-control advocates to criticize him.
- “He annoyed other members of the group by issuing a statement two days before the nominating vote declaring that he was willing to negotiate with Pelosi about the broader leadership team, upending their strategy.
- “Other members of the rebel group urged Rep. Kathleen Rice (D-N.Y.) to take a more aggressive role as a female face of the anti-Pelosi effort, but she bristled at being asked to step forward as a token woman — especially by Moulton, whom she blamed for strategic missteps.”



-- “Moulton told his colleagues that he’d win over the incoming freshmen, even referring to these lawmakers as ‘my candidates,’ according to multiple Democratic sources,” [per Politico’s Rachael Bade, Heather Caygle and John Bresnahan](#). “Moulton had a personal connection to the anti-Pelosi candidates who had military backgrounds. He campaigned with them, raised money for them and worked alongside VoteVets, a progressive political organization supporting veterans running for office, to try to get them elected. Moulton told these members-elect that Pelosi was going to be ousted and that it would be good for them politically to join the movement. But **Moulton oversold his sway, rebel sources complained**. Rep.-elect Mikie Sherrill, a former Navy helicopter pilot running in New Jersey, had released an ad against Pelosi and campaigned with Moulton. But she wouldn’t go anywhere near the letter. Several other freshmen who received help from Moulton also avoided the letter.

“**Pelosi had neutered Moulton right under his nose**. Just days after the election, she phoned VoteVets’ Chairman Jon Soltz and asked for his help wooing the incoming freshmen. Soltz had been working with Moulton but also had a close relationship with Pelosi. Soltz decided his group would remain neutral. But he gave the candidates advice that proved critical to helping Pelosi, sources said: Think about the long game. To be an effective legislator, you will have to work with the next

speaker — which more likely than not would be Pelosi. The advice worked. The candidates refused to sign the rebels' document. And when Moulton lobbied harder for their signatures, he repelled them even more. In fact, **some female veterans told other Democrats that they were annoyed with Moulton, these lawmakers said, concluding that they were being used for Moulton's own political gain. ...**

**“He asked for a meeting with Pelosi to start talks between the two sides — then misled his fellow rebels about who initiated the discussion, according to three sources familiar with the incident.** Moulton told [Rice] and Rep. Tim Ryan (D-Ohio) — perhaps Pelosi's staunchest critics in the group — that Pelosi requested the meeting. In reality, he had gone to Pelosi's staff and said he wanted to sit down. It created an awkward dynamic before a terrible meeting. Rice walked into Pelosi's office and said, ‘Thank you for calling this meeting.’ ‘I didn't ask for this meeting,’ Pelosi scoffed. An awkward silence ensued, and the meeting unraveled from there.”

**-- The term-limit deal Pelosi negotiated has once again cast a spotlight on her complicated relationship with her No. 2, Steny Hoyer (D-Md.). [The New York Times's Sheryl Gay Stolberg reports](#):** “The friction goes back decades. The last time Democrats took power from Republicans, in 2006, Ms. Pelosi backed



then-Representative John P. Murtha in his effort to oust Mr. Hoyer from the majority leader's slot. The putsch failed spectacularly, but she's ready to handcuff him again with a deal on term limits. ... Some see Mr. Hoyer as the ultimate corporate pol, out of sync with a Democratic caucus in which women, millennials and people of color are in ascendance, with the loudest new voices on the left. ... But over his more than 50 years in public life, 37 of them in Congress, Mr. Hoyer has proved himself a quiet survivor."



## **MIDTERMS FALLOUT:**

**-- GOP congressional candidate Mark Harris directed the hiring of the operative now at the center of election fraud allegations in North Carolina, despite warnings about his tactics.** [Amy Gardner and Beth Reinhard report](#): “Harris sought out the operative, Leslie McCrae Dowless, after losing a 2016 election in which Dowless had helped one of Harris’s opponents win an overwhelming share of the mail-in vote in a key county. State and local investigators say that whether Harris knew that his campaign may have engaged in improper tactics has become a focus of the expanding probes into whether election irregularities affected the 9th District election, in which Harris leads Democrat Dan McCready by 905 votes. That question is also roiling the state Republican Party, whose leaders had rallied around Harris, a 52-year-old evangelical pastor from the suburbs of Charlotte. **Party leaders are now backing away from Harris and trying to limit the fallout** of a scandal that has delayed certification of the last undecided federal contest of the 2018 election cycle. ...

**“Harris was warned about possible fraud on primary day in June 2016**, during his first bid for the 9th District congressional seat, according to people familiar with the conversation. The incumbent congressman and winner of the primary had received just one mail-in vote in rural



Bladen County. Harris, who came in second place, had won four. Johnson, the last-place contender, meanwhile, had received nearly all of them — 221. The only explanation, advisers told Harris that night in Charlotte, was that something shady had occurred on that third-place campaign, according to the people. A year later, they said, when Harris resolved to run for Congress again, the candidate personally directed the hiring of Dowless, an adept field operative and Bladen County native who had helped deliver that unusual result in 2016.”

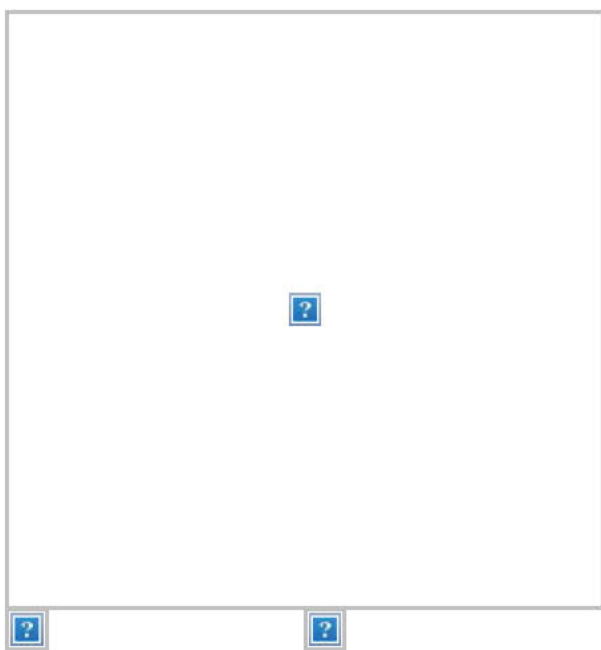
**-- Arizona Gov. Doug Ducey (R) is cooling on the idea of appointing former Senate candidate Martha McSally to John McCain’s old Senate seat if Sen. Jon Kyl (R) steps aside. [Sean Sullivan reports](#):** “Ducey has made no firm decision and McSally, who narrowly lost this year’s Senate race, remains a finalist. ... But her stock has fallen in the eyes of the governor, according to two people familiar with his thinking, as Ducey approaches one of the most significant decisions of his political career. Ducey’s choice would affect not only the future of the Senate but the 2020 elections in an increasingly competitive battleground state. It could also impact his relationship with [Mitch McConnell], a McSally advocate, as well as other party leaders who want to see more Republican women in Congress.”

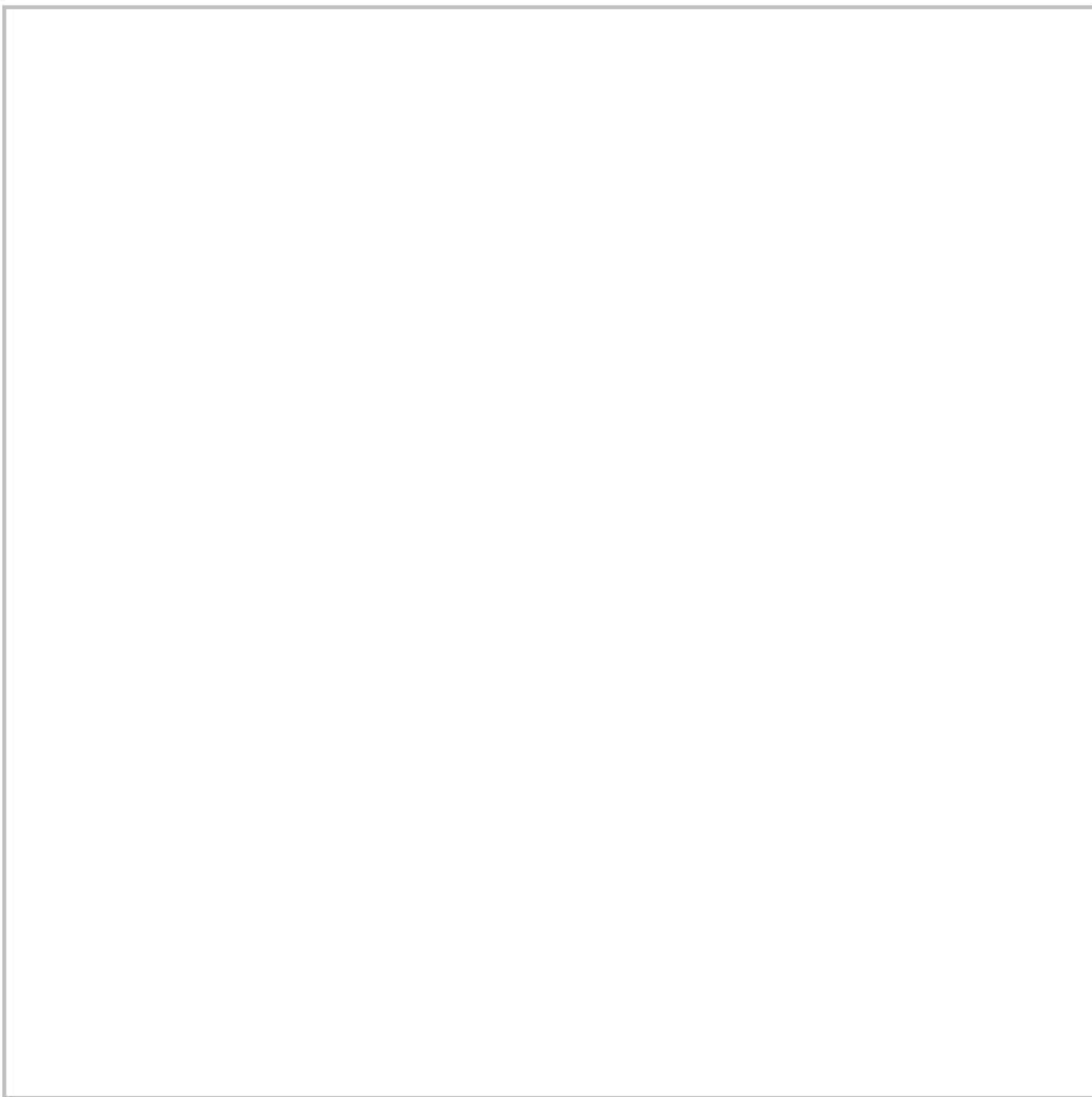
**-- A federal judge rejected GOP Rep. Bruce Poliquin’s**



**lawsuit challenging Maine's candidate-ranking system.** [The AP's Marina Villeneuve and Patrick Whittle report](#): "Poliquin sought to have the voting system declared unconstitutional after he lost the election to Democrat Jared Golden despite having the most first-place votes. Poliquin asked U.S. District Judge Lance Walker either to declare him the winner or order another election for the 2nd Congressional District. But Walker, appointed by [Trump], said states are given great leeway in how they conduct elections. Critics can question the wisdom of ranked-choice voting, Walker said, but such criticism 'falls short of constitutional impropriety.'"

**-- Kansas's incoming Democratic governor turned down a White House invitation to meet with Trump and other governors-elect,** [according to the Wichita Eagle's Jonathan Shorman and Bryan Lowry](#). "Trump campaigned aggressively for Gov-elect Laura Kelly's Republican opponent, Kansas Secretary of State Kris Kobach, this fall. ... Kelly's team said she was unable to travel to Washington because she is focused on the transition and the state budget. ... Kelly and every other newly elected governor was invited to attend the Thursday meeting to discuss shared state and federal priorities, including workforce development, infrastructure, support for veterans and military families and fighting the opioid crisis, according to the White House."





Blake Farenthold, pictured in 2017, resigned as a Republican congressman from Texas after sexual harassment accusations. (Susan Walsh/AP)

## **MORE FROM THE HILL:**

**-- The House and Senate quickly passed a bill aimed at overhauling how Congress handles sexual harassment complaints and sent the legislation to Trump's desk. [Elise Viebeck reports](#):** "Advocates welcomed the measure, which mandates an annual report of all settlements and awards and eliminates the



confidentiality agreements required for accusers at the beginning of the existing process. ... The measure approved on Thursday only requires lawmakers to pay for settlements involving harassment and retaliation, not discrimination. Cases in which a woman is fired for being pregnant, for example, would not trigger the liability. Republicans and Democrats in the lower chamber said they plan to introduce legislation next year to change this on the House side.” Why it matters: **Trump will now sign into law a bill made possible by the #MeToo movement, which was triggered in part by his electoral victory despite accusations of sexual misconduct and which he has [repeatedly mocked](#) over the past year.**

**-- House Republicans are increasing pressure on the Trump administration to end government funding for research using fetal tissue. [Amy Goldstein reports](#):** “[A] hearing before subcommittees of the House Oversight and Government Reform Committee grew testy at times over whether cells from sources other than aborted fetuses are as useful as fetal tissue in advancing therapies and possible cures for diseases from HIV to cancer. ... The hearing, which played to Republicans’ base of social and religious conservatives, comes amid moves by Trump health officials to rethink whether federal money should continue to support the research. In the past three months, the Department of Health and Human Services has [severed one contract](#) with a

California firm that has been a major supplier of such tissue for laboratories.”

**-- For the second consecutive year, the Senate will allow to lapse Barry Lee Myers’s nomination to lead the National Oceanic and Atmospheric Administration.** [The New York Times’s Lisa Friedman reports](#): “Democrats have said that Mr. Myers has significant conflicts of interest, including his past eagerness to privatize the National Weather Service. ... Republicans blamed Democrats for the delay. Mr. Trump had to renominate Mr. Myers in January after the Senate failed to act last year. Mr. Myers has twice been advanced by the Commerce Committee, said Senator John Thune of South Dakota, the Republican chairman.”

**-- Senate Armed Services Committee Chairman Jim Inhofe (R-Okla.) tried to defend his purchase (and rapid sale) of stock in a defense contractor after he voiced support for record Pentagon spending.** [Karoun Demirjian reports](#): “Inhofe said through spokeswoman Leacy Burke that the purchase was made without his knowledge by a third-party adviser, and that he had ‘no involvement’ in the transaction. ‘The Senator has called his financial adviser and they reversed, or busted, the transaction,’ Burke said, referring to a Wednesday letter in which Inhofe instructed adviser Keith Goddard ‘to no longer purchase defense or aerospace companies as part of my financial holdings.’”



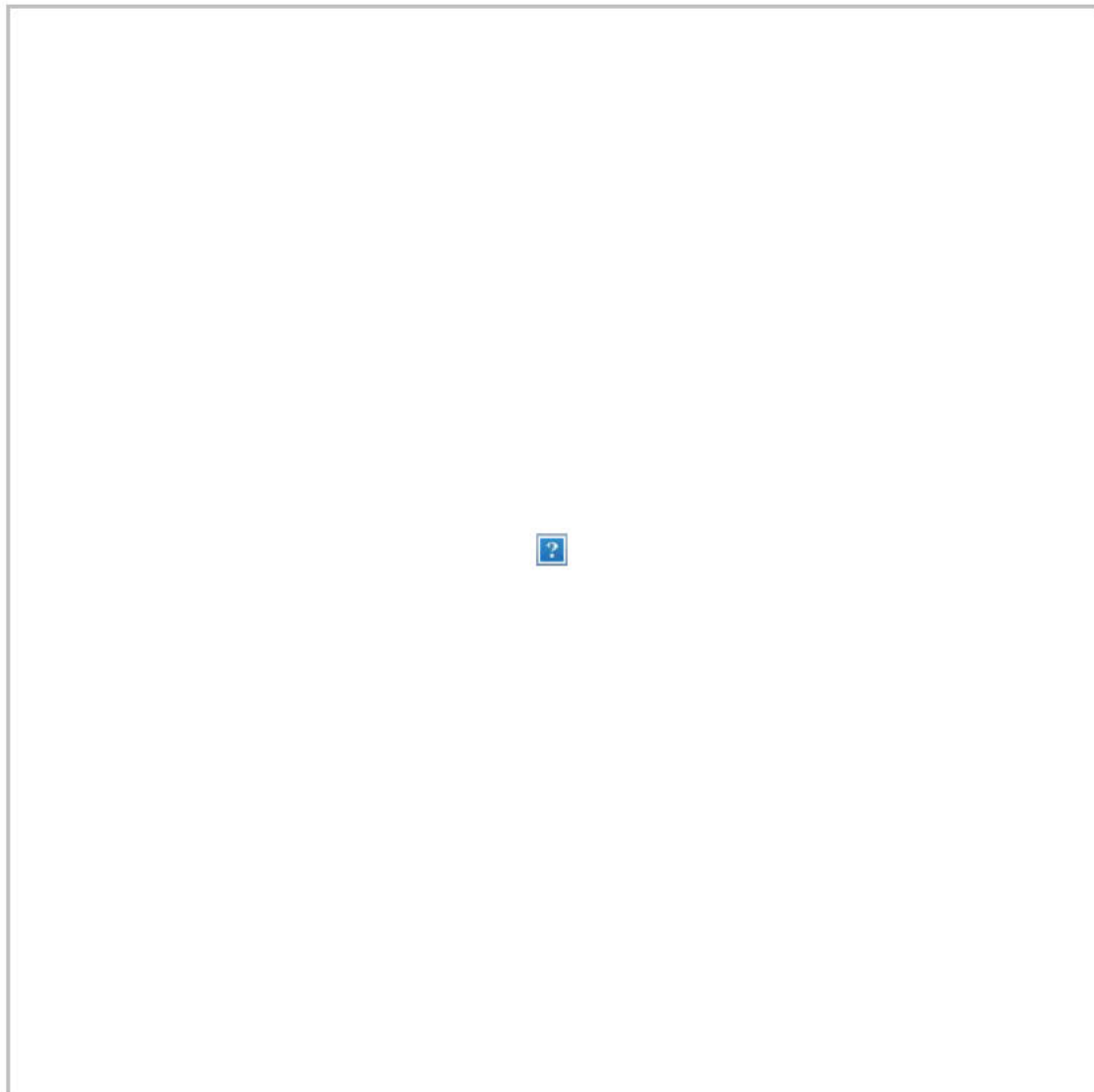
**-- Sens. Claire McCaskill (D-Mo.) and Jeff Flake (R-Ariz.) used their farewell addresses to blast the dysfunction of the Senate and politics generally. [NBC News's Allan Smith reports](#):** “Peter Morgan, an author, wrote that no family is complete without an embarrassing uncle,’ said [McCaskill]. ‘We have too many embarrassing uncles in the United States Senate. Lots of embarrassing stuff.’ She said that if senators ‘don’t have the strength to look in the mirror and fix’ the Senate, ‘the American people are going to grow more and more cynical, and they might do something crazy like elect a reality TV star president.’ McCaskill added: ‘The United States Senate is no longer the world’s greatest deliberative body. And everybody needs to quit saying it until we recover from this period of polarization and the fear of the political consequences of tough votes.’

**“Earlier, Flake used his final address on the Senate floor to warn of threats to America’s democracy ‘from within and without.’** ‘We of course are testing the institutions of American liberty in ways that none of us likely ever imagined we would — and in ways that we never should again,’ Flake said. ‘My colleagues, to say that our politics is not healthy is something of an understatement. I believe that we all know well that this is not a normal time, that the threats to our democracy from within and without are real, and none of us can say with confidence how the situation that we now find ourselves

in will turn out.’”

## **SOCIAL MEDIA SPEED READ:**

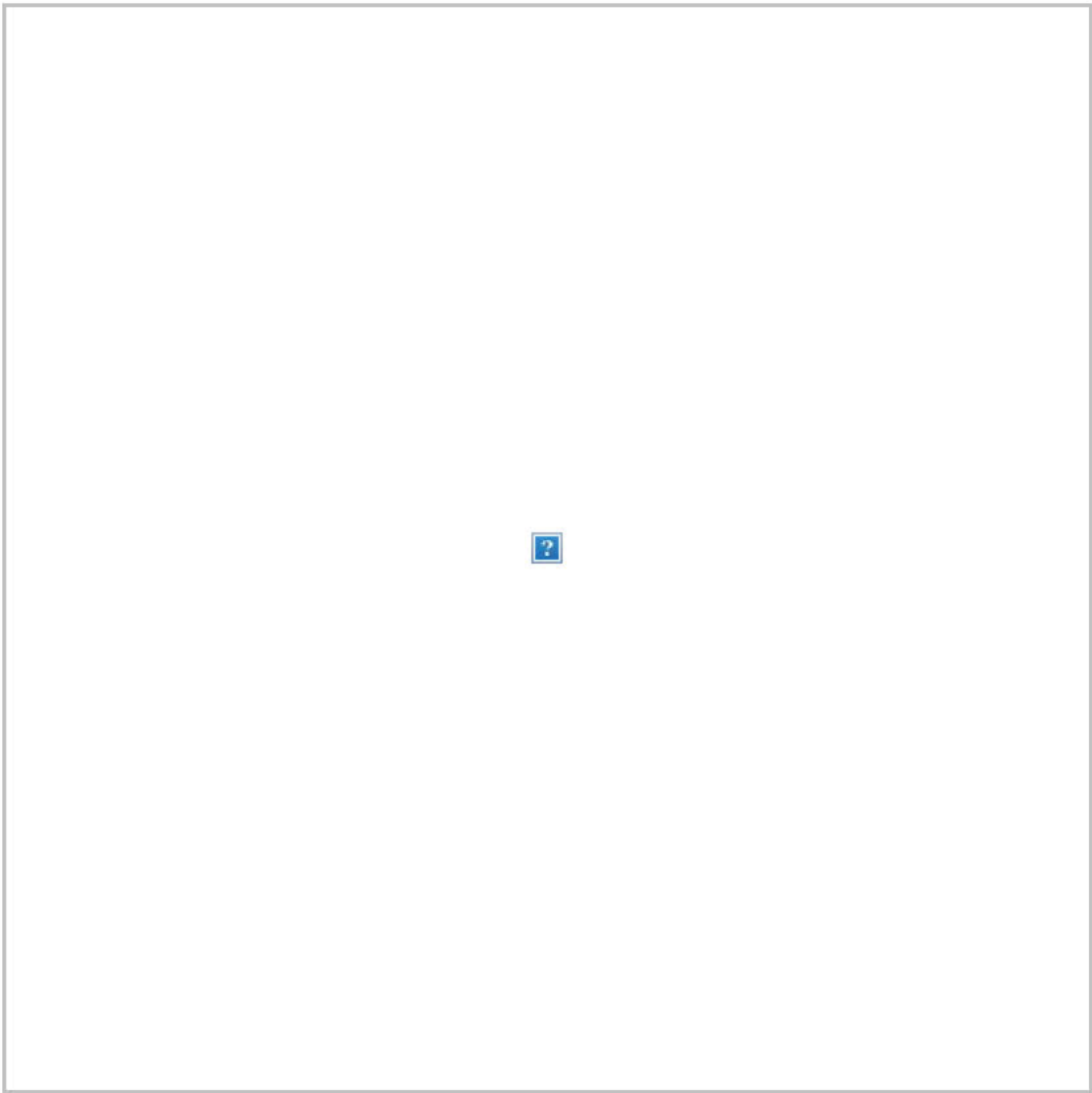
George Conway, who is married to White House adviser Kellyanne Conway, said he didn't believe Trump's comments about Michael Cohen:



A former CIA director explained the three different types of Russian espionage after Butina's guilty plea:



Per a Washington Post reporter, a White House official challenged the HuffPost story that Kushner is under consideration for the chief of staff job:



Trump's two chiefs of staff met again at the White House:

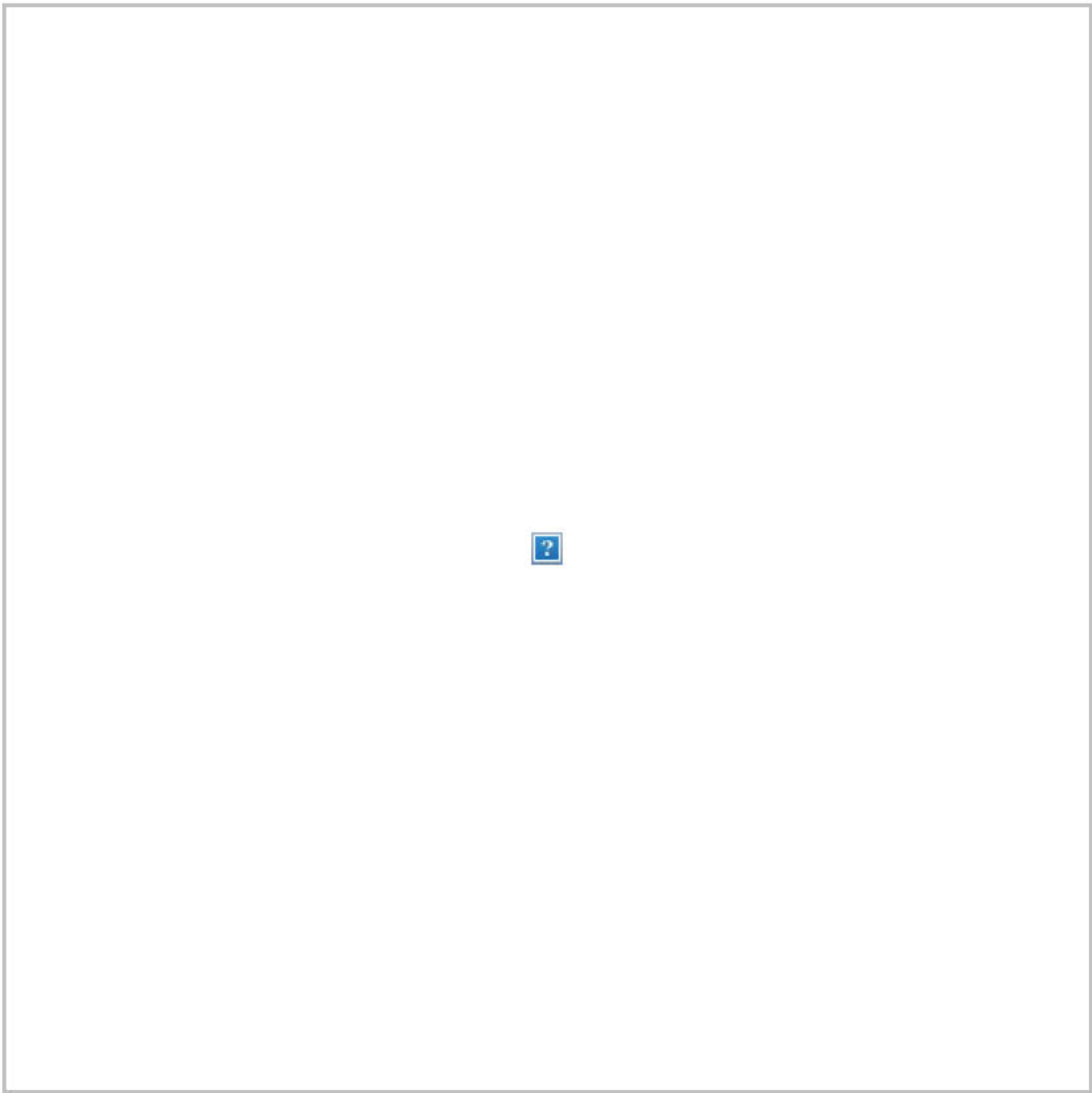


Former secretary of state John Kerry had harsh words for a Trump administration proposal to deport certain Vietnam War refugees:

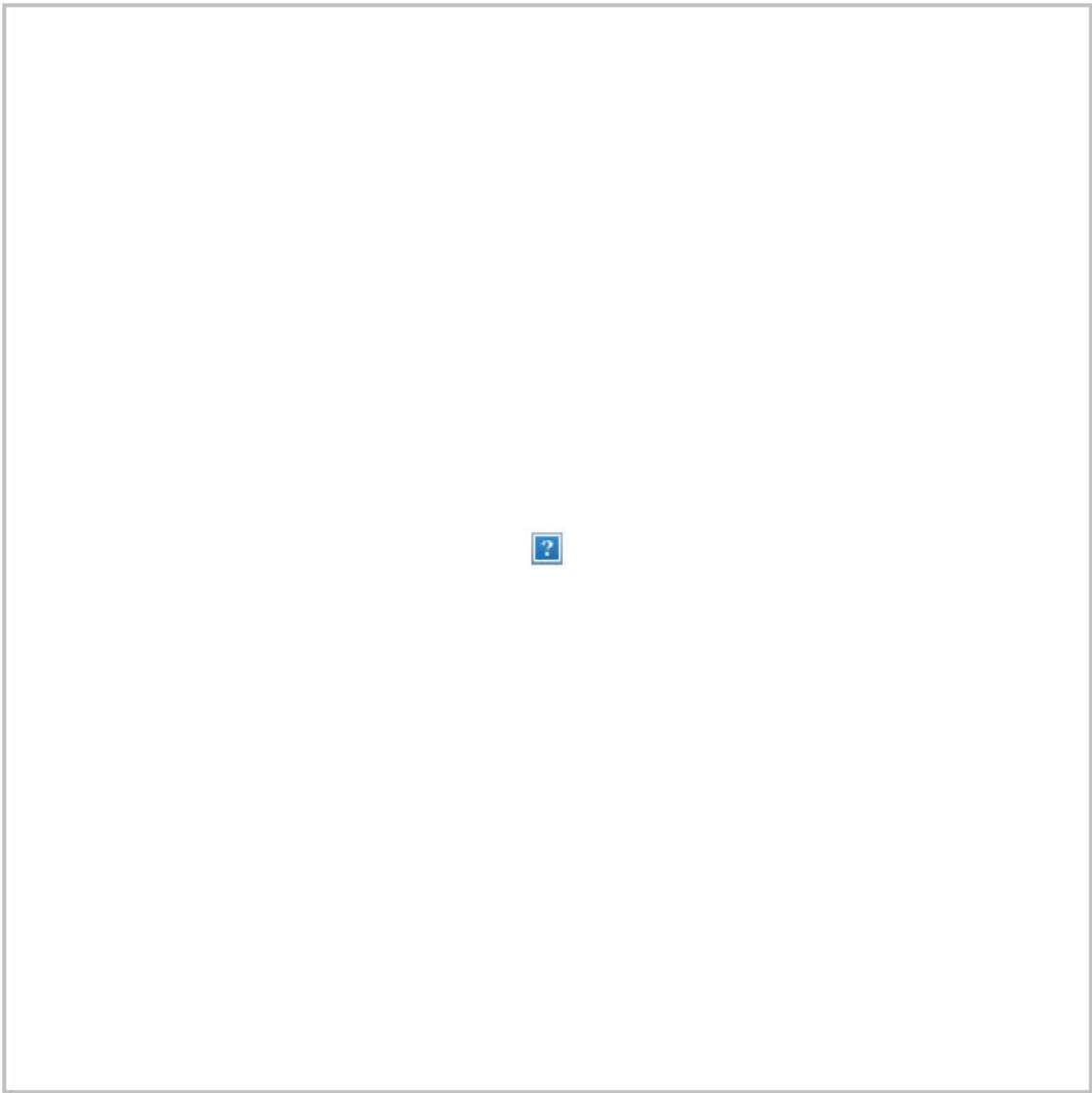




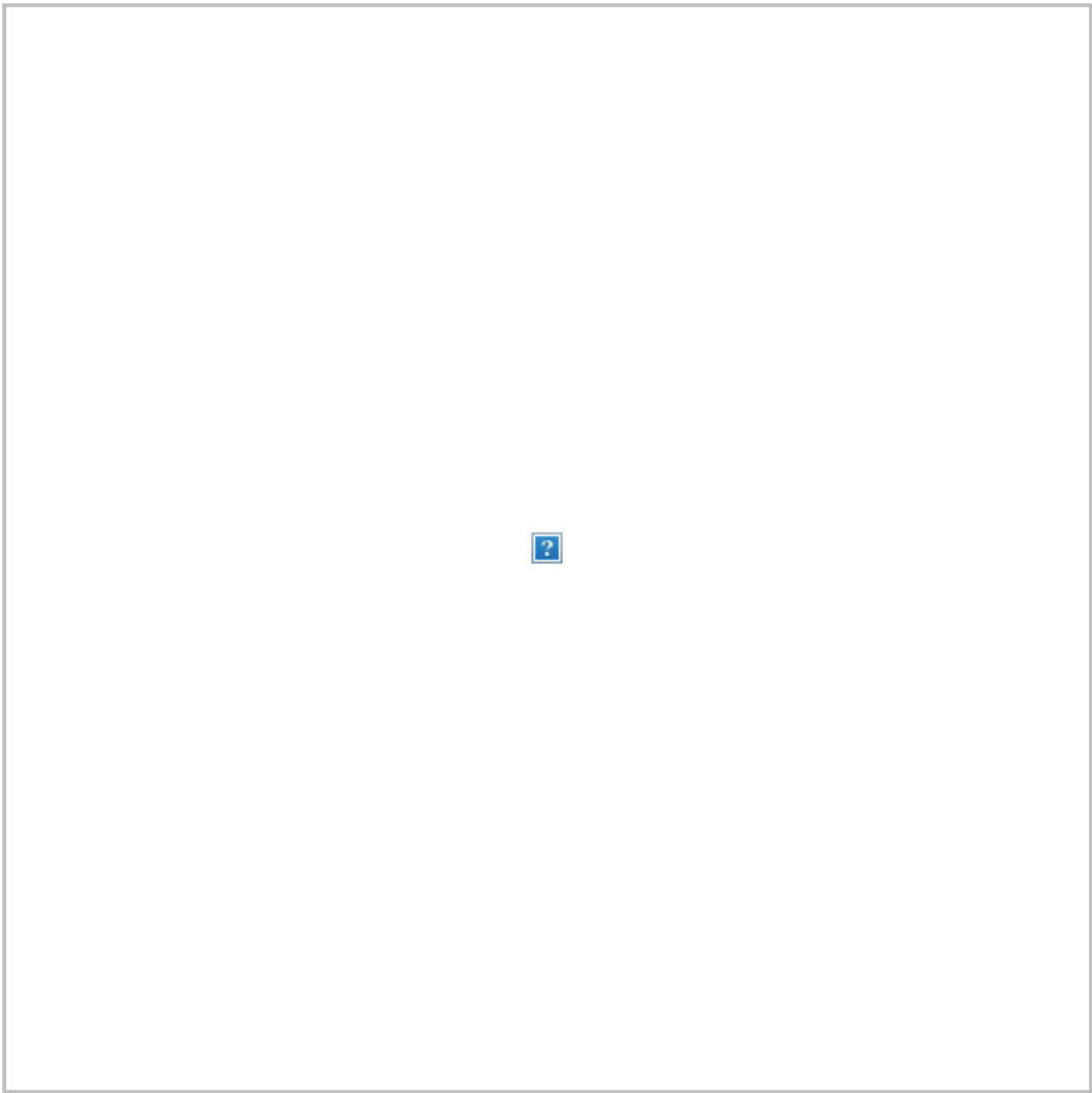
A House Democrat also criticized the policy:



A Post reporter shared messages between a migrant who has repeatedly attempted to cross the southern border and his daughter:



A Post reporter attempted to fact-check Trump's comment about the renegotiated NAFTA covering the cost of a border wall:



A Post columnist mocked Trump for the suggestion:



Jim Comey slammed a top House Republican's description of the former FBI director's congressional testimony:





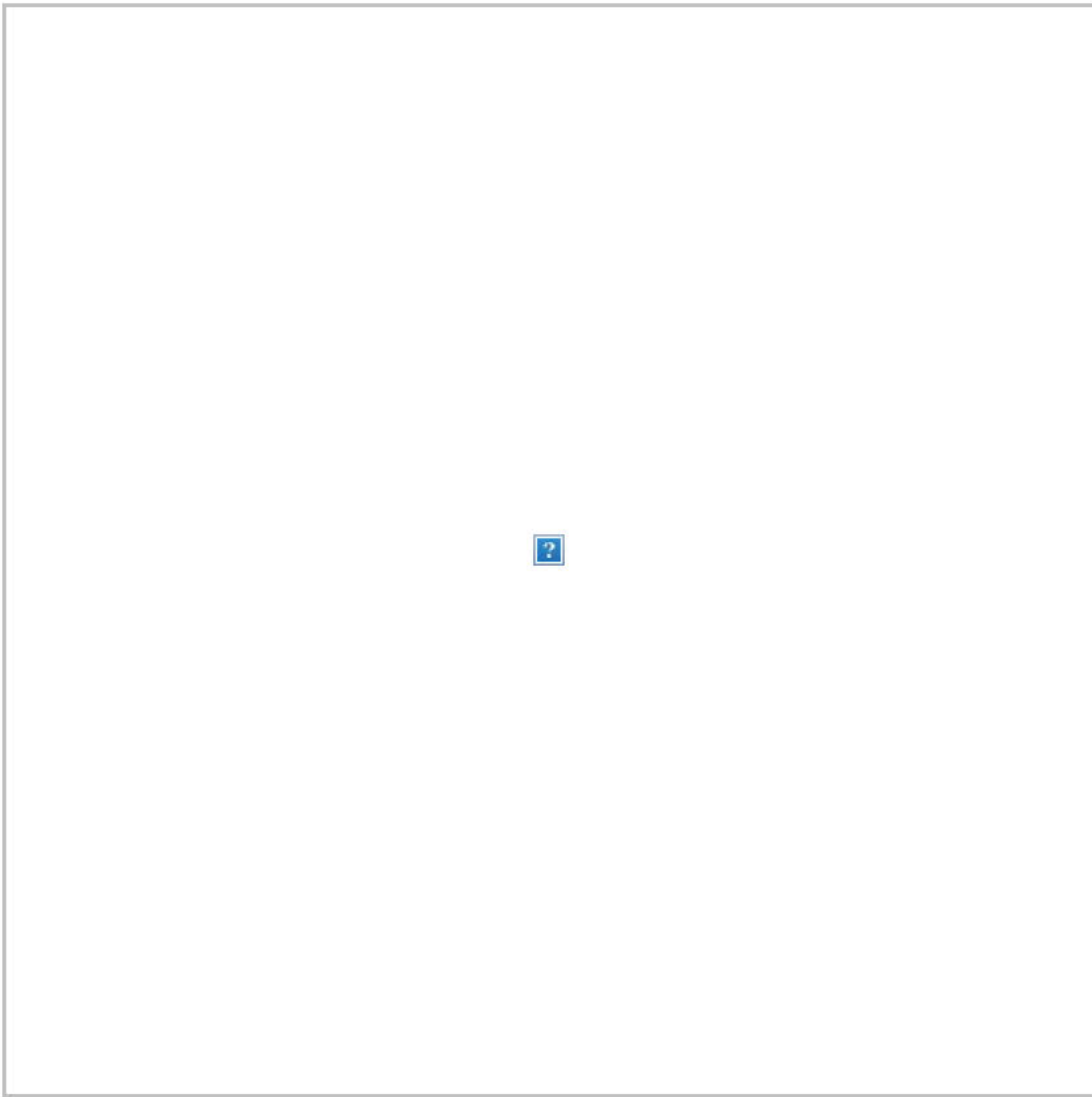
Sen. Jim Inhofe (R-Okla.) took a novel approach to answering reporters' tough questions about a stock purchase he made:



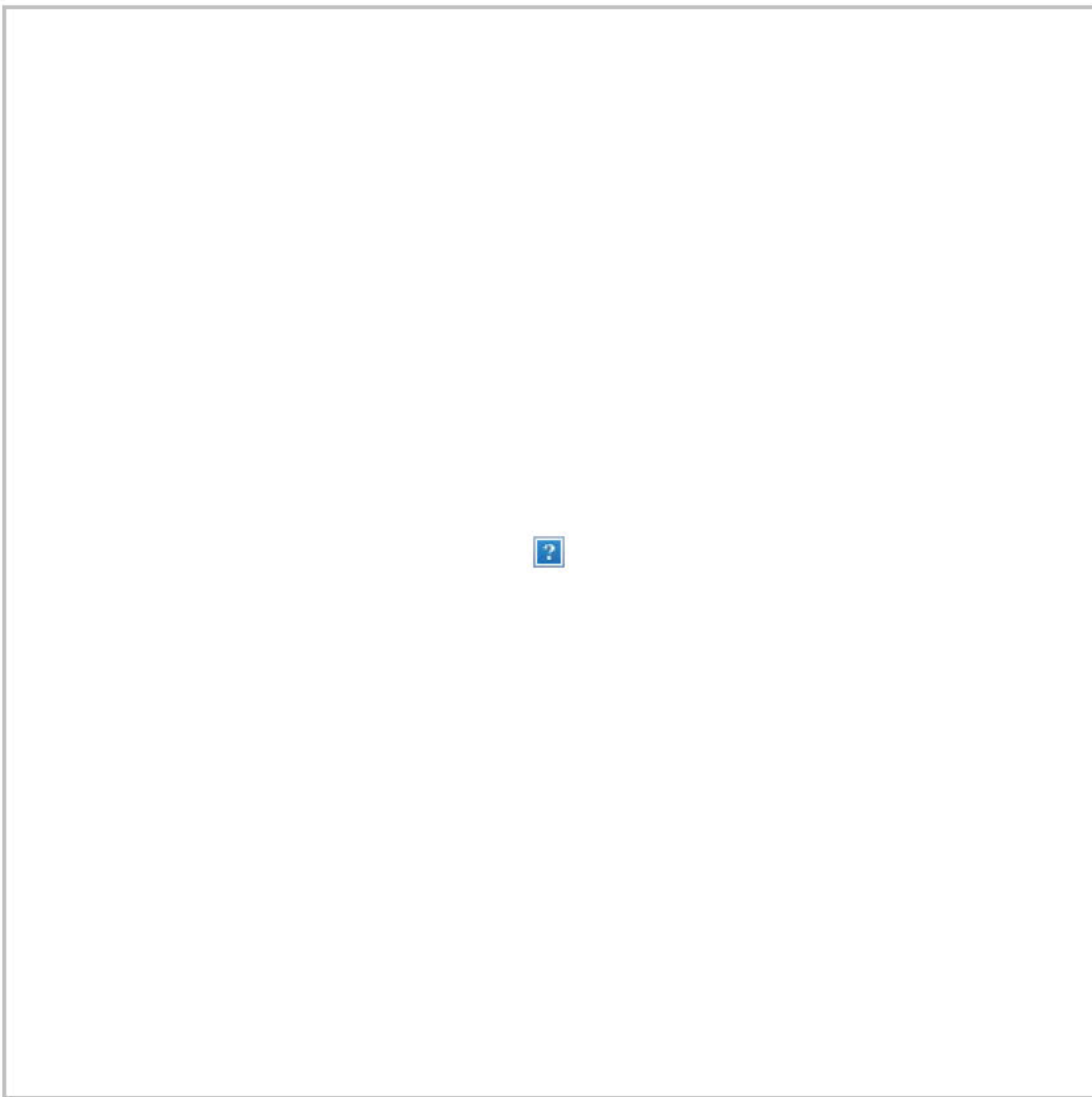
Sen. Marco Rubio (R-Fla.) argued against stock buybacks in a [piece](#) for the Atlantic:



A former chief of staff to Joe Biden replied to Rubio:



Retweeting a story that identifies him as a "potential presidential candidate," Sen. Sherrod Brown (D-Ohio) went after an airline over tip jars:



A Tennessee government agency issued this statement after a congressman-elect claimed vaccines might cause autism:

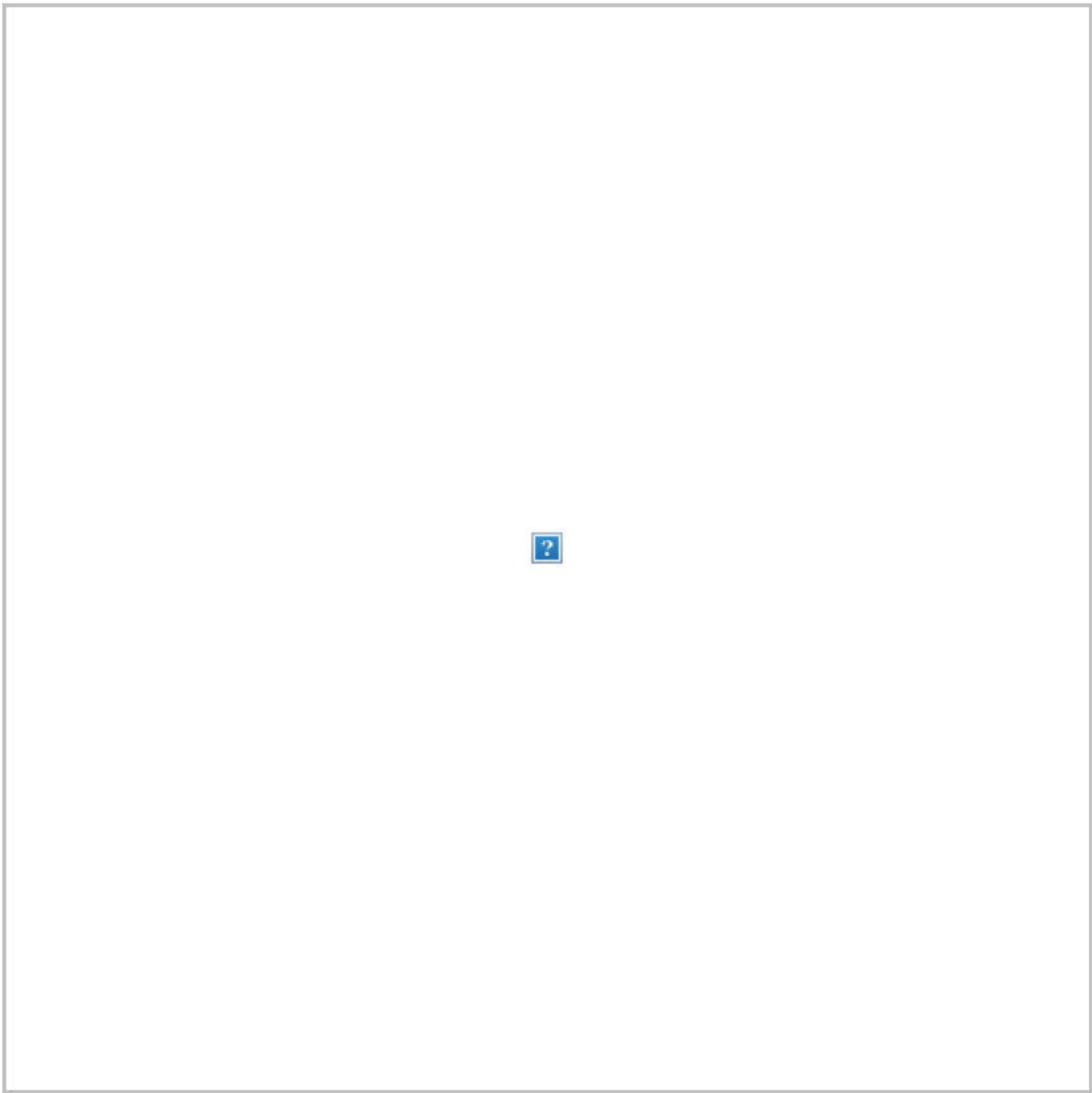




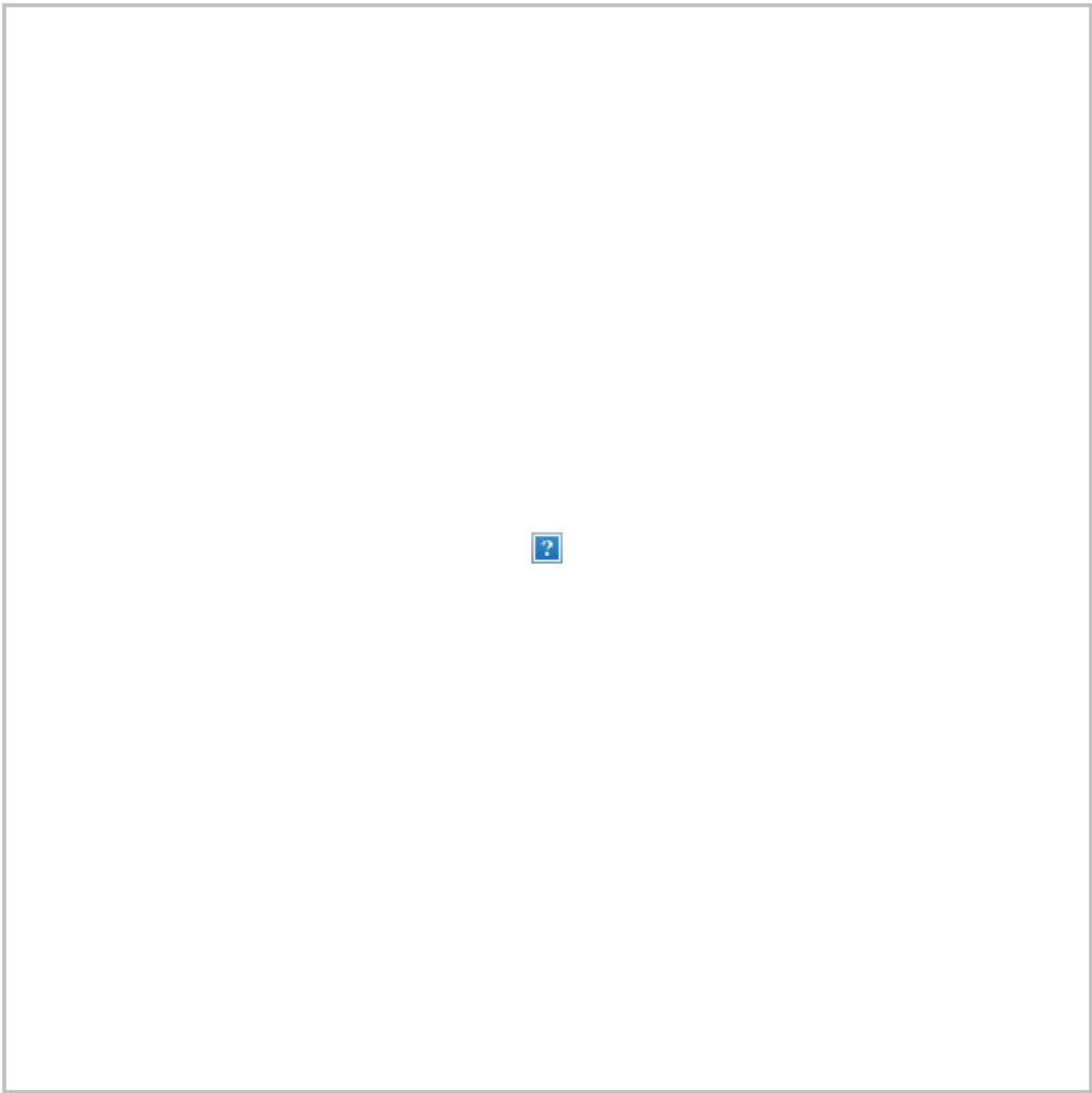
One of the co-founders of March for Our Lives was accepted to Harvard:



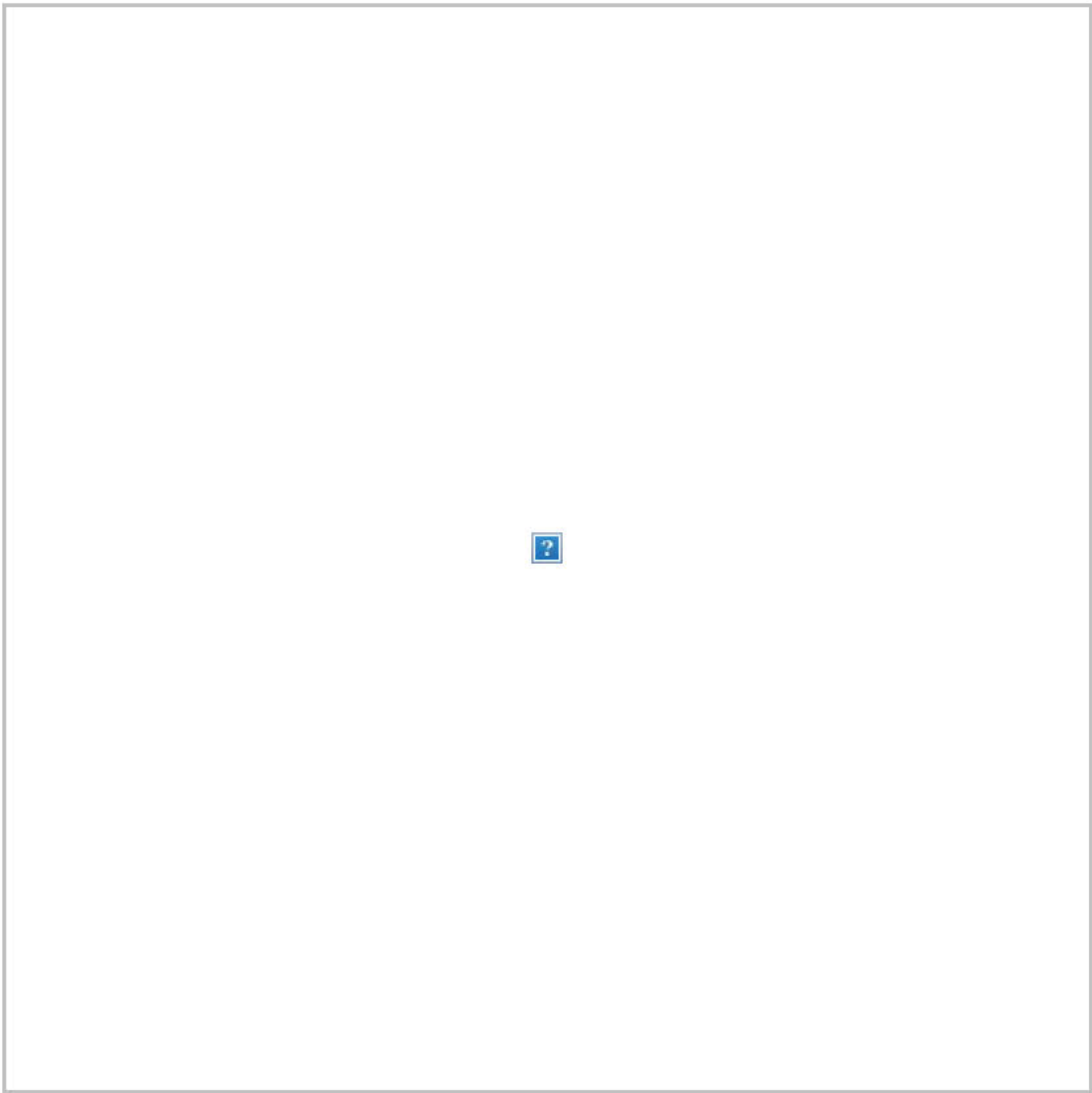
Rep.-elect Anthony Brindisi (D-N.Y.), [whom I profiled on Nov. 1](#), packed up his state assembly office in Albany and prepared to make the move to Washington:



A new Senate caucus was formed:



Nancy Pelosi celebrated her fashion success:



And Sen. Jeff Flake requested a blanket imprinted with his tweets from the Daily Show:





The host responded with what the kids call a sick burn:



## **GOOD READS:**

-- "[The boy on the bridge](#)," by Jessica Contrera:

"There was no way she could have seen him, the boy on the bridge. Marisa Harris was driving her Ford Escape down a Northern Virginia highway, heading home after a peaceful afternoon hike at Burke Lake. Her boyfriend, Perry Muth, was stretched out in the passenger seat as they cruised east on Interstate 66 toward the bridge, an overpass suspended across the busy highway. ... The

boy on the bridge was 12. What led him there would always be a mystery to Marisa's family, even after police and prosecutors came to their conclusions. There was no fence on the part of the bridge he'd reached. There was a pedestrian sidewalk, and beside it, a three-foot, two-inch-tall guardrail. But there was nothing to stop the boy from climbing over it. And nothing to stop him from jumping — just as Marisa's car reached the spot below."

-- **BuzzFeed News**, "[The Cities Where The Cops See No Hate](#)," by **Peter Aldhous**: "Year after year, the vast majority of police departments across the country report zero hate crimes to the FBI. After sifting through more than 2,400 police incident reports from 2016 obtained from 10 of the largest such departments, BuzzFeed News identified 15 assaults in which the cops' own narratives suggested that the suspect may have been motivated by bias."

-- **New York Times**, "[How 'Baby, It's Cold Outside' Went From Parlor Act to Problematic](#)," by **Jacey Fortin**: "Rock Hudson did it with Mae West. Ray Charles did it with Betty Carter. Lady Gaga and Joseph Gordon-Levitt did it with a modern twist. And somewhere along the line, the 74-year-old song 'Baby, It's Cold Outside' became a holiday standard, in heavy radio rotation, playing overhead in department stores, and covered on Christmas albums. ... Now, a long-simmering debate over the lyrics has reached a boil. The annual holiday

culture wars and the reckoning over #MeToo have swirled together into a potent mix. Say — what's in this drink?"

#### **HOT ON THE LEFT:**

**"U.S. Budget Deficit Hits Widest on Record for Month of November," from Bloomberg News:**

"The U.S. posted the widest November budget deficit on record as spending doubled revenue. Outlays jumped 18 percent to \$411 billion last month, while receipts were little changed at \$206 billion, the Treasury Department said in a monthly report on Thursday. That left a \$205 billion shortfall, compared with a \$139 billion gap a year

#### **HOT ON THE RIGHT:**


**"Florida Senate won't consider reinstating former Broward elections supervisor Brenda Snipes," from the South Florida Sun Sentinel:** "The Florida Senate has declined to take action on former Broward County elections head Brenda Snipes' suspension, paving the way for an ally of Republican Gov. Rick Scott to fill the remainder of her term, according to a memo on Thursday from Senate President Bill Galvano. Snipes had



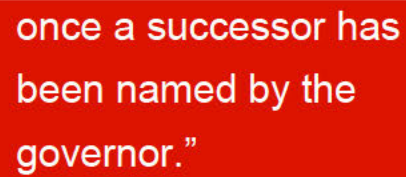
earlier. The U.S. ran the largest deficit in six years in fiscal 2018, the first full year of Donald Trump's presidency when his Republican party enacted a tax-cut package and raised federal spending for the military and other priorities. The measures have added to the growing federal deficit, which is forecast to push past \$1 trillion by 2020 when the U.S. next holds presidential elections. In the first two months of the fiscal year that began Oct. 1, the gap widened to \$305.4 billion, compared with \$201.8 billion the same period a year earlier."

announced she would resign her post effective Jan. 4, amid an outcry over stumbles by her office during Florida's recount. A day after Scott suspended her from office on Nov. 30, Snipes she said she would withdraw her resignation. Citing 'misfeasance, incompetence and neglect of duty,' Scott installed Pete Antonacci, his former top lawyer, to fill the remainder of Snipes' term, which ends after the 2020 presidential election. ... Galvano, R-Bradenton, said legal precedent in Florida has established that Snipes cannot take back her resignation





once a successor has  
been named by the  
governor.”



## **DAYBOOK:**

**Trump** will receive his intelligence briefing and later attend two Christmas receptions with the first lady.

The president is also expected to spend 16 days at Mar-a-Lago over the Christmas and New Year's holidays. It will be his longest sojourn to the “Southern White House” since his inauguration. ([Palm Beach Post](#))

Pelosi: 'Oval Office is an evidence-free zone'

### **QUOTE OF THE DAY:**

"I think the Oval Office is an evidence-free zone. You've got to have facts, data, evidence, truth in order to make an agreement on how you go forward." – Nancy Pelosi on Trump's argument that economic benefits from a renegotiated NAFTA would cover the cost of a border wall.



## **NEWS YOU CAN USE IF YOU LIVE IN D.C.:**

**-- Rain will become increasingly likely in Washington as the day goes on. [The Capital Weather Gang forecasts](#):** “Clouds thicken, with a few morning sprinkles possible. Steadier rain should hold off until later afternoon or perhaps into evening locally. We likely stay stuck in the 40s for high temperatures, with a very light but steady east-northeast breeze off the Bay and Atlantic. Monitor radar with us by midday for any rain timing and intensity updates.”

**-- The Metro board advanced measures to charge peak fares for special events and expand rush-hour service. [Faiz Siddiqui reports](#):** “But the board tabled action on a measure to continue the system’s early-closing hours for another year after board members representing the District threatened to veto it. ... Metro has proposed continuing the early closings to expand a preventive maintenance program implemented in the wake of its SafeTrack rehabilitation work.”

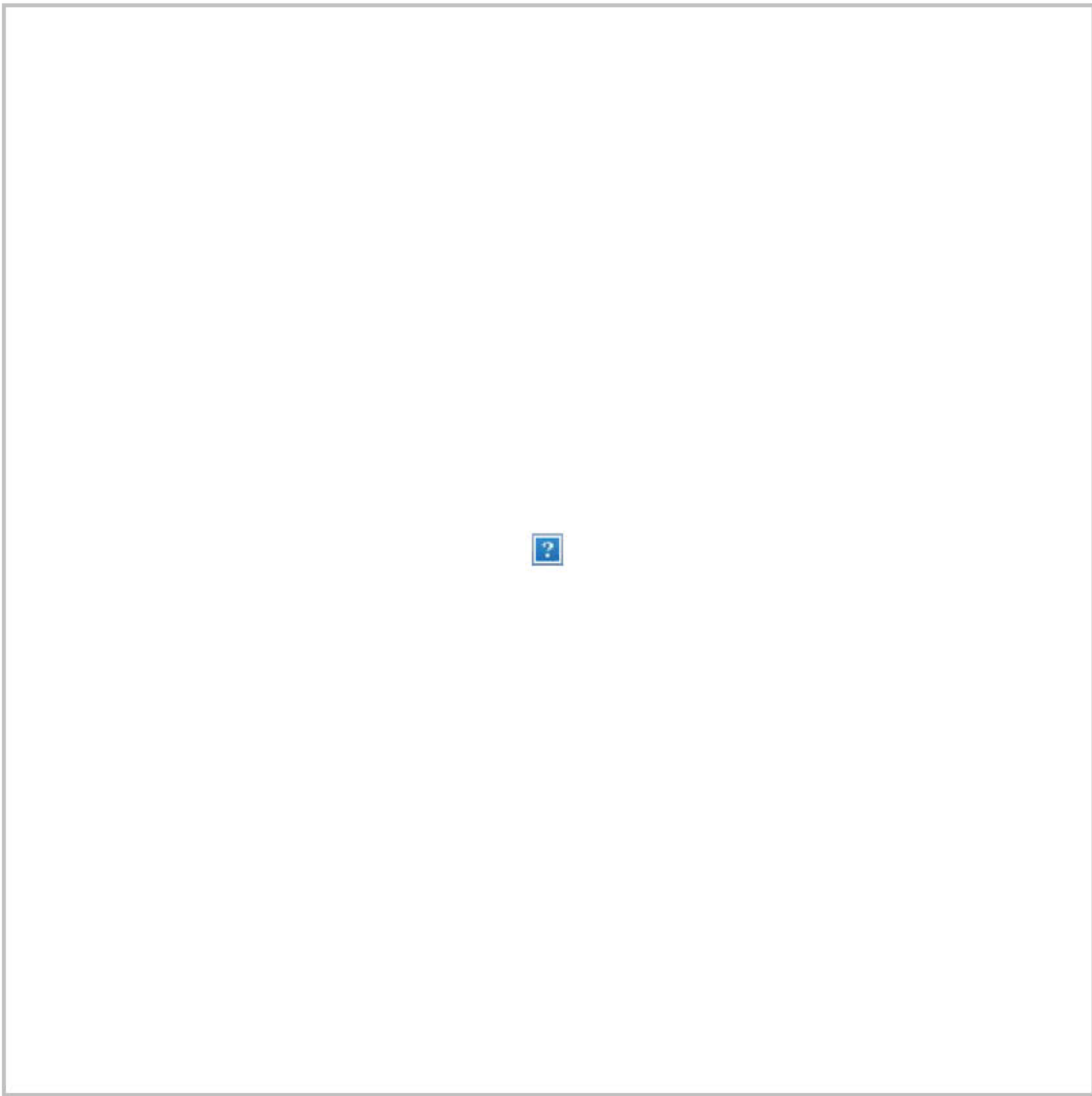
**-- A U-Va. professor retired after an internal investigation concluded he had inappropriate sexual contact with a student 17 years ago. [Nick Anderson reports](#):** “John Casey, an award-winning fiction writer,

kissed and touched the student in an unwelcome manner one night in 2001, according to a letter summarizing conclusions last week from a disciplinary review panel. The investigation also determined Casey had sex with the student at a time when she was likely to have been enrolled in his class, according to the letter. The panel characterized his conduct as 'reprehensible,' according to the letter, and recommended termination. But the panel cleared Casey on a major charge: It concluded there was not enough evidence to support former student Lisa Schievelbein's allegation that the professor had sexual intercourse with her repeatedly without her consent."

**-- The earliest known painting of George Washington returned to his Mount Vernon estate for the first time since 1802.** The Charles Willson Peale painting is on loan from Washington and Lee University and will be on display for the next two years. ([Michael E. Ruane](#))

## **VIDEOS OF THE DAY:**

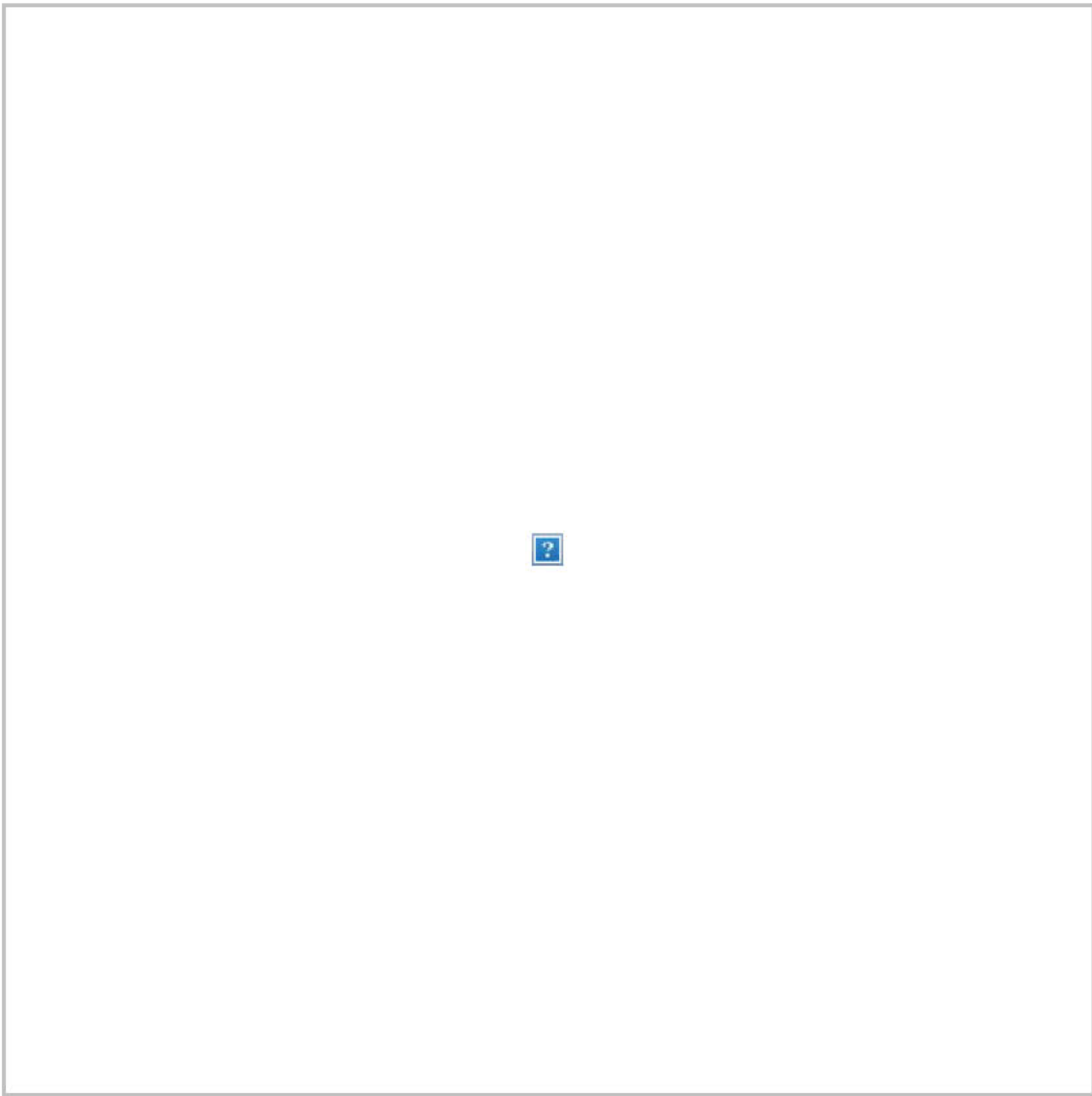
Stephen Colbert updated the presidential seal to reflect the latest developments from the Russia investigation:



The Embarrassing President Feels Embarrassed

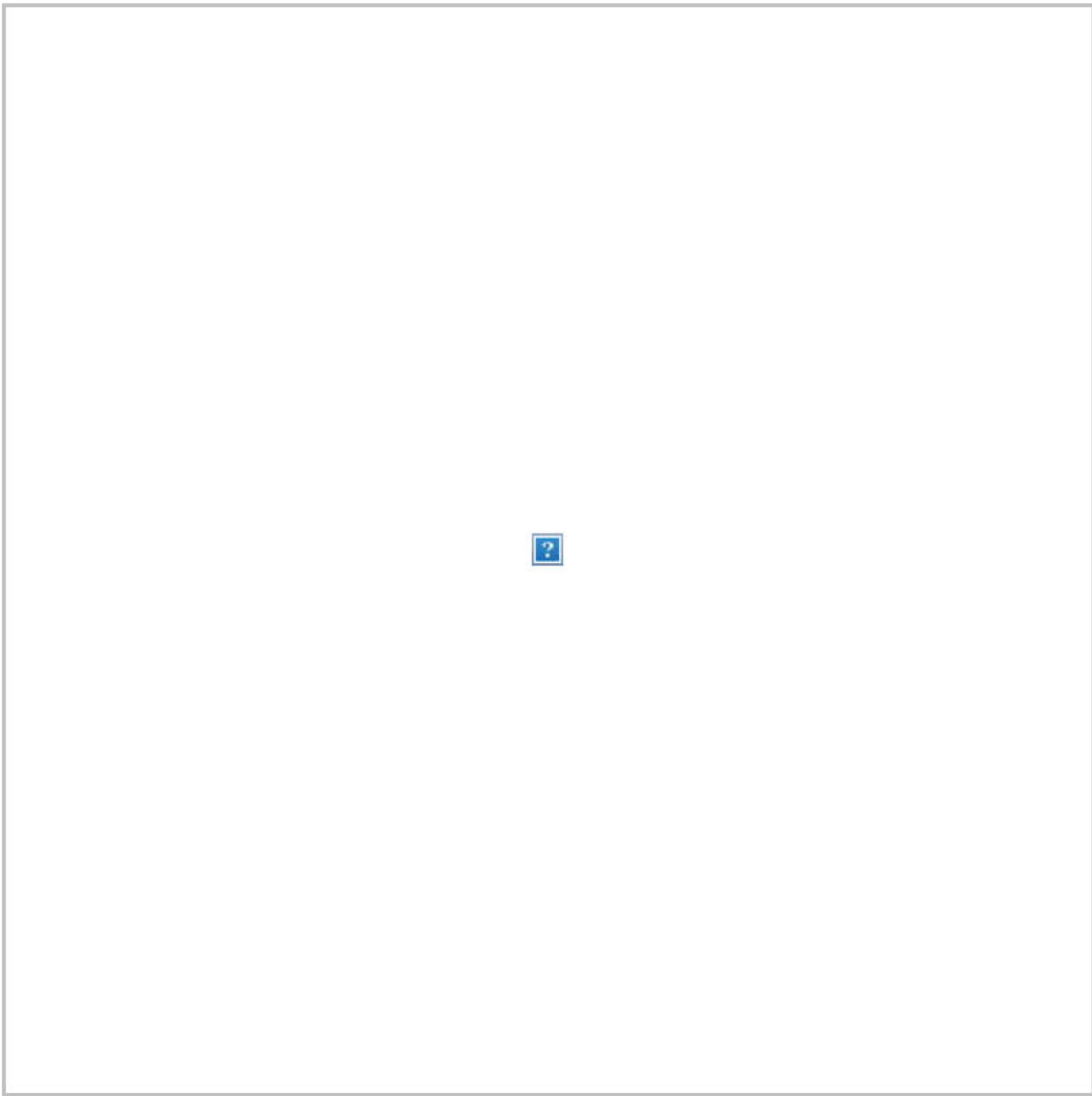
Melania Trump visited a D.C. children's hospital:





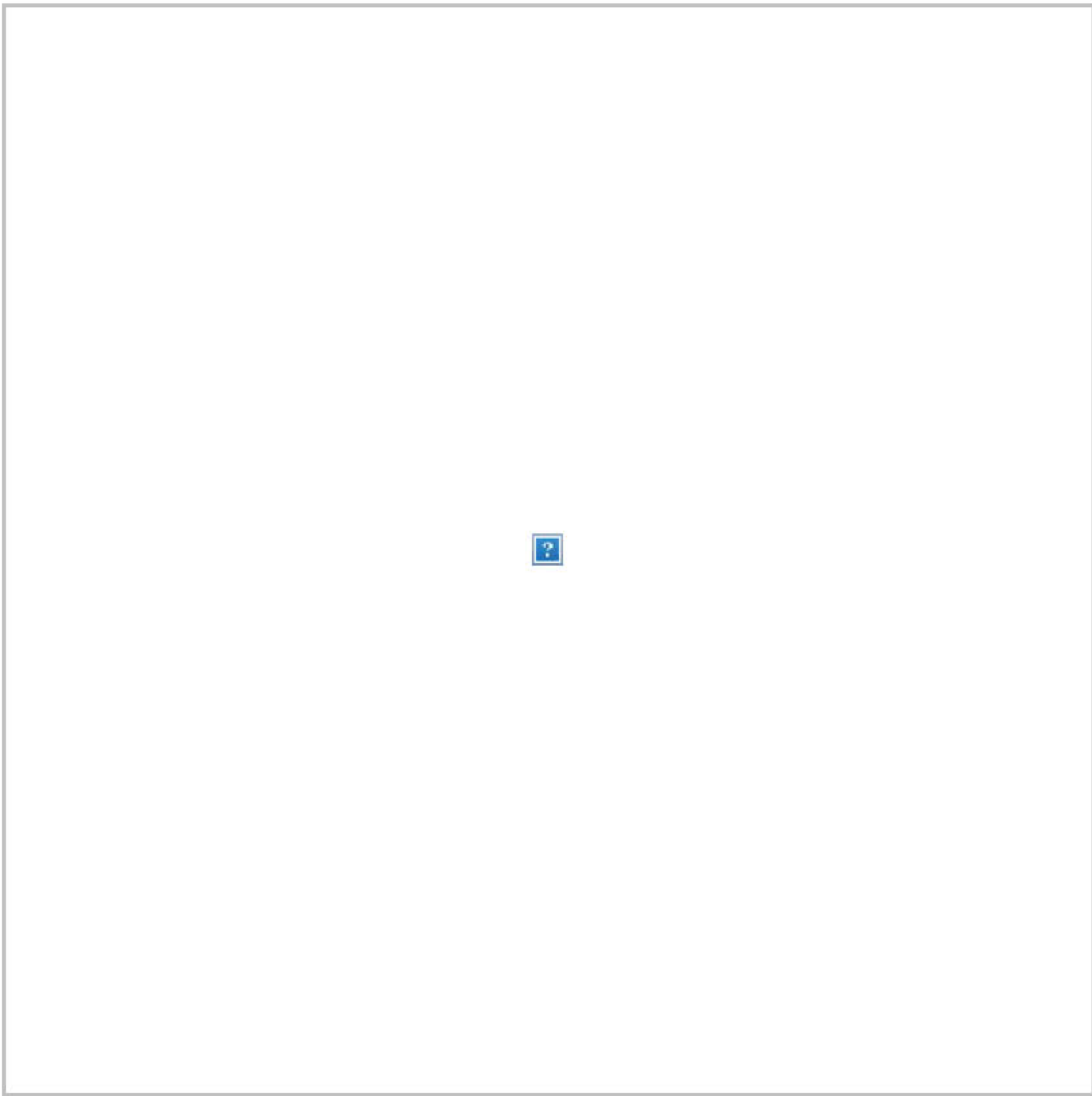
Melania Trump visits children's hospital

Virgin Galactic launched a spacecraft that reached an altitude of more than 50 miles, making it the first manned U.S. spacecraft to reach space since 2011:



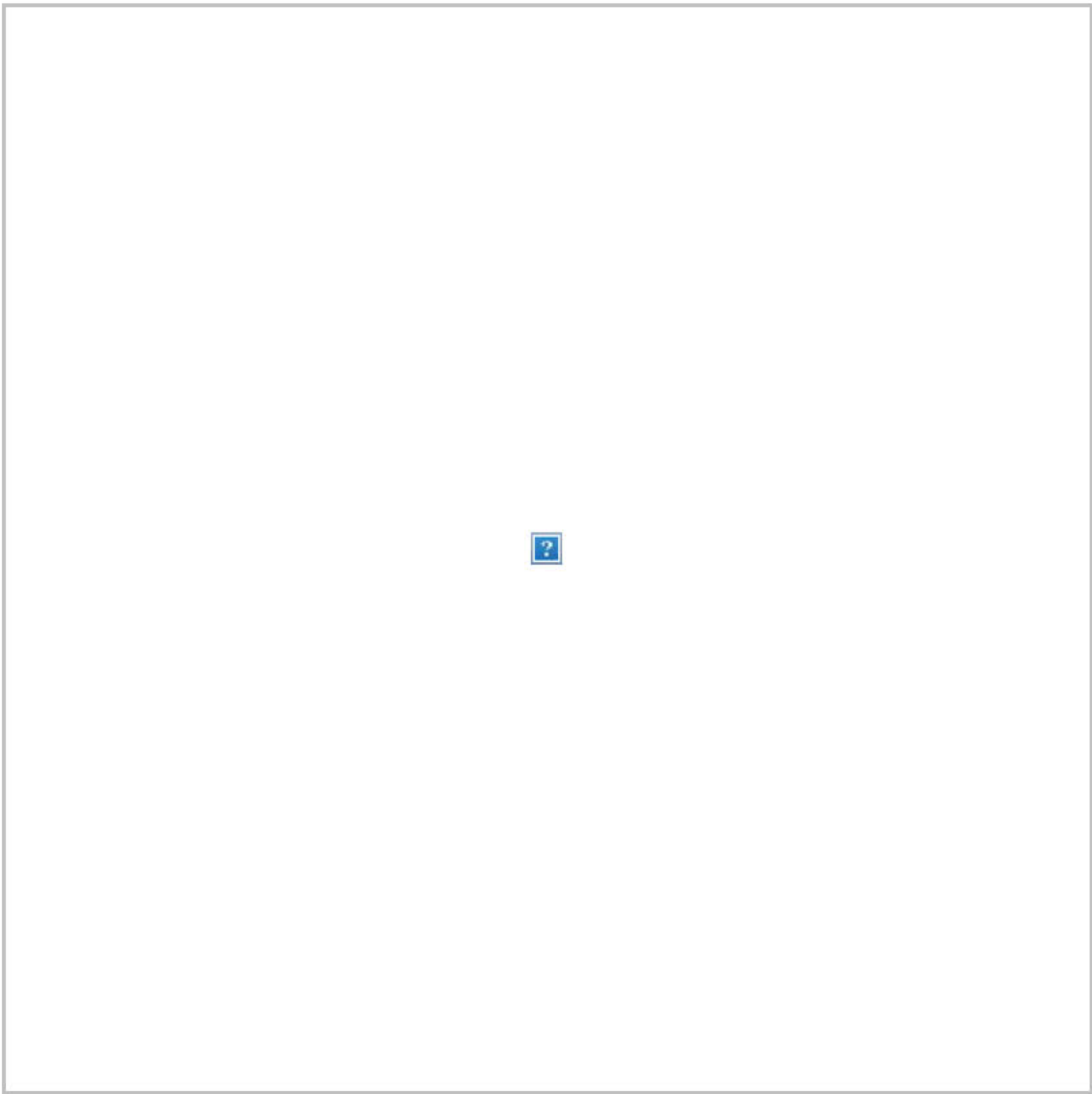
Virgin Galactic launches the first manned U.S. spacecraft to reach space since 2011

Miss USA apologized for comments she made about the English-speaking abilities of two Miss Universe contestants:



Miss USA apologizes for comments about Miss Universe contestants' English

**And officials at JFK Airport discovered live birds hidden in hair rollers:**



Airport officials discover 70 finches hidden in hair rollers

You received this email because you signed up for The Daily 202 or because it is included in your subscription.

[Manage my email newsletters and alerts](#) | [Unsubscribe from The Daily 202](#)

[Privacy Policy](#) | [Help](#)



**From:** [noreply+feedproxy@google.com](mailto:noreply+feedproxy@google.com) on behalf of [SCOTUSblog](#)  
**To:** [Rebecca Moon](#)  
**Subject:** SCOTUSblog  
**Date:** Tuesday, December 04, 2018 12:55:29 PM

---

## SCOTUSblog

---

- [Argument transcripts](#)
- [Tuesday round-up](#)
- [Argument analysis: What would John Marshall do?](#)
- [Argument analysis: Justices appear divided in debate over anti-fraud securities rules](#)

### Argument transcripts

Posted: 04 Dec 2018 11:16 AM PST

The transcript of oral argument in ***Biestek v. Berryhill*** is available on the [Supreme Court's website](#); the transcript in ***Helsinn Healthcare S.A. v. Teva Pharmaceuticals USA Inc.*** is also available.

The post [Argument transcripts](#) appeared first on [SCOTUSblog](#).



Argument transcripts



### Tuesday round-up

Posted: 04 Dec 2018 04:09 AM PST

There are two oral arguments on the Supreme Court's agenda today. The first is in ***Biestek v. Berryhill***, in which the justices will consider social-security-benefits claimants' ability to scrutinize the data on which benefits denials are based. David Super had [this blog's](#) preview. Tyler Schmitt and Grace Brososky preview the case for Cornell Law School's [Legal Information Institute](#). This morning's second case is ***Helsinn Healthcare v. Teva Pharmaceuticals***, which asks whether the "on sale" bar to the patentability of an invention is triggered by a sale in which the purchaser is required to keep the details of the invention confidential. Ronald Mann previewed the case for [this blog](#). Lauren Kloss and Nayanthika Ramakrishnan have a preview for [Cornell](#).

Yesterday the justices issued orders from last week's conference; Amy Howe has [this blog's](#) coverage, which first appeared at [Howe on the Court](#). At [Greenwire](#) (subscription required), Ellen Gilmer reports that the court "invited the solicitor general to weigh in on two closely watched cases involving pollution that moves through groundwater before reaching a surface waterway." Kevin Daley reports at [The Daily Caller](#) that the justices "declined to take up a challenge to President Donald Trump's border wall ..., which asserted that the administration violated the Constitution when it exempted border barrier projects from

Tuesday round-up





environmental regulations.” At the [Pacific Legal Foundation](#)’s blog, Deborah LaFetra comments on the court’s order in *[Fleck v. Wetch](#)*, a challenge to North Dakota’s mandatory bar dues, that the court of appeals reconsider the case in light of *Janus v. AFSCME*; she argues that “[t]he First Amendment principles outlined in *Janus* ... demand that no one should be forced into associations as the price of earning a living, including attorneys.”

Mark Walsh has a first-hand view of yesterday’s courtroom proceedings, which featured nods to both the late President George H.W. Bush and recently retired Justice Anthony Kennedy, for [this blog](#). Daniel Hemel has [this blog](#)’s analysis of yesterday’s oral argument in *[Dawson v. Steager](#)*, which asks whether federal law or the doctrine of intergovernmental tax immunity prevents West Virginia from differential taxation of retirement benefits of certain former state and federal employees. At [AP](#), Jessica Gresko reports that the justices “seemed inclined ... to side with a retired U.S. marshal who argues West Virginia is discriminating against former federal law enforcement officers like him by giving a more generous tax break to former state law enforcement officers.”

Ronald Mann analyzes the oral argument in yesterday’s second case, *[Lorenzo v. Securities and Exchange Commission](#)*, in which the justices considered whether someone who distributed false statements drafted by someone else can be held liable under federal securities laws for participating in a fraudulent scheme, for [this blog](#). At [Bloomberg](#), Greg Stohr and Benjamin Bain report that the court appeared “likely to reinforce the Securities and Exchange Commission’s powers,” and that a “ruling favoring the SEC would mark a turnaround from a trend of Supreme Court rulings against the agency.” The editorial board of [The Wall Street Journal](#) calls the case “a textbook example of regulators stretching the law to make an example of an unsympathetic defendant.”

Briefly:

- For [The Washington Post](#), Robert Barnes explains why, when the Supreme Court “takes up the case of a small-time Alabama felon, Terance Gamble, who complains [in *[Gamble v. United States](#)*] that his convictions by state and federal prosecutors for the same gun possession crime violate constitutional protections against double jeopardy,” “likely to be watching the proceedings closely will be those concerned about a big-time felon, Republican consultant and former Trump campaign chairman Paul Manafort, who was prosecuted by special counsel Robert S. Mueller III for tax fraud.”
- At [PrawfsBlawg](#), Rory Little weighs in on last week’s oral argument in *[Timbs v. Indiana](#)*, which asks whether the Eighth Amendment’s prohibition on excessive fines applies to the states, noting that “for one Bill of Rights provision in particular – the Fifth Amendment’s right to be charged by a Grand Jury for any ‘capital or otherwise infamous crime’ – the decision to not incorporate is long-standing and quite considered”; “[y]et ... it appears to be a ‘blank spot’ in the doctrinal understanding of the Court’s two newest Justices, Gorsuch and Kavanaugh.”
- At [The World and Everything In It](#), Mary Reichard discusses the oral arguments in *[Apple v. Pepper](#)*, in which the justices considered whether iPhone-app purchasers can bring an antitrust suit against Apple for monopolizing the market for the apps and making consumers overpay, and *[Frank v. Gaos](#)*, in which the court has been asked to make it harder for companies to settle class-action lawsuits without providing direct compensation to class members, through a process known as cy pres.
- At [E&E News](#), Ellen Gilmer looks at the implications of the court’s recent decision in

***Weyerhaeuser Company v. U.S. Fish and Wildlife Service***, in which the court held that the Endangered Species Act allows the government to designate land as a “critical habitat” only if it is habitat for the listed species, and that the designating agency’s assessment of the costs and benefits of the designation is reviewable in court; she notes that “[t]hough narrow in its holdings, the justices’ unanimous opinion... is expected to have ripple effects in federal courts.”

*We rely on our readers to send us links for our round-up. If you have or know of a recent (published in the last two or three days) article, post, podcast, or op-ed relating to the Supreme Court that you’d like us to consider for inclusion in the round-up, please send it to roundup [at] scotusblog.com. Thank you!*

The post **Tuesday round-up** appeared first on **SCOTUSblog**.



## Argument analysis: What would John Marshall do?

Posted: 04 Dec 2018 03:31 AM PST

“[I]n *McCulloch vs. Maryland*, the court said that in general we don’t want to be micromanaging all the details of state taxation,” attorney Lawrence Rosenberg told the justices at the end of Monday’s oral argument in ***Dawson v. Steager***. That’s not the way that ***McCulloch*** is usually remembered—far more famous is Chief Justice John Marshall’s statement in the 1819 case equating “the power to tax” with “the power to destroy.” But in any event, it was apparent by the end of the argument that the current court does not want to be micromanaging state tax regimes.



The argument also made clear, however, that an easily administrable rule for cases like *Dawson* won’t be so easy to find. The approach suggested by the U.S. solicitor general—who urged the justices to vacate the West Virginia state supreme court’s decision and send the case back down for further proceedings—seemed to attract the most support from the bench. But as Michael Huston, an assistant to the solicitor general, acknowledged, that approach still would leave lower courts with “difficult questions.” Further splits are almost inevitable, and so the justices may soon find themselves immersed yet again in the details of state taxation.

At first glance, *Dawson* looks like a straightforward case. Petitioner James Dawson, a retired U.S. marshal, wants West Virginia to exempt his federal retirement benefits from state income tax. Dawson points to the fact that West Virginia already exempts benefits paid to retired state and local law-enforcement officials who participate in particular pension plans. West Virginia emphasizes the fact that Dawson and other federal retirees receive the same tax treatment as the 98 percent of former state and local government workers who do not participate in one of the favored plans. Lurking in the background is the intergovernmental-tax-immunity doctrine—created in *McCulloch* and codified at **4 U.S.C. § 111**—which bars states from discriminating against federal officers or employees through their tax laws.

Rosenberg, representing Dawson, led off with an attractively simple summary of the issues at play. West Virginia’s tax regime violates federal law, Rosenberg said, because it “facially discriminates” against retired U.S. marshals and in favor of retired state law-enforcement officials with the same job duties. Justice Sonia Sotomayor quickly pushed back, noting that

although some retired state law enforcement officials are eligible for the exemption that Dawson seeks, others are not. Rosenberg responded that “there would still be discrimination” if any retired state law enforcement officials with the same job duties as U.S. marshals enjoyed exemption, but several justices seemed skeptical. As Justice Elena Kagan put it, “an antidiscrimination provision doesn’t necessarily require a most favored nation clause.”

Justice Ruth Bader Ginsburg then asked Rosenberg whether a U.S. marshal is more similar to the West Virginia state and local law enforcement officials whose pensions are exempt or to the officials whose pensions are taxed. Rosenberg responded that Dawson is “plainly most like a deputy sheriff”—a position that is eligible for the pension exemption—but Chief Justice John Roberts was not convinced. The role of a U.S. marshal—a presidentially appointed, Senate-confirmed official who oversees the marshals service for an entire federal judicial district—is “more policy, administrative,” said Roberts. Rosenberg responded that Dawson’s “basic duties as a law enforcement officer didn’t change” once he became the U.S. marshal for all of West Virginia, but Roberts was unmoved. “I mean, would you say that the attorney general would qualify [for a state tax exemption] in this situation?” the chief justice asked rhetorically. “He has law enforcement duties.”

Roberts asked the same question when Huston rose to represent the United States: “[A]re the benefits that, say ... your boss, the Attorney General receives, exempt?” The chief justice added that Huston, his former law clerk, should “[t]hink carefully before answering”—a line that drew laughter but did not draw a yes-or-no answer from Huston.

Huston instead urged the justices to apply a two-step approach. First, he said, the court should hold that “this West Virginia tax exemption here is facially discriminatory” and therefore in violation of the intergovernmental-tax-immunity doctrine and 4 U.S.C. § 111. “A tax is facially discriminatory,” said Huston, “when it’s not open to any federal employees ever, regardless of what job duties they perform or what their benefit level is or what their contribution rate is.”

“If that’s the problem,” asked Kagan, “why were you suggesting that we remand this?”

Huston had a reply at the ready. “[E]ven when a tax is facially discriminatory,” he told Kagan, “there is going to be a second question, which is, is this particular employee actually suffering discrimination?” He added that if West Virginia granted an exemption to retired state law enforcement officers, then a hypothetical “federally employed teacher” would be “the wrong plaintiff” to challenge the facially discriminatory state tax law. His response seemed to please Kagan, who said: “[O]kay, I get it. I get it.”

The other justices seemed to get it too, and they began to toss out the sorts of implementation questions that one might ask if one were imagining how an opinion might be written. When Justice Brett Kavanaugh asked what to do if a federal retiree is “equivalent to both the favored and the disfavored class,” Huston replied that “in that sort of unusual situation,” the federal retiree should win because “the state would not be able to meet its burden to defend its facially discriminatory law.” Justice Samuel Alito then asked how to resolve “situations where the federal employees are pretty similar to the [state employees] in the favored class, but they’re not identical.” Huston responded that in those close-to-the-line cases, what mattered most was whether states applied the court’s standard “in good faith.”

By the time that West Virginia solicitor general Lindsay See rose to speak, several of the justices already seemed to be on board with the United States’ approach, and See struggled to make inroads. She said that “Dawson is treated the same as similarly situated state employees,” but as Sotomayor quickly noted, the state supreme court “didn’t find that, so you can’t rely on that.”



See next tried to argue that the intergovernmental-tax-immunity doctrine and 4 U.S.C. § 111 are concerned only with “discrimination that at some level interferes with government functions,” but that didn’t seem to sway the bench either. “The statute is quite explicit,” said Ginsburg, that the test is not whether a state is “burdening the federal government.” Roberts soon joined in. It’s “not permissible,” he said, for a state to categorically exclude federal employees from a tax benefit. “[I]f your basis is something else, you ought to say that,” Roberts told See.

Justice Stephen Breyer seemed frustrated with West Virginia as well. “[V]irtually all the state police ... [and] also the local police ... can get [the exemption] and the feds can’t. Why isn’t that just the end of it?” Breyer asked. See responded that many local law enforcement retirees are not eligible for the full exemption, but “the State of West Virginia Tax Department does not keep those exact numbers.” That answer did not satisfy Breyer. “You can’t give them to me at all?” he asked. See replied that officers in only 30 of the “roughly 200 cities” with separate police forces are eligible for the exemption, though Roberts interjected that “[t]hat statistic doesn’t tell us anything” if Charleston—the state’s largest city—is one of the 30.

As the hour drew to a close, it seemed that the justices had little appetite for arguing about whether U.S. marshals are more similar to deputy sheriffs or Charleston cops. But the justices also did not seem ready to embrace a bright-line rule that would allow any federal retiree to recover when a state tax regime facially discriminates on the basis of federal or state service. If the court did adopt such a rule, the fiscal consequences for West Virginia could be severe. The state is home to **nearly 19,000** retired federal employees, and it would be flooded with viable refund claims if relief were not limited to law-enforcement officials whose job duties mirrored those of the exempt West Virginia ex-workers.

All that makes the solicitor general’s suggestion for vacatur and remand seem rather alluring. But although that approach would stave off some of the more difficult intergovernmental-tax-immunity questions, it wouldn’t make those questions go away. One such question—the one that dominated the discussion Monday—is how to determine whether a federal employee or retiree is similarly situated to state workers who receive special tax benefits. A second question—not directly implicated by *Dawson* but in the offing—is what to do about state tax regimes that are facially neutral but gerrymandered to favor state employees and retirees over their federal counterparts. To be sure, nitty-gritty state tax issues are not the ones that most excite the justices (or, for that matter, most SCOTUS-watchers). But if *Dawson* turns out as expected, we can expect to see these issues back on the court’s docket in short order.

The post **Argument analysis: What would John Marshall do?** appeared first on **SCOTUSblog**.



## Argument analysis: Justices appear divided in debate over anti-fraud securities rules

Posted: 03 Dec 2018 08:43 PM PST

The dividing lines were apparent at Monday’s argument in *Lorenzo v Securities and Exchange Commission*, as several justices seemed to think it self-evident that the conduct of petitioner Francis Lorenzo amounted to a fraudulent scheme under the federal securities laws, while at least one justice, Neil Gorsuch, appeared

ready to rule for Lorenzo.

To understand the debate, some background is useful. This case follows from the Supreme Court's 2011 decision in *Janus Capital v First Derivative Traders*, which held that only the "maker" of a statement is liable for its falsity. Lorenzo distributed a set of emails to his clients urging them to invest in securities of a particular firm. All agree that the emails included false statements about the firm, but that Lorenzo cannot be charged with "making" those false statements because Lorenzo's supervisor crafted the text of the statements (which Lorenzo pasted into the emails that he sent). Faced with *Janus*, the SEC charged Lorenzo with engaging in a fraudulent scheme rather than making a false statement.

Lorenzo's central argument is that permitting the SEC to charge him tolerates a plain evasion of *Janus*, leaving *Janus* a dead letter. For several justices, the biggest problem with that argument is that the *Janus* court relied on the statutory text that condemns the "making" of a false statement; the *Janus* court reasoned that a person does not "make" a statement when parroting words produced by another. Because the rules and statutes under which the SEC charged Lorenzo do not include any references to the "making" of statements, the textual analysis of *Janus* says little about those provisions.

As for those provisions, several of the justices (including Justices Stephen Breyer, Samuel Alito, Elena Kagan and Sonia Sotomayor) suggested that the conduct in which Lorenzo engaged falls squarely within the relevant language. Alito, for example, repeatedly pressed Robert Heim, who represented Lorenzo, to suggest any reason why the alleged conduct did not "fall squarely within the language" of the statute. In the same vein, Kagan asked early on with apparent incredulity if Heim seriously thought that his client had "not engaged in an act which operates as a fraud." Sotomayor went even further, suggesting that she thought that Lorenzo's conduct was so plainly condemnable that Heim's admissions regarding Lorenzo's state of mind seemed to her to "give away your case."

The only strongly contrary comments came from Gorsuch, who pressed the view that the only "actus reus" (the classic Latin phrase for wrongful conduct) in the SEC's charges was the transmission of emails. For Gorsuch, the appeals court's ruling that Lorenzo did not "make" the false statements contained in the emails meant that he could not be held responsible for deceiving the investors. It was plain, however, that other justices did not share his views. Kagan, for example, stepped in to emphasize that the relevant conduct was the transmission of the false statement, which could not "cause the deception unless it gets to those readers."

An exchange between Kagan and Heim encapsulated the argument. Kagan explained that Heim's view made sense only if the justices thought of the various provisions of the anti-fraud statutes as entirely separate and "mutually exclusive" — so that conduct involving misstatements could be sanctioned, if at all, only under the provisions directed specifically at misstatements. Echoing the analysis of the U.S. solicitor general, Kagan suggested that it made more sense to regard the provisions as overlapping, in what she described as a "belt-and-suspenders approach where ... we're going to find every possible way to say this thing in order to make sure that fraudulent acts are covered."



Alito's skepticism is a bad sign for Lorenzo, because all four of the dissenters from *Janus* (Breyer, Justice Ruth Bader Ginsburg, Kagan and Sotomayor) remain on the bench, and none of them showed any inclination to extend *Janus* to this case. If the government picks up an additional vote from Alito, then Lorenzo will have no chance to prevail. My guess is that we can expect a short and straightforward opinion affirming Lorenzo's liability.

The post **Argument analysis: Justices appear divided in debate over anti-fraud securities rules** appeared first on **SCOTUSblog**.



---

You are subscribed to email updates from [SCOTUSblog](#).  
To stop receiving these emails, you may [unsubscribe now](#).

Email delivery powered by Google

Google, 1600 Amphitheatre Parkway, Mountain View, CA 94043, United States

**From:** [InfraGard Los Angeles](#)  
**To:** [Kevin Woodworth](#)  
**Subject:** Service Members Killed, Cyber Shield and more  
**Date:** Tuesday, November 27, 2018 1:14:07 PM



## **The InfraGard Los Angeles Daily Brief**

**27November2018**

**Attached to Today's Brief:**

**CAL FIRE**

**3 US service members killed in Afghanistan roadside bomb blast; deadliest incident this year**

**GM will no longer make these 6 cars**

[Try Landing InSight on Mars \(Without Exploding\)](#)

["Horrrifying": Global outrage after Chinese researcher claims first gene-edited babies](#)

**Upcoming Training and Events:**

[IGLA Active Shooter Survival Kit  
Now Available For Purchase at InfraGard Training  
Events](#)

[A Culture of Preparedness: Federal, State, and Local  
Training Resources: 06December2018](#)

[OSINT \(Open Source Intelligence Exploitation\)  
Course, Temecula, California: 12December2018](#)



The US is warning other countries against using Huawei's 5G tech  
Uber fined after 'serious breach' allows hackers to download 2.7 million customers' data  
Half of phishing sites trick you into thinking they're 'secure'  
Microsoft reveals bugs that knocked out Azure, Office 362.5 multi-factor auth logins  
Lenovo to Pay \$7.3 Million in Settlement for Installing Adware on 800K Notebooks  
Microsoft patches Patch Tuesday's Outlook 2010 problem patch  
Increasing Risk of Cyber Attacks During Holidays Says Report

## **The Cyber Shield: 27November2018**



### **CONUS**

1. US woman pleads guilty to bitcoin ploy aiding Islamic State [ABC via



## **AP]**

- A Pakistani-born New York woman has acknowledged her role in defrauding numerous financial institutions in a bitcoin scheme to help the Islamic State group.
- Prosecutors say Zoobia Shahnaz, a naturalized U.S. citizen living on Long Island, pleaded guilty in federal court in Central Islip Monday to providing material support to a foreign terrorist organization.
- The 27-year-old Shahnaz was charged with laundering bitcoin and wiring money to the Islamic State group. After quitting her job, she was stopped at Kennedy Airport last year attempting to fly to Pakistan.
- She faces up to 20 years in prison.
- See also DOJ: [New York Woman Pleads Guilty to Providing Material Support to ISIS](#)

## **2. [Judge accepts novel plea deal for Chicago terrorist Adel Daoud](#) [WLS/ABC7, Chicago, IL]**

- Guilty, but no admission of guilt, was the unusual plea deal made by a west suburban man in a major terrorism case that has stretched on for six years.
- Against the government's wishes, 25-year-old Adel Daoud, of Hillside, was permitted by a federal judge in Chicago to enter what is known as an "Alford plea," in which a defendant pleads guilty while maintaining they are actually innocent.
- Judge Johnson Coleman set a sentencing plan that will be what amounts to a "mini-trial" in late April that will last as long as one week and feature the evidence and witnesses that prosecutors and defense attorneys might have used at a regular criminal trial had it come to that.
- The judge accepted the Alford plea because she said Daoud understood what he was doing, he had received good counseling from his attorney and that this was the best option for his mental health.
- Daoud's sentencing is set for April 29, 2019.

## **3. [For Dzhokar Tsarnaev, TV lineup's better than basic](#) [Boston Herald – embedded photo]**

- Boston Marathon bomber Dzhokhar Tsarnaev has the outside world "piped into his cell" through a TV offering 50 channels of TV programming while awaiting execution at a prison dubbed the "Alcatraz of the Rockies," according to newly unsealed court documents.
- As the December deadline for producing his first appeal looms, dozens of motions, transcripts and exhibits barred from public view for more than three years are shedding light on the behind-the-scenes story of Tsarnaev's 2015 trial — including his willingness to plead guilty if guaranteed his life would be spared.
- In the days leading up to a federal jury's verdicts that Tsarnaev be put to death for terrorism and murder, incensed prosecutors were fighting behind closed doors to show jurors that life in solitary confinement at the Supermax penitentiary was not crueler than lethal injection.
- [AUSA] Weinreb told [Judge] O'Toole during an April 13, 2015, closed



motion hearing that what Tsarnaev refused to do was “help the government” by answering questions about additional threats and “many, many, many things the government very badly wanted to know.”

#### **4. Few charged despite thousands of active FBI terrorism investigations [Washington Times]**

- The FBI says it has thousands of active terrorism investigations, but few are resulting in criminal charges.
- Only nine people have been publicly charged with crimes related to involvement with major terrorist groups this year, according to the Center on National Security at Fordham University, suggesting a major disconnect between the scope of the investigations and the criminal activity discovered.
- Five cases associated with the Islamic State have been prosecuted this year, compared with 17 last year and 35 in 2016.
- The Trump administration identifies terrorism, particularly attacks affiliated with al Qaeda or the Islamic State, as the top priority for the Justice Department.

#### **5. LA police, FBI Investigate Potential Jewish Hate Crime [Newsweek]**

- The Los Angeles Police Department announced its investigation into a potential hate crime in a Jewish neighborhood after the suspect attempted to drive his car into two men and yelled racial slurs as they walked down the street after exiting a synagogue.
- Mohamed Mohamed Abdi, 32, was arrested on charges of assault with a deadly weapon after eventually slamming into a car in the Hancock Park neighborhood, the LAPD announced on Monday. Abdi also faces a special enhancement of a hate crime charge.
- Abdi allegedly tried to run over the two men twice before colliding with the vehicle. The FBI and the U.S. Attorney General's office have joined the investigation, according to the report.
- Analyst comment: Included in ONN for situational awareness.

#### **6. U.S. prosecutors oppose request for unsealing possible Assange charges [Reuters]**

- Federal prosecutors have told a United States District Court judge that they oppose a request by a journalists' group for the unsealing of any pending U.S. criminal indictment against WikiLeaks founder Julian Assange, and declined to admit whether such charges exist.
- In a filing submitted on Monday, prosecutors in Alexandria, Virginia said a recent disclosure in a court document filed in an unrelated criminal case that prosecutors had obtained a sealed indictment against Assange was an “unintentional error.”
- Prosecutors said the erroneous filing does not constitute a confirmation or denial by them as to whether sealed criminal charges against Assange exist, and argued that neither the U.S. constitution nor U.S. common law “require that the government provide such a confirmation or denial.”
- On Tuesday, Judge Brinkema is scheduled to hear arguments in a case brought by the Reporters Committee for Freedom of the Press, which has

applied for the unsealing of court records “including the docket and any criminal complaint, indictment or other charging document” related to any sealed U.S. charges against Assange.

- Analyst comment: Included in ONN for situational awareness.

#### **7. Ex-New York teacher, brother plead guilty to attempted bomb-making [Reuters]**

- A former New York City high school teacher and his brother on Monday pleaded guilty to attempting to build a bomb using explosive materials stashed in their apartment, federal prosecutors announced.

- Christian Toro, the former teacher, and his brother Tyler Toro, both 28, were arrested in February and charged with stockpiling materials for making bombs in their shared apartment in the city’s Bronx borough.

- In a criminal complaint filed at the time of the brothers’ arrest, prosecutors said law enforcement agents who searched their apartment found explosive substances and a backpack with an index card reading, “Under the full moon the small ones will know terror.”

- Christian Toro was a teacher at a high school in Manhattan’s Harlem neighborhood before resigning last year. Following the resignation, Tyler Toro returned to the school a computer that had been provided to his brother, and staff found instructions on it for building explosive devices.

- Investigators said Christian Toro told them he had found the document while researching the 2013 Boston Marathon bombing and never read it or had built a bomb, according to the complaint.



[Data Shows Assaults on Border Agents are Rising as Use of Force Drops](#)  
Between October 1, 2017 and August 31 of this year, border agents reported 471 “use of force” incidents in which they took physical measures against a person or vehicle at the border or point of entry, while during the same period reporting 721 individual assaults against border agents at or between points of entry. The article identifies this as a trend, as assaults against agents began rising in FY15.

[California School District Implements Visitor Management \(Raptor\) System](#)  
In an effort to increase school security, Delano Union School District (DUSD) in California has implemented a visitor management system at its 12 schools. The Raptor system, which was recently rolled-out to all schools after finishing its pilot programs in Texas, allows administration to monitor the people who come to campus as well as check to ensure they are authorized to enter. The system also allows the school to send rapid alerts in an emergency situation, something DUSD was very interested in implementing on their campuses, according to District Director of Safety and Security James Hay.

### What Concerning Behaviors Should Be Reported to an Intervention Team?

To keep colleges and universities safe, behavioral intervention teams monitor individuals showing potentially dangerous behavior both on-campus and in online classrooms. Intervention teams are tasked with stepping in before an individual takes violent action, but they rely heavily on individuals reporting when someone is exhibiting concerning behavior. The story examines several instances of concerning behavior?

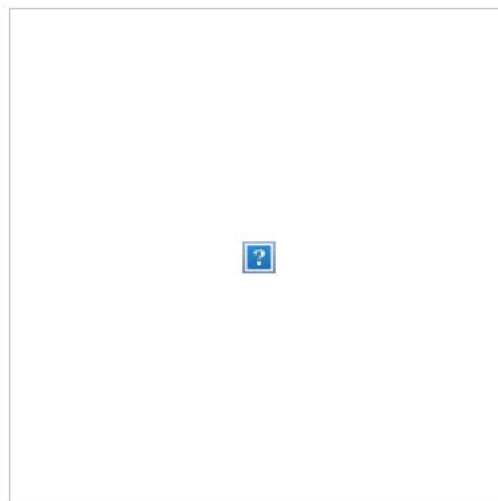
### **Police Killed/Injured in Action**

1. [Four Deputies, One Suspect Wounded in Two St. Bernard \(LA\) Shooting Incidents](#)
2. [Man Carrying AK-47 Shoots Dayton Beach \(FL\) Police Officer, Officials Say](#)

### **Use of Force**

1. [Suspect Shot by Michigan State Police Trooper After High-Speed Chase in Livonia](#)
2. ['Suspected Shooter' Shot, Wounded by US Marshals Conducting Surveillance Near 28<sup>th</sup> and Wells \(Milwaukee, WI\)](#)
3. [Two Suspects At Large After Police Chase, Officer Involved Shooting \(Corpus Christi, TX\)](#)
4. [Justine Damond Shooting \(Minneapolis, MN\): Prosecutors Seek to Question Jurors About Police Use of Force](#)
5. [Wallingford \(CT\) Police Officer Suspended for Excessive Force: Report](#)

## **This Date in History**



On this day in 1911, Elizabeth Jaffray, a [White House](#) housekeeper, writes in her diary about a conversation she'd had with President [William Howard Taft](#) and his wife about the commander in chief's ever-expanding waistline.

According to the White House Historical Association, Jaffray was also quoted regarding Taft's growing girth in a 1926 book called *Secrets of the White House*. In it, she detailed a typical breakfast consumed by the 332-pound president: "two oranges, a twelve-ounce beefsteak, several pieces of toast and butter and a vast quantity of coffee with cream and sugar." When she and Taft's wife, Nellie, commented on his eating habits, he jovially responded that he was planning to go on a diet, but lamented the fact that "things are in a sad state of affairs when a man can't even call his gizzard his own."

Taft's 5' 11" frame carried anywhere between 270 pounds and 340 pounds over the course of his adult life. According to his biographers, he had to have his shoes tied by his valet and often got stuck in the White House bathtub and had to be lifted out by two or more men. Once, while visiting the czar of Russia, Taft split his pants seam while descending from a carriage.

Taft's weight did not stop him from serving a full term as president, nor did it prevent him from accepting a subsequent appointment as chief justice of the [Supreme Court](#) in 1921—he was the first and only president to hold both offices. In fact, he successfully dropped down to 270 pounds after leaving the White House. Still, by today's body-mass indices, Taft remained clinically obese. Although he rarely drank more than the occasional beer and did not smoke, his obesity and a lifelong struggle with severe sleep apnea eventually took its toll. In March 1930, he retired as chief justice citing poor health. He died the following month from heart failure.

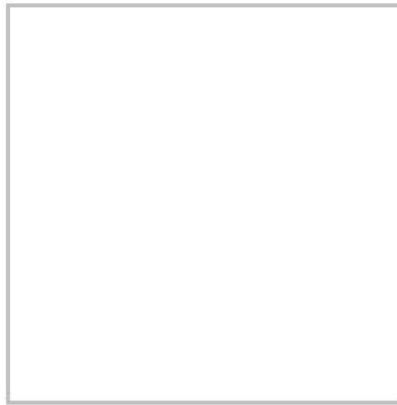
**"Don't write so that you can be understood, write so that you can't be misunderstood."**

**William Howard Taft**

**Threat Reporting: As a reminder, for immediate, specific threat information, call 911. Please report all other threat information online at <https://tips.fbi.gov> or via phone at 1-800-CALL-FBI (225-5324).**

**[Click Here for tips.fbi.gov](https://tips.fbi.gov)**





**Be Safe,  
InfraGard Los Angeles**

**Copyright InfraGard Los Angeles Members Alliance 2016  
11000 Wilshire Blvd. Ste. 1700  
Los Angeles CA, 90024  
562.345.1166**

(U) WARNING: RECEIPT OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF ALL TERMS AND CONDITIONS REGARDING ITS USE, HANDLING, STORAGE, FURTHER DISSEMINATION OR DESTRUCTION. AT A MINIMUM, RECEIPT ACKNOWLEDGES A COMMITMENT TO COMPLY WITH ALL APPLICABLE LAWS PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE COLLECTION, USE, ANALYSIS, RETENTION, DESTRUCTION, SHARING AND DISCLOSURE OF INFORMATION. This information is the property of the JRIC and is UNCLASSIFIED // FOR OFFICIAL USE ONLY. This information may not be distributed to federal, state, tribal, and local government or public safety personnel on a need-to-know basis without further approval from the JRIC. This information is sensitive, and cannot be released to the public, the media, or other individuals who do not have a valid need-to-know, without prior approval of an authorized JRIC official. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

**You have opted to receive this email as part of your membership to the InfraGard Los Angeles Members' Alliance.**

[Visit our website](#)



InfraGard Los Angeles | 12440 E. Imperial Highway, Suite 700, Norwalk, CA 90650

[Unsubscribe kwoodworth@sunnyvale.ca.gov](mailto:kwoodworth@sunnyvale.ca.gov)

[Update Profile](#) | [About our service provider](#)

Sent by [info@infragardlosangeles.org](mailto:info@infragardlosangeles.org)

**From:** [Microsoft Exchange Approval Assistant](#) on behalf of [Ao9YUFL3KSymZPqt/MOWcoq=== 1125768951830\\_BapBjHX1EeqSKdSuUpk7UJA==@in.constantcontact.com](#)  
**To:** [Admin.QYin; Wil Guitarte](#)  
**Subject:** Approval requested:Service Members Killed, Cyber Shield and more  
**Date:** Tuesday, November 27, 2018 1:12:58 PM  
**Attachments:** [Service Members Killed Cyber Shield and more \(91.6 KB\).msg](#)

## Your decision is requested.

InfraGard Los Angeles([info@infragardlosangeles.org](mailto:info@infragardlosangeles.org)) has asked you to approve the attached message for delivery to:

Kevin Woodworth

A preview of the message is below. To view the complete message, open the attachment.

**From:** InfraGard Los Angeles([info@infragardlosangeles.org](mailto:info@infragardlosangeles.org))

**To:** [kwoodworth@sunnyvale.ca.gov](mailto:kwoodworth@sunnyvale.ca.gov)

**Subject:** Service Members Killed, Cyber Shield and more



# **The InfraGard Los Angeles Daily Brief**

**27November2018**

**Attached to Today's Brief:**

## **CAL FIRE**

**3 US service members killed in Afghanistan roadside bomb blast; deadliest incident this year**

**GM will no longer make these 6 cars**

**Try Landing InSight on Mars (Without Exploding)**

**"Horrific": Global outrage after Chinese researcher claims first gene-edited babies**

**Upcoming Training and Events:**

**IGLA Active Shooter Survival Kit**  
**Now Available For Purchase at InfraGard Training Events**

**A Culture of Preparedness: Federal, State, and Local Training Resources: 06December2018**

**OSINT (Open Source Intelligence Exploitation) Course, Temecula, California: 12December2018**



The US is warning other countries against using Huawei's 5G tech  
Uber fined after 'serious breach' allows hackers to download 2.7 million customers' data  
Half of phishing sites trick you into thinking they're 'secure'  
Microsoft reveals bugs that knocked out Azure, Office 362.5 multi-factor auth logins  
Lenovo to Pay \$7.3 Million in Settlement for Installing Adware on 800K Notebooks  
Microsoft patches Patch Tuesday's Outlook 2010 problem patch  
Increasing Risk of Cyber Attacks During Holidays Says Report

## **The Cyber Shield: 27November2018**





## **CONUS**

### **1. US woman pleads guilty to bitcoin ploy aiding Islamic State [ABC via AP]**

- A Pakistani-born New York woman has acknowledged her role in defrauding numerous financial institutions in a bitcoin scheme to help the Islamic State group.
- Prosecutors say Zoobia Shahnaz, a naturalized U.S. citizen living on Long Island, pleaded guilty in federal court in Central Islip Monday to providing material support to a foreign terrorist organization.
- The 27-year-old Shahnaz was charged with laundering bitcoin and wiring money to the Islamic State group. After quitting her job, she was stopped at Kennedy Airport last year attempting to fly to Pakistan.
- She faces up to 20 years in prison.
- See also DOJ: **New York Woman Pleads Guilty to Providing Material Support to ISIS**

## **2. Judge accepts novel plea deal for Chicago terrorist Adel Daoud [WLS/ABC7, Chicago, IL]**

- Guilty, but no admission of guilt, was the unusual plea deal made by a west suburban man in a major terrorism case that has stretched on for six years.
- Against the government's wishes, 25-year-old Adel Daoud, of Hillside, was permitted by a federal judge in Chicago to enter what is known as an "Alford plea," in which a defendant pleads guilty while maintaining they are actually innocent.
- Judge Johnson Coleman set a sentencing plan that will be what amounts to a "mini-trial" in late April that will last as long as one week and feature the evidence and witnesses that prosecutors and defense attorneys might have used at a regular criminal trial had it come to that.
- The judge accepted the Alford plea because she said Daoud understood what he was doing, he had received good counseling from his attorney and that this was the best option for his mental health.
- Daoud's sentencing is set for April 29, 2019.

## **3. For Dzhokar Tsarnaev, TV lineup's better than basic [Boston Herald – embedded photo]**

- Boston Marathon bomber Dzhokhar Tsarnaev has the outside world "piped into his cell" through a TV offering 50 channels of TV programming while awaiting execution at a prison dubbed the "Alcatraz of the Rockies," according to newly unsealed court documents.
- As the December deadline for producing his first appeal looms, dozens of motions, transcripts and exhibits barred from public view for more than three years are shedding light on the behind-the-scenes story of Tsarnaev's 2015 trial — including his willingness to plead guilty if guaranteed his life would be spared.
- In the days leading up to a federal jury's verdicts that Tsarnaev be put to death for terrorism and murder, incensed prosecutors were fighting behind closed doors to show jurors that life in solitary confinement at the Supermax penitentiary was not crueler than lethal injection.
- [AUSA] Weinreb told [Judge] O'Toole during an April 13, 2015, closed motion hearing that what Tsarnaev refused to do was "help the government" by answering questions about additional threats and "many, many, many things the government very badly wanted to know."

## **4. Few charged despite thousands of active FBI terrorism investigations [Washington Times]**

- The FBI says it has thousands of active terrorism investigations, but few are resulting in criminal charges.
- Only nine people have been publicly charged with crimes related to involvement with major terrorist groups this year, according to the Center on National Security at Fordham University, suggesting a major disconnect between the scope of the investigations and the criminal activity discovered.
- Five cases associated with the Islamic State have been prosecuted this year, compared with 17 last year and 35 in 2016.



- The Trump administration identifies terrorism, particularly attacks affiliated with al Qaeda or the Islamic State, as the top priority for the Justice Department.

#### **5. LA police, FBI Investigate Potential Jewish Hate Crime [Newsweek]**

- The Los Angeles Police Department announced its investigation into a potential hate crime in a Jewish neighborhood after the suspect attempted to drive his car into two men and yelled racial slurs as they walked down the street after exiting a synagogue.
- Mohamed Mohamed Abdi, 32, was arrested on charges of assault with a deadly weapon after eventually slamming into a car in the Hancock Park neighborhood, the LAPD announced on Monday. Abdi also faces a special enhancement of a hate crime charge.
- Abdi allegedly tried to run over the two men twice before colliding with the vehicle. The FBI and the U.S. Attorney General's office have joined the investigation, according to the report.
- Analyst comment: Included in ONN for situational awareness.

#### **6. U.S. prosecutors oppose request for unsealing possible Assange charges [Reuters]**

- Federal prosecutors have told a United States District Court judge that they oppose a request by a journalists' group for the unsealing of any pending U.S. criminal indictment against WikiLeaks founder Julian Assange, and declined to admit whether such charges exist.
- In a filing submitted on Monday, prosecutors in Alexandria, Virginia said a recent disclosure in a court document filed in an unrelated criminal case that prosecutors had obtained a sealed indictment against Assange was an "unintentional error."
- Prosecutors said the erroneous filing does not constitute a confirmation or denial by them as to whether sealed criminal charges against Assange exist, and argued that neither the U.S. constitution nor U.S. common law "require that the government provide such a confirmation or denial."
- On Tuesday, Judge Brinkema is scheduled to hear arguments in a case brought by the Reporters Committee for Freedom of the Press, which has applied for the unsealing of court records "including the docket and any criminal complaint, indictment or other charging document" related to any sealed U.S. charges against Assange.
- Analyst comment: Included in ONN for situational awareness.

#### **7. Ex-New York teacher, brother plead guilty to attempted bomb-making [Reuters]**

- A former New York City high school teacher and his brother on Monday pleaded guilty to attempting to build a bomb using explosive materials stashed in their apartment, federal prosecutors announced.
- Christian Toro, the former teacher, and his brother Tyler Toro, both 28, were arrested in February and charged with stockpiling materials for making bombs in their shared apartment in the city's Bronx borough.
- In a criminal complaint filed at the time of the brothers' arrest, prosecutors

said law enforcement agents who searched their apartment found explosive substances and a backpack with an index card reading, "Under the full moon the small ones will know terror."

- Christian Toro was a teacher at a high school in Manhattan's Harlem neighborhood before resigning last year. Following the resignation, Tyler Toro returned to the school a computer that had been provided to his brother, and staff found instructions on it for building explosive devices.

- Investigators said Christian Toro told them he had found the document while researching the 2013 Boston Marathon bombing and never read it or had built a bomb, according to the complaint.



[Data Shows Assaults on Border Agents are Rising as Use of Force Drops](#)  
Between October 1, 2017 and August 31 of this year, border agents reported 471 "use of force" incidents in which they took physical measures against a person or vehicle at the border or point of entry, while during the same period reporting 721 individual assaults against border agents at or between points of



entry. The article identifies this as a trend, as assaults against agents began rising in FY15.

California School District Implements Visitor Management (Raptor) SystemIn an effort to increase school security, Delano Union School District (DUSD) in California has implemented a visitor management system at its 12 schools. The Raptor system, which was recently rolled-out to all schools after finishing its pilot programs in Texas, allows administration to monitor the people who come to campus as well as check to ensure they are authorized to enter. The system also allows the school to send rapid alerts in an emergency situation, something DUSD was very interested in implementing on their campuses, according to District Director of Safety and Security James Hay.

#### What Concerning Behaviors Should Be Reported to an Intervention Team?

To keep colleges and universities safe, behavioral intervention teams monitor individuals showing potentially dangerous behavior both on-campus and in online classrooms. Intervention teams are tasked with stepping in before an individual takes violent action, but they rely heavily on individuals reporting when someone is exhibiting concerning behavior. The story examines several instances of concerning behavior?

#### **Police Killed/Injured in Action**

1. Four Deputies, One Suspect Wounded in Two St. Bernard (LA) Shooting Incidents
2. Man Carrying AK-47 Shoots Dayton Beach (FL) Police Officer, Officials Say

#### **Use of Force**

1. Suspect Shot by Michigan State Police Trooper After High-Speed Chase in Livonia
2. 'Suspected Shooter' Shot, Wounded by US Marshals Conducting Surveillance Near 28<sup>th</sup> and Wells (Milwaukee, WI)
3. Two Suspects At Large After Police Chase, Officer Involved Shooting (Corpus Christi, TX)
4. Justine Damond Shooting (Minneapolis, MN): Prosecutors Seek to Question Jurors About Police Use of Force
5. Wallingford (CT) Police Officer Suspended for Excessive Force: Report

## **This Date in History**





On this day in 1911, Elizabeth Jaffray, a [White House](#) housekeeper, writes in her diary about a conversation she'd had with President [William Howard Taft](#) and his wife about the commander in chief's ever-expanding waistline.

According to the White House Historical Association, Jaffray was also quoted regarding Taft's growing girth in a 1926 book called *Secrets of the White House*. In it, she detailed a typical breakfast consumed by the 332-pound president: "two oranges, a twelve-ounce beefsteak, several pieces of toast and butter and a vast quantity of coffee with cream and sugar." When she and Taft's wife, Nellie, commented on his eating habits, he jovially responded that he was planning to go on a diet, but lamented the fact that "things are in a sad state of affairs when a man can't even call his gizzard his own."

Taft's 5' 11" frame carried anywhere between 270 pounds and 340 pounds over the course of his adult life. According to his biographers, he had to have his shoes tied by his valet and often got stuck in the White House bathtub and had to be lifted out by two or more men. Once, while visiting the czar of Russia, Taft split his pants seam while descending from a carriage.

Taft's weight did not stop him from serving a full term as president, nor did it prevent him from accepting a subsequent appointment as chief justice of the [Supreme Court](#) in 1921—he was the first and only president to hold both offices. In fact, he successfully dropped down to 270 pounds after leaving the White House. Still, by today's body-mass indices, Taft remained clinically obese. Although he rarely drank more than the occasional beer and did not smoke, his obesity and a lifelong struggle with severe sleep apnea eventually took its toll. In March 1930, he retired as chief justice citing poor health. He died the following month from heart failure.

**"Don't write so that you can be understood, write so that you can't be misunderstood."**

**William Howard Taft**

**Threat Reporting: As a reminder, for immediate, specific threat**

information, call 911. Please report all other threat information online at <https://tips.fbi.gov> or via phone at 1-800-CALL-FBI (225-5324).

[Click Here for tips.fbi.gov](https://tips.fbi.gov)



**Be Safe,  
InfraGard Los Angeles**

**Copyright InfraGard Los Angeles Members Alliance 2016  
11000 Wilshire Blvd. Ste. 1700  
Los Angeles CA, 90024  
562.345.1166**

(U) WARNING: RECEIPT OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF ALL TERMS AND CONDITIONS REGARDING ITS USE, HANDLING, STORAGE, FURTHER DISSEMINATION OR DESTRUCTION. AT A MINIMUM, RECEIPT ACKNOWLEDGES A COMMITMENT TO COMPLY WITH ALL APPLICABLE LAWS PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE COLLECTION, USE, ANALYSIS, RETENTION, DESTRUCTION, SHARING AND DISCLOSURE OF INFORMATION. This information is the property of the JRIC and is UNCLASSIFIED // FOR OFFICIAL USE ONLY. This information may not be distributed to federal, state, tribal, and local government or public safety personnel on a need-to-know basis without further approval from the JRIC. This information is sensitive, and cannot be released to the public, the media, or other individuals who do not have a valid need-to-know, without prior approval of an authorized JRIC official. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

**You have opted to receive this email as part of your membership to the InfraGard Los Angeles Members' Alliance.**

Visit our website



InfraGard Los Angeles | 12440 E. Imperial Highway, Suite 700, Norwalk, CA 90650

[Unsubscribe kwoodworth@sunnyvale.ca.gov](mailto:kwoodworth@sunnyvale.ca.gov)

[Update Profile](#) | [About our service provider](#)

Sent by [info@infragardlosangeles.org](mailto:info@infragardlosangeles.org)



**From:** [Security Management Daily](#)  
**To:** [Ruben Cortez](#)  
**Subject:** Security Management Daily - November 27, 2018  
**Date:** Tuesday, November 27, 2018 8:52:23 AM



Banner



Advertising/Sponsorship Opportunities | Professional Edition

## Top Security News

**Chicago Hospital Shooting Sparks Workplace Security Concerns**  
From "Chicago Hospital Shooting Sparks Workplace Security Concerns"  
*Crain's Chicago Business (11/20/18) Goldberg, Stephanie*

A shooting at Mercy Hospital & Medical Center left an emergency room doctor, a pharmacy resident, and a police officer dead, and serves as a reminder for employers to update workplace violence prevention plans. Medicare and Medicaid participating providers and suppliers, which includes hospitals, are required by the Centers for Medicare and Medicaid Services to ensure adequate planning for natural and man-made disasters by performing a risk assessment, developing and implementing policies and procedures, creating a communication plan, and conducting training and testing. Dick Sem, president of security and workplace violence consultant Sem Security Management in Burlington, Wisconsin, said about half the workplace violence prevention plans and policies he sees at hospitals are not comprehensive enough. Sem said he starts by asking his clients if staff are trained to recognize early signs of potential violence, or if they know when to remove themselves from a situation. "More often than not, I see very little training," Sem said. "They might train high-risk staff, like emergency and security and behavioral health, but not all the staff." A few days before the shooting at Mercy Hospital, Rep. Joe Courtney, D-Conn., a member of the House Education and Workforce Committee, introduced H.R. 7141, which would require the U.S. Occupational Safety and Health Administration to issue a standard requiring health care and social service employers to write and implement a workplace violence prevention plans.

Share   | [Web Link](#)



**Free Webinar: Tuesday November 27, 2018, 2pm EST.  
Protecting Houses of Worship: Evolving Threats in an Ever-  
Changing Landscape.**

Acts of domestic terrorism are again in the headlines, starkly confronting us with the relentless growth of violence against ordinary citizens who are targeted for practicing their religion.

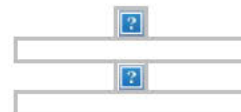
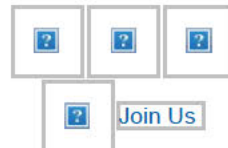
Earn 1 hour CEU



## Top Security News

November 27, 2018

### Follow Us



### Calendar of Events

#### UPCOMING EVENTS

- [Strategy and Tactics in Crisis Management: From Prevention to Recovery \(10-11 Dec\)](#)
- [Conducting Advanced Internal Investigations \(10-12 Dec\)](#)

#### UPCOMING WEBINARS

- [The Security Manager's Response to Opiates in the Workplace \(5 Dec\)](#)
- [The Security Manager's Response to Opiates in the Workplace \(6 Dec\)](#)
- [Preventing Mass Casualty Events in Hospitality, Gaming, and Event Venues \(12 Dec\)](#)

[Global Events](#)  
[More Classroom Programs](#)  
[More Webinars](#)

## **Handgun Buyers Would Have to Give Police Social Media Passwords Under New York Proposal**

From "Handgun Buyers Would Have to Give Police Social Media Passwords Under New York Proposal"

*McClatchy News Service (11/23/18) Gilmour, Jared*

A new proposal would require New York state residents who want handgun licenses to undergo search engine and social media checks, including handing over log-in information and passwords to police. State Sen. Kevin Parker (D-Brooklyn) introduced the bill this month. Facebook, Snapchat, Twitter, and Instagram are the social media platforms that would be scrutinized under the bill. Investigators would review applicants' Google, Yahoo, and Bing search results as well. Under the proposed legislation, police are instructed to watch for posts that include profane slurs or biased language related to race, color, ancestry, gender, religion, age, disability, and sexual orientation. Other red flags would include threats to other people and acts of terrorism that turn up in the search. Critics warn the bill opens the door for discrimination. The bill is in the state Senate's rules committee. New York residents have to recertify their pistol licenses every five years. Applicants for the license are already required to submit their criminal history, mental health history, and offer character references. They have to be over 21 and cannot have felony or serious offense convictions.

Share    | [Web Link](#)



### **Free Webinar: November 17, 2018 @ 2pm ET How Open Supervised Device Protocol (ODSP) Is Revolutionizing Access Control Systems**

Today, 41 percent of security professionals indicate their organizations' physical access control system is being upgraded to, or already running on the latest industry standard: Open Supervised Device Protocol (ODSP). However, this means the security and efficiency of many physical access control systems are still performing below accepted industry guidelines. With OSDP on the rise, it's important to know how it enables ROI.

## **FCA Says Financial Firms Not Getting Basics Right on Cybersecurity**

From "FCA Says Financial Firms Not Getting Basics Right on Cybersecurity"

*Reuters (11/27/18) Jones, Huw*

A senior official at Britain's Financial Conduct Authority recently warned that the markets watchdog will punish firms that are failing to get the basics right on cybersecurity. The watchdog surveyed almost 300 regulated firms between 2017 and 2018 and found that in the year to October, the firms reported a 138 percent rise in technology outages, and an 18 percent increase in cyber incidents. Megan Butler, the FCA's executive director of supervision, said under-reporting of incidents is still a problem, with many linked to an "over-confidence bias" at banks about managing major IT changes. She added that boards of financial firms need to understand technology issues.

Share    | [Web Link](#)

## **Stoneman Douglas Commission Looks at Quick Fixes to Boost School Security**

From "Stoneman Douglas Commission Looks at Quick Fixes to Boost School Security"

*SunSentinal (11/19/18) Fleshler, David*

The Florida state commission investigating the Parkland massacre will consider recommending a series of quick fixes to strengthen school security, such as



guarding all open gates and training teachers in emergency procedures. The draft list of recommendations submitted by individual commission members includes ambitious proposals such as equipping schools with bulletproof glass, requiring live video surveillance monitoring, and rewriting federal student-privacy law to make it easier for schools to share information with law enforcement agencies. However, the initial focus will be on things that can be done quickly, cheaply, and without major changes to the law, according to Pinellas County Sheriff Bob Gualtieri, chairman of the Marjory Stoneman Douglas High School Public Safety Commission. The commission's hearings revealed several points at which the shooting might have been averted, or at least minimized. The commission, which is made up of law enforcement officers, public officials, and parents of children killed in the attack, is required to complete an initial report to the governor and state legislature. It will hold its final hearings of the year Dec. 12-13 in Tallahassee.

Share    | [Web Link](#)

### **U.S. Forces in Afghanistan: 3 American Service Members Have Been Killed in a Roadside Bombing**

From "U.S. Forces in Afghanistan: 3 American Service Members Have Been Killed in a Roadside Bombing"  
*USA Today (11/27/18) Bacon, John*

A roadside bomb exploded Tuesday in Afghanistan's Ghazni province, killing three American service members, U.S. military officials said. Lt. Ubon Mendie, a spokesman for the U.S. forces, said that three other service members and one American civilian contractor were injured in the blast. The Taliban claimed responsibility for the attack. The American death toll from the war in Afghanistan has exceeded 2,200.

Share    | [Web Link](#)

### **China Reportedly Steps Up Efforts to Steal Australian Company Secrets**

From "China Reportedly Steps Up Efforts to Steal Australian Company Secrets"  
*CNBC (11/21/18) Choudhury, Saheli Roy*

China allegedly directed an increase in cyberattacks on Australian companies this year, a move that breached a bilateral agreement between the two countries pledging not to steal each other's commercial secrets. Nine News and Fairfax Media found that China's Ministry of State Security was responsible for "Operation Cloud Hopper," which involved a wave of attacks directed at Australia and its partners in the "Five Eyes" intelligence sharing alliance: the United States, the United Kingdom, New Zealand, and Canada. China's activity was a "constant, significant effort" to steal intellectual property, according to a senior Australian government source. China's Foreign Ministry spokesperson Geng Shuang addressed the report by saying that cyberattacks are a common challenge faced by all countries. Western countries have long accused China of stealing intellectual property as well as commercial and military secrets, which Beijing has denied. In recent years, China has increased efforts to create sophisticated home-grown technologies as it tries to catch up with other high-tech countries like the U.S. and Germany.

Share    | [Web Link](#)

### **Vision Direct Hacked**

From "Vision Direct Hacked"  
*BBC News (11/19/18) Kelion, Leo*

Vision Direct said anyone who entered their details into its site between Nov. 3 and Nov. 8 could be affected by a hack attack, which exposed the personal data of thousands of its customers. The company said a fake Google Analytics script placed within its websites' code was the apparent cause. A spokeswoman for Vision Direct said that 6,600 customers were believed to have had details including financial data compromised, while an additional 9,700 people had had personal data, but not card details exposed.

Share    | [Web Link](#)

### **Surveying the Public in a City Being Used as Federal Drone Testing Site**

From "Surveying the Public in a City Being Used as Federal Drone Testing Site"  
*NextGov.com (11/26/18) Grass, Michael*

The FAA has designated San Diego and other U.S. cities as testbeds for aerial drone tech to inform federal policymakers' regulatory approach. The San Diego project will, among other things, test drones' ability to help local firefighters gather intelligence on wildfires, and to aid medical professionals at UC San Diego with transporting blood and supplies faster.

Share   | [Web Link](#)

### **Something in the Water**

From "Something in the Water"  
*Security Management (11/18) Gates, Megan*

From Aug. 28 to Sept. 18, 2013, an Iranian hacker with links to the Islamic Revolutionary Guard gained unauthorized access to the SCADA (supervisory control and data acquisition) systems of the Bowman Avenue Dam in Rye Brook, N.Y. The hacker was able to obtain information about the status and operation of the dam, but was prevented from gaining control of the gate because it was manually disconnected for maintenance. After a lengthy probe, the U.S. Department of Justice indicted seven Iranians for their alleged roles in both the dam hacking and a broader series of distributed denial of service attacks on financial institutions in New York state. Since then, the U.S. Department of Homeland Security (DHS) has designated critical infrastructure verticals and created information sharing and analysis centers for each vertical. The DHS also recently released a cybersecurity strategy for 2018 to 2022 and has unveiled a National Risk Management Center focused on defending U.S. critical infrastructure. According to the U.S. Environmental Protection Agency's Cybersecurity Guide for States, a key hurdle for water and wastewater utilities is the lack of resources for information technology and security specialists to assist with creating a cybersecurity program. Chris Grove, director of industrial security at Indegy, says many executives of water treatment facilities believe the air gap is a fail-safe system. However, mapping could be used to determine what assets are in the system and how they are vulnerable, while a monitoring system could detect when an infiltration has occurred.

Share   | [Web Link](#)

### **U.K. and Netherlands Fine Uber Over Data Breach**

From "U.K. and Netherlands Fine Uber Over Data Breach"  
*Financial Times (11/27/18) Samson, Adam*

British and Dutch data protection regulators have fined Uber after a data breach compromised information about customers and drivers. Britain's Information Commissioner's Office it would fine Uber £385,000 for "failing to protect customers' personal information during a cyber attack." The personal details of around 2.7 million U.K. customers were accessed and downloaded by attackers. Meanwhile, the Dutch Data Protection Authority hit Uber with a fine of €600,000 (£532,000) for "violating the Dutch data breach regulation." In September, Uber agreed to pay a record \$148 million to settle claims with all 50 U.S. states and the District of Columbia over the data breach.

Share   | [Web Link](#) - May Require Paid Subscription

---

News summaries © copyright 2018 [SmithBucklin](#)



If you have questions, please contact Member Services at [asis@asisonline.org](mailto:asis@asisonline.org) or +1.703.519.6200, or via 1625 Prince Street, Alexandria, VA 22314 USA.

[Log in to manage your privacy settings.](#) | [Unsubscribe SM Daily](#)

ASIS International values the privacy and integrity of our members, partners, attendees, exhibitors, and sponsors, and we do not sell your contact information, nor do we provide it to third-party vendors for distribution. [View privacy policy.](#)

**From:** [Association of Deputy District Attorneys](#)  
**To:** [fgurina@sunnyvale.ca.gov](mailto:fgurina@sunnyvale.ca.gov)  
**Subject:** Monday Morning Memo for November 12, 2018  
**Date:** Monday, November 12, 2018 5:02:39 AM

---

Having trouble viewing this email? [Click here](#)



## Courts/Rulings

### **Circuit Judge Bea distances himself from advice by majority to prison officials**

Ninth U.S. Circuit Court of Appeals Judge Carlos T. Bea, in a concurring



opinion, yesterday gently accused a colleague on the court and a visiting jurist of needlessly meddling in prison affairs by suggesting changes in procedures. Bea agreed with affirmance of the dismissal of a prisoner's civil rights action based on his failure to exhaust administrative remedies, but disassociated himself from comments, in two footnotes, by the majority - comprised of Circuit Judge Mary H. Murguia and District Court Judge Alan Soto of the District of Arizona, sitting by designation.

[Metropolitan News-Enterprise](#)

### **Gang expert's opinion, standing alone, insufficient for enhancement**

The Ninth U.S. Circuit Court of Appeals yesterday reversed a district judge's denial of a California inmate's petition for a writ of habeas corpus, holding that a gang expert's testimony on the possible benefit of a solo robbery to the convict's gang was not enough to support a 10-year gang enhancement.

[Metropolitan News-Enterprise](#)

### **Ex-LA County Sheriff's attorney argues Alzheimer's diagnosis was improperly excluded from trial**

A panel of justices on the 9th Circuit Court of Appeals heard arguments Tuesday from attorneys for former LA County Sheriff Lee Baca, who said his 2017 convictions on federal charges of obstruction of justice, conspiracy, and making false statements should be reversed because of legal errors.

[NBC4 Los Angeles](#)

### **Gov. Jerry Brown appoints Jason Chin as Alameda County Superior Court judge**

Gov. Jerry Brown announced his appointment of Jason Chin to a judgeship in the Alameda County Superior Court on Oct. 29. Chin, a longtime Alameda County resident, filled the seat that was vacant after the retirement of former judge Vernon Nakahara. Since 2004, Chin worked as the deputy district attorney at the Alameda County District Attorney's Office.

[The Daily Californian](#)

### **Ninth Circuit upholds illicit-sex convictions of man sentenced to 150 years in prison**

The Ninth U.S. Court of Appeals yesterday affirmed the conviction of a man sentenced to 150 years in prison, and supervised release for life after that, for illicit sex outside the United States. Defendant Yuzef Abramov was sentenced March 14, 2016 by District Court Judge Otis D. Wright II. He was ordered to serve 30 years in prison on each of five counts, with the terms to be concurrent.

[Metropolitan News-Enterprise](#)

### **Marin bank robber's conviction affirmed on appeal**



A state appeals court has affirmed the conviction of a Marin County bank robber who was sentenced to 105 years to life in prison. Roy Donovan Lacy, 37, was convicted by a jury in 2016 for robbing two Westamerica branches in San Rafael and another Westamerica in Novato. Judge Andrew Sweet ruled that the case qualified as a "third strike" toward a life sentence because of Lacy's extensive criminal history.

[Marin Independent Journal](#)

### **Innocence of felony requires reversal of gang activity charge - Court of Appeal**

The Fourth District Court of Appeal has reversed two men's convictions for active participation in a criminal street gang because there was no reason to believe that one of the men, a passenger in a stolen car, had aided and abetted his compatriot in driving it. The unpublished opinion by Justice David A. Thompson of Div. Three was filed Monday.

[Metropolitan News-Enterprise](#)

### **'No evidence to substantiate any of the claims': Takeaways from report on Kavanaugh allegations**

The Republican-controlled Senate Judiciary Committee concluded there "was no evidence to substantiate any of the claims" of sexual misconduct leveled against Supreme Court Justice Brett Kavanaugh in a report released over the weekend. Kavanaugh's initial Senate hearings were contentious, with Democrats working to expose what they felt were his more extreme views and accusing Republicans of withholding relevant documents.

[USA Today](#)

### **Opinion denying new judge is no bar to peremptory challenge on remand**

The Third District Court of Appeal has held that where an appellate court reverses a judgment and declines to order that the matter be shifted to a different judge on remand, there is no bar to a party filing a peremptory challenge against that judge. A writ of mandate was issued ordering the Plumas Superior Court to vacate an order striking a challenge, pursuant to Code of Civil Procedure §170.6, by the Department of Forestry and Fire Protection ("Cal Fire") to retired Santa Clara Superior Court Judge Leslie C. Nichols, who is sitting on assignment, and to enter a new order honoring the challenge.

[Metropolitan News-Enterprise](#)

### **Evidence derived from dog's sniffing during traffic stop properly admitted**

The Fourth District Court of Appeal has held that a narcotics-certified dog's discovery of more than four kilograms of methamphetamine during a traffic stop did not violate the Fourth Amendment because the dog's sniffing did not prolong the time needed to issue a citation. The opinion by newly installed Justice Michael J. Raphael of Div. Two, formerly a Los Angeles Superior Court judge, was filed Monday.

[Metropolitan News-Enterprise](#)

### **Supreme Court turns away challenge to California gun control**

The Supreme Court is refusing a new invitation to rule on gun rights, leaving in place California restrictions on carrying concealed handguns in public. The justices on Monday rejected an appeal from Sacramento residents who argued that they were unfairly denied permits to be armed in public. The complaint alleged that a prior Sacramento sheriff who was in charge of handgun permits arbitrarily rewarded friends.

[AP](#)

### **Pregnant victim's inability to travel didn't justify use of testimony via live video**

The Ninth U.S. Court of Appeals on Friday invalidated the conviction of a man on one count of sex trafficking of a minor or by force, fraud, or coercion and one count of transportation of a minor in interstate commerce to engage in prostitution based on a Confrontation Clause violation because the victim, who was in a late stage of pregnancy, could not travel from Minnesota and testified by two-way closed circuit television.

[Metropolitan News-Enterprise](#)

### **Pro tem justice bound by appellate, not trial court, ethics**

A superior court judge who is assigned to sit on an appellate court is bound by ethics rules applicable to appellate justices not trial court judges, a California Supreme Court committee has advised, telling an inquiring judge that recusal from a case based on campaign contributions from parties is not mandatory, but might be considered to avoid the appearance of impropriety.

[Metropolitan News-Enterprise](#)

### **Reporters Committee and media coalition ask California Supreme Court to reverse ruling that could "gut public access to government data"**

The Reporters Committee for Freedom of the Press and 13 media organizations are urging the Supreme Court of California to review and reverse a Court of Appeal decision that would make it harder for journalists and researchers to access large sets of data under the state's public records act. The case involves researchers' request for demographic information about California Bar Examination applicants from 1972 to 2008.

[Reporters Committee for Freedom of the Press](#)

### **Maquiz MacDonald v. Hedgpeth, No. 16-55240 (9th Cir. 2018)**

The Ninth Circuit reversed the district court's denial of habeas relief to petitioner, holding that the state trial court's admission of opinion testimony from a law enforcement expert on street gangs, who described for the jury the potential benefits that a street gang might receive when a member commits a robbery by himself, did not deny

petitioner a fundamentally fair trial and due process.

[Justia](#)

### **Supreme Court declines case challenging New Jersey's near elimination of cash bail**

The Supreme Court has declined to get involved in the debate over limiting the use of money bail to control who is freed from jail prior to trial. The court has turned away a lawsuit challenging New Jersey's nearly two-year-old bail system. New Jersey's system has all but eliminated the use of money bail.

[Reason](#)

### **Presiding justice seeking judges' support for retention of justices raises concerns**

There is no blanket prohibition on a Court of Appeal presiding justice soliciting support from the presiding judges of the superior courts within the appellate district for voter-retention of the justices, and asking that backing by the judges of their courts according to an ethics opinion released yesterday, but a concern is expressed that rules would be violated in the process.

[Metropolitan News-Enterprise](#)

### **Applying state preclusion rule to federal dismissal is error**

The First District Court of Appeal yesterday revived a case brought by a man who challenged his ineligibility to become a corrections officer based on his prior use of a false social security number, holding that the judge mistakenly applied state rather than federal claim preclusion rules. The opinion was written by Acting Presiding Justice Jon B. Streeter of Div. Four.

[Metropolitan News-Enterprise](#)

## **Prosecutors/Prosecutions**

### **Spitzer unseats Orange County D.A. Rackauckas**

Ending a bitter campaign that features accusations of ethical lapses from both sides, Orange County Supervisor Todd Spitzer appeared Wednesday to have unseated his former boss, District Attorney Tony Rackauckas. With all precincts reporting, Spitzer had nearly 53 percent of the vote from Tuesday's election, compared to 47 percent for the incumbent. The county has about 418,600 votes still to count, and Spitzer has a roughly 30,000-vote, likely insurmountable lead.

[My News LA](#)

### **Mental health hearing set for transient accused of choking jogger**

A mental health court update has been scheduled for a man accused of choking a jogger during an incident that happened a little more than a year ago. Colton Ford, 30, described by the deputies who arrested him as a transient living in the Santa Clara River wash, is charged with one count of attempted willful, deliberate and premeditated murder.

## [The Signal](#)

### **Suspected serial killer Danueal Drayton found competent to stand trial in Los Angeles**

Accused killer Danueal Drayton has been found mentally competent to stand trial in Los Angeles, a judge announced Friday. The Brooklyn man - who allegedly murdered Queens nurse Samantha Stewart inside her Springfield Gardens home last July then flew to California and allegedly raped and tried to kill another victim - appeared in a Los Angeles courtroom as the judge reinstated his criminal case.

[New York Daily News](#)

### **Father of boy who shot himself charged with child abuse**

Prosecutors in Northern California have charged the father of a 3-year-old boy who climbed a cabinet, grabbed his gun and shot himself in the groin with child abuse. The East Bay Times reports Friday the 3-year-old survived the gunshot, but remains in critical condition at an Oakland hospital. Court documents show the boy's father, 29-year-old Covonne Page, was charged Thursday with two counts of felony child abuse, being a felon in possession of a gun, and first-degree criminal firearm storage.

[AP](#)

### **Uber driver charged with kidnapping passengers in Santa Monica**

The Uber driver who was arrested for kidnapping four passengers in Santa Monica on Halloween night and leading police on a chase with victims in the car, has been charged by the Los Angeles County District Attorney's Office with four counts of kidnapping and one count of fleeing a pursuing peace officer's motor vehicle while driving recklessly. All these charges are felonies.

[Santa Monica Mirror](#)

### **Recent conviction of stoned driver shows potentially deadly consequences of driving after smoking marijuana**

While alcohol-related DUIs remain far more common, this past week a case involving a motorist prosecutors say was solely under the influence of marijuana provided a stark example of the danger of driving while stoned. Prosecutors say John Sebastian Hernandez, 23, smoked pot before getting behind the wheel in June of last year.

[Bakersfield.com](#)

### **New federal grants seek to boost prosecutions of gun ballistics cases**

For almost two decades, the Department of Justice has been urging police departments to use the National Integrated Ballistic Information Network, an innovative ballistics system, to solve gun crimes. Now the DOJ is looking beyond police chiefs and crime labs, who test the ballistics evidence, to prosecutors, who can find important links between cases and make charges stick in court.

## [The Trace](#)

### **Ex-Santa Monica Police Athletic League volunteer pleads not guilty to molestation charges**

A former Santa Monica Police Athletic League volunteer who's accused of molesting four boys beginning as far back as 1986 pleaded not guilty on Monday to a half-dozen felony charges. Eric Uller, 50, is facing three of lewd acts on a child, two counts of oral copulation of a person under 18 and one count of continuous sexual abuse, and more charges could be forthcoming.

[NBC4 Los Angeles](#)

### **Maywood mayor avoids time in jail in dog abuse case**

After being convicted, Maywood Mayor Ramon Medina filed the legal equivalent of a Hail Mary: a motion asking a judge to dismiss an animal abuse case by claiming, in part, that he did not own the dog in question. It did not work. On Wednesday, Los Angeles Superior Court Judge Michelle M. Ahnn denied the motion and ordered the mayor to complete five days of community service, attend animal care classes and not get into any more legal trouble for a year.

[Los Angeles Times](#)

### **Bakersfield City Council candidate Gilberto de la Torre charged with voter fraud**

On the afternoon of Election Day, the District Attorney's office announced three people have been charged with voter fraud. One of them is 29-year-old Gilberto de la Torre, who is running for Bakersfield City Council in Ward 1. Voter fraud is a misdemeanor for illegal voting in its various forms and fashions. According to Deputy District Attorney Chris Dominguez, de la Torre and John Byrne were charged with attempting to vote more than once.

[KGET](#)

## **AB 1810/ Prop 47/AB 109**

### **Man is arrested for allegedly attempting to meet an underage girl for sexual acts**

A 25-year-old man was arrested on a charge of attempting to meet an underage girl for sexual acts, according to the San Bernardino County Sheriff's Department. On Nov. 3, deputies were advised of an unknown man approaching underage girls in the Target parking lot in the 10500 block of Foothill Boulevard in Rancho Cucamonga, attempting to sell them marijuana and passing out business cards with his name and phone number.

[Fontana Herald News](#)

### **Concern over new state law and its impact on Steven Wooding case**

The man charged with stabbing a student at Cabrillo College was



arraigned in a Santa Cruz County Superior courtroom today. 49-year-old Steven Wooding was arraigned on multiple felony charges including attempted murder. He has a history of mental illness and there are concerns about how a new state law could impact his case and where he receives treatment.

[KSBW](#)

### **Ace Hardware in Cathedral City looking to prevent further shoplifting**

The ACE Hardware in Cathedral City has been the target of shoplifting since the store was first opened in April and the problems its experiencing are not unique to Coachella Valley or the state of California, according to local law enforcement." "We've had four attempts, three of them were successful," said store manager Jeremy Sieben.

[KESQ](#)

## **Law Enforcement**

### **LAPD officers among those in bar during Borderline mass shooting**

A Pepperdine University student was among those still missing today following an overnight shooting massacre at a Thousand Oaks nightclub crowded with patrons, including a group of students from the Malibu college and three off-duty Los Angeles Police Department officers. The three LAPD officers who were at the club were not injured.

[City News Service](#)

### **"We're making entry": Listen to police encounter Thousand Oaks nightclub shooter**

About five minutes after Ventura County sheriff deputies were dispatched to Borderline Bar & Grill for an active shooter, one officer alerted dispatch he was making entry with CHP assistance. "One subject advised she didn't see (the shooter) come out," the officer told dispatch, according to hours of Ventura County Sheriff's Office radio traffic reviewed by the Bay Area News Group.

[The Mercury News](#)

### **LAPD surveillance caught assistant chief in sex act with subordinate officer just before his sudden retirement, sources say**

Undercover officers tailing a high-ranking Los Angeles Police Department official witnessed him apparently engaging in sexual activity in a parking lot with a female subordinate, sources with knowledge of the investigation said. The official, Assistant Chief Jorge Villegas, retired suddenly after the surveillance operation caught him engaging in conduct that sources said may have violated the department's policy against sexual relationships with lower-ranking officers and also may

have ran afoul of a criminal statute prohibiting lewd conduct in public places.

[Los Angeles Times](#)

### **U.S. law enforcement failed to see the threat of white nationalism. Now they don't know how to stop it.**

The first indication to Lt. Dan Stout that law enforcement's handling of white supremacy was broken came in September 2017, as he was sitting in an emergency-operations center in Gainesville, Fla., preparing for the onslaught of Hurricane Irma and watching what felt like his thousandth YouTube video of the recent violence in Charlottesville, Va. Jesus Christ, he thought, studying the footage in which crowds of angry men, who had gathered to attend or protest the Unite the Right rally, set upon one another with sticks and flagpole spears and flame throwers and God knows what else.

[New York Times](#)

### **Prostitution in Los Angeles is so bad, the city had to ban right turns at night**

Prostitution is illegal in the state of California, but that doesn't mean it isn't a common practice across the state. This may be more evident in Los Angeles than anywhere else, where police enforced a ban on right turns during the night hours to try to stop the surge of human trafficking. Buying and selling sexual favors is a business as old as the world itself. That doesn't make it, however, an illegal affair.

[TopSpeed](#)

### **Local Jewish centers aim to balance security and community in the wake of recent anti-Semitic incidents**

A recent surge in anti-Semitic incidents, including the mass shooting at Tree of Life synagogue in Pittsburgh, PA last Saturday and anti-Semitic graffiti at an Irvine synagogue last Wednesday has caused local Jewish organizations to shine a spotlight on security. "There's a rising tide of anti-Semitism," said Neil Spears, executive director at Silverlake Independent Jewish Community Center (SIJCC). "The idea is to stop it before it happens."

[Los Feliz Ledger](#)

### **Think the DMV is all about long waits? Feds targeting workers issuing phony licenses**

California's Department of Motor Vehicles has become infamous in recent months for long lines, ancient computing technology and mismanagement of its Motor Voter registration program. But those are hardly the only challenges facing the DMV. The department also has become the epicenter of federal probes into DMV workers using computers to crack into citizen's confidential information to steal their identities, and clerks taking bribes to alter driver's license test results.

[Sacramento Bee](#)

## **FBI serves search warrant at LA City Councilman Jose Huizar's Boyle Heights home**

Federal agents served a search warrant at L.A. City Councilman Jose Huizar's house in Boyle Heights on Wednesday. Federal agents were seen outside Huizar's home around 6 a.m., but it was unclear what they were looking for. The warrant was under seal, authorities said. Agents were seen walking out of the home with bags of evidence, including a computer.

[ABC7](#)

## **Criminal Justice/Public Safety**

### **Former FBI paralegal sentenced to prison for embezzlement**

A paralegal specialist for the FBI in San Diego was sentenced Monday to two years in prison for embezzling nearly \$250,000 in government funds. Lynn M. Morris provided legal and administrative support to the FBI's asset forfeiture unit, which seizes money and property from suspected criminals during investigations.

[Los Angeles Times](#)

### **Murrieta ICE agent sentenced for helping felon enter U.S.**

A former immigration agent from Riverside County was sentenced Monday to a year and a day in federal prison for helping a Mexican national with multiple convictions re-enter the country illegally. Felix Cisneros Jr., 44, must also serve a year under supervised release following his prison term. He was ordered by U.S. District Judge Christina Snyder to surrender on Jan. 23 to begin his sentence.

[City News Service](#)

## **Los Angeles County**

### **Goldstein investigation: Hundreds of deceased voters still on LA County rolls**

While early voters have been stuffing the ballot boxes or dropping off their vote by mail choices for the midterm election, CBSLA's David Goldstein found hundreds of people who are eligible to vote but shouldn't be - because they're dead. One Los Angeles man who wished to remain anonymous said he was surprised to see an official mail-in voting pamphlet addressed to his mother.

[CBS LA](#)

### **City of Industry appoints new city manager eight months after shakeup**

Troy Helling was selected last week as the next city manager for City of Industry after serving in the role on a temporary basis for six months. The Industry City Council voted unanimously at its Oct. 25 meeting to remove the interim tag from Helling's title. "I am honored by the City Council's confidence and am focused on doing what is in the best interests for the City of Industry's residents and business community,"

Helling said in a statement.  
[San Gabriel Valley Tribune](#)

### **New document raises questions among Porter Ranch residents**

A new public document is raising questions about what came out of a broken well during a four-month-long Aliso Canyon gas leak that emitted methane into the air and covered Porter Ranch schools, homes and cars with an oily mist. The Porter Ranch Neighborhood Council expressed concerns in a letter filed with the California Public Utilities Commission Oct. 30, expressing residents' ire about the presence of crude oil at the nearby Aliso Canyon site, based on documents they examined that were submitted to air-quality officials by the Southern California Gas Co.

[Los Angeles Daily News](#)

### **Can cities ban e-scooters in the name of public safety? Bird says no way**

The transportation startup Bird has sued the city of Beverly Hills over its temporary, six-month e-scooter ban. The suit argues that state law, which explicitly allows for "motorized scooters," actually preempts any municipal prohibitions. The lawsuit, Bird Rides v. City of Beverly Hills, was filed Thursday in Los Angeles County Superior Court.

[Ars Technica](#)

### **L.A. County will pay \$3.9 million to settle jail sexual assault claims**

The Los Angeles County Board of Supervisors on Wednesday agreed to pay \$3.9 million to settle federal civil rights claims against the Sheriff's Department and a deputy accused in a sexual assault involving female jail inmates. The board's action ends one lawsuit, and another potential claim, brought by three women alleging sexual assault by Deputy Giancarlo Scotti last year at the Century Regional Detention Facility in Lynwood.

[Los Angeles Times](#)

### **Supes move to improve health care for jailed juveniles**

The Los Angeles County Board of Supervisors on Wednesday approved a motion by Supervisor Kathryn Barger, coauthored by Supervisor Solis, to incorporate a holistic approach to care for young people in county probation halls and camps. Barger's motion creates a new leadership position within the Department of Mental Health - the Director of Coordinated Care for Juvenile Health - who will work in collaboration with the Probation Department's Juvenile Services unit to facilitate a continuum of care equipped to address each individual's needs.

[SCV News](#)

## **Elections**

### **Why a retired lieutenant could upset LA's sheriff**

It's close. Very close. But with 100 percent of precincts reporting, Alex

Villanueva, a retired sheriff's lieutenant, has taken the lead over Los Angeles County Sheriff Jim McDonnell. Villanueva, 55, ran as a reformer, accusing McDonnell of failing to clean house in the wake of Lee Baca's tenure. By 5:45 Wednesday morning, he had a slight lead over McDonnell - about one-third of a percentage point.

[LAist](#)

### **Chad Bianco wins Riverside County Sheriff's race**

Lt. Chad Bianco is the next Sheriff for Riverside County. With all 1072 precincts reporting, the law enforcement veteran edged out incumbent Stan Sniff by just over 13 points. Bianco secured 56.52% of the vote (145,026), overcoming Sniff's share of 43.48% (111,558). According to Ray Smith, spokesman for Riverside County, by law Bianco would officially begin his tenure as Sheriff on January 7, 2019, at noon.

[KESQ](#)

### **How strong is the Trump effect in California?**

Was the 2016 presidential election a sign of things to come - presaging an ever-bluer California? Or was it a one-off result driven by the personalities of the candidates? These are important questions in California, which voted more Democratic for president in 2016 than it had in 2012, even as the rest of the country moved in the opposite direction. Even more important, parts of the state that had been reliably Republican - most notably Orange County - suddenly shifted Democratic.

[Public Policy Institute of California](#)

## **Corrections**

### **Two California death row inmates die less than 48 hours apart from apparent suicide**

Two death row inmates at a California prison were found dead from apparent suicide less than 48 hours apart, California Department of Corrections and Rehabilitation officials said. Andrew Urdiales, an ex-Marine convicted and sentenced to death for murdering five women in Southern California between 1986 and 1995, was found unresponsive in his cell around 11:15 p.m. PST (2:15 a.m. ET) Friday during a security check, officials said in a press release.

[NBC News](#)

## **California/National**

### **State-county conflict could flare up again soon**

When California became the 31st state in 1850, the Legislature quickly created 27 counties to provide basic local services, such as roads, sheriffs and courts, to a sparse, mostly rural population. Over the next 57 years, as California's population grew, the Legislature carved up the original 27, some of them quite immense, to form 31 more counties.

[CALmatters](#)



### **Qatar likely hacked American rabbi, others with ties to GOP donor Sheldon Adelson, report suggests**

The nation of Qatar likely targeted an American Rabbi in a hacking scheme because of his ties to Republican donor Sheldon Adelson, according to court documents that reportedly show communications between two Qatari agents.

[Daily Wire](#)

### **Anti-ICE activist facing deportation alleges political retaliation from U.S. government**

A Mexican national who has spent several years organizing Californians against federal immigration policy filed a lawsuit last week against the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), U.S. Border Patrol, and other federal agencies.

[Daily Wire](#)

## **Marijuana**

### **CBD-infused products are being sold everywhere in California - but are they legal?**

Greg and Gary Avetisyan make no secret of it: They proudly sell all manner of products infused with CBD, from essential oils to bath bombs to fruity tea-like beverages that promise calming relief in a frantic world. CBD, short for cannabidiol, is a molecule derived from cannabis. But unlike its chemical cousin THC, it won't get you high. What it might do, according to some research, is alleviate anxiety, seizures, chronic pain and dozens of other ailments.

[Los Angeles Times](#)

## **Pensions**

### **Public pensions attack workers, SF Prof Abdulhadi under attack & labor & rise of fascism**

KPFA's WorkWeek Radio looks at the use of pension funds controlled by hedge funds to fund anti-labor propositions. It also hears about the attack on SFSU professor Rabab Abdulhadi who runs the Arab and Muslim Ethnicities and Diasporas Studies. WorkWeek looks at labor's role in the defense of Professor Abdulhadi and her students by Zionists and a Nazi signed up for her classes.

[KPFA WorkWeek Radio](#)

### **Orange County senator predicts financial crisis in public schools**

California State Sen. John Moorlach may well be giving an encore performance of his role as the canary in the coal mine preceding Orange County's bankruptcy almost a quarter-century ago when he correctly predicted financial disaster while a candidate for county Treasurer-Tax Collector. This time Moorlach, a Certified Public Accountant who represents Orange County's 37th District and serves on the Senate

Budget & Fiscal Review Committee and its education subcommittee, isn't concerned about county government.

[Newport Beach Patch](#)

### **\$1 billion lawsuit over CalPERS insurance rates moves forward with trial date**

A class-action lawsuit that could cost CalPERS \$1 billion is headed to trial in June, and many of the 122,000 retirees who bought an insurance plan at the center of the case are receiving small checks from an agreement that settled a portion of the claims. A Los Angeles County Superior Court judge on Friday set a date for the main trial, known as Sanchez. vs. CalPERS. The three- to four-week trial is scheduled to begin on June 10.

[Sacramento Bee](#)

### **CalPERS can't find enough private equity commitments**

A consultant's review of the California Public Employees' Retirement System's \$27.6 billion private equity portfolio has found that the current investment pace is not likely to be sufficient to maintain the pension system's 8% target to the asset class. The \$361.1 billion CalPERS is below the 8% allocation right now; 7.7% of its portfolio is invested in private equity as of August 31. CalPERS is the largest private equity investor in the US.

[Chief Investment Officer](#)

---

**For more ADDA news and information, visit [www.laadda.com](http://www.laadda.com).**

---



Association of Deputy District Attorneys, 515 S. Flower St., 18th Floor, Los Angeles, CA 90071

[SafeUnsubscribe™ fgrgurina@sunnyvale.ca.gov](#)

[Forward this email](#) | [Update Profile](#) | [About our service provider](#)

Sent by [newswatch@laadda.com](mailto:newswatch@laadda.com)

**From:** [emr-isac](#)  
**To:** [vmata@sunnyvale.ca.gov](mailto:vmata@sunnyvale.ca.gov)  
**Subject:** HSIN Emergency Services Update October 16-31, 2018: IEDs sent to political figures; shooting in Pittsburgh  
**Date:** Wednesday, November 07, 2018 12:23:25 PM



**WARNING:** This document contains FOR OFFICIAL USE ONLY (FOUO) information. It is subject to release restrictions as detailed in the Homeland Security Act of 2002 (6 U.S.C. 482) and the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy for FOUO information and is not to be released to the public, media, or other personnel who do not have an authorized "need-to-know" without appropriate prior approval of an authorized DHS official.

Below is a list of some of the many information products posted to the Emergency Services community on the Homeland Security Information Network (HSIN) between October 16-31, 2018.

State and federal partners were busy this month, see below for the list of analyses of the mailed IEDs sent to political figures, the shooting in Pittsburgh, cyber attack bulletins, and more.

#### **HSIN Emergency Services Update October 16-31, 2018**

CBRNE (State & Local)	
<a href="#">Arrest Made in Connection to Package Bombs Sent to Prominent Political Figures</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of suspicious Devices Sent to Obama, Clinton, and Others (Update 4)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 5)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 6)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Explosive Devices Mailed to Public Figures in Multiple States</a>	Wisconsin Statewide Intelligence Center (WSIC)
<a href="#">Increasing Use of Aerial Improvised Incendiary Devices Overseas</a>	CA State Threat Assessment Center (STAC)
<a href="#">Multiple Explosive Devices Mailed to Public Figures</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Pipe Bombs - Very Common IEDs, Used by Various Actors</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Suspicious Packages Sent to Political Figures Nationwide - Including the NCR</a>	WRTAC/MCAC/NVRIC/VFC
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 1)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 2)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 3)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Heightened Awareness Urged for Security Personnel Regarding Suspicious Packages</a>	NYPD Shield
<a href="#">Pipe Bombs Mailed to Public Figures</a>	New Jersey Regional Operations Intelligence Center (ROIC)
<a href="#">Responding to Bomb Threat and Suspicious Package Incidents</a>	Washington State Fusion Center (WSFC)

<a href="#">Suspicious Devices Sent to Obama, Clinton, and Others</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Suspicious Packages Containing Explosive Devices</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Suspicious Packages Sent to Political Figures Nationwide Including National Capital Region</a>	Washington Regional Threat and Analysis Center (WRTAC)
<b>CONTROLLED DANGEROUS SUBSTANCES/DRUGS (State &amp; Local)</b>	
<a href="#">Naloxone Deployment Mapping Underscores San Diego County Opioid Trends in the Second Quarter of CY2018</a>	San Diego Law Enforcement Coordination Center (SD-LECC)
<a href="#">Narcotics Bulletin - October 22-28, 2018</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">Methamphetamine Trends in Oregon and Idaho - Deaths and Forensic Submissions</a>	Oregon-Idaho HIDTA
<a href="#">NH DMI Drug Environment Report - September 2018</a>	New Hampshire Information and Analysis Center (NHIAC)
<a href="#">New Pills Containing Fentanyl Seen in Orange County</a>	Orange County (CA) Intelligence Assessment Center (OCIAC)
<a href="#">Narcotics Bulletin - October 15-21, 2018</a>	Greater Cincinnati Fusion Center (GCFC)
<b>CYBER SECURITY (State &amp; Local)</b>	
<a href="#">Threat of Spear Phishing Attack Targeting Government Agencies in Maryland</a>	Maryland Coordination and Analysis Center (MCAC)
<a href="#">Cyber Actors Target U.S. Elections</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Cyber Threat Actors and Lone Offenders are the Primary Threat to 2018 Midterm Elections</a>	VFC / NVRIC
<a href="#">Bi-Weekly Cybersecurity Rollup - October 26, 2018</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<a href="#">Apple AirDrop Technology Threats</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">DDoS Attacks Remain a Significant Threat to Critical Infrastructure Organizations and Law Enforcement Agencies</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">Cutting Through the Cybersecurity Noise - October 19, 2018</a>	Phoenix UASI/Arizona Counter Terrorism Information Center (ACTIC)
<a href="#">Cyber Considerations for General Election</a>	Orange County (CA) Intelligence Assessment Center (OCIAC)
<a href="#">Threats to 2018 U.S. Elections and Wisconsin Election Security</a>	Wisconsin Statewide Intelligence Center (WSIC)
<a href="#">Security Snippets for Organizations - 2018 10</a>	Phoenix UASI/Arizona Counter Terrorism Information Center (ACTIC)
<b>BORDER SECURITY (State &amp; Local)</b>	
<a href="#">Border Security Alert - October 21-27, 2018</a>	Patrick Henry College Strategic Intelligence Program
<a href="#">Border Security Alert - October 14-21, 2018</a>	Patrick Henry College Strategic Intelligence Program
<b>OTHER (State &amp; Local)</b>	
<a href="#">Jewish Center Vandalized with Graffiti</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">Disease Outbreak and Investigation Report - October 30, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Lethal Shooting at Jewish Synagogue in Pittsburgh</a>	Wisconsin Statewide Intelligence Center (WSIC)
<a href="#">Weekly Major Recall Summary Report - October 20-26, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)

<a href="#">Summary of House of Worship Attacks in the United States and Canada 2015-2018</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Shooting Incident at Pittsburgh Synagogue</a>	NYPD Shield
<a href="#">Tree of Life Shooting</a>	Colorado Information Analysis Center (CIAC)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting UPDATE 1</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Initial Report on Synagogue Shooting in Pittsburgh, Pennsylvania</a>	Oregon Titan Fusion Center (TITAN)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting UPDATE 2</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting UPDATE 3</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Media Facilities- Increase in Suspicious Activity Reporting in the District of Columbia</a>	Washington Regional Threat and Analysis Center (WRTAC)
<a href="#">Disease Outbreak and Investigation Report - October 22, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Emerging Indicators of MS-13 Gang Membership</a>	New York State Intelligence Center (NYSIC)
<a href="#">Weekly Major Recall Summary Report - October 13-19, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Typhus Outbreak in Southern California</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Disease Outbreak and Investigation Report - October 16, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<b>SPECIAL EVENTS - LISTS AND THREAT ASSESSMENTS (State &amp; Local)</b>	
<a href="#">Muslim Association of Puget Sound Event</a>	Washington State Fusion Center (WSFC)
<a href="#">The 4th Annual Philadelphia Veterans Day Parade - 04 November 2018</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">VFC NVRIC Joint Special Event Assessment - Midterm Elections</a>	Virginia Fusion Center (VFC) Northern Virginia Regional Intelligence Center (NVRIC)
<a href="#">TSU Homecoming Parade</a>	Houston Regional Intelligence Service Center (HRISC)
<a href="#">Wenatchee Festival of Trees</a>	Washington State Fusion Center (WSFC)
<a href="#">2018 California Statewide General Election - Orange County</a>	Orange County (CA) Intelligence Assessment Center (OCIAAC)
<a href="#">Physical Security Considerations for General Election</a>	Orange County (CA) Intelligence Assessment Center (OCIAAC)
<a href="#">Rock 'n' Roll Marathon Weekend</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">2018 Pride Parade - Downtown Las Vegas</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">2018 Wings Over Houston Airshow</a>	Houston Regional Intelligence Service Center (HRISC)
<b>TERRORISM (State &amp; Local)</b>	
<a href="#">Inspiring Terror on the Railways</a>	Pennsylvania Criminal Intelligence Center (PaCIC)
<a href="#">ISIS Will Likely Continue to Promote Attacks Targeting Concert Venues</a>	Central Florida Intelligence Exchange (CFIX)
<a href="#">Increasing Use of Aerial Improvised Incendiary Devices Overseas</a>	STAC CalFire
<a href="#">Snapshot Graphic U.S Terrorism Cases</a>	CA State Threat Assessment Center (STAC)



<a href="#">Al-Qa'ida - Increase in Propaganda Targeting the US</a>	Washington Regional Threat and Analysis Center (WRTAC)
<a href="#">Pro-Islamic State Al-Adiyat Media Foundation Releases Tips for Lone Wolf Arson Attacks</a>	Minnesota Fusion Center
<b>STATE &amp; LOCAL FUSION CENTER PERIODICALS</b>	
<a href="#">ARIC Quarterly SAR Report</a>	Austin Regional Intelligence Center (ARIC)
<a href="#">Critical Infrastructure Monthly Open Source Review</a>	Massachusetts Commonwealth Fusion Center (CFC)
<a href="#">CIAC Weekly Summary</a>	Colorado Information Analysis Center (CIAC)
<a href="#">DVIC Biweekly Open Source Bulletin</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">The Watchline</a>	FDNY Center for Counter Terrorism & Domestic Preparedness (CTDP)
<a href="#">Fire, HazMat, and EMS Intelligence Bulletin</a>	Georgia Information Sharing and Analysis Center (GISAC)
<a href="#">Weekly Intelligence Bulletin</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">KCTEW Bulletin</a>	Kansas City (MO) Regional TEW (KCTEW)
<a href="#">KIFC Open Source Weekly</a>	Kentucky Intelligence Fusion Center (KIFC)
<a href="#">Monthly Threat Awareness Bulletin</a>	Indiana Intelligence Fusion Center (IIFC)
<a href="#">MCAC Critical Infrastructure Bi-Weekly Summary</a>	Maryland Coordination & Analysis Center (MCAC)
<a href="#">MN Fusion Center Weekly Partner Brief</a>	Minnesota Fusion Center
<a href="#">NCRIC Partner Update Brief</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">ND Anti-Terrorism Weekly Summary</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<a href="#">NHIAC All Hazards Digest</a>	New Hampshire Information & Analysis Center (NHIAC)
<a href="#">NIAC Weekly Infrastructure Awareness Brief</a>	Nebraska Information Analysis Center (NIAC)
<a href="#">NNRIC Bi-Weekly Briefing</a>	Northern Nevada Regional Intelligence Center (NNRIC)
<a href="#">Weekly Intelligence Feed</a>	Northern Virginia Regional Intelligence Center (NVRIC)
<a href="#">CBRN Weekly</a>	New York Police Department (NYPD)
<a href="#">OCIAC Partner Bi-Weekly Brief</a>	Orange County Intelligence Assessment Center (OCIAC)
<a href="#">OTFC Weekly Bulletin</a>	Oregon TITAN Fusion Center
<a href="#">CI - KR Monthly Report</a>	Pennsylvania Criminal Intelligence Center (PaCIC)
<a href="#">Pittsburgh Regional Intelligence Brief</a>	Region 13 Fusion Center (Pittsburgh, PA)
<a href="#">SD-LECC Extremism Open Source Bulletin</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">SC Fusion Center Information Bulletin</a>	South Carolina Fusion Center (SCFC)
<a href="#">Emergency Services Chronicle</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">STAC Bi-Weekly Review</a>	California State Threat Assessment Center (STAC)
<a href="#">WA State Fusion Center Insider</a>	Washington State Fusion Center (WSFC)

<a href="#">WSIC Weekly Bulletin</a>	Wisconsin Statewide Information Center (WSIC)
<a href="#">WRTAC DC FEMS Intelligence Size-Up</a>	Washington Regional Threat and Analysis Center (WRTAC)
<b>JCAT</b>	
<a href="#">Counterterrorism Weekly - 31 October 2018</a>	National Counterterrorism Center
<a href="#">Counterterrorism Weekly - 24 October 2018</a>	National Counterterrorism Center
<a href="#">Counterterrorism Weekly - 17 October 2018</a>	National Counterterrorism Center
<a href="#">JCAT Newsletter 3rd QTR 2018</a>	NCTC-FBI-DHS
<b>FEDERAL DOCUMENTS</b>	
<a href="#">Gaseous Buildup Reported Cause of Explosion Inside Shipping Container - Los Angeles Port Facility, San Pedro, CA</a>	Railway Alert Network (RAN)
<a href="#">Update 4 - Joint News Conference on Arrest of Suspect in Suspicious Packages Sent to Public Figures</a>	Railway Alert Network (RAN)
<a href="#">Update 3 - Arrest Confirmed in Investigation of Apparent Explosive Devices Addressed to Public Figures</a>	Railway Alert Network (RAN)
<a href="#">Terrorist Attacks Involving Package Bombs, 1970-2017</a>	START
<a href="#">Update 2 - Suspicious Packages and Explosive Devices Sent to Public Figures</a>	Railway Alert Network (RAN)
<a href="#">Update 1 - Explosive Devices in Packages Addressed to Public Figures in Multiple Locations</a>	Railway Alert Network (RAN)
<a href="#">Quick Look Report NY-DC-FL Suspicious Packages</a>	National Explosive Task Force
<a href="#">Multiple Destructive Devices Mailed to Individuals</a>	U.S. Secret Service
<a href="#">Explosives Devices in Packages Addressed to Public Figures in Multiple Locations</a>	Railway Alert Network (RAN)
<a href="#">Explosive Devices Mailed to Public Figures</a>	DHS/FBI
<a href="#">Additional Mailings of Ricin-Laced Letters to High Profile Officials Continue Following Arrest of Suspect</a>	FBI
<a href="#">Cyber Criminals Likely To Shift Toward Small-Scale, Targeted Campaigns and Cryptocurrency Mining</a>	FBI Cyber Division
<a href="#">This Week in Transportation Cyber Security - October 26, 2018</a>	Transportation Security Administration
<a href="#">Dark Web Contains Tools That Very Likely Would Enhance Malign Influence Operations Against 2018 US Midterm Elections</a>	DHS
<a href="#">Update to North Korean Cyber Threats to US Private Industry</a>	FBI Cyber Division
<a href="#">Trickbot Banking Trojan Targets US Institutions and Maximizes Profits through SMB Propagation or Ransomware</a>	FBI Cyber Division
<a href="#">Unidentified Cyber Actors Use Likely APT Infrastructure to Send Spear-Phishing Emails to State-Level Governments</a>	DHS
<a href="#">This Week in Transportation Cyber Security - October 19, 2018</a>	Transportation Security Administration
<a href="#">Changing Fentanyl Pill Production in Mexico Poses Increased Risk to Law Enforcement, Users</a>	DHS/EI Paso Intelligence Center (EPIC)
<a href="#">Emerging Threat Report 2018 - Quarter 3</a>	Drug Enforcement Administration
<a href="#">The Rise of Commercial Unmanned Aircraft Systems (UASs)</a>	DHS NRMCC
<a href="#">Pittsburgh Synagogue Shooting</a>	DHS/FBI
<a href="#">Understanding Elicitation Approaches</a>	U.S. Department of State Diplomatic Security
<a href="#">Telephony Denial of Service Disrupts Calls to MD Police Departments Non-Emergency Public Switched Telephone Networks</a>	FBI Baltimore Division
<a href="#">Threat Actors May Attempt to Suppress Voter Turnout Via</a>	

<a href="#">Social Media Platforms</a>	FBI Criminal Investigative Division
<a href="#">2018 Major League Baseball World Series</a>	FBI/JRIC/LAPD/LAFD/LAFD-JHAT/LACoDPH/LADOT
<a href="#">US Army CID 2018 Veteran's Day Threat Assessment</a>	US Army Criminal Investigation Command
<a href="#">German Authorities Investigating Failed Attempt to Derail High Speed Train as Possible Terrorist Attack</a>	Railway Alert Network (RAN)
<a href="#">Monthly Counterintelligence Bulletin - October 2018</a>	FBI
<a href="#">Criminal - Terrorism Intelligence Report - October 29, 2018</a>	Army Threat Integration Center (ARTIC)
<a href="#">Trend Analysis Terrorist Incidents in the West May 2017 - June 2018</a>	DHS
<a href="#">Lethal Shooting at Jewish Synagogue in Pittsburgh</a>	DHS/FBI
<a href="#">FBI Arrests Ohio-Based Individual for Attempting to Provide Material Support to ISIS</a>	DHS/FBI
<a href="#">FBI Arrests Ohio-based Individual for Attempting To Provide Material Support to al-Qaida</a>	DHS/FBI
<a href="#">Criminal - Terrorism Intelligence Report - October 22, 2018</a>	Army Threat Integration Center (ARTIC)
<a href="#">FBI Arrests Illinois-Based Naturalized US Citizen for Attempting To Provide to ISIS</a>	DHS/FBI
<a href="#">Timeline of Significant Threats to Aviation Worldwide</a>	TSA I&A
<a href="#">Timeline of Threats to US Surface Transportation</a>	TSA I&A
<b>OTHER DOCUMENTS</b>	
<a href="#">Current Situation Reports</a>	<a href="#">Daily Reports</a>
<a href="#">BATS</a>	<a href="#">PT/ST-ISAC Cyber Report</a>
<a href="#">Counterterrorism Daily - NCTC</a>	<a href="#">Joint Counterterrorism Assessment Team (JCAT)</a>
<a href="#">IT-ISAC Open Source News</a>	<a href="#">IED News</a>
<a href="#">Emerging Diseases</a>	<a href="#">FEMA Disaster Emergency Communications Division Newsletter</a>
<a href="#">NH-ISAC Daily Security Intelligence Report</a>	<a href="#">Training &amp; Conference Calendar</a>

For HSIN password resets, [click here](#). For further assistance with your HSIN account, contact the HSIN 24/7 Help Desk at 866-430-0162. For other difficulties opening FOUO documents (e.g., not nominated and validated), contact the EMR-ISAC at [emr-isac@fema.dhs.gov](mailto:emr-isac@fema.dhs.gov) or at 301-447-1325.

You are subscribed to Bulletin - FOUO Template for EMR-ISAC. This information has recently been updated, and is now available.

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your [Subscriber Preferences Page](#). You will need to use your email address to log in. If you have questions or problems with the subscription service, please visit [subscriberhelp.govdelivery.com](http://subscriberhelp.govdelivery.com).

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.



**From:** [emr-isac](#)  
**To:** [Jeffrey Hunter](#)  
**Subject:** HSIN Emergency Services Update October 16-31, 2018: IEDs sent to political figures; shooting in Pittsburgh  
**Date:** Wednesday, November 07, 2018 12:22:07 PM

---



**WARNING:** This document contains FOR OFFICIAL USE ONLY (FOUO) information. It is subject to release restrictions as detailed in the Homeland Security Act of 2002 (6 U.S.C. 482) and the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy for FOUO information and is not to be released to the public, media, or other personnel who do not have an authorized "need-to-know" without appropriate prior approval of an authorized DHS official.

---

Below is a list of some of the many information products posted to the Emergency Services community on the Homeland Security Information Network (HSIN) between October 16-31, 2018.

State and federal partners were busy this month, see below for the list of analyses of the mailed IEDs sent to political figures, the shooting in Pittsburgh, cyber attack bulletins, and more.

---

#### **HSIN Emergency Services Update October 16-31, 2018**

<b>CBRNE (State &amp; Local)</b>	
<a href="#">Arrest Made in Connection to Package Bombs Sent to Prominent Political Figures</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of suspicious Devices Sent to Obama, Clinton, and Others (Update 4)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 5)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 6)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Explosive Devices Mailed to Public Figures in Multiple States</a>	Wisconsin Statewide Intelligence Center (WSIC)
<a href="#">Increasing Use of Aerial Improvised Incendiary Devices Overseas</a>	CA State Threat Assessment Center (STAC)
<a href="#">Multiple Explosive Devices Mailed to Public Figures</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Pipe Bombs - Very Common IEDs, Used by Various Actors</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Suspicious Packages Sent to Political Figures Nationwide - Including the NCR</a>	WRTAC/MCAC/NVRIC/VFC
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 1)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 2)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others (Update 3)</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Timeline of Suspicious Devices Sent to Obama, Clinton, and Others</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Heightened Awareness Urged for Security Personnel Regarding Suspicious Packages</a>	NYPD Shield
<a href="#">Pipe Bombs Mailed to Public Figures</a>	New Jersey Regional Operations Intelligence Center (ROIC)
<a href="#">Responding to Bomb Threat and Suspicious Package Incidents</a>	Washington State Fusion Center (WSFC)

<a href="#">Suspicious Devices Sent to Obama, Clinton, and Others</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Suspicious Packages Containing Explosive Devices</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Suspicious Packages Sent to Political Figures Nationwide Including National Capital Region</a>	Washington Regional Threat and Analysis Center (WRTAC)
<b>CONTROLLED DANGEROUS SUBSTANCES/DRUGS (State &amp; Local)</b>	
<a href="#">Naloxone Deployment Mapping Underscores San Diego County Opioid Trends in the Second Quarter of CY2018</a>	San Diego Law Enforcement Coordination Center (SD-LECC)
<a href="#">Narcotics Bulletin - October 22-28, 2018</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">Methamphetamine Trends in Oregon and Idaho - Deaths and Forensic Submissions</a>	Oregon-Idaho HIDTA
<a href="#">NH DMI Drug Environment Report - September 2018</a>	New Hampshire Information and Analysis Center (NHIAC)
<a href="#">New Pills Containing Fentanyl Seen in Orange County</a>	Orange County (CA) Intelligence Assessment Center (OCIAC)
<a href="#">Narcotics Bulletin - October 15-21, 2018</a>	Greater Cincinnati Fusion Center (GCFC)
<b>CYBER SECURITY (State &amp; Local)</b>	
<a href="#">Threat of Spear Phishing Attack Targeting Government Agencies in Maryland</a>	Maryland Coordination and Analysis Center (MCAC)
<a href="#">Cyber Actors Target U.S. Elections</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">Cyber Threat Actors and Lone Offenders are the Primary Threat to 2018 Midterm Elections</a>	VFC / NVRIC
<a href="#">Bi-Weekly Cybersecurity Rollup - October 26, 2018</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<a href="#">Apple AirDrop Technology Threats</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">DDoS Attacks Remain a Significant Threat to Critical Infrastructure Organizations and Law Enforcement Agencies</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">Cutting Through the Cybersecurity Noise - October 19, 2018</a>	Phoenix UASI/Arizona Counter Terrorism Information Center (ACTIC)
<a href="#">Cyber Considerations for General Election</a>	Orange County (CA) Intelligence Assessment Center (OCIAC)
<a href="#">Threats to 2018 U.S. Elections and Wisconsin Election Security</a>	Wisconsin Statewide Intelligence Center (WSIC)
<a href="#">Security Snippets for Organizations - 2018 10</a>	Phoenix UASI/Arizona Counter Terrorism Information Center (ACTIC)
<b>BORDER SECURITY (State &amp; Local)</b>	
<a href="#">Border Security Alert - October 21-27, 2018</a>	Patrick Henry College Strategic Intelligence Program
<a href="#">Border Security Alert - October 14-21, 2018</a>	Patrick Henry College Strategic Intelligence Program
<b>OTHER (State &amp; Local)</b>	
<a href="#">Jewish Center Vandalized with Graffiti</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">Disease Outbreak and Investigation Report - October 30, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Lethal Shooting at Jewish Synagogue in Pittsburgh</a>	Wisconsin Statewide Intelligence Center (WSIC)
<a href="#">Weekly Major Recall Summary Report - October 20-26, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)



<a href="#">Summary of House of Worship Attacks in the United States and Canada 2015-2018</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Shooting Incident at Pittsburgh Synagogue</a>	NYPD Shield
<a href="#">Tree of Life Shooting</a>	Colorado Information Analysis Center (CIAC)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting UPDATE 1</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Initial Report on Synagogue Shooting in Pittsburgh, Pennsylvania</a>	Oregon Titan Fusion Center (TITAN)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting UPDATE 2</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Multiple Fatalities in Pittsburgh Synagogue Shooting UPDATE 3</a>	CA Joint Regional Intelligence Center (JRIC)
<a href="#">Media Facilities- Increase in Suspicious Activity Reporting in the District of Columbia</a>	Washington Regional Threat and Analysis Center (WRTAC)
<a href="#">Disease Outbreak and Investigation Report - October 22, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Emerging Indicators of MS-13 Gang Membership</a>	New York State Intelligence Center (NYSIC)
<a href="#">Weekly Major Recall Summary Report - October 13-19, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Typhus Outbreak in Southern California</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">Disease Outbreak and Investigation Report - October 16, 2018</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<b>SPECIAL EVENTS - LISTS AND THREAT ASSESSMENTS (State &amp; Local)</b>	
<a href="#">Muslim Association of Puget Sound Event</a>	Washington State Fusion Center (WSFC)
<a href="#">The 4th Annual Philadelphia Veterans Day Parade - 04 November 2018</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">VFC NVRIC Joint Special Event Assessment - Midterm Elections</a>	Virginia Fusion Center (VFC) Northern Virginia Regional Intelligence Center (NVRIC)
<a href="#">TSU Homecoming Parade</a>	Houston Regional Intelligence Service Center (HRISC)
<a href="#">Wenatchee Festival of Trees</a>	Washington State Fusion Center (WSFC)
<a href="#">2018 California Statewide General Election - Orange County</a>	Orange County (CA) Intelligence Assessment Center (OCIAAC)
<a href="#">Physical Security Considerations for General Election</a>	Orange County (CA) Intelligence Assessment Center (OCIAAC)
<a href="#">Rock 'n' Roll Marathon Weekend</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">2018 Pride Parade - Downtown Las Vegas</a>	Southern Nevada Counter Terrorism Center (SNCTC)
<a href="#">2018 Wings Over Houston Airshow</a>	Houston Regional Intelligence Service Center (HRISC)
<b>TERRORISM (State &amp; Local)</b>	
<a href="#">Inspiring Terror on the Railways</a>	Pennsylvania Criminal Intelligence Center (PaCIC)
<a href="#">ISIS Will Likely Continue to Promote Attacks Targeting Concert Venues</a>	Central Florida Intelligence Exchange (CFIX)
<a href="#">Increasing Use of Aerial Improvised Incendiary Devices Overseas</a>	STAC CalFire
<a href="#">Snapshot Graphic U.S Terrorism Cases</a>	CA State Threat Assessment Center (STAC)

<a href="#">Al-Qa'ida - Increase in Propaganda Targeting the US</a>	Washington Regional Threat and Analysis Center (WRTAC)
<a href="#">Pro-Islamic State Al-Adiyat Media Foundation Releases Tips for Lone Wolf Arson Attacks</a>	Minnesota Fusion Center
<b>STATE &amp; LOCAL FUSION CENTER PERIODICALS</b>	
<a href="#">ARIC Quarterly SAR Report</a>	Austin Regional Intelligence Center (ARIC)
<a href="#">Critical Infrastructure Monthly Open Source Review</a>	Massachusetts Commonwealth Fusion Center (CFC)
<a href="#">CIAC Weekly Summary</a>	Colorado Information Analysis Center (CIAC)
<a href="#">DVIC Biweekly Open Source Bulletin</a>	Delaware Valley Intelligence Center (DVIC)
<a href="#">The Watchline</a>	FDNY Center for Counter Terrorism & Domestic Preparedness (CTDP)
<a href="#">Fire, HazMat, and EMS Intelligence Bulletin</a>	Georgia Information Sharing and Analysis Center (GISAC)
<a href="#">Weekly Intelligence Bulletin</a>	Greater Cincinnati Fusion Center (GCFC)
<a href="#">KCTEW Bulletin</a>	Kansas City (MO) Regional TEW (KCTEW)
<a href="#">KIFC Open Source Weekly</a>	Kentucky Intelligence Fusion Center (KIFC)
<a href="#">Monthly Threat Awareness Bulletin</a>	Indiana Intelligence Fusion Center (IIFC)
<a href="#">MCAC Critical Infrastructure Bi-Weekly Summary</a>	Maryland Coordination & Analysis Center (MCAC)
<a href="#">MN Fusion Center Weekly Partner Brief</a>	Minnesota Fusion Center
<a href="#">NCRIC Partner Update Brief</a>	Northern California Regional Intelligence Center (NCRIC)
<a href="#">ND Anti-Terrorism Weekly Summary</a>	North Dakota State & Local Intelligence Center (NDSLIC)
<a href="#">NHIAC All Hazards Digest</a>	New Hampshire Information & Analysis Center (NHIAC)
<a href="#">NIAC Weekly Infrastructure Awareness Brief</a>	Nebraska Information Analysis Center (NIAC)
<a href="#">NNRIC Bi-Weekly Briefing</a>	Northern Nevada Regional Intelligence Center (NNRIC)
<a href="#">Weekly Intelligence Feed</a>	Northern Virginia Regional Intelligence Center (NVRIC)
<a href="#">CBRN Weekly</a>	New York Police Department (NYPD)
<a href="#">OCIAC Partner Bi-Weekly Brief</a>	Orange County Intelligence Assessment Center (OCIAC)
<a href="#">OTFC Weekly Bulletin</a>	Oregon TITAN Fusion Center
<a href="#">CI - KR Monthly Report</a>	Pennsylvania Criminal Intelligence Center (PaCIC)
<a href="#">Pittsburgh Regional Intelligence Brief</a>	Region 13 Fusion Center (Pittsburgh, PA)
<a href="#">SD-LECC Extremism Open Source Bulletin</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">SC Fusion Center Information Bulletin</a>	South Carolina Fusion Center (SCFC)
<a href="#">Emergency Services Chronicle</a>	San Diego – Law Enforcement Coordination Center (SD-LECC)
<a href="#">STAC Bi-Weekly Review</a>	California State Threat Assessment Center (STAC)
<a href="#">WA State Fusion Center Insider</a>	Washington State Fusion Center (WSFC)

<a href="#">WSIC Weekly Bulletin</a>	Wisconsin Statewide Information Center (WSIC)
<a href="#">WRTAC DC FEMS Intelligence Size-Up</a>	Washington Regional Threat and Analysis Center (WRTAC)
<b>JCAT</b>	
<a href="#">Counterterrorism Weekly - 31 October 2018</a>	National Counterterrorism Center
<a href="#">Counterterrorism Weekly - 24 October 2018</a>	National Counterterrorism Center
<a href="#">Counterterrorism Weekly - 17 October 2018</a>	National Counterterrorism Center
<a href="#">JCAT Newsletter 3rd QTR 2018</a>	NCTC-FBI-DHS
<b>FEDERAL DOCUMENTS</b>	
<a href="#">Gaseous Buildup Reported Cause of Explosion Inside Shipping Container - Los Angeles Port Facility, San Pedro, CA</a>	Railway Alert Network (RAN)
<a href="#">Update 4 - Joint News Conference on Arrest of Suspect in Suspicious Packages Sent to Public Figures</a>	Railway Alert Network (RAN)
<a href="#">Update 3 - Arrest Confirmed in Investigation of Apparent Explosive Devices Addressed to Public Figures</a>	Railway Alert Network (RAN)
<a href="#">Terrorist Attacks Involving Package Bombs, 1970-2017</a>	START
<a href="#">Update 2 - Suspicious Packages and Explosive Devices Sent to Public Figures</a>	Railway Alert Network (RAN)
<a href="#">Update 1 - Explosive Devices in Packages Addressed to Public Figures in Multiple Locations</a>	Railway Alert Network (RAN)
<a href="#">Quick Look Report NY-DC-FL Suspicious Packages</a>	National Explosive Task Force
<a href="#">Multiple Destructive Devices Mailed to Individuals</a>	U.S. Secret Service
<a href="#">Explosives Devices in Packages Addressed to Public Figures in Multiple Locations</a>	Railway Alert Network (RAN)
<a href="#">Explosive Devices Mailed to Public Figures</a>	DHS/FBI
<a href="#">Additional Mailings of Ricin-Laced Letters to High Profile Officials Continue Following Arrest of Suspect</a>	FBI
<a href="#">Cyber Criminals Likely To Shift Toward Small-Scale, Targeted Campaigns and Cryptocurrency Mining</a>	FBI Cyber Division
<a href="#">This Week in Transportation Cyber Security - October 26, 2018</a>	Transportation Security Administration
<a href="#">Dark Web Contains Tools That Very Likely Would Enhance Malign Influence Operations Against 2018 US Midterm Elections</a>	DHS
<a href="#">Update to North Korean Cyber Threats to US Private Industry</a>	FBI Cyber Division
<a href="#">Trickbot Banking Trojan Targets US Institutions and Maximizes Profits through SMB Propagation or Ransomware</a>	FBI Cyber Division
<a href="#">Unidentified Cyber Actors Use Likely APT Infrastructure to Send Spear-Phishing Emails to State-Level Governments</a>	DHS
<a href="#">This Week in Transportation Cyber Security - October 19, 2018</a>	Transportation Security Administration
<a href="#">Changing Fentanyl Pill Production in Mexico Poses Increased Risk to Law Enforcement, Users</a>	DHS/EI Paso Intelligence Center (EPIC)
<a href="#">Emerging Threat Report 2018 - Quarter 3</a>	Drug Enforcement Administration
<a href="#">The Rise of Commercial Unmanned Aircraft Systems (UASs)</a>	DHS NRMCC
<a href="#">Pittsburgh Synagogue Shooting</a>	DHS/FBI
<a href="#">Understanding Elicitation Approaches</a>	U.S. Department of State Diplomatic Security
<a href="#">Telephony Denial of Service Disrupts Calls to MD Police Departments Non-Emergency Public Switched Telephone Networks</a>	FBI Baltimore Division
<a href="#">Threat Actors May Attempt to Suppress Voter Turnout Via</a>	

<a href="#">Social Media Platforms</a>	FBI Criminal Investigative Division
<a href="#">2018 Major League Baseball World Series</a>	FBI/JRIC/LAPD/LAFD/LAFD-JHAT/LACoDPH/LADOT
<a href="#">US Army CID 2018 Veteran's Day Threat Assessment</a>	US Army Criminal Investigation Command
<a href="#">German Authorities Investigating Failed Attempt to Derail High Speed Train as Possible Terrorist Attack</a>	Railway Alert Network (RAN)
<a href="#">Monthly Counterintelligence Bulletin - October 2018</a>	FBI
<a href="#">Criminal - Terrorism Intelligence Report - October 29, 2018</a>	Army Threat Integration Center (ARTIC)
<a href="#">Trend Analysis Terrorist Incidents in the West May 2017 - June 2018</a>	DHS
<a href="#">Lethal Shooting at Jewish Synagogue in Pittsburgh</a>	DHS/FBI
<a href="#">FBI Arrests Ohio-Based Individual for Attempting to Provide Material Support to ISIS</a>	DHS/FBI
<a href="#">FBI Arrests Ohio-based Individual for Attempting To Provide Material Support to al-Qaida</a>	DHS/FBI
<a href="#">Criminal - Terrorism Intelligence Report - October 22, 2018</a>	Army Threat Integration Center (ARTIC)
<a href="#">FBI Arrests Illinois-Based Naturalized US Citizen for Attempting To Provide to ISIS</a>	DHS/FBI
<a href="#">Timeline of Significant Threats to Aviation Worldwide</a>	TSA I&A
<a href="#">Timeline of Threats to US Surface Transportation</a>	TSA I&A
<b>OTHER DOCUMENTS</b>	
<a href="#">Current Situation Reports</a>	<a href="#">Daily Reports</a>
<a href="#">BATS</a>	<a href="#">PT/ST-ISAC Cyber Report</a>
<a href="#">Counterterrorism Daily - NCTC</a>	<a href="#">Joint Counterterrorism Assessment Team (JCAT)</a>
<a href="#">IT-ISAC Open Source News</a>	<a href="#">IED News</a>
<a href="#">Emerging Diseases</a>	<a href="#">FEMA Disaster Emergency Communications Division Newsletter</a>
<a href="#">NH-ISAC Daily Security Intelligence Report</a>	<a href="#">Training &amp; Conference Calendar</a>

For HSIN password resets, [click here](#). For further assistance with your HSIN account, contact the HSIN 24/7 Help Desk at 866-430-0162. For other difficulties opening FOUO documents (e.g., not nominated and validated), contact the EMR-ISAC at [emr-isac@fema.dhs.gov](mailto:emr-isac@fema.dhs.gov) or at 301-447-1325.

You are subscribed to Bulletin - FOUO Template for EMR-ISAC. This information has recently been updated, and is now available.

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time on your [Subscriber Preferences Page](#). You will need to use your email address to log in. If you have questions or problems with the subscription service, please visit [subscriberhelp.govdelivery.com](http://subscriberhelp.govdelivery.com).

[Privacy Policy](#) | GovDelivery is providing this information on behalf of U.S. Department of Homeland Security, and may not use the information for any other purposes.



**From:** [Government Technology Bulletin](#)  
**To:** [Carmen Talavera](#)  
**Subject:** Includes: Protecting User Privacy vs. Helping with a Hoax  
**Date:** Wednesday, November 07, 2018 9:19:52 AM

[View Online](#) | [Unsubscribe](#)



## Government Technology Bulletin



### IN THIS ISSUE

[Secret iOS 12 Tricks You Need to Know](#)

[How to Find Hidden Programs Running in the Background](#)

[Protecting User Privacy vs. Helping with a Hoax](#)

[AI Features in Gmail and Hangouts](#)

[5 Dangerous Types of DDoS Attacks](#)

### Secret iOS 12 Tricks You Need to Know

You downloaded iOS 12 and your iPhone is working faster than ever. Now you just need to know how to use it. This interactive infographic walks you through cool features hidden in Apple's new mobile operating system.

[Watch now](#)

### How to Find Hidden Programs Running in the Background

Not all programs are visibly displayed on your computer's taskbar. Other programs are intentionally hidden from being viewed because they act as valid background services or processes that do not need constant access via the taskbar. Some programs remain open even



after closing them. Discover how to locate (and exit) these hidden programs.

[Read more](#)

## Protecting User Privacy vs. Helping with a Hoax

People are no longer content to give away their information without understanding how businesses intend to use and protect it. Businesses need to prepare for the changing expectations of data privacy — not just by securing their information, but also by verifying those making requests for access to or deletion of data are who they say they are.

[Download now](#)

## AI Features in Gmail and Hangouts

At the recent Google Cloud Next, experts spoke on artificial intelligence-powered upgrades the company has added to its G Suite, which is made up of Gmail, Docs, Sheets, Slides, Hangouts Meet, Hangouts Chat and more. If you use these products — and let's face it, if you work in an office, you do — here are several newer features you should explore.

[Read more](#)

### FEATURED DOWNLOAD

## 5 Dangerous Types of DDoS Attacks

Rate-based technologies, once considered adequate to handle the

most advanced distributed denial-of-service (DDoS) threats are nearly obsolete as adversaries become more tech-savvy. These ultra-adaptive hackers have given rise to five nasty attack techniques. Learn what they are and how you can mitigate risk.

[Download now](#)

To unsubscribe from this title, or manage your bulletin preferences [click here](#). Please see our [Terms & Conditions](#) and [Privacy Policy](#). To ensure you get our next send, please add us to your address book. You are currently subscribed to Government Technology Bulletin with the email address: [ctalavera@sunnyvale.ca.gov](mailto:ctalavera@sunnyvale.ca.gov).



emedia Communications LLC  
200 N LaSalle St., Suite 2450  
Chicago, IL 60601. USA  
866-879-5757  
e-mail: [inquiries@emedia.com](mailto:inquiries@emedia.com)



**From:** [Government Technology Bulletin](#)  
**To:** [blu@ci.sunnyvale.ca.us](mailto:blu@ci.sunnyvale.ca.us)  
**Subject:** Includes: Protecting User Privacy vs. Helping with a Hoax  
**Date:** Wednesday, November 07, 2018 9:19:49 AM

[View Online](#) | [Unsubscribe](#)



## Government Technology Bulletin



### IN THIS ISSUE

[Secret iOS 12 Tricks You Need to Know](#)

[How to Find Hidden Programs Running in the Background](#)

[Protecting User Privacy vs. Helping with a Hoax](#)

[AI Features in Gmail and Hangouts](#)

[5 Dangerous Types of DDoS Attacks](#)

### Secret iOS 12 Tricks You Need to Know

You downloaded iOS 12 and your iPhone is working faster than ever. Now you just need to know how to use it. This interactive infographic walks you through cool features hidden in Apple's new mobile operating system.

[Watch now](#)

### How to Find Hidden Programs Running in the Background

Not all programs are visibly displayed on your computer's taskbar. Other programs are intentionally hidden from being viewed because they act as valid background services or processes that do not need constant access via the taskbar. Some programs remain open even

after closing them. Discover how to locate (and exit) these hidden programs.

[Read more](#)

## Protecting User Privacy vs. Helping with a Hoax

People are no longer content to give away their information without understanding how businesses intend to use and protect it. Businesses need to prepare for the changing expectations of data privacy — not just by securing their information, but also by verifying those making requests for access to or deletion of data are who they say they are.

[Download now](#)

## AI Features in Gmail and Hangouts

At the recent Google Cloud Next, experts spoke on artificial intelligence-powered upgrades the company has added to its G Suite, which is made up of Gmail, Docs, Sheets, Slides, Hangouts Meet, Hangouts Chat and more. If you use these products — and let's face it, if you work in an office, you do — here are several newer features you should explore.

[Read more](#)

## FEATURED DOWNLOAD

### 5 Dangerous Types of DDoS Attacks

Rate-based technologies, once considered adequate to handle the

most advanced distributed denial-of-service (DDoS) threats are nearly obsolete as adversaries become more tech-savvy. These ultra-adaptive hackers have given rise to five nasty attack techniques. Learn what they are and how you can mitigate risk.

[Download now](#)

To unsubscribe from this title, or manage your bulletin preferences [click here](#). Please see our [Terms & Conditions](#) and [Privacy Policy](#). To ensure you get our next send, please add us to your address book. You are currently subscribed to Government Technology Bulletin with the email address: blu@ci.sunnyvale.ca.us.



emedia Communications LLC  
200 N LaSalle St., Suite 2450  
Chicago, IL 60601. USA  
866-879-5757  
e-mail: [inquiries@emedia.com](mailto:inquiries@emedia.com)





**From:** [SFO-ECTF](#)  
**To:** [Undisclosed recipients:](#)  
**Subject:** INFO Website Security  
**Date:** Thursday, November 01, 2018 2:56:36 PM  
**Attachments:** [image001.png](#)  
[image002.png](#)

---

Dear ECTF Partners;

Listed below is a document pertaining to Website Security.

As a reminder, this product is TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Respectfully,

SFO-ECTF



Official website of the Department of Homeland Security

[Top of Form](#)

[Search query](#)

[Bottom of Form](#)



# US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Main menu

[Home](#)

[About Us](#)

[Careers](#)

[Publications](#)

[Alerts and Tips](#)

[Related Resources](#)

[C<sup>3</sup> VP](#)



# NCCIC

TLP:WHITE

TLP:WHITE

[View Previous Tips](#)

## **Security Tip (ST18-006)**

### **Website Security**

Original release date: November 01, 2018

[Print Document](#)

[Tweet](#)

[Like Me](#)

[Share](#)

#### **What is website security?**

Website security refers to the protection of personal and organizational public-facing websites from cyberattacks.

#### **Why should I care about website security?**

Cyberattacks against public-facing websites—regardless of size—are common. An attack to your website could

- Cause defacement,
- Cause a denial-of-service (DoS) condition,
- Enable the attacker to obtain sensitive information, or
- Enable the attacker to take control of the affected website.

Organization and personal websites that fall victim to defacement or DoS may experience financial loss due to eroded user trust or a decrease in website visitors.

A cyberattack that causes a data breach places your company's intellectual property and your users' personally identifiable information (PII) at risk of theft.

Cyber criminals may attack websites because of financial incentives such as the theft and sale of intellectual property and PII, ransomware payouts, and cryptocurrency mining (see [Defending Against Illicit Cryptocurrency Mining Activity](#)). Cyber criminals may also be motivated to attack websites for ideological reasons, e.g., to gain publicity and notoriety for a terrorist organization through defacing a government website.

#### **What security threats are associated with websites?**

Possible cyberattacks against your website include those commonly reported in the media, such as website defacement and DoS—which make the information services provided by the website unavailable for users (see [Understanding Denial-of-Service Attacks](#)). An even more severe website attack scenario may result in the compromise of customer data (e.g., PII). These threats affect all aspects of security—confidentiality, integrity, and availability—and can gravely damage the reputation of the website and its owner.

A more subtle attack—one that may not be immediately evident to the website's owner or user—occurs when an attacker pivots from a compromised web server to the website owner's corporate network, which contains an abundance of sensitive information that may be at risk of exposure, modification, or destruction. Once an attacker uses a compromised website to enter a corporate network, other assets may be available to the attacker, including user credentials, PII, administrative information, and technical vulnerabilities. Additionally, by compromising the website platform, an attacker may be able to repurpose the website infrastructure as a platform from which they can launch attacks against other systems.

#### **How can I improve my cybersecurity protection against website attacks?**

Organizations and individuals can protect their websites by applying the following the best practices to

their web servers:

- **Implement the principle of least privilege.** Ensure that all users have the least amount of privilege necessary on the web server (including interactive end users and service accounts).
- **Use multifactor authentication.** Implement multifactor authentication for user logins to web applications and the underlying website infrastructure.
- **Change default vendor usernames and passwords.** Default vendor credentials are not secure—they are usually readily available on the internet. Changing default usernames and passwords will prevent an attack that leverages default credentials.
- **Disable unnecessary accounts.** Disable accounts that are no longer necessary, such as guest accounts or individual user accounts that are no longer in use.
- **Use security checklists.** Audit and harden configurations based on security checklists specific to each application (e.g., Apache, MySQL) on the system.
- **Use application whitelisting.** Use application whitelisting and disable modules or features that provide capabilities that are not necessary for business needs.
- **Use network segmentation and segregation.** Network segmentation and segregation makes it more difficult for attackers to move laterally within connected networks. For example, placing the web server in a properly configured demilitarized zone (DMZ) limits the type of network traffic permitted between systems in the DMZ and systems in the internal corporate network.
- **Know where your assets are.** You must know where your assets are in order to protect them. For example, if you have data that does not need to be on the web server, remove it to protect it from public access.
- **Protect the assets on the web server.** Protect assets on the web server with multiple layers of defense (e.g., limited user access, encryption at rest).
- **Practice healthy cyber hygiene.**
  - Patch systems at all levels—from web applications and backend database applications, to operating systems and hypervisors.
  - Perform routine backups, and test disaster recovery scenarios.
  - Configure extended logging and send the logs to a centralized log server.

#### **What are some additional steps I can take to protect against website attacks?**

- **Sanitize all user input.** Sanitize user input, such as special characters and null characters, at both the client end and the server end. Sanitizing user input is especially critical when it is incorporated into scripts or structured query language statements.
- **Increase resource availability.** Configure your website caching to optimize resource availability. Optimizing your website's resource availability increases the chance that your website will withstand unexpectedly high amounts of traffic during DoS attacks.
- **Implement cross-site scripting (XSS) and cross-site request forgery (XSRF) protections.** Protect your website system, as well as visitors to your website, by implementing XSS and XSRF protections.
- **Implement a Content Security Policy (CSP).** Website owners should also consider implementing a CSP. Implementing a CSP lessens the chances of an attacker successfully loading and running malicious JavaScript on the end user machine.
- **Audit third-party code.** Audit third-party services (e.g., ads, analytics) to validate that no unexpected code is being delivered to the end user. Website owners should weigh the pros and cons of vetting the third-party code and hosting it on the web server (as opposed to loading the code from the third party).
- **Implement hypertext transfer protocol secure (HTTPS) and HTTP strict transport security (HSTS).**

Website visitors expect their privacy to be protected. To ensure communications between the website and user are encrypted, always enforce the use of HTTPS, and enforce the use of HSTS where possible. For further information and guidance, see the U.S. Chief Information Officer (CIO) and the Federal CIO Council's webpage on the [HTTPS-Only Standard](#).

- **Implement additional security measures.** Additional measures include
  - Running static and dynamic security scans against the website code and system,
  - Deploying web application firewalls,
  - Leveraging content delivery networks to protect against malicious web traffic, and
  - Providing load balancing and resilience against high amounts of traffic.

For additional guidance, visit the [Open Web Application Security Project Top 10 Cheat Sheet](#) on common critical risks to web applications, the National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-44: Guidelines on Securing Public Web Servers](#), and NIST [SP 800-95: Guide to Secure Web Services](#). [Subscribe to NCCIC Current Activities](#) to stay current on the latest website technology vulnerabilities.

**This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.**

Was this document helpful? [Yes](#) | [Somewhat](#) | [No](#)

## I Want To

[Report incidents](#)

[Share indicators](#)

[Report phishing](#)

[Report malware](#)

[Report software vulnerabilities](#)

## Subscribe to Alerts

Receive security alerts, tips, and other updates.

Top of Form

Enter email address

Bottom of Form

[Mailing Lists and Feeds](#)

[Twitter](#)

## Contact Us

**(888) 282-0870**

[Send us email](#)

[Download PGP/GPG keys](#)

All e-mail to/from this account is subject to official review and is for official use only. Action may be taken in response to any inappropriate use of the Secret Service's e-mail system. This e-mail may contain information that is privileged, law enforcement sensitive, or subject to other disclosure limitations. Such information is loaned to you and should not be further disseminated without the permission of the Secret Service. If you have received this e-mail in error, do not keep, use, disclose, or copy it; notify the sender immediately and delete it.

**From:** [InfraGard Los Angeles](#)  
**To:** [Kevin Woodworth](#)  
**Subject:** Cyber Criminals, The Cyber Shield, Law Enforcement Watch and More.  
**Date:** Thursday, November 01, 2018 1:09:13 PM



## **The InfraGard Los Angeles Daily Brief**

**01November2018**

**Attached to Today's Brief:**

**[FBI PIN: Cyber Criminals Likely To Shift Toward Sophisticated Small-Scale, Targeted Campaigns and Cryptocurrency Mining](#)**

**[Migrant caravan coordinator says demand for Mexico to provide buses has 'failed'](#)**

**[Watch the Russian rocket failure that forced two astronauts to make an emergency landing](#)**



[Pittsburgh synagogue shooting suspect pleads not guilty to federal charges](#)

[Chinese company charged with stealing trade secrets from U.S. computer firm](#)

### **Upcoming Training and Events:**

[IGLA Active Shooter Survival Kit  
Now Available For Purchase at InfraGard Training  
Events](#)

[OSINT \(Open Source Intelligence Exploitation\)  
Course: 08November2018](#)



[Radisson Hotel Group 'fesses up to 'security incident'](#)

[Unsure why you can't log into Office 365? So is Microsoft](#)

[Apple pulls watchOS update that was bricking some Watches](#)

[Google Home Hub secret API leaves door open for remote commands](#)

[iOS 12.1 extends controversial processor throttling feature to the iPhone 8, 8](#)

Plus, and X

Tiny Twitter thumbnail tweaked to transport different file types

Why 5G (and even 6G) could put your business at risk for a cyberattack

## **The Cyber Shield: 01November2018**

Publicly Available Tools Seen in Cyber Incidents Worldwide

Windows 10 UWP Bug Lets Hackers Access All Your Files

Mirai Author Gets Only Six Months of House Arrest, \$8.6 Million Restitution

Facebook Removed 82 Iranian Pages, Groups, Accounts Posing as US or UK citizens

DOD Is Looking for Private Vendors to Create a Cloud Computing Platform

How to Delete Your Google Search History

Police Can No Longer Unlock iPhones as iOS 12 Blocks Hacking Box

Survey Finds U.S. Maritime Industry Unprepared for Cyber Attacks

Iranian Hackers Hit U.K. Cybersecurity Universities

## **The Cyber Shield: 31October2018**

Civil servant who watched porn at work infected a US government network with malware

Jinhua Added to Entity List by DoC to Fend Off Supply Chain Tampering

TravisMathew's Website Breached, Card Numbers and CVV2 Codes Stolen

Crooks Stole Data of 64,000 Tomorrowland Festival-Goers

Secret Service Confirms Focus on Email Compromise Cybercrimes Worth \$12 Billion

Remote Denial of Service Vulnerability Patched in Squid Proxy Cache Server

Advanced Malware Protection Affected by Bug That Can Inhibit Intrusion

Detection

53 Percent of All SMBs Experienced at Least a Security Breach in the Last Year

## **The Cyber Shield: 30October2018**



**UNCLASSIFIED//FOR OFFICIAL USE ONLY**

Warning: This document is Unclassified//For Official Use Only (U//FOUO). It contains sensitive information that cannot be released to the public or outside of the public safety community.

UNCLASSIFIED//FOR OFFICIAL USE ONLY



*(U) The information was taken from open source unclassified media outlets; it is preliminary in nature and currently has not been verified through FBI Sources. The following list of overnight Counterterrorism related news articles are intended as information only and are not official FBI opinion.*

### **CONUS**

#### **1. 'Hipster terrorist' pleads guilty to traveling to Syria to join precursor to ISIS [Chicago Tribune – embedded photo]**

- He's been dubbed the "hipster terrorist" for the glamorous social media shots of him posing in snazzy shirts and designer sunglasses, an iced latte in hand and jacket slung casually over a shoulder.
- But Aws Mohammed Younis al-Jayab cut a much different profile Wednesday in a federal courtroom in Chicago, where he pleaded guilty to charges of aiding a terrorist organization and lying to immigration officials.



- Al-Jayab, 25, a Palestinian native with ties to Wisconsin, admitted in a plea agreement with prosecutors that he flew from O'Hare International Airport to Turkey in November 2013 and then entered Syria.
- Once there, he joined Ansar Al-Islam, a U.S.-designated terrorist group that was a precursor to the Islamic State, also known as ISIS.
- After al-Jayab returned to the U.S. in 2014 and settled in California, he told immigration officials that he'd been overseas visiting relatives.

## **2. Judge orders alleged Islamic State propagandist held [Fox via AP]**

- A judge says a Chicago computer-science specialist accused of running online propaganda campaigns for Islamic State poses a threat and so must stay jailed until trial.
- At a Wednesday hearing in Chicago, the federal judge cited photos arresting agents allegedly found on Ashraf Al Safoo's phone this month showing bomb-making components.
- The 34-year-old naturalized U.S. citizen from Iraq is charged with conspiracy to provide material support to terrorists. A conviction carries a maximum 20-year prison term.
- The propaganda allegedly included video showing a Christmas gift containing a ticking time-bomb.
- The complaint also describes the propagandists' annoyance at becoming the butt of jokes after a text meant to warn about "beheading (President Donald) Trump" actually warned about "kissing and hugging" Trump.
- An app used to translate the Arabic apparently led to the error.

## **3. How a Nazi-sympathizing cop went to jail for aiding ISIS [CNN – embedded photos]**

- On July 28, 2016, FBI Special Agent John Sikorski received an encrypted message with a list of Google Play gift card codes. The total value of the gift cards was \$245. Despite the modest sum, it was a big win years in the making for the FBI's counterterrorism unit.
- Sikorski was working undercover, posing as an American named Mo who had joined ISIS in Syria. He had sent a message to terror suspect Nicholas Young, requesting gift cards to help fighters communicate with recruits via an encrypted app.
- It took six years and millions of dollars to prosecute Young, according to a court filing. Young, 38, was a Virginia-based Metro DC transit officer who converted to Islam after the death of his father sent him spiraling into depression.
- Even as the FBI was investigating Young as a possible terrorist sympathizer, he continued to work as a transit cop, carrying a service weapon and patrolling train stations around the nation's capital.
- During a jailhouse interview with The Washington Post, Young acknowledged he enjoyed violent movies, death metal and dark humor but he stressed he did not support the Islamic State.

## **4. Bundy Son Sues US for Nevada Standoff Prosecution [Courthouse News]**

- A rancher's son best known for participating in an armed standoff with federal land agents four years ago and now an independent candidate for Nevada governor is suing the federal government for malicious prosecution.
- In a federal lawsuit filed in Washington, D.C. on Wednesday, Ryan Bundy contends the government wrongfully tried to convict he and his father, Cliven Bundy, after the men tried to stop a roundup of Bundy cattle from federal land.
- Charges were dismissed against most defendants by a federal judge in Las Vegas in January, after a whistleblower, Larry Wooten, revealed federal prosecutors had engaged in intentional and willful prosecutorial misconduct.
- Bundy's complaint names U.S. Attorney General Jeff Sessions, former Attorney Generals Loretta Lynch and Eric Holder, former Bureau of Land Management chief Neil Kornze, and former FBI Director James Comey as defendants.
- Analyst comment: Included in ONN for situational awareness.





[America's Teens Are Extremely Stressed Out About School Shootings](#)This week, the American Psychological Association released its annual Stress in America survey, asking thousands of people variations on one simple question: What stresses you out? The poll, like its recent iterations, found that Americans are stressed the heck out. Forty-five percent of the survey respondents said they "lay awake at night due to stress." Sixty-two percent said the current political climate is a significant stressor in their lives. And 56 percent agreed "this is the lowest point in the nation's history they could remember." (Hey, at least that's slightly down from last year.) This year's report took a special look at young people ages 15 to 21, a.k.a. Generation Z (the generation that comes after millennials). An additional 300 people in this group were polled to get a closer look at their stressors and what it's like to be entering adulthood at this fraught time. Two things in the report are clear. Teens are especially concerned about guns. And they are most likely of any of us to describe their mental health as poor.

#### [How To Move Forward After A School Shooting \(NC\)](#)

Matthews, N.C. -- After a deadly school shooting at Butler High School, students and parents are wondering how to move forward. Mental health experts say students and teachers may be wondering how could they have prevented the incident. Schools officials say counseling is available for anyone who needs it. Butler High School will be closed again Wednesday. School officials say the violence stemmed from bullying that had gotten out of control. Dr. Ryan Kelly, a psychologist at Southeastern Psych in Charlotte, says students and teachers may be left wondering if they should have stepped in earlier to prevent the violence.

#### **Police Killed/Injured In Action:**

- 1.[EPD Officer Injured During Suspicious Person Investigation At Fairlawn Elementary School \(IN\)](#)
- 2.[SHERIFF: Greene Co. Deputy Apparently Hit By Friendly Fire \(NC\)](#)

#### **Use of Force:**

- 1.[Latest: 22-Year-Old Moline Man Killed In Shooting In Downtown Moline \(IL\)](#)
- 2.[Offender Shot, Wounded In Police-Involved Shooting In East Chatham \(IL\)](#)
- 3.[KBI Investigates Officer-Involved Shooting In Atchison \(KS\)](#)
- 4.[Man Dead After Chase, Officer-Involved Shooting, Sheriff's Office Says \(TX\)](#)
- 5.[Suspect Shot In Officer-Involved Shooting In Elyria \(OH\)](#)
- 6.[JSO: Suspect In Armed Carjacking Shot And Killed By Police In Moncrief \(FL\)](#)
- 7.[Leadville Man Wounded By Officer Responding To Domestic Call \(CO\)](#)

## **This Date in History**



On this day, William Tilghman is murdered by a corrupt prohibition agent who resented Tilghman's refusal to ignore local bootlegging operations. Tilghman, one of the famous marshals who brought law and order to the Wild West, was 71 years old.

Known to both friends and enemies as "Uncle Billy," Tilghman was one of the most honest and effective lawmen of his day. Born in Fort Dodge, [Iowa](#), in 1854, Tilghman moved west when he was only 16 years old. Once there, he flirted with a life of crime after falling in with a crowd of disreputable young men who stole horses from Indians. After several narrow escapes with angry Indians, Tilghman decided that rustling was too dangerous and settled in Dodge City, [Kansas](#), where he briefly served as a deputy marshal before opening a saloon. He was arrested twice for alleged train robbery and rustling, but the charges did not stick.

Despite this shaky start, Tilghman gradually built a reputation as an honest and respectable young man in Dodge City. He became the deputy sheriff of Ford County, Kansas, and later, the marshal of Dodge City. Tilghman was one of the first men into the territory when [Oklahoma](#) opened to settlement in 1889, and he became a deputy U.S. marshal for the region in 1891. In the late 19th century, lawlessness still plagued Oklahoma, and Tilghman helped restore order by capturing some of the most notorious bandits of the day.

Over the years, Tilghman earned a well-deserved reputation for treating even the worst criminals fairly and protecting the rights of the unjustly accused. Any man in Tilghman's custody knew he was safe from angry vigilante mobs, because Tilghman had little tolerance for those who took the law into their own hands. In 1898, a wild mob lynched two young Indians who were falsely accused of raping and murdering a white woman. Tilghman arrested and secured prison terms for eight of the mob leaders and captured the real rapist-murderer.

In 1924, after serving a term as an Oklahoma state legislator, making a movie about his frontier days, and serving as the police chief of Oklahoma City, Tilghman might well have been expected to quietly retire. However, the old lawman was unable to hang up his gun, and he accepted a job as city marshal in Cromwell, Oklahoma. Tilghman was shot and killed while trying to arrest a drunken [Prohibition](#) agent.

**"I have acted fearless and independent and I never**



**will regret my course. I would rather be politically buried than to be hypocritically immortalized.” — Davy Crockett**

**Threat Reporting: As a reminder, for immediate, specific threat information, call 911. Please report all other threat information online at <https://tips.fbi.gov> or via phone at 1-800-CALL-FBI (225-5324).**

**[Click Here for tips.fbi.gov](https://tips.fbi.gov)**



**Be Safe,  
InfraGard Los Angeles**

**Copyright InfraGard Los Angeles Members Alliance 2016  
11000 Wilshire Blvd. Ste. 1700  
Los Angeles CA, 90024  
562.345.1166**

(U) WARNING: RECEIPT OF THIS INFORMATION CONSTITUTES ACCEPTANCE OF ALL TERMS AND CONDITIONS REGARDING ITS USE, HANDLING, STORAGE, FURTHER DISSEMINATION OR DESTRUCTION. AT A MINIMUM, RECEIPT ACKNOWLEDGES A COMMITMENT TO COMPLY WITH ALL APPLICABLE LAWS PROTECTING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE COLLECTION, USE, ANALYSIS, RETENTION, DESTRUCTION, SHARING AND DISCLOSURE OF INFORMATION. This information is the property of the JRIC and is UNCLASSIFIED //

FOR OFFICIAL USE ONLY. This information may not be distributed to federal, state, tribal, and local government or public safety personnel on a need-to-know basis without further approval from the JRIC. This information is sensitive, and cannot be released to the public, the media, or other individuals who do not have a valid need-to-know, without prior approval of an authorized JRIC official. Precautions should be taken to ensure this information is stored and/or destroyed in a manner that precludes unauthorized access.

**You have opted to receive this email as part of your membership to the InfraGard Los Angeles Members' Alliance.**

[Visit our website](#)

basicImage



InfraGard Los Angeles | 12440 E. Imperial Highway, Suite 700, Norwalk, CA 90650

[Unsubscribe kwoodworth@sunnyvale.ca.gov](mailto:kwoodworth@sunnyvale.ca.gov)

[Update Profile](#) | [About our service provider](#)

Sent by [info@infragardlosangeles.org](mailto:info@infragardlosangeles.org)